TRUSTED® COMPUTING GROUP

SPECIFICATION

TCG Storage Opal Family Feature Set: C_PIN Enhancements

Version 1.00
Revision 1.20
January 26, 2023

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

CONTENTS

List of Tables

1 Introduction

1.1 Document Purpose

The Storage Workgroup specifications provide a comprehensive architecture for Storage Devices (SDs) under policy control as determined by the trusted platform host, the capabilities of the SD to conform to the policies of the trusted platform, and the lifecycle state of the SD as a Trusted Peripheral.

1.2 Scope and Intended Audience

This specification defines C_PIN Enhancements for the Opal family Security Subsystem Classes (SSCs). Any SD that claims compliance to the C_PIN Enhancements Feature Set SHALL conform to this specification.

The intended audience for this specification is both trusted SD manufacturers and developers that want to use these SDs in their systems.

1.3 Conventions

1.3.1 Key Words

Key words are used to signify requirements.

The Key Words “SHALL”, “SHALL NOT”, “SHOULD,” and “MAY” are used in this document. These words are a subset of the RFC 2119 (see [1]) key words used by TCG. 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.

1.3.2 Font Conventions

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.

Hexadecimal numbers are in `Courier New font`.
All other text is in the Arial font.

1.3.3 Statement Types

There are two distinctive kinds of text: informative comment and normative statements.

By default, all statements are normative statements.

Informative statements are specifically marked by flagging the beginning and end of each informative comment and highlighting its text in gray.

EXAMPLE:

Start of Informative Comment

This is the first paragraph of 1-n paragraphs containing text of the kind informative comment ...

This is the second paragraph of text of the kind informative comment ...

This is the nth paragraph of text of the kind informative comment ...

To understand the TCG specification the user must read the specification. (This use of MUST does not require any action).

End of Informative Comment

1.3.4 SP Table Cell Color Legend

The legend in Table 1 defines the SP table cell color 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 (230, 230, 230)	Read-only	C_PIN Enhancements Feature Set specified	Fixed	• Cell content is Read-Only. • Access control is fixed. • Value is specified by the C_PIN Enhancements Feature Set
Arial Narrow bold-under (230, 230, 230)	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 (0, 0, 0)	Not Defined	(N)	Not Defined	• Cell 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 (179, 179, 179)	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 (179, 179, 179)	Write	Preconfigured, user personalizable	Fixed	• Cell content is writable. • Access control is fixed. • `Get` Access Control is not described by this color coding

1.3.5 List Conventions

1.3.5.1 Lists Overview

Lists are associated with an introductory paragraph or phrase, and are numbered relative to that paragraph or phrase (i.e., all lists begin with an a) or 1) entry).

Each item in a list is preceded by an identification with the style of the identification being determined by whether the list is intended to be an ordered list or an unordered list.

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.

1.3.5.2 Unordered Lists

An unordered list is one in which the order of the listed items is unimportant (i.e., it does not matter where in the list an item occurs as all items have equal importance). Each list item shall start with a lowercase letter followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an uppercase letter followed by a close parenthesis.

The following is an example of an unordered list with a nested unordered list:

EXAMPLE - The following are the items for the assembly:
a) a box containing:
    A) a bolt;
    B) a nut; and
    C) a washer;
b) a screwdriver; and
c) a wrench.

1.3.5.3 Ordered Lists

An ordered list is one in which the order of the listed items is important (i.e., item n is required before item n+1). Each listed item starts with a Western-Arabic numeral followed by a close parenthesis. If it is necessary to subdivide a list item further with an additional unordered list (i.e., have a nested unordered list), then the nested unordered list shall be indented and each item in the nested unordered list shall start with an uppercase letter followed by a close parenthesis.

The following is an example of an ordered list with a nested unordered list:

EXAMPLE - The following are the instructions for the assembly:
1) remove the contents from the box;
2) assemble the item;
    A) use a screwdriver to tighten the screws; and
    B) use a wrench to tighten the bolts;
    and
3) take a break.

1.3.6 Numbering

A binary number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 and 1 immediately followed by a lowercase b (e.g., 0101b). Underscores or spaces may be included

between characters in binary number representations to increase readability or delineate field boundaries (e.g., 0 0101 1010b or 0_0101_1010b).

A hexadecimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 and/or the uppercase English letters A through F immediately preceded by "`0x`". Underscores or spaces may be included between characters in hexadecimal number representations to increase readability or delineate field boundaries (e.g., `0xFD8C FA23` or `0x0B_FD8C_FA23`). Hexadecimal numbers are in `Courier New font`.

A decimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 not immediately followed by a lowercase b or lowercase h (e.g., 25). This standard uses the following conventions for representing decimal numbers:

a) the decimal separator (i.e., separating the integer and fractional portions of the number) is a period;
b) the thousands separator (i.e., separating groups of three digits in a portion of the number) is a space; and
c) the thousands separator is used in both the integer portion and the fraction portion of a number.

A decimal number represented in this standard with an overline over one or more digits following the decimal point is a number where the overlined digits are infinitely repeating (e.g., 666.$\bar{6}$ **Error! Bookmark not defined.**means 666.666 666… or 666 2/3, and 12.$\overline{142857}$ means 12.142 857 142 857… or 12 1/7).

1.3.7 Bit Conventions

Name (n:m), where n is greater than m, denotes a set of bits (e.g., Feature (7:0)).

1.3.8 Number Range Conventions

p..q, where p is less than q, represents a range of numbers (e.g., words 100..103 represents words 100, 101, 102, and 103).

1.4 Document References

1.4.1 Document Precedence

If there is a conflict between this specification and any other reference, then the precedence is (where a lower number indicates higher precedence):

1. this specification;
2. references under development (see section 1.4.3); and
3. approved references (see section 1.4.2).

Each reference under development and each approved reference may specify its own document precedence.

1.4.2 Approved 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), "Storage Interface Interactions Specification", Version 1.10

[4] Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opal", Version 2.02

[5] Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Opalite", Version 1.00

[6] Trusted Computing Group (TCG), "TCG Storage Security Subsystem Class: Ruby", Version 1.00

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

1.4.3 References Under Development

None

1.5 Dependencies on Other Feature Sets

This feature set does not depend upon any other feature sets.

