TCG Storage
Opal SSC Feature Set:
Single User Mode

Specification Version 1.00
Revision 2.00

August 5, 2015

Contact: admin@trustedcomputinggroup.org

TCG

PUBLISHED

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.

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

Version 1.00	Date	Description
Rev 1.00	February 27, 2012	First publication
Rev 2.00	August 5, 2015	Corrected incorrect type for SingleUserModeRanges column of LockingInfo table, various editorial modifications for clarity

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 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"

[2]. Trusted Computing Group (TCG), "TCG Storage Architecture Core Specification", Version 2.01

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

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

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 does not define any interactions with other feature sets.

1.8 Legend

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

Table 1 SP Table Legend

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

```
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

3.1.1.1.1 Parameter Descriptions

3.1.1.1.1.1 SingleUserModeSelectionList

SingleUserModeSelectionList has parameter number `0x060000`.

This TypeOr parameter allows the host to select which Locking object ranges to be controlled by a single User authority

a. 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 method, the parameter value SHALL be the UID of the `Locking` table (00 00 08 02 00 00 00 00).

b. 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 method, the parameter value SHALL be a list of UIDs of `Locking` table objects.

3.1.1.1.1.2 RangeStartRangeLengthPolicy

RangeStartRangeLengthPolicy has parameter number `0x060001`.

This parameter allows the host to select the ownership policy for the `RangeStart` and `RangeLength` columns of non-Global Range Locking objects (`RangeStart` and `RangeLength` columns of the Global Range are not modifiable regardless of this policy) 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 (either a list of Locking objects, or all objects in the Locking table).

a. 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.

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

3.1.1.1.1.3 Admin1PIN

Admin1PIN has parameter number 0x060002.

This parameter allows the host to define the Admin1 authority's credential value upon successful invocation of the Reactivate method.

a. If this parameter is omitted, then upon successful invocation of the Reactivate method, the Admin1 PIN SHALL remain at its current value.

b. 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.

3.1.1.1.2 Method Description

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.PIN` column value of the User authority associated with that range.

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

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

3.1.1.2.1 Method Description

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 NOT_AUTHORIZED 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

3.1.2.1.1 Parameter Descriptions

3.1.2.1.1.1 SingleUserModeSelectionList

SingleUserModeSelectionList has parameter number 0x060000.

This TypeOr parameter allows the host to select which Locking object ranges to be controlled by a single User authority. See 3.1.1.1.1.1 for details on this parameter.

3.1.2.1.1.2 RangeStartRangeLengthPolicy

RangeStartRangeLengthPolicy has parameter number 0x060001.

This parameter allows the host to select the ownership policy for the `RangeStart` and `RangeLength` columns of non-Global Range Locking objects (`RangeStart` and `RangeLength` are not modifiable for the Global Range regardless of this policy) 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 (either a list of Locking objects, or all objects in the Locking table). See 3.1.1.1.1.2 for additional details on this parameter.

3.1.2.1.2 Method Description

