TRUSTED® COMPUTING GROUP

SPECIFICATION

# TCG Storage Feature Set: Block SID Authentication

Version 1.01
Revision 1.14
November 10, 2020

Contact: admin@trustedcomputinggroup.org

PUBLIC REVIEW

## Work in Progress

*This document is an intermediate draft for comment only and is subject to change without notice. Readers should not design products based on this document.*

# 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

| REVISION | DATE | DESCRIPTION |
|---|---|---|
| 1.01/1.01 | February 5, 2020 | • New initial draft with only changes tracked minus changes related to template conversion, created from the published TCG Storage Feature Set: Block SID Authentication Specification Version 1.00 Revision 1.00 |
| 1.01/1.02 | April 6, 2020 | • Resolved comments in multiple places.<br>• Added transition definitions in section 4.3.3 |
| 1.01/1.03 | June 12, 2020 | • Change to keep consistency (added LifeCycle)<br>• Rewording section 4.2.2 |
| 1.01/1.04 | June 23, 2020 | • Incorporated comments at June Virtual F2F meeting. |
| 1.01/1.05 | June 24, 2020 | • Incorporated comments at June 24 conference call |
| 1.01/1.06 | July 29, 2020 | • Added ‘and’ and ‘or’ to lists as appropriate<br>• Changed lists from ordered to unordered as appropriate<br>• Changed ‘successful execution’ to ‘successful completion’ in some places<br>• Added a missing cross reference<br>• Added a missing word ‘the’<br>• Reconstructed chapter 1, and change the title of section 1.1<br>• Fixed the title of section 4.1.1<br>• Adjusted the size of font |
| 1.01/1.07 | September 8, 2020 | • Addressed WD comments<br>• Changed “SID Blocked State” to “SID Authentication Blocked State” and cleaned up usage throughout the document to standardize on “SID Authentication Blocked” state<br>• Cleaned up usage of Locking SP Freeze Lock state<br>• Fixed LifeCycle state figure to reflect transition from Manufactured-Frozen to Manufactured-Inactive<br>• Cleaned up most redundant rules in section 4.2.4<br>• Fixed rule in 4.2.2 to allow Block SID Authentication to work for freezing Locking SP when SID PIN is not equal to MSID PIN<br>• Fixed use of “set to 1” and “set to 0” for bits to instead indicate “set to one” and “cleared to zero” |
| 1.01/1.08 | September 15, 2020 | • Moved statement related to Tries count for the Locking SP into the Locking SP Manufactured-Frozen Lifecycle state description in section 4.3.2. |
| 1.01/1.09 | September 15, 2020 | • Cleaned up section 4.3.2 further to consistently refer to the Locking SP rather than “an SP”<br>• Added 1.4 Conventions section to be consistent with other new documents |
| 1.01/1.10 | September 28, 2020 | • Added and addressed Kioxia comments<br>• Converted all use of “LifeCycle” to “life cycle” except when referring to the LifeCycle column<br>• Cleaned up Table Legend which referred to Configurable Namespace Locking Feature Set<br>• Cleaned up use of “SID Authentication Block State” and “Locking SP Freeze Lock State” bits<br>• Cleaned up use of “command” instead of “Command”<br>• Cleaned up use of “SHALL” instead of “shall”<br>• Removed blank section 4.3.1 “Manufactured SPs”<br>• Added more text describing what happens to the Locking SP Freeze Lock State, and Frozen column values when transitioning out of the Manufactured-Frozen life cycle state<br>• Added statement indicating what occurs to Locking SP’s LifeCycle column in the Admin SP’s SP table when transitioning in and out of Manufactured-Frozen life cycle state. |
| 1.01/1.11 | September 29, 2020 | • Changed language from “a Manufactured… life cycle state” to “the Manufactured… life cycle state” |
| 1.01/1.12 | September 29, 2020 | • Cleaned up one instance of “State” to instead be “state” in section 4.3.1 |
| 1.01/1.13 | October 6, 2020 | • Moved section 4.1.1.6 “Level 0 requirements for the Block SID Authentication Feature Descriptor” closer to the beginning of section 4.1.1. |

| | | |
|---|---|---|
| 1.01/1.14 | November 10, 2020 | • Updated section 1.4.1 to be consistent with this document and other TCG storage documents convention to identify informative text/content.<br>• Globally cleaned up use of “see x.y.z” to instead be “see section x.y.z”<br>• Cleaned up sentence in section 4.3.2.1 related to transition to Manufactured-Frozen state when the Block SID Authentication command is sent with the Freeze Locking SP field set to one<br>• Added reference to Ruby SSC |



# CONTENTS





# 1 SCOPE

## 1.1 Storage Workgroup Specifications 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 life cycle state of the Storage Device as a Trusted Peripheral.