1.6 Interactions with Other Feature Sets

This feature set does not interact with other feature sets.

1.7 Definition of Terms

Term	Definition
Default PIN authority	An authority that uses its default PIN
Default PIN(s)	For a given Authority, the set of PIN values at manufacturing, at SP activation, and as defined in the relevant C_PIN Table Preconfiguration of the applicable SSC. The specific Default PIN values are detailed in section 4.3.4.3.
DPCR	Default PIN Change Required
Non-default PIN Authority	An authority that uses a non-default PIN
Opal Family	Any of: Opal SSC [4], Opalite SSC [5], Ruby SSC [6], or Pyrite SSC [7]
PIN	Personal Identification Number
SD	Storage Device
SP	Security Provider
TPer	The Trusted Peripheral is the subset of a Storage Device for which TCG manages security
VU	Vendor Unique. A property that is set by the SD vendor

2 C_PIN Enhancements Feature Set Overview

The C_PIN Enhancements Feature Set is a collection of features surrounding authentication and PIN management, which expands the functionality defined in the Core Specification (See [2]).

All the features in this feature set are optional for SD vendors. Supported features and their configuration are reported in the feature descriptor for Level 0 discovery. Some of the features are configurable by a host.

The C_PIN Enhancements individual features are:

- **Minimum and Maximum PIN Length**: This feature defines the range of PIN lengths supported by the TPer. The SD vendor sets the minimum PIN length to a value in the range 0 – 128 bytes, and sets the maximum PIN length to a value in the range 32 – 128 bytes. An attempt by the host to set a PIN shorter than the minimum PIN length or longer than the maximum PIN length will be rejected by the TPer.

  A minimum and maximum PIN length value setting that is backward compatible with the Core Specification definition is 0 and 32 bytes, respectively.

  The Minimum and Maximum PIN lengths are reported in the feature descriptor. The values are not modifiable by the host.

  These values affect all C_PIN objects in the TPer, in the sense that any explicit attempt to set the PIN column of a C_PIN object is checked against the minimum and maximum lengths. In case this check fails, the attempted method will fail too.

  This feature does not affect the Initial PIN values, and any implicit PIN change (such as the side-effects of Revert, RevertSP and Locking SP activation).

- **Configurable C_PIN TryLimit**: The SD vendor may optionally allow the enablement and value-range configuration of the C_PIN objects TryLimit column by the host. This feature is determined by the SD vendor separately for authorities or groups of authorities. When this feature is allowed, the TryLimit column may be modified by the host. The original factory setting of this column remains as defined in the applicable SSC.

  The range of TryLimit values supported by the TPer (for configuration by the host) is reported in the feature descriptor for each of the authorities and groups of authorities. A special setting allows or disallows the host to configure a TryLimit value of zero (a TryLimit of zero disables the Tries/TryLimit mechanism).

- **Configurable C_PIN Persistence**: The SD vendor may optionally allow the configuration of the C_PIN objects Persistence column by the host. This feature is determined by the SD vendor separately for authorities or groups of authorities. When this feature is allowed, the Persistence column may be modified by the host. The original factory setting of this column remains FALSE, as defined in the applicable SSCs.

  Start of Informative Comment

  The persistence functionality bears a potential security risk of authorities' lock-out. If malicious software running on the host exhausts the Tries counter that relates to an authority, when the Persistence column is TRUE, that authority becomes locked-out, even after a power-cycle. SD vendors should be aware of this risk when allowing the configurable Persistence feature.

  For this reason, the PSID_C_PIN Persistence column is not settable by the host to TRUE (Access control disallows).

  An authority lock-out may be released by using one of the following techniques (if access control permits):

  1) Another authority may increase the TryLimit column of the locked-out authority.
  2) Another authority may reset the Persistence column of the locked-out authority to FALSE, and power-cycle.
  3) Another authority may change the PIN column of the locked-out authority.

Additionally, there is a risk of all-authorities' lock-out: If an SD supports TryLimit and Persistence configurability by the host for all authorities and groups of authorities, and if the host sets the Persistence column of all C_PIN objects to TRUE, malicious software can lock-out each and every Admin and User authority on the TPer by exhausting authentication tries.

In this situation, even after a power-cycle, Admin and User authorities cannot start sessions and user-data cannot be accessed if it is locked by the locking feature, as defined in Opal Family SSCs. An SD owner can still repurpose the drive by using the PSID to revert the SD to its original factory state, but all user-data on the SD will be lost.

All authorities' lock-out has security benefits for certain use cases where high security assurances around data confidentiality may be the top priority security requirement. For example, the use cases where the data in the SD is intended to become permanently inaccessible after a certain number of failed authentication attempts. In such cases, potentially losing data stored on a single device may be an acceptable risk, as opposed to that data being potentially stolen via repeated attacks against authorities' credentials.

As specified by this feature set, the SID authority's Persistence configurability feature is optional for the SD. Therefore, it is assumed that SD vendors will implement this functionality with intention to support specific security requirements as discussed above. Additionally, because the default SID authority Persistence Column is initialized as FALSE, it is also assumed that the host software will consider allowing the SID authority Persistence to be set to TRUE for its application, after careful examination of all the risks and benefits articulated in the previous paragraphs.

End of Informative Comment

- **Default PIN Change Required (DPCR)**: The SD vendor may optionally support the Default PIN Change Required feature. When supported, the host may enable it, and when enabled, authorities with a default PIN are required to specify a new PIN in their next authentication attempt. The new PIN may be specified by a new parameter of the `StartSession` and the `Authenticate` methods.

  The original factory setting of the DPCR feature is Disabled.

  The feature descriptor specifies whether this feature is supported and whether it is enabled. If supported, a new column DefaultPINChangeRequired in the `TPerInfo` table allows a host to enable or disable the feature.

This specification defines a new password type, password_128, to support an extended PIN length (See 3.3.1).

It adds a new column to the `TPerInfo` table, DefaultPINChangeRequired (see 3.2.2.1), to support the DPCR feature.