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 [3], 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 2 Locking_object _ref

UID	Name	Format
00 00 00 05 00 00 0C 0E	Locking_object_ref	Restricted_Reference_Type{6}, uidref {LockingTableUID}

3.3.1.2 Locking_object_ref_list

This section describes the type that is a list of uidrefs to objects in the `Locking` table.

Table 3 Locking_object _ref_list

UID	Name	Format
00 00 00 05 00 00 08 07	Locking_object_ref_list	List_Type, *, Locking_object_ref

The `*` in the Format column of Table 3 is equal to the number of total number of ranges supported in the `Locking` table (Global Range plus configurable Locking ranges).

3.3.1.3 single_user_ranges

This section describes the type used in the `SingleUserModeRanges` column.

Table 4 single_user_ranges

UID	Name	Format
00 00 00 05 00 00 06 07	single_user_ranges	Alternative_Type, Locking_object_ref_list, table_ ref

3.3.1.4 policy_enum

This section describes the type used in the `RangeStartLengthPolicy` column.

Table 5 policy_enum

UID	Name	Format
00 00 00 05 00 00 04 1E	policy_enum	Enumeration_Type, 0, 7

The enumeration values are associated as defined in Table 6.

Table 6 policy_enum Enumeration Values

Enumeration Value	Associated Value
0	User authority ownership policy for RangeStart, RangeLength and CommonName columns
1	Admins authority ownership policy for RangeStart, RangeLength, and CommonName columns
2-7	Reserved

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 7.

Table 7 Level 0 Discovery - Single User Mode Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code						
1								(LSB)
2	Version				Reserved			
3	Length							
4-7	Number of Locking Objects Supported							
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`, `RangeLength`, and `CommonName` 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`, `RangeLength`, and `CommonName` 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 successsfully 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 8.

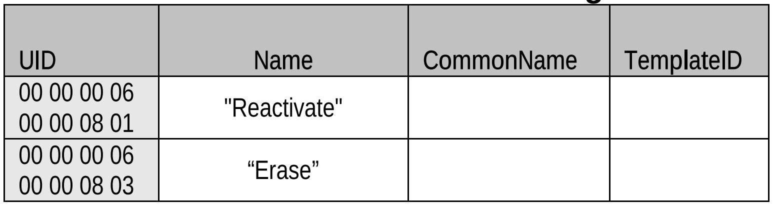
Table 8 User Authority/Locking Object Associations

Locking Object UID	Locking Object Name	Associated User Authority UID	Associated User Authority Name
00 00 08 02 00 00 00 01	Locking_GlobalRange	00 00 00 09 00 03 00 01	User1
00 00 08 02 00 03 00 01	Locking_Range1	00 00 00 09 00 03 00 02	User2
00 00 08 02 00 03 NN NN	Locking_RangeNNNN	00 00 00 09 00 03 (NN NN+1)	User(NNNN+1)

4.4.2 MethodID (M)

Table 9 lists the additional entries in the Locking SP's `MethodID` table that are required for the Single User Mode feature set.

Table 9 MethodID Table Modifications For Single User Mode Support



UID	Name	CommonName	TemplateID
00 00 00 06 00 00 08 01	"Reactivate"		
00 00 00 06 00 00 08 03	"Erase"		

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 1. 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; or the Locking table UID if all ranges are in Single User Mode. The value of the second column is an enumeration value that identifies the management policy for the `RangeStart`, `RangeLength`, and `CommonName` columns of Locking objects that are in Single User Mode.

Table 10 LockingInfo Table Description

Column Number	Column Name	IsUnique	Column Type
0x00	UID		uid
0x01	Name		name
0x02	Version		uinteger_4
0x03	EncryptSupport		enc_supported
0x04	MaxRanges		uinteger_4
0x05	MaxReEncryptions		uinteger_4
0x06	KeysAvailableCfg		keys_avail_conds
0x060000	SingleUserModeRanges		single_user_ranges
0x060001	RangeStartLengthPolicy		policy_enum

4.4.3.1 SingleUserModeRanges column

1. Column Number: `0x060000`
2. Name: `SingleUserModeRanges`
3. Contents: Either a list of Locking object UIDs, OR the `Locking` Table UID
    a. A list of Locking object UIDs identifies the Locking objects activated in Single User Mode.
        i. An empty list indicates no Locking objects are activated in Single User Mode.
    b. The `Locking` table UID indicates all of the Locking objects in the `Locking` table are activated in Single User Mode
4. Special: Column is READ-ONLY