## 1.2 Scope and Intended Audience

This specification defines the Block SID Authentication Feature. Any Storage Device that claims Block SID Authentication 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 Conventions

### 1.4.1 Informative Text

Informative text is used to provide background and context. Informative text does not define requirements. Informative text is formatted as follows:

*Begin Informative Content*

Hello World!

*End Informative Content*

### 1.4.2 Precedence

The order of precedence to resolve conflicts between text, tables, or figures is text, then tables, then figures.



### 1.4.3 Lists

If the item in a list is not a complete sentence, the first word in the item is not capitalized. If the item in a list is a complete sentence, the first word in the item is capitalized.

Each item in a list ends with a semicolon, except the last item, which ends in a period. The next to the last entry in the list ends with a semicolon followed by an “and” or an “or” (i.e., “…; and”, or “…; or”). The “and” is used if all the items in the list are required. The “or” is used if only one or more items in the list are required.

Lists sequenced by letters show no ordering among the listed items. The leftmost level uses lower case letters and the next level uses capital letters. The following list shows no ordering among the named items:

a) oak;
b) maple; and
c) soft wood:
    A) pine; or
    B) cedar.

List sequenced by numbers show an ordering relationship among the listed items. All levels use Arabic numerals. The following list shows an ordered relationship among the named items:

1) hydrogen;
2) helium; and
3) lithium:
    1) lithium-6; and
    2) lithium-7.

### 1.4.4 Table Legend

The following legend defines SP table cell coloring coding, with the RGB values for the shading of each cell indicated in parentheses. 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<br>(230, 230, 230) | Read-only | Specified by specification | Fixed | • Cell content is Read-Only.<br>• Access control is fixed.<br>• Value is specified by this specification. |
| **Arial Narrow bold-under**<br>(230, 230, 230) | Read-only | VU | Fixed | • Cell content is Read-Only.<br>• Access Control is fixed.<br>• Values are Vendor Unique (VU). A minimum or maximum value may be specified. |



| Table Cell Legend | R-W | Value | Access Control | Comment |
|---|---|---|---|---|
| Arial-Narrow<br>(0, 0, 0) | Not Defined | (N) | Not Defined | • Cell content is (N).<br>• Access control is not defined.<br>• Any text in table cell is informative only.<br>• A `Get` MAY omit this column from the method response. |
| **Arial Narrow bold-under**<br>(179, 179, 179) | Write | Preconfigured, user personalizable | Preconfigured, user personalizable | • Cell content is writable.<br>• Access control is personalizable<br>• `Get` Access Control is not described by this color coding |
| Arial-Narrow<br>(179, 179, 179) | Write | Preconfigured, user personalizable | Fixed | • Cell content is writable.<br>• Access control is fixed.<br>• `Get` Access Control is not described by this color coding |

### 1.4.5 Fonts

Names of methods and SP tables are in Courier New font (e.g., the `Set` method, the `Locking` table). This convention does not apply to method and table names appearing in headings or captions.

## 1.5 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”, Version 1.00

[4]. Trusted Computing Group (TCG), “TCG Storage Security Subsystem Class: Opal”, Version 2.00

[5]. Trusted Computing Group (TCG), “TCG Storage Security Subsystem Class: Opal”, Version 2.01

[6]. Trusted Computing Group (TCG), “TCG Storage Security Subsystem Class: Opalite”, Version 1.00

[7]. Trusted Computing Group (TCG), “TCG Storage Security Subsystem Class: Pyrite”, Version 1.00

[8]. Trusted Computing Group (TCG), “TCG Storage Interface Interactions Specification“, Version 1.09

[9]. Trusted Computing Group (TCG), “TCG Storage Security Subsystem Class: Ruby”, Version 1.00

## 1.6 Document Precedence

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

a) This specification and [3] or [4] or [5] or [6] or [7] or [9] (this document and an SSC are at the same level of precedence, and SHALL NOT conflict with each other)
b) TCG Storage Interface Interactions Specification [8]



c) TCG Storage Architecture Core Specification [2]

## 1.7 Dependencies on Other Feature Sets

This feature set has no dependencies on other feature sets.