It optionally modifies `AccessControl` table entries and adds ACE table entries related to the C_PIN TryLimit and Persistence features and to the DPCR feature.

3 SSC Specific Functionality

This section specifies the additional SSC-specific functionality (not contained in the Core Specification [2] or the applicable Opal Family SSC) required to support the C_PIN Enhancements Feature Set.

3.1 Methods

This section defines new methods and modifications to existing methods required for this feature set.

3.1.1 New Methods

This feature set does not add new methods.

3.1.2 Modified Methods

The following methods are modified to support the DPCR feature:

a) `StartSession`

b) `Authenticate`

3.1.2.1 StartSession

The StartSession method is modified as follows:

3.1.2.1.1 StartSession Method

The `StartSession` method signature is modified as follows:

```
SMUID.StartSession [
    HostSessionID : uinteger,
    SPID : uidref {SPObjectUID},
    Write : boolean,
    HostChallenge = bytes,
    HostExchangeAuthority = uidref {AuthorityObjectUID},
    HostExchangeCert = bytes,
    HostSigningAuthority = uidref {AuthorityObjectUID},
    HostSigningCert = bytes,
    SessionTimeout = uinteger,
    TransTimeout = uinteger,
    InitialCredit = uinteger,
    SignedHash = bytes,
    NewPIN = bytes ]
=>
SMUID.SyncSession [ see SyncSession definition in the Core Specification ([2]) ]
```

An optional parameter (highlighted in yellow) is added to the `StartSession` method: NewPIN.

3.1.2.1.2 New Parameter Description: NewPIN

The `StartSession` method's NewPIN parameter number is `0x80`.

The NewPIN parameter provides an alternative mechanism to set the PIN column of a C_PIN object that corresponds to the authenticating authority. This alternative mechanism is in effect if the DPCR feature is supported, regardless of whether the feature is enabled.

As such, processing of the NewPIN parameter by the TPer adheres to the access control restrictions that are setup for that PIN column. If access control permits a certain authority to use the `Set` method on the PIN column of the C_PIN object that corresponds to that authority, then the use of the NewPIN parameter is permitted by the TPer. Otherwise, the use of this parameter results in a method status code that indicates failure, as described in 3.1.2.1.4.

Start of Informative Comment

For a Default PIN authority, using the NewPIN parameter in a `StarSession` or `Authenticate` method invocation, is the only possible way to successfully authenticate to a session, when the DPCR feature is enabled.

End of Informative Comment

3.1.2.1.3 Method Description

In addition to the method operation as described in the Core Specification ([2]), a successful `StartSession` method invocation that includes the NewPIN parameter has the side-effect of setting the PIN column of the C_PIN object that corresponds to the authenticating authority.

3.1.2.1.4 Method Status Codes

In case a SUCCESS status code (indicating successful authentication) would otherwise be sent as the `SyncSession` method status code (due to previous checks, as described in the Core Specification [2]), a status code of NOT_AUTHORIZED or INVALID_PARAMETER SHALL be sent if the conditions described below are met:

A status code of NOT_AUTHORIZED SHALL be sent as the `SyncSession` method status code in the following cases:

1) The NewPIN parameter is included in the method invocation, but access control settings do not permit access to the PIN column of the C_PIN object that corresponds to the authenticating authority; or
2) The NewPIN parameter is not included in the method invocation, but it's required because the DPCR feature is enabled and the authenticating authority uses its default PIN.

A status code of INVALID_PARAMETER SHALL be sent as the `SyncSession` method status code in the following cases:

1) The NewPIN parameter value does not adhere to the type and size restrictions of the PIN column of the `C_PIN` table;
2) The NewPIN parameter attempts to set a default PIN value to the PIN column of the C_PIN object that corresponds to the authenticating authority, and the DPCR feature is enabled;
3) The NewPIN parameter is included in the method invocation, but the DPCR feature is not supported by the TPer; or
4) The NewPIN parameter is included in the method invocation, but the value of the Operation column of the Authority object that corresponds to the authenticating authority is not "Password".

3.1.2.2 Authenticate

The Authenticate method signature is modified as follows:

```
ThisSP.Authenticate [
     Authority : uidref { AuthorityObjectUID },
     Proof = bytes,
     NewPIN = bytes ]
=>
[ Result : typeOr { Success : boolean, Challenge : bytes } ]
```

An optional parameter (highlighted in yellow) is added to the Authenticate method: NewPIN.

3.1.2.2.1 New Parameter Description: NewPIN

The Authenticate method's NewPIN parameter number is `0x80`.

As with the `StartSession` method, the NewPIN parameter provides an alternative mechanism to set the PIN column of a C_PIN object that corresponds to the authenticating authority. This alternative mechanism is in effect if the DPCR feature is supported, regardless of whether the feature is enabled.

As with the `StartSession` method, processing of the NewPIN parameter by the TPer adheres to the access control restrictions that are setup for that PIN column. If access control permits a certain authority to use the `Set` method on the PIN column of the C_PIN object that corresponds to that authority, then the use of the NewPIN parameter is permitted by the TPer. Otherwise, the use of this parameter results in a method status code that indicates failure, as described in 3.1.2.2.3.

3.1.2.2.2 Method Description

In addition to the method operation as described in the Core Specification ([2]), a successful `Authenticate` method invocation that includes the NewPIN parameter has the side-effect of setting the PIN column of the C_PIN object that corresponds to the authenticating authority.

If the side-effect of setting the appropriate PIN column succeeds, and if there are no other reasons for the `Authenticate` method to fail, then the `Authenticate` method SHALL return a method status code of SUCCESS and a Result of TRUE.

If the `Authenticate` method fails, then PIN column change (to the value specified by the NewPIN parameter) SHALL NOT occur.

If the `Authenticate` method is invoked within a transaction and the transaction is eventually aborted, then any PIN column change as a side-effect of the `Authenticate` method (using the NewPIN parameter) SHALL be reverted.