5. Column Type: `single_user_ranges`

For compatibility purposes, when encoding of the value of the `SingleUserModeRanges` column for transmission across the interface, the device SHALL NOT include the identifying half_UID of the selected component of the Alternative type (required when encoding an Alternative type – see [2]). The device SHALL omit the half_UID from the encoding of the column value when transmitting the value across the interface.

4.4.3.2 RangeStartLengthPolicy column

1. Column Number: `0x060001`
2. Name: `RangeStartLengthPolicy`
3. Contents: An enumeration with one of the following defined values:
    a. 0 : the associated User authorities own access to modify the `RangeStart`, `RangeLength`, and `CommonName` columns of Single User Mode Locking objects.
    b. 1 : the Admins authority maintains ownership of the `RangeStart` , `RangeLength`, and `CommonName` columnsof 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 `RangeStartLengthPolicy` 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.

4.4.4.1.1.1 Reactivate Method AccessControl Table Changes

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

Table 10 AccessControl Table Modifications for Reactivate Method Support

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 00 00 00 00 01	ThisSP	Reactivate		ACE_SP_Reactivate_Admin				ACE_Anybody						

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 08 00 04 20 01	ACE_SP_Reactivate_Admin	Set		ACE_ACE_Set_BooleanExpression				ACE_Anybody						

4.4.4.1.1.2 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

UID	Name	CommonName	BooleanExpr	Columns
00 00 00 08 00 04 20 01	" ACE_SP_Reactivate_Admin"		Admins	

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. The updated Authority table row is presented in Table 12. The updated AccessControl table is presented in Table 13.

Table 12 Admin1 Authority – Authority Table Modifications

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 00 01	“Admin1”	“”	F	Admins	T	None	None	F	Password	C_PIN_Admin1	Null	Null						

Table 13 Admin1 Authority – AccessControl Table Changes

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 09 00 01 00 01	Admin1	Set		ACE_Admins_Set_CommonName, ACE_Authority_Set_Enabled				ACE_Anybody						

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 14 General AccessControl Table Changes

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 08 ** ** ** **	ACE Name	Get		ACE_ACE_Get_All				ACE_Anybody						

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` column.
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` column.

Table 11 Access Control Table Modifications for Global Range Single User Mode

InvokingID	InvokingID Name informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 09 00 03 00 01	User1	Set		ACE_User1_Set_CommonName				ACE_Anybody						
00 00 08 02 00 00 00 01 *Policy1	Locking_GlobalRange	Set		ACE_Locking_GlobalRange_Set_ ReadLockEnabledToLOR, ACE_Admins_Set_CommonName				ACE_Anybody						
00 00 08 02 00 00 00 01 *Policy0	Locking_GlobalRange	Set		ACE_Locking_GlobalRange_Set_ ReadLockEnabledToLOR, ACE_User1_Set_CommonName				ACE_Anybody						

InvokingID	InvokingID Name informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 08 02 00 00 00 01	Locking_GlobalRange	Erase		ACE_Locking_GlobalRange_Erase				ACE_Anybody						
00 00 00 08 00 04 30 00	ACE_Locking_GlobalRange_Erase	Set		ACE_ACE_Set_BooleanExpression				ACE_Anybody						
00 00 00 0B 00 03 00 01	C_PIN_User1	Get		ACE_C_PIN_Anybody_Get_NoPIN				ACE_Anybody						

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

UID	Name	CommonName	BooleanExpr	Columns
00 00 00 08 00 04 00 00 *New	"ACE_Locking_GlobalRange_Set_ReadLockEnabledToLOR"		User1	ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset
00 00 00 08 00 03 D0 00 *Modified	"ACE_Locking_GlobalRange_Get_ RangeStartToActiveKey"		Anybody	RangeStart, RangeLength, ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset, ActiveKey
00 00 00 08 00 04 20 00 *New	" ACE_C_PIN_Anybody_Get_NoPIN "		Anybody	UID, CharSet, TryLimit, Tries, Persistence