## 1.8 Interactions with Other Feature Sets

This feature set has no interactions with other feature sets.



# 2 Block SID Authentication Overview

*Begin Informative Content*

This specification defines a mechanism by which a host application can alert the storage device to block attempts to authenticate the SID authority until a subsequent device power cycle occurs.

This mechanism can be used by BIOS/platform firmware to prevent a malicious entity from taking ownership of a SID credential that is still set to its default value of MSID.

Additionally, this feature can optionally be used by BIOS/platform firmware to prevent a malicious entity with stolen credentials from making credential or access control changes that would lock out an authorized user.

*End Informative Content*



# 3 SSC Specific Functionality

This feature set requires no additional SSC-specific functionality.



# 4 Feature Set Requirements

This section defines the Mandatory (M) and Optional (O) requirements for the Block SID Authentication Feature Set.

## 4.1 Level 0 Discovery

A SD that implements the Block SID Authentication Feature Set SHALL return the Block SID Authentication Feature Descriptor as described in 4.1.1, in addition to the Level 0 Discovery response requirements defined in other applicable specifications.

### 4.1.1 Block SID Authentication Feature (Feature Code = 0402)

This feature descriptor SHALL be returned when the SD supports the Block SID Authentication Feature Set. The contents of the feature descriptor are defined in Table 2.

**Table 2 Level 0 Discovery - Block SID Authentication Feature Descriptor**

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | (MSB) | | | Feature Code | | | | |
| 1 | | | | | | | | (LSB) |
| 2 | Version | | | | Reserved | | | |
| 3 | Length | | | | | | | |
| 4 | Reserved | | | | Locking SP Freeze Lock State | Locking SP Freeze Lock supported | SID Authentication Blocked State | SID Value State |
| 5 | Reserved | | | | | | | Hardware Reset |
| 6-15 | Reserved | | | | | | | |

#### 4.1.1.1 Level 0 requirements for the Block SID Authentication Feature Descriptor

Feature Code: SHALL be set to 0x0402
Version: SHALL be set to 0x2 or any version that supports the defined features in this specification
Length: SHALL be set to 0x0C

#### 4.1.1.2 SID Value State

This field specifies whether the C_PIN_SID object's PIN column value is equal to the C_PIN_MSID object's PIN column value.

This bit SHALL be cleared to zero if the C_PIN_SID object's PIN column value is equal to the C_PIN_MSID object's PIN column value.

This bit SHALL be set to one if the C_PIN_SID object's PIN column value is not equal to the C_PIN_MSID object's PIN column value.

#### 4.1.1.3 SID Authentication Blocked State

This field specifies whether the authentication of the SID feature is blocked (see section 4.2.2).

This bit SHALL be cleared to zero if authentication of the SID authority is not blocked due to the Block SID Authentication command.



This bit SHALL be set to one if authentication of the SID authority is currently blocked due to the Block SID Authentication command.

#### 4.1.1.4 Locking SP Freeze Lock supported

This field specifies whether the Locking SP Freeze Lock capability is supported.

This bit SHALL be cleared to zero if the Locking SP Freeze Lock capability is not supported.

This bit SHALL be set to one if the Locking SP Freeze Lock capability is supported.

#### 4.1.1.5 Locking SP Freeze Lock State

This field specifies whether the Locking SP is in the Manufactured-Frozen life cycle state (see section 4.3.1).

This bit SHALL be cleared to zero if the Locking SP is not in the Manufactured-Frozen life cycle state.

This bit SHALL be set to one if the Locking SP is in the Manufactured-Frozen life cycle state.

#### 4.1.1.6 Hardware Reset

This bit SHALL be set to one if a Hardware Reset was selected in the Block SID Authentication command to be able to clear the SID Authentication Blocked State and the Locking SP Freeze Lock State bits.

This bit SHALL be cleared to zero if a Hardware Reset was not selected in the Block SID Authentication command to clear the SID Authentication Blocked State and the Locking SP Freeze Lock State bits.

*Begin Informative Content*

The following events are always Clear Events (see 4.2.3), and as such there is no field in Level 0 discovery identifying that either has been selected as a Clear Event:

a) Power Cycle; and
b) Revert.

*End Informative Content*

## 4.2 Block SID Authentication Command (M)

### 4.2.1 Command Structure and Execution

The Block SID Authentication command is delivered by the transport IF-SEND command.