3.1.2.2.3 Method Results List and Status Code in case of Failure

In case a SUCCESS status code with a Result parameter value of TRUE (indicating successful authentication) would otherwise be returned by the `Authenticate` method (by previous checks, as described in the Core Specification [2]), a status code of NOT_AUTHORIZED or INVALID_PARAMETER and an empty results list SHALL be returned if the conditions described below are met:

A method status code of NOT_AUTHORIZED and an empty results list SHALL be returned in response to the `Authenticate` method in the following cases:

1) The NewPIN parameter is included in the method invocation, but access control settings do not permit access to the PIN column of the C_PIN object that corresponds to the authenticating authority; or
2) The NewPIN parameter is not included in the method invocation, but it's required because the DPCR feature is enabled, and the authenticating authority uses its default PIN.

A method status code of INVALID_PARAMETER and an empty results list SHALL be returned in response to the `Authenticate` method in the following cases:

1) The NewPIN parameter value does not adhere to the type and size restrictions of the PIN column of the C_PIN table;
2) The NewPIN parameter attempts to set a default PIN value to the PIN column of the C_PIN object that corresponds to the authenticating authority, and the DPCR feature is enabled;
3) The NewPIN parameter is included in the method invocation, but the DPCR feature is not supported by the TPer; or
4) The NewPIN parameter is included in the method invocation, but the value of the Operation column of the Authority object that corresponds to the authenticating authority is not "Password".

3.2 Tables

This section defines new tables and modifications to existing tables required for this feature set.

3.2.1 New Tables

This feature set does not add new tables.

3.2.2 Modified Tables

This feature set modifies the following tables:

- Admin SP `TPerInfo` table
- Admin SP and Locking SP `C_PIN` tables
- Admin SP and Locking SP `AccessControl` tables
- Admin SP and Locking SP `ACE` tables

3.2.2.1 Admin SP TPerInfo Table

This feature set modifies the `TPerInfo` table by adding the following column (see Table 2), in addition to those defined in the Core Specification [2] and in the applicable Opal Family SSCs:

Table 2 – Admin SP TPerInfo Table new column

Column Number	Column Name	IsUnique	Column Type
`0x80`	DefaultPINChangeRequired		boolean

3.2.2.1.1 DefaultPINChangeRequired (M)

The DefaultPINChangeRequired column's preconfiguration value is FALSE.

This column determines whether the DPCR feature is enabled.

For a detailed description of this column's functionality, see 4.3.4.1.

Start of Informative Comment

To avoid confusing configurations, access control to this column is conditionally allowed, depending on whether the DPCR feature is supported by the TPer.

End of Informative Comment

3.2.2.2 Admin SP and Locking SP C_PIN Tables

3.2.2.2.1 PIN Column

3.2.2.2.1.1 PIN Column Type

This feature set modifies the Admin SP and Locking SP `C_PIN` tables by changing the type of the PIN column. The new type is as described in Table 3:

Table 3 - Admin SP and Locking SP C_PIN table changed column

Column Number	Column Name	IsUnique	Column Type
0x03	PIN		password_128

The type password_128 is defined in this feature set specification. See its definition in 3.3.1.

Start of Informative Comment

The PIN's column type is changed from password to password_128 to accommodate longer passwords as required by the Minimum/Maximum PIN length feature.

End of Informative Comment

3.2.2.2.1.2 PIN Column Setting

This feature set adds restrictions to the supported PIN lengths, as defined in 4.3.1.

3.2.2.2.2 TryLimit Column Setting

This feature set adds restrictions to the supported TryLimit column values, as defined in 4.2.1.5, 4.2.1.6 and 4.2.1.7.

3.2.2.3 Admin SP and Locking SP AccessControl Tables

This feature set modifies the Admin SP and Locking SP `AccessControl` tables by adding ACEs to ACL columns. The added ACEs allow access to the `C_PIN` table TryLimit and Persistence columns and to the `TPerInfo` table DefaultPINChangeRequired new column.

These ACEs are added conditionally, depending on individual features support as indicated by the feature descriptor.

The `AccessControl` table modifications are detailed in 4.4.1.2 and in 4.5.1.1.

3.2.2.4 Admin SP and Locking SP ACE Tables

This feature set adds ACE entries to the Admin SP and Locking SP `ACE` tables. The added ACEs allow access to the `C_PIN` table TryLimit and Persistence columns and to the `TPerInfo` table DefaultPINChangeRequired new column.

These ACEs are added conditionally, depending on features support as indicated by the feature descriptor.

The new ACE entries are detailed in 4.4.1.3.1 and in 4.5.1.2.1.

3.3 Types

This section defines new types and modifications to existing types required for this feature set.

3.3.1 New Types

This feature set adds the following type (see Table 4) for supporting the Minimum/Maximum PIN Length feature:

Table 4 - password_128 type

UID	Name	Format
00 00 00 05 00 00 20 0F	password_128	Simple_Type, max_bytes, 128

3.3.2 Modified Types

This feature set does not modify any type.

4 Feature Set Requirements

This section defines the Mandatory (M) and Optional (O) requirements for the C_PIN Enhancements Feature Set.

4.1 Requirements Overview

The C_PIN Enhancements Feature Set consists of `C_PIN` table functionality related capabilities that MAY be implemented in a TPer. A host discovers the C_PIN Enhancements capabilities and properties of a TPer by examining the Feature Descriptor returned in Level 0 Discovery.

4.2 Level 0 Discovery

An SD implementing the C_PIN Enhancements Feature Set SHALL:

a) return the C_PIN Enhancements Feature Descriptor as defined in 4.2.1; and

b) support the Level 0 Discovery response requirements defined in the various Opal Family SSCs.

