

JEDEC STANDARD

Universal Flash Storage (UFS) Security Extension

JESD225

NOVEMBER 2016

JEDEC SOLID STATE TECHNOLOGY ASSOCIATION



NOTICE

JEDEC standards and publications contain material that has been prepared, reviewed, and approved through the JEDEC Board of Directors level and subsequently reviewed and approved by the JEDEC legal counsel.

JEDEC standards and publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for use by those other than JEDEC members, whether the standard is to be used either domestically or internationally.

JEDEC standards and publications are adopted without regard to whether or not their adoption may involve patents or articles, materials, or processes. By such action JEDEC does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the JEDEC standards or publications.

The information included in JEDEC standards and publications represents a sound approach to product specification and application, principally from the solid state device manufacturer viewpoint. Within the JEDEC organization there are procedures whereby a JEDEC standard or publication may be further processed and ultimately become an ANSI standard.

No claims to be in conformance with this standard may be made unless all requirements stated in the standard are met.

Inquiries, comments, and suggestions relative to the content of this JEDEC standard or publication should be addressed to JEDEC at the address below, or refer to www.jedec.org under Standards and Documents for alternative contact information.

Published by
©JEDEC Solid State Technology Association 2016
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

This document may be downloaded free of charge; however JEDEC retains the copyright on this material. By downloading this file the individual agrees not to charge for or resell the resulting material.

PRICE: Contact JEDEC

Printed in the U.S.A.
All rights reserved

PLEASE!

DON'T VIOLATE
THE
LAW!

This document is copyrighted by JEDEC and may not be
reproduced without permission.

For information, contact:

JEDEC Solid State Technology Association
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

or refer to www.jedec.org under Standards-Documents/Copyright Information.

UNIVERSAL FLASH STORAGE (UFS) SECURITY EXTENSION

Contents

Foreword.....	iii
Introduction.....	iii
1 Scope.....	1
2 Normative Reference	1
3 Terms and Definitions.....	2
4 IEEE Functional Requirements.....	3
4.1 IEEE 1667 Overview	3
4.2 IEEE 1667's split command structure	3
4.3 IEEE 1667 structure.....	4
4.4 Requirements for IEEE 1667 functionality in the UFS security extension	4
5 TCG Storage Security Functional Requirements.....	5
5.1 TCG Storage Security overview	5
5.2 Requirements for the TCG Storage Core in the UFS security specification.....	5
5.3 Requirements for the TCG Storage Opal SSC in the UFS security specification.....	5
5.3.1 Level 0 Discovery	6
5.3.2 Properties Requirements	10
5.4 Requirements for the TCG Storage DataStore Tables feature set in the UFS security specification.....	10
5.5 Requirements for the TCG Storage Support Single User Mode feature set in the UFS security specification.....	12
5.6 Requirements for security characteristics for UFS devices that support the security extension....	12
6 UFS Security Data Transport.....	13
6.1 SECURITY PROTOCOL IN/OUT Commands	13
6.1.1 SECURITY PROTOCOL IN command.....	13
6.1.2 SECURITY PROTOCOL OUT command.....	14
6.2 Discovery of IEEE 1667 protocol support.....	14
7 Security Interactions with UFS Operations	15
7.1 Security Support Restrictions on Logical Unit	15
7.2 Authentication and Access Control Management on Logical Unit	15

Contents (cont'd)

8	Error Handling	15
8.1	IEEE 1667 errors (Informative)	15
8.1.1	Command Out of Sequence	15
8.1.2	Silo Index mismatch in SECURITY_PROTOCOL_IN, SECURITY_PROTOCOL_OUT	16
8.1.3	Transport Specific Error	16
8.2	UFS Transport Errors	16
8.2.1	SECURITY PROTOCOL IN/OUT Specific Error	16
8.2.2	Unauthorized Access	16
9	Configuration	17
9.1	SE Logical Unit Configuration	17

Tables

Table 5-1: Level 0 Discovery - TPer Feature Descriptor	6
Table 5-2: Level 0 Discovery - Geometry Reporting Feature Descriptor	8
Table 5-3: Level 0 Discovery - Opal SSC V2.01 Feature Descriptor	9
Table 5-4: Property Requirements	10
Table 5-5: Level 0 Discovery - DataStore Table Feature Descriptor	11
Table 6-1: SECURITY PROTOCOL IN Command Descriptor Block	13
Table 6-2: SECURITY PROTOCOL field value	13
Table 6-3: SECURITY PROTOCOL OUT Command Descriptor Block	14
Table 9-1: bLUWriteProtect parameter	17

Foreword

This UFS Security Extension Standard is an extension to the UFS Standards, JESD220.