If the Block SID Authentication command is supported, the TPer SHALL accept and acknowledge it at the interface level.

If the Block SID Authentication command is not supported, the TPer SHALL abort attempted invocations of the command at the interface level with the “Other Invalid Command Parameter” status (see [8]).

There is no IF-RECV response to the Block SID Authentication command.

The Block SID Authentication command is defined in Table 3.

The Transfer Length SHALL be non-zero. Transferred data is formatted as indicated in Table 3.

The Clear Events field identifies the SD resets that clear the SID Authentication Blocked and Locking SP Freeze Lock states . See Table 4 for the structure of the Clear Events field.

**Table 3 Block SID Authentication Command**

| FIELD | VALUE |
|---|---|
| Command | IF-SEND |
| Protocol ID | 0x02 |
| Transfer Length | Non-zero |
| ComID | 0x0005 |
| Byte 0 | Clear Events (see Table 4) |
| Byte 1 | Freeze SPs (see Table 5) |
| Bytes 2 to Transfer Length – 1 | Reserved (00) |

### 4.2.2 Command Operation

If the SID C_PIN credential is not the same as the value of the MSID C_PIN credential, then the Block SID Authentication command SHALL result in success but SHALL have no effect on the SID Authentication Blocked State.

If the SID C_PIN credential is the same as the value of the MSID C_PIN credential, then upon successful completion of the Block SID Authentication command and until the next applicable SD Clear Event:

a) Otherwise valid invocations of the Authenticate method in which the Authority parameter is the SID authority's UID SHALL result in a method status of SUCCESS, and a method result of False;

b) Otherwise valid invocations of the StartSession method in which the HostSigningAuthority parameter is the SID authority's UID SHALL result in a SyncSession method with a status of NOT AUTHORIZED; and

c) The Tries column of the SID C_PIN credential SHALL NOT be incremented as a result of authentication attempts that were unsuccessful due to the Block SID Authentication.

If:

a) the Locking SP Freeze Lock capability is supported;

b) the Locking SP is in the Manufactured life cycle state; and

c) a Freeze Locking SP bit (see section 4.2.4) in the Freeze SPs field of a Block SID Authentication command is set to one,

then the Locking SP SHALL transition to the Manufactured-Frozen life cycle state (see section 4.3.1) and the Locking SP Freeze Lock State SHALL be set to one upon successful completion of the Block SID Authentication command.

The Locking SP SHALL stay in the Manufactured-Frozen life cycle state until the next applicable SD Clear Event occurs.

If:

a) the Locking SP Freeze Lock capability is supported;

b) the Locking SP is in the Manufactured-Inactive life cycle state; and

c) the Freeze Locking SP bit (see section 4.2.4) in the Freeze SPs field of a Block SID Authentication command is set to one,



then the Freeze Locking SP bit SHALL be ignored.

If the Freeze SPs byte is not included in the payload for the Block SID Authentication command, then the TPer SHALL process the Block SID Authentication command as if the Freeze Locking SP bit was cleared to zero.

If:

a) the Locking SP Freeze Lock capability is not supported; and

b) the Freeze Locking SP bit (see section 4.2.4) in the Freeze SPs field of a Block SID Authentication command is set to one,

then the Block SID Authentication command SHALL fail with status “Other Invalid Command Parameter”.

If a Block SID Authentication command has been successfully executed and SID authentication is blocked or the Locking SP is in the Manufactured-Frozen life cycle state, then:

a) Subsequent invocations of the Block SID Authentication command SHALL fail with status “Other Invalid Command Parameter”;

b) The SID Authentication Blocked State SHALL NOT change; and

c) Clear Events in effect SHALL remain the same as identified in the most recent successful invocation of the Block SID Authentication command.

After an applicable Clear Event occurs, attempts to authenticate the SID authority or start sessions with the Locking SP SHALL be processed normally until the Block SID Authentication command is successfully executed.

Clear Events selected by the successful completion of the Block SID Authentication command are reset when a Clear Event occurs.

### 4.2.3 Clear Events

Clear Events are mechanisms that reset the SID Authentication Blocked State and Locking SP Freeze Lock State bits, in order to permit normal authentication of the SID authority and use of the Locking SP. Clear Events also reset the current selection of host-selectable Clear Events.