4.2.1 C_PIN Enhancements Feature Descriptor (Feature Code = 0x0409) (M)

The C_PIN Enhancements Feature Descriptor SHALL be returned when the SD supports the C_PIN Enhancements Feature Set. The contents of the feature descriptor are defined in Table 5:

Table 5 - Level 0 Discovery – C_PIN Enhancements Feature Descriptor

Byte \ Bit	7	6	5	4	3	2	1	0
0	(MSB)				Feature Code			
1								(LSB)
2	Feature Descriptor Version Number				Feature Set Minor Version Number			
3	Length							
4	Admin SP Admin1-AdminXX C_PIN TryLimit Configurability							
	Reserved	The exponent in max TryLimit configurable value (XMTLCV)					Zero Allowed (ZA)	TryLimit Configurable (TLC)
5	Admin SP SID C_PIN TryLimit Configurability							
	Reserved	The exponent in max TryLimit configurable value (XMTLCV)					Zero Allowed (ZA)	TryLimit Configurable (TLC)
6	Admin SP PSID C_PIN TryLimit Configurability							
	Reserved	The exponent in max TryLimit configurable value (XMTLCV)					Zero Allowed (ZA)	TryLimit Configurable (TLC)
7	Locking SP Admin1-AdminXXXX C_PIN TryLimit Configurability							
	Reserved	The exponent in max TryLimit configurable value (XMTLCV)					Zero Allowed (ZA)	TryLimit Configurable (TLC)
8	Locking SP User1-UserMMMM C_PIN TryLimit Configurability							
	Reserved	The exponent in max TryLimit configurable value (XMTLCV)					Zero Allowed (ZA)	TryLimit Configurable (TLC)
9	C_PIN Persistence Configurability							
	Reserved				Locking SP User1-UserMMMM Persistence Configurable (LSP_UPC)	Locking SP Admin1-AdminXXXX Persistence Configurable (LSP_APC)	Admin SP SID Persistence Configurable (ASP_SPC)	Admin SP Admin1-AdminXX Persistence Configurable (ASP_APC)
10	Minimum PIN Length (0 – 128 bytes)							
11	Maximum PIN Length (32 – 128 bytes)							
12	Reserved						DPCR Enabled	DPCR Supported
13 - 19	Reserved							

4.2.1.1 Feature Code

The Feature Code field value SHALL be set to `0x0409`.

4.2.1.2 Feature Descriptor Version Number

The Feature Descriptor Version Number field SHALL be set to `0x1` or any version that supports the features described in this specification.

4.2.1.3 Feature Set Minor Version Number

The Feature Set Minor Version Number reflects the minor version of the C_PIN Enhancements Feature Set supported by the SD.

The Feature Set Minor Version Number field SHALL be set to a value as specified in Table 6:

Table 6 - Feature Set Minor Versions

Feature Set Minor Version Number	Standard Referenced
0x0	C_PIN Enhancements Feature Set v1.00
All others	Reserved for future versions of the feature set

4.2.1.4 Length

The Length field indicates the number of bytes in the descriptor following byte 3. The value of the Length field SHALL be set to `0x10`.

4.2.1.5 TryLimit Configurable (TLC)

The TryLimit Configurable (TLC) bit indicates whether the TPer supports C_PIN TryLimit configurability by the host, for a certain authority or group of authorities. If the TPer supports TryLimit configurability, then the TLC bit SHALL be set to 1. Otherwise, the TLC bit SHALL be reset to 0.

The TLC bit is defined for each of the following authorities and groups of authorities: Admin SP Admin1-AdminXX, Admin SP SID, Admin SP PSID, Locking SP Admin1-AdminXXXX, and Locking SP User1-UserMMMM (bytes 4-8 of the feature descriptor).

Start of Informative Comment

The C_PIN TryLimit Configurability feature is described in the Overview section (2) and in 4.3.2.

End of Informative Comment

4.2.1.6 Zero Allowed (ZA)

The Zero Allowed (ZA) bit indicates whether the TPer allows the host to configure a TryLimit value of zero, for a certain authority or group of authorities. A TryLimit value of zero effectively disables the Tries/TryLimit mechanism. If the TPer allows the host to configure a TryLimit value of zero, then the ZA bit SHALL be set to 1. Otherwise, the ZA bit SHALL be reset to 0.

The ZA bit is defined for the same authorities and groups of authorities as the TLC bit (see 4.2.1.5).

4.2.1.7 The Exponent in Max TryLimit Configurable Value (XMTLCV)

The Max TryLimit configurable value is the result of a calculation of the maximum TryLimit column value supported by the TPer. The calculation is based on the XMTLCV, which is a 5 bits field capable of specifying values in the range 0 – 31.

The calculation of Max TryLimit Configurable value is as follows:

Max TryLimit configurable Value = $2^{(XMTLCV + 1)} – 1$.

Start of Informative Comment

Table 7 shows calculation examples of Max TryLimit Configurable value as a function of the exponent XMTLCV:

Table 7 - Max TryLimit Configurable Value Calculation Example

XMTLCV	Max TryLimit Configurable value
0	$2^{(0+1)} - 1 = 1$
1	$2^{(1+1)} - 1 = 3$
2	$2^{(2+1)} - 1 = 7$

XMTLCV	Max TryLimit Configurable value
3	$2^{(3+1)} - 1 = 15$
…	
31	$2^{(31+1)} - 1 = 0xFFFFFFFF$

End of Informative Comment

The XMTLCV is defined for the same authorities and groups of authorities as the TLC bit (see 4.2.1.5).

4.2.1.8 Persistence Configurable

The Persistence Configurable bit indicates whether the TPer supports C_PIN Persistence configurability by the host, for a certain authority or group of authorities. If the TPer supports C_PIN Persistence configurability, then the Persistence Configurable bit SHALL be set to 1. Otherwise, it SHALL be reset to 0.

This bit is defined for each of the following authorities and groups of authorities: Admin SP Admin1-AdminXX, Admin SP SID, Locking SP Admin1-AdminXXXX, and Locking SP User1-UserMMMM (byte 9, bits 0 – 3 of the feature descriptor).

Start of Informative Comment

The C_PIN Persistence Configurability feature is described in the Overview section (2) and in 4.3.3.

End of Informative Comment

4.2.1.9 Minimum PIN Length

The Minimum PIN Length field indicates the minimum length of C_PIN PIN supported by the TPer. The SD SHALL specify the Minimum PIN Length as a value in the range 0 – 128 bytes.

The Minimum PIN Length SHALL be smaller than or equal to the Maximum PIN Length.

The scope of the Minimum PIN Length is the whole TPer (it affects both the Admin SP and the Locking SP).