00 00 00 08 00 03 A8 01 *Modified	"ACE_C_PIN_User1_Set_PIN"		User1	PIN
00 00 00 08 00 03 ** ** *Modified	"ACE_K_AES_*_GlobalRange_GenKey"		User1	All
00 00 00 08 00 04 30 00 *New	" ACE_Locking_GlobalRange_Erase"		Admins OR User1	
00 00 00 08 00 04 40 01 *Modified	ACE_User1_Set_CommonName		User1	CommonName

** ** depends on AES key size

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

UID	Name	CommonName	IsClass	Class	Enabled	Secure	HashAndSign	PresentCertificate	Operation	Credential	ResponseSign	ResponseExch	ClockStart	ClockEnd	Limit	Uses	Log	LogTo
00 00 00 09 00 03 00 01	"User1"		F		T	None	None	F	Password	C_PIN_User1	Null	Null						

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 Range NNNN 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 UserNNNN+1 has ownership over RangeNNNN's `RangeStart`, `RangeLength`, and `CommonName`.
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`, and `CommonName`.

Table 17 AccessControl Table Modifications for RangeNNNN Single User Mode

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 09 00 03 00 00 (+NNNN+1)	UserNNNN+1	Set		ACE_UserNNNN+1_Set_CommonName				ACE_Anybody						
00 00 08 02 00 03 00 00 (+NN NN) *Policy1	Locking_RangeNNNN	Set		ACE_Locking_RangeNNNN_Set_ReadLockEnabledToLOR, ACE_Locking_RangeNNNN_Set_RangeStartToRangeLength, ACE_Admins_Set_CommonName				ACE_Anybody						

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 08 02 00 03 00 00 (+NN NN) *Policy0	Locking_RangeNNNN	Set		ACE_Locking_RangeNNNN_Set_ ReadLockEnabledToLOR, ACE_Locking_RangeNNNN_Set_ RangeStartToRangeLength, ACE_UserNNNN+1_Set_CommonName				ACE_Anybody						
00 00 08 02 00 03 00 00 (+NN NN)	Locking_RangeNNNN	Erase		ACE_Locking_RangeNNNN_Erase				ACE_Anybody						
00 00 00 08 00 04 30 01 (+NNNN)	ACE_Locking_RangeNNNN_Erase	Set		ACE_ACE_Set_BooleanExpression				ACE_Anybody						

InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
00 00 00 0B 00 03 00 00 (+NNNN+1)	C_PIN_UserNNNN+1	Get		ACE_C_PIN_Anybody_Get_NoPIN				ACE_Anybody						

4.4.4.2.2.2 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, RangeLength, and CommonName is owned by the associated User authority.
4. *Policy1 – indicates that the ability to modify RangeStart, RangeLength, and CommonName is owned by the Admins class authority.

Table 18 New/Modified ACEs for RangeNNNN Single User Mode

UID	Name	CommonName	BooleanExpr	Columns
00 00 00 08 00 04 00 00 (+NNNN) *New	"ACE_Locking_RangeNNNN_Set_ReadLockEnabledToLOR"		UserNNNN+1	ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset
00 00 00 08 00 04 10 00 (+NNNN) *Policy0 *New	"ACE_Locking_RangeNNNN_Set_RangeStartToRangeLength"		UserNNNN+1	RangeStart, RangeLength
00 00 00 08 00 04 10 00 (+NNNN) *Policy1 *New	"ACE_Locking_RangeNNNN_Set_RangeStartToRangeLength"		Admins	RangeStart, RangeLength
00 00 00 08 00 03 D0 00 (+NNNN) *Modified	"ACE_Locking_RangeNNNN_Get_RangeStartToActiveKey"		Anybody	RangeStart, RangeLength, ReadLockEnabled, WriteLockEnabled, ReadLocked, WriteLocked, LockOnReset, ActiveKey
00 00 00 08 00 04 20 00 *New	" ACE_C_PIN_Anybody_Get_NoPIN "		Anybody	UID, CharSet, TryLimit, Tries, Persistence
00 00 00 08 00 03 A8 00 (+NNNN+1) *Modified	" ACE_C_PIN_UserNNNN+1_Set_PIN"		UserNNNN+1	PIN
00 00 00 08 00 03 ** ** (+NNNN) *Modified	"ACE_K_AES_*_RangeNNNN_GenKey"		UserNNNN+1	All
00 00 00 08 00 04 30 00 (+NNNN) *New	"ACE_Locking_RangeNNNN_Erase"		Admins OR UserNNNN+1	
00 00 00 08 00 04 40 00 (+NNNN+1) *Modified	ACE_UserNNNN+1_Set_CommonName		UserNNNN+1	CommonName

** ** 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 19 Authority Table Modifications for RangeNNNN Single User Mode

UID	Name	CommonName	IsClass	Class	Enabled	Secure	HashAndSign	PresentCertificate	Operation	Credential	ResponseSign	ResponseExch	ClockStart	ClockEnd	Limit	Uses	Log	LogTo
00 00 00 09 00 03 00 00 (+NNNN+1)	"UserNNNN+1"		F		T	None	None	F	Password	C_PIN_User1	Null	Null						

4.5 Additional SPs

This feature set requires no additional SPs.