The following SHALL always be Clear Events, and upon their occurrence SHALL clear the SID Authentication Blocked State and Locking SP Freeze Lock State bits and reset the selection of Clear Events:

a) A SD Power Cycle. See [8] for a mapping of TCG Storage Power Cycle reset type to resets defined by the underlying interface; and

b) A successful invocation of the `Revert` method on the Admin SP’s object in the Admin SP’s `SP` table. See [3], [4], [5], [6], [7], and [9] for SSC-specific definitions of the `Revert` method.

The following possible Clear Event MAY be selected by the host during execution of the Block SID Authentication:

a) Hardware Reset. See [8] for a mapping of TCG Storage Hardware Reset reset type to resets defined by the underlying interface.

   A) A host selects Hardware Reset as a Clear Event by setting the Hardware Reset bit (Table 4) to one when invoking the Block SID Authentication command.

After a successful completion of the Block SID Authentication command:

a) Any default Clear Events (e.g. Power Cycle, Revert) SHALL clear the SID Authentication Blocked State bit;

b) Any Clear Events supported by the device and selected in the command SHALL clear the SID Authentication Blocked State;

c) If the Locking SP is in the Manufactured-Frozen life cycle state, then any default Clear Events SHALL transition the Locking SP to the Manufactured life cycle and clear the Locking SP Freeze Lock State bit to zero;

d) If the Locking SP is in the Manufactured-Frozen life cycle state, then any Clear Events supported by the device and selected in the command SHALL transition the Locking SP to the Manufactured life cycle state and clear the Locking SP Freeze Lock State bit to zero; and

e) The Clear Events selected in the command SHALL NOT be modifiable by subsequent invocations of the Block SID Authentication command until after a Clear Event has occurred (see section 4.2.2).

**Table 4 Clear Events**

| Bit<br>Byte | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | (MSB) Reserved | | | | | | | Hardware Reset |

### 4.2.4 Freeze SPs

The Freeze SPs field allows the ability to specify specific SPs to be frozen as part of the Block SID Authentication command.

If the Locking SP Freeze Lock supported bit is set to one, then the TPer SHALL support freezing the Locking SP when the Freeze Locking SP bit is set to one.

*Begin Informative Content*

This specification does not specify transitions from the Manufactured-Inactive life cycle state to Manufactured-Frozen life cycle state. The reason for this is that if the Locking SP was in the Manufactured-Inactive life cycle state where the Freeze Locking SP bit had been set to one, then the SID Authentication Blocked State bit would likely also be set to one, making it unlikely for an SP to ever transition from the Manufactured-Inactive life cycle state to the Manufactured-Frozen life cycle state.

*End Informative Content*

If the Locking SP is in the Manufactured life cycle state and the TPer receives a Block SID Authentication command with the Freeze Locking SP bit set to one, then the Locking SP SHALL transition to the Manufactured-Frozen life cycle state. See section 4.3.1 for more details on the Manufactured-Frozen state and 4.3.2.1 for more details on the transition from Manufactured to Manufactured-Frozen life cycle state.



**Table 5 Freeze SPs**

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | Reserved | | | | | | | Freeze Locking SP |

## 4.3 Life Cycle

For the Locking SP, this feature set defines an additional Optional Life Cycle State and additional Life Cycle State transitions.

### 4.3.1 Locking SP Manufactured-Frozen Life Cycle State (O)

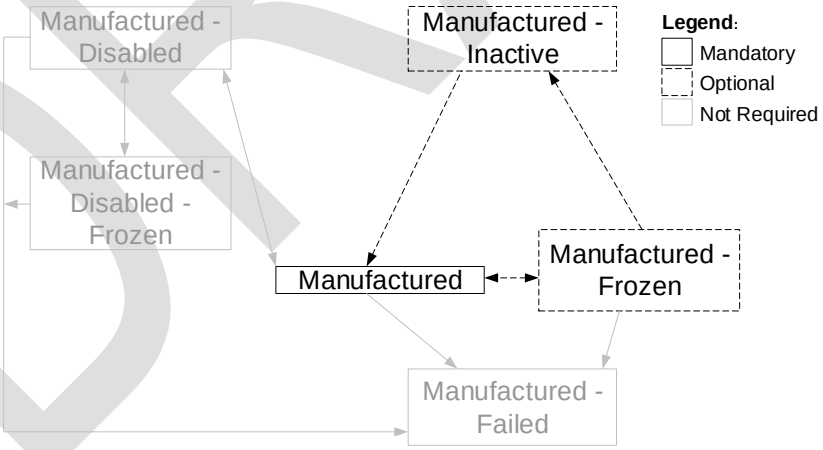
The Manufactured-Frozen life cycle state occurs after the Locking SP has been Manufactured and the value of the Locking SP's `Frozen` column in the Admin SP's `SP` table is True. See section 4.3.2 for details on how the Locking SP transitions between the Manufactured, Manufactured-Frozen, and Manufactured-Inactive life cycle states.