4.2.1.10 Maximum PIN Length

The Maximum PIN Length field indicates the maximum length of C_PIN PIN supported by the TPer. The SD SHALL specify the Maximum PIN Length as a value in the range 32 – 128 bytes.

The Maximum PIN Length SHALL be greater than or equal to the Minimum PIN Length.

The scope of the Maximum PIN Length is the whole TPer (it affects both the Admin SP and the Locking SP).

Start of Informative Comment

A configuration of Minimum PIN Length and Maximum PIN Length that is backward-compatible with the PIN length as defined in [2] is 0 and 32 bytes, respectively.

End of Informative Comment

4.2.1.11 DPCR Supported

The DPCR Supported bit indicates whether the SD vendor supports the DPCR feature (a bit value of 1 indicates that the feature is supported). If the feature is supported, the host may enable it by setting the new DefaultPINChangeRequired column of the `TPerInfo` table (See 3.2.2.1.1) to TRUE.

The scope of the DPCR Supported bit is the whole TPer (it affects both the Admin SP and the Locking SP).

4.2.1.12 DPCR Enabled

The DPCR Enabled bit is a mirror of the current setting of the new DefaultPINChangeRequired column of the `TPerInfo` table.

The scope of the DPCR Enabled bit is the whole TPer (it affects both the Admin SP and the Locking SP).

4.3 TPer Scope Requirements

This section defines the behavior of TPer scope features (TPer scope features affect both the Admin SP and the Locking SP):

4.3.1 Minimum and Maximum PIN Lengths

If a TPer supports the C_PIN Enhancements Feature Set, the TPer SHALL validate the length of a received `Set` method on a C_PIN object with the PIN column by verifying that the PIN length is in the range defined by the feature set descriptor fields Minimum PIN Length and Maximum PIN Length. See 0 and 4.2.1.10.

If the host attempts to configure C_PIN PIN that is out of this length range, then the TPer SHALL fail the command with a status of INVALID_PARAMETER.

4.3.2 C_PIN Tables TryLimit Configurability

If a TPer supports the C_PIN Enhancements Feature Set, and if the TPer supports TryLimit configurability by the host, for a certain authority or group of authorities (as indicated by the TLC bit in the feature descriptor), then the proper access control settings are set up to allow this configurability. See the required modifications to the AccessControl and the ACE tables, in 4.4.1.2 and 4.4.1.3 (Admin SP), and in 4.5.1.1 and 4.5.1.2 (Locking SP).

The TryLimit column's behavior is as defined in the Core Specification (See [2]).

The TPer SHALL validate that the configured TryLimit value is within the supported range for that authority.

The supported TryLimit value range for a certain authority is defined by the following statements:

1) The value is between 0 and the calculated Max TryLimit Configurable value (as a function of the XMTLCV field). This calculated value is detailed in 4.2.1.7; and
2) If the Zero-Allowed (ZA) bit in the feature descriptor is set to 1, the configured TryLimit value may be zero, otherwise, it may not be zero. See 4.2.1.6.

If the host attempts to configure the TryLimit column with a value that is not within this supported range, then the TPer SHALL fail the command with a status of INVALID_PARAMETER.

4.3.3 C_PIN Tables Persistence Configurability

If a TPer supports the C_PIN Enhancements Feature Set, and if the TPer supports Persistence configurability by the host, for a certain authority or group of authorities (as indicated by Persistence configurability byte in the feature descriptor), then the proper access control settings are set up to allow this configurability. See the required modifications to the AccessControl and the ACE tables, in 4.4.1.2 and 4.4.1.3 (Admin SP), and in 4.5.1.1 and 4.5.1.2 (Locking SP).

The Persistence column's behavior is as defined in the Core Specification (See [2]).

4.3.4 Default PIN Change Required (DPCR) Feature

The DPCR feature, when supported and enabled (see 4.3.4.1), expects the host to provide a new PIN when a default PIN authority attempts to start a session or to authenticate to an existing session. If the new PIN is required but not provided by the host, the authentication attempt SHALL fail.

The new PIN is specified as a parameter to the `StartSession` or `Authenticate` methods.

Upon a successful authentication attempt, the new PIN replaces the existing PIN in the C_PIN object that corresponds to the authenticating authority. This PIN replacement depends on access control allowing the authenticating authority to set the PIN column of this C_PIN object.

See description of changes to the `StartSession` method (See 3.1.2.1) and to the `Authenticate` method (See 3.1.2.2).

4.3.4.1 Conditions when the DPCR Feature is Enabled

When the DPCR feature is supported by the TPer, the TPerInfo object DefaultPINChangeRequired column's configuration determines whether the feature is enabled.

If:

a) The SD supports the DPCR feature, as indicated by the corresponding bit in the feature descriptor; and

b) The `TPerInfo` table object DefaultPINChangeRequired column value is TRUE;

Then, the DPCR feature is enabled. Otherwise, the feature is disabled.

4.3.4.2 Authorities Checked for Default PIN

The following section determines which authorities are checked for using their default PIN, and which authorities are not.

If the DPCR feature is not supported or it is disabled, none of the authorities are checked for using their default PIN.

For authorities in the DPCR Authorities Group (see group definition below), if the DPCR feature is enabled, then when each of these authorities authenticates (using the `StartSession` method or the `Authenticate` method), its PIN is checked to determine whether it's a default or non-default PIN, and the method acts as defined in the method's description (3.1.2.1.3 and 3.1.2.2.2, respectively).

The DPCR Authorities Group includes the following authority objects:

- Admin SP individual Admin authorities (e.g. Admin1, Admin2, etc.).
- Locking SP individual Admin authorities (e.g. Admin1, Admin2, etc.).
- Locking SP individual User authorities (e.g. User1, User2, etc.).

For authorities in the Non-DPCR Authorities Group (see group definition below), if the DPCR feature is enabled, these authorities are not checked for using a default PIN when authenticating.

The Non-DPCR Authorities Group includes the following authority objects:

- Admin SP SID
- Admin SP PSID (the PSID authority's PIN column value is fixed).
- Anybody (the Anybody authority does not use a PIN).
- Class authorities (Class authorities are not being authenticated).