Introduction

The UFS Standard, JESD220, defines a managed memory device capable of storing code and data. UFS devices are intended to offer the performance and features required by mobile devices while maintaining low power consumption. The UFS device contains features that support high throughput for large data transfers and performance for small random data accesses more commonly found in code usage. It also contains many desirable features for mobile applications.

This document describes the requirements to implement security functionality described in [IEEE1667], [TCGCore], [TCGOpal], [TCGAddDST], [TCGSUM] and [TCGSIIS] in an UFS device.

There are three external sets of requirements on the class of UFS device that support this security extension. These are IEEE 1667 layer requirements, the TCG layer requirements, and requirements related to UFS security data transport and interaction with UFS functionality.

UNIVERSAL FLASH STORAGE (UFS) SECURITY EXTENSION

(From JEDEC Board Ballot JCB-12-60, formulated under the cognizance of the JC-64.1 Subcommittee on Electrical Specifications and Command Protocols.)

1 Scope

This document provides a comprehensive definition of the UFS security requirements for implementation of IEEE 1667 and TCG Opal security functionality. It also provides design guidelines and defines a tool box of macro functions and algorithms intended to reduce design-in overhead.

2 Normative Reference

The following normative documents contain provisions that through reference in this text, constitutes provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated. For undated references, the latest edition of the normative document referred to applies.

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SAM], *SCSI 30 Architecture Model – 5 (SAM-5)*, Revision 05, 19 May 2010

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SPC], *SCSI Primary Commands – 4 (SPC-4)*, Revision 27, 11 October 2010

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SBC], *SCSI Block Commands - 3 (SBC-3)*, Revision 24, 05 August 2010

IEEE 1667, *IEEE P1667™ 2015 Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices*.

Trusted Computing Group [TCGCore], *TCG Storage Architecture Core Specification*, Version 2.01, Revision 1.00

Trusted Computing Group [TCGOpal], *TCG Storage Security Subsystem Class: Opal Specification*, Version 2.01, Revision 1.00

Trusted Computing Group [TCGAddDST], *TCG Storage Opal SSC Feature Set: Additional DataStore Tables Specification*, Version 1.00, Revision 1.00

Trusted Computing Group [TCGSUM], *TCG Storage Opal SSC Feature Set: Single User Mode Specification*, Version 1.00, Revision 2.00

Trusted Computing Group [TCGSIIS], *TCG Storage Interface Interactions Specification (SIIS)*, Version 1.05, Revision 1.00

JEDEC JESD220A [UFS], *Universal Flash Storage (UFS 2.0)*

3 Keywords and Abbreviations

Keywords

Several keywords are used to differentiate levels of requirements and options, as follow:

can - A keyword used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

expected - A keyword used to describe the behavior of the hardware or software in the design models assumed by this standard. Other hardware and software design models may also be implemented.

ignored - A keyword that describes bits, bytes, quadlets, or fields whose values are not checked by the recipient.

mandatory - A keyword that indicates items required to be implemented as defined by this standard.

may - A keyword that indicates a course of action permissible within the limits of the standard (*may* equals *is permitted*).

must - The use of the word *must* is deprecated and shall not be used when stating mandatory 61 requirements; *must* is used only to describe unavoidable situations.

optional - A keyword that describes features which are not required to be implemented by this standard. However, if any optional feature defined by the standard is implemented, it shall be implemented as defined by the standard.

reserved - A keyword used to describe objects—bits, bytes, and fields—or the code values assigned to these objects in cases where either the object or the code value is set aside for future standardization. Usage and interpretation may be specified by future extensions to this or other standards. A reserved object shall be zeroed or, upon development of a future standard, set to a value specified by such a standard. The recipient of a reserved object shall not check its value. The recipient of a defined object shall check its value and reject reserved code values.

shall - A keyword that indicates a mandatory requirement strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*). Designers are required to implement all such mandatory requirements to assure interoperability with other products conforming to this standard.

should - A keyword used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).

will - The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.

3 Keywords and Abbreviations (cont'd)

Abbreviations

etc. - And so forth (Latin: et cetera)

e.g. - For example (Latin: exempli gratia)

i.e. - That is (Latin: id est)

4 IEEE 1667 Functional Requirements

4.1 IEEE 1667 Overview

IEEE 1667 [IEEE1667] was designed to support native security protocols and tunneling of externally defined security protocols (e.g. TCG SWG and Smart Cards) across multiple transports (e.g., SCSI, USB, ATA).

For a full description of IEEE 1667 see <http://www.ieee1667.com> and <http://standards.ieee.org>.

4.2 IEEE 1667's split command structure

IEEE 1667 uses an output and input transport specific command pair to execute a single IEEE 1667 command. This command pairing only affects the security protocols, and not the transport's normal user data access commands.