If the Locking SP is in the Manufactured-Frozen state, any attempt to start a session with the Locking SP SHALL result in a SyncSession with a status of SP_FROZEN.

If the Locking SP is in the Manufactured-Frozen life cycle state, then the Tries column of the C_PIN credential associated with any authority within the Locking SP SHALL NOT be incremented as a result of authentication attempts that were unsuccessful due to the Manufactured-Frozen life cycle state.

If an SD that supports the Block SID Authentication feature set also supports the Locking SP Freeze Lock capability, then the Locking SP SHALL support the Manufactured-Frozen life cycle state. See section 4.3.2 for details how the Locking SP transitions in and out of the Manufactured-Frozen life cycle state.

**Figure 1 Updated Life Cycle State Diagram for SSCs which support this feature set**




Note: Each SSC may specify different life cycle state requirements. This specification defines the Manufactured-Frozen life cycle state as an Optional life cycle state.



### 4.3.2 Additional Life Cycle State Transitions

This section identifies additional optional state transitions that are supported when the Locking SP Freeze Lock capability is supported (see section 4.1.1.4).

#### 4.3.2.1 Manufactured to Manufactured-Frozen

If the Locking SP Freeze Lock capability is supported, then the Locking SP SHALL transition from the Manufactured life cycle state to the Manufactured-Frozen life cycle state as a result of successful completion of the Block SID Authentication command with the Freeze Locking SP field set to one.

When the Locking SP transitions from the Manufactured life cycle state to the Manufactured-Frozen life cycle state:

a) The value of the Locking SP's `Frozen` column in the Admin SP's `SP` table SHALL be set to True.

b) The Locking SP Freeze Lock State bit SHALL be set to one.

c) The value of the Locking SP's LifeCycle column in the Admin SP's `SP` table SHALL be set to Manufactured-Frozen.

If the Locking SP transitions to the Manufactured-Frozen life cycle state, any open sessions with the Locking SP SHALL be aborted.

#### 4.3.2.2 Manufactured-Frozen to Manufactured

If the Locking SP is in the Manufactured-Frozen life cycle state, then the Locking SP SHALL transition from the Manufactured-Frozen life cycle state to the Manufactured life cycle state as a result of any default or selected Clear Event (see section 4.2.3) with the exception of successful invocation of the `Revert` method.

If the Original Factory State of the Locking SP is the Manufactured life cycle state and the Locking SP is in the Manufactured-Frozen life cycle state, then successful invocation of the `Revert` method on the Admin SP or Locking SP SHALL transition the Locking SP from the Manufactured-Frozen life cycle state to the Manufactured life cycle state.

When the Locking SP transitions from the Manufactured-Frozen life cycle state to the Manufactured life cycle state:

a) The value of the Locking SP's `Frozen` column in the Admin SP's `SP` table SHALL be set to False.

b) The Locking SP Freeze Lock State bit SHALL be cleared to zero.

c) The value of the Locking SP's LifeCycle column in the Admin SP's `SP` table SHALL be set to Manufactured.

#### 4.3.2.3 Manufactured-Frozen to Manufactured-Inactive

If the Original Factory State of the Locking SP is the Manufactured-Inactive life cycle state and the Locking SP is in the Manufactured-Frozen life cycle state, then successful invocation of the `Revert` method on the Admin SP or the Locking SP SHALL transition the Locking SP from the Manufactured-Frozen life cycle state to the Manufactured-Inactive life cycle state.

When the Locking SP transitions from the Manufactured-Frozen life cycle state to the Manufactured-Inactive life cycle state:

a) The value of the Locking SP's `Frozen` column in the Admin SP's `SP` table SHALL be set to False.

b) The Locking SP Freeze Lock State bit SHALL be cleared to zero.

c) The value of the Locking SP's LifeCycle column in the Admin SP's `SP` table SHALL be set to Manufactured-Inactive.



## 4.4 Locking SP

This feature set requires no additions to the Locking SP.

## 4.5 Additional SPs

This feature set requires no additional SPs.