4.3.4.3 Specification of Default PIN Values

This section specifies the default PIN values for authorities in the DPCR Authorities group. The DPCR Authorities Group is defined in the previous section (4.3.4.2).

- For the Locking SP Admin1 Authority:
  The Default PINs are the Admin SP MSID PIN and the initial value of Admin SP SID PIN at manufacturing (if different from MSID PIN).
- For other authorities in the DPCR Authorities Group:
  The Default PINs are "" and the initial value of the associated C_PIN's PIN at manufacturing (if different from "").

4.4 Admin SP Requirements

An SD implementing this feature set SHALL support the changes to the Admin SP specified in this section, in addition to the Admin SP requirements defined in their applicable Opal Family SSCs.

4.4.1 Tables

4.4.1.1 TPerInfo Table Changes

The changes to the `TPerInfo` table are detailed in section 3.2.2.1.

4.4.1.2 AccessControl Table Changes

`AccessControl` table changes depend on support of the various features by the TPer.

Conditional items are designated with *Cond_ACn.

4.4.1.2.1 New AccessControl Table Rows

In addition to the requirements in the various Opal Family SSCs, the following `AccessControl` table row SHALL be added and preconfigured as specified in Table 8, conditionally.

The condition to add the following new row to the Admin SP `AccessControl` table is specified by *Cond_AC1:

- *Cond_AC1: Addition of this row depends on the support of Configurable C_PIN TryLimit for PSID, as indicated by the Feature Descriptor (Feature Descriptor Byte 6, TLC field).

Table 8 - Admin SP AccessControl Table Preconfiguration – New row

Table association - Informative text	UID	InvokingID	InvokingID Name - informative text	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_PIN																
		00 00 00 0B 00 01 FF 01 (*Cond_AC1)	C_PIN_PSID	Set		ACE_C_PIN_PSID_Set_TryLimit				ACE_Anybody						

4.4.1.2.2 Modified AccessControl Table Rows

In addition to the requirements in the various Opal Family SSCs, the following `AccessControl` table rows SHALL be preconfigured as specified in Table 9, conditionally. The condition for modifying table rows is indicated in the table by *Cond_ACn tags.

Conditional changes:

- *Cond_AC2: Inclusion of this ACE depends on the support of Configurable C_PIN TryLimit for SID by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 5, TLC field).
- *Cond_AC3: Inclusion of this ACE depends on the support of Configurable C_PIN Persistence for SID by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, ASP_SPC field).
- *Cond_AC4: Inclusion of this ACE depends on the support of Configurable C_PIN TryLimit for Admin SP Admin1-AdminXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 4, TLC field).
- *Cond_AC5: Inclusion of this ACE depends on the support of Configurable C_PIN Persistence for Admin SP Admin1-AdminXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, ASP_APC field).
- *Cond_AC6: Inclusion of this ACE depends on the support of DPCR feature by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 12, DPCR Supported Field).

Table 9 - Admin SP AccessControl Table Preconfiguration – Modified rows

Table association - Informative text	UID	InvokingID	InvokingID Name - informative text	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_PIN																
		00 00 00 0B 00 00 00 01	C_PIN_SID	Set		ACE_C_PIN_SID_Set_PIN ACE_C_PIN_SID_Set_TryLimit (*Cond_AC2) ACE_C_PIN_SID_Set_Persistence (*Cond_AC3)				ACE_Anybody						

Table association - Informative text	UID	InvokingID	InvokingID Name - informative text	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
		00 00 00 0B 00 00 02 01	C_PIN_Admin1	Set		ACE_C_PIN_Admins_Set_PIN ACE_C_PIN_Admins_Set_TryLimit (*Cond_AC4) ACE_C_PIN_Admins_Set_Persistence (*Cond_AC5)				ACE_Anybody						
		00 00 00 0B 00 00 02 00 (+XX)	C_PIN_AdminXX	Set		ACE_C_PIN_Admins_Set_PIN ACE_C_PIN_Admins_Set_TryLimit (*Cond_AC4) ACE_C_PIN_Admins_Set_Persistence (*Cond_AC5)				ACE_Anybody						

TPerInfo																
		00 00 02 01 00 03 00 01	TPerInfoObj	Set		ACE_TPerInfo_Set_ProgrammaticResetEnable ACE_TPerInfo_Set_ DefaultPINChangeRequired (*Cond_AC6)				ACE_Anybody						

4.4.1.3 ACE Table Changes

ACE table changes depend on support of the various features by the TPer.

Conditional items are designated by *Cond_ACEn.

4.4.1.3.1 New ACE Table Rows

In addition to the requirements in the various Opal Family SSCs, the following ACE table rows SHALL be added and preconfigured as specified in Table 10, conditionally. The Condition column is not numbered. It provides guidance to SD vendors as to whether a specific row is to be included in the ACE Table.

Conditional changes:

- *Cond_ACE1: Inclusion of this ACE table row depends on the support of Configurable C_PIN TryLimit for PSID by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 6, TLC field).
- *Cond_ACE2: Inclusion of this ACE table row depends on the support of Configurable C_PIN TryLimit for SID by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 5, TLC field).
- *Cond_ACE3: Inclusion of this ACE table row depends on the support of Configurable C_PIN Persistence for SID by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, ASP_SPC field).
- *Cond_ACE4: Inclusion of this ACE table row depends on the support of Configurable C_PIN TryLimit for Admin SP Admin1-AdminXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 4, TLC field).
- *Cond_ACE5: Inclusion of this ACE table row depends on the support of Configurable C_PIN Persistence for Admin SP Admin1-AdminXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, ASP_APC field).
- *Cond_ACE6: Inclusion of this ACE table row depends on the support of DPCR feature by the TPer, as indicated in the Feature Descriptor.

Table 10 - Admin SP ACE Table Preconfiguration – New rows

Table Association - Informative text	Condition	UID	Name	CommonName	BooleanExpr	Columns
C_PIN						
	*Cond_ACE1	00 00 00 08 00 05 10 01	"ACE_C_PIN_PSID_Set_TryLimit"		SID	TryLimit
	*Cond_ACE2	00 00 00 08 00 05 10 02	"ACE_C_PIN_SID_Set_TryLimit"		SID	TryLimit
	*Cond_ACE3	00 00 00 08 00 05 10 03	"ACE_C_PIN_SID_Set_Persistence"		SID	Persistence
	*Cond_ACE4	00 00 00 08 00 05 10 04	"ACE_C_PIN_Admins_Set_TryLimit"		Admins OR SID	TryLimit
	*Cond_ACE5	00 00 00 08 00 05 10 05	"ACE_C_PIN_Admins_Set_Persistence"		Admins OR SID	Persistence
TPerInfo						
	*Cond_ACE6	00 00 00 08 00 05 10 06	"ACE_TPerInfo_Set_ DefaultPINChangeRequired"		SID	DefaultPINChangeRequired

4.5 Locking SP Requirements

An SD implementing this feature set SHALL support the changes to the Locking SP specified in this section, in addition to the Locking SP requirements defined in their applicable Opal Family SSCs.

4.5.1 Tables

4.5.1.1 AccessControl Table Changes

`AccessControl` table changes depend on support of the various features by the TPer.

Conditional items are designated with *Cond_ACn.

4.5.1.1.1 Modified AccessControl Table Rows

In addition to the requirements in the various Opal Family SSCs, the following `AccessControl` table rows SHALL be preconfigured as specified in Table 11, conditionally. The condition to modify table rows is indicated in the table by *Cond_ACn tags.

Conditional changes:

- *Cond_AC7: Inclusion of this ACE depends on the support of Configurable C_PIN TryLimit for Locking SP Admin1-AdminXXXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 7, TLC field).
- *Cond_AC8: Inclusion of this ACE depends on the support of Configurable C_PIN Persistence for Locking SP Admin1-AdminXXXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, LSP_APC field).
- *Cond_AC9: Inclusion of this ACE depends on the support of Configurable C_PIN TryLimit for Locking SP User1-UserMMMM by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 8, TLC field).
- *Cond_AC10: Inclusion of this ACE depends on the support of Configurable C_PIN Persistence for Locking SP User1-UserMMMM by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, LSP_UPC field).

Table 11 - Locking SP AccessControl Table Preconfiguration – Modified rows

Table Association - informative only	UID	InvokingID	InvokingID Name - informative only	MethodID	CommonName	ACL	Log	AddACEACL	RemoveACEACL	GetACLACL	DeleteMethodACL	AddACELog	RemoveACELog	GetACLLog	DeleteMethodLog	LogTo
C_PIN																
		00 00 00 0B 00 01 00 01	C_PIN_Admin1	Set		ACE_C_PIN_Admins_Set_PIN ACE_C_PIN_Admins_Set_TryLimit (*Cond_AC7) ACE_C_PIN_Admins_Set_Persistence (*Cond_AC8)				ACE_Anybody						
		00 00 00 0B 00 01 00 00 (+XX XX)	C_PIN_AdminXXXX	Set		ACE_C_PIN_Admins_Set_PIN ACE_C_PIN_Admins_Set_TryLimit (*Cond_AC7) ACE_C_PIN_Admins_Set_Persistence (*Cond_AC8)				ACE_Anybody						

		Table Association - informative only
		UID
00 00 00 0B 00 03 00 00 (+MM MM)	00 00 00 0B 00 03 00 01	InvokingID
C_PIN_UserMMMM	C_PIN_User1	InvokingID Name - informative only
Set	Set	MethodID
		CommonName
ACE_C_PIN_UserMMMM_Set_PIN ACE_C_PIN_ Admins_Set_TryLimit (*Cond_AC9) ACE_C_PIN_ Admins_Set_Persistence (*Cond_AC10)	ACE_C_PIN_User1_Set_PIN ACE_C_PIN_Admins_Set_TryLimit (*Cond_AC9) ACE_C_PIN_ Admins_Set_Persistence (*Cond_AC10)	ACL
		Log
		AddACEACL
		RemoveACEACL
ACE_Anybody	ACE_Anybody	GetACLACL
		DeleteMethodACL
		AddACELog
		RemoveACELog
		GetACLLog
		DeleteMethodLog
		LogTo

4.5.1.2 ACE Table Changes

ACE table changes depend on support of the various features by the TPer.

Conditional items are designated with *Cond_ACEn.

4.5.1.2.1 New ACE Table Rows

In addition to the requirements in the various Opal Family SSCs, the following ACE table rows SHALL be preconfigured as specified in Table 12, conditionally. The Condition column is not numbered. It provides guidance to SD vendors as to whether a specific row is to be included in the ACE Table.

Conditional changes:

- *Cond_ACE7: Inclusion of this ACE table row depends on the support of Configurable C_PIN TryLimit for Locking SP Admin1-AdminXXXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 7, TLC field).
- *Cond_ACE8: Inclusion of this ACE table row depends on the support of Configurable C_PIN Persistence for Locking SP Admin1-AdminXXXX by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, LSP_APC field).
- *Cond_ACE9: Inclusion of this ACE table row depends on the support of Configurable C_PIN TryLimit for Locking SP User1-UserMMMM by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 8, TLC field).
- *Cond_ACE10: Inclusion of this ACE table row depends on the support of Configurable C_PIN Persistence for Locking SP User1-UserMMMM by the TPer, as indicated in the Feature Descriptor (Feature Descriptor Byte 9, LSP_UPC field).

Table 12 - Locking SP ACE Table Preconfiguration – New rows

Table Association	Condition	UID	Name	CommonName	BooleanExpr	Columns
C_PIN						
	*Cond_ACE7 or *Cond_ACE9	00 00 00 08 00 05 11 01	"ACE_C_PIN_Admins_Set_TryLimit"		Admins	TryLimit
	*Cond_ACE8 or *Cond_ACE10	00 00 00 08 00 05 11 02	"ACE_C_PIN_Admins_Set_Persistence"		Admins	Persistence

4.6 Additional SPs

This feature set does not require additional SPs.

End of C_PIN Enhancements Feature Set