The output transport command consists of a transport specific command data block (CDB) and an associated output payload. Together, these include the IEEE 1667 command, any IEEE 1667 output parameters and any tunneled command/data.

This is followed by an input transport command with a transport specific CDB and an associated input payload. Together, these carry the same IEEE 1667 command, any IEEE 1667 input parameters, an IEEE 1667 status response, any tunneled input data, and any tunneled status information.

In this split command process, the command is not executed in the output phase, but is executed in the input phase (i.e., after receipt of the input transport command) where status can be reported in the command payload. This split command structure was designed to enable two desirable features:

- the transport status, the IEEE 1667 command status and the tunneled protocol status are reported such that each can be processed by the appropriate driver layer; and
- the host OS can support a single security communication protocol that supports multiple transports and does not have to implement multiple security-application-specific protocols in multiple transport drivers.

4.3 IEEE 1667 structure

IEEE 1667 functionality is contained by a device in one or more IEEE 1667 Addressable Command Targets (ACT). Each ACT consists of one or more addressable IEEE 1667 command processing blocks called silos. Each IEEE 1667 ACT is required to include one IEEE 1667 Probe silo which provides discovery of additional IEEE 1667 silos. Additional IEEE 1667 silos are optional in IEEE 1667.

The IEEE 1667 TCG silo was designed to enable wrapping of the TCG Storage communications protocol within the IEEE 1667 communications protocol. The IEEE 1667 TCG silo provides an interface for capability discovery and communication with the underlying TCG Storage compliant security subsystem, a Trusted Peripheral (TPer). The IEEE 1667 TCG silo allows a host TCG application to communicate through any transport supported by IEEE 1667 to a TPer without requiring native support of the TCG Storage communication protocols in the transport driver. Note that the while TPer typically contains cryptographic functionality, the IEEE 1667 TCG silo does not; the 1667 TCG silo is a conduit to TCG functionality.

4.4 Requirements for IEEE 1667 functionality in the UFS security extension

An UFS device which supports the UFS Security Extension shall contain exactly one IEEE 1667 ACT which shall contain:

- exactly one IEEE 1667 Probe silo,
- exactly one IEEE 1667 TCG silo, and
- no additional IEEE 1667 silos

The IEEE 1667 Probe silo of an UFS device which supports the UFS Security Extension shall return a status of Default Behavior upon successfully processing an IEEE 1667 Probe command.

The IEEE 1667 TCG silo of an UFS device which supports the UFS Security Extension shall support all defined commands and not only the Get Silo Capabilities commands.

5 TCG Storage Security Functional Requirements

5.1 TCG Storage Security overview

The TCG Storage Security specifications were defined to provide an architecture that puts storage devices under the policy control of a trusted platform host;

- The TCG Storage Core specification [TCGCore] provides a general security framework
- The TCG Storage Security Subclass Opal [TCGOpal] provides a specific functional security set
- The TCG Storage Additional DataStore Tables feature set [TCGAddDST] adds specific functionality to the Opal SSC
- The TCG Storage Single User Mode feature set [TCGSUM] adds specific functionality to the Opal SSC
- The TCG Storage Interface Interaction specification [TCGSIIS] provides a description of the functional interactions between the security subsystem and the external interface (e.g. UFS) functionality.

5.2 Requirements for the TCG Storage Core in the UFS security extension

An UFS device, compliant with this standard, shall implement TPer functionalities defined in [TCGCore] required to support: [TCGOpal] , [TCGAddDST] and [TCGSUM]. In particular, it shall support:

- the Locking Feature (0x0002);
- the TCG Stack reset; and
- the following Session Manager methods:
 - TPer Properties Method;
 - Start Session Method;
 - Close Session Method.

The device is not required to support the following features:

- Asynchronous protocol communication
- Creation or deletion of tables, and creation or deletion of table rows post-manufacturing

5.3 Requirements for the TCG Storage Opal SSC in the UFS security extension

An UFS device which supports the UFS Security Extension shall support the TCG Storage Opal SSC specification (see [TCGOpal]) and in particular:

- Geometry Reporting Feature in level 0 Discovery
- ability to disable SID authority in the Admin SP;
- the Locking SP shall be created by the device manufacturer

The device is not required to support the following features:

- Dynamic ComID Management
- RestrictedCommands (Object Table)

5.3.1 Level 0 Discovery

Devices compliant with this standard shall return the following elements in the Level 0 response as defined in [TCGOpal]:

- Level 0 Discovery Header
- TPer Feature Descriptor
- Locking Feature Descriptor
- Opal SSC Feature Descriptor
- Geometry Reporting

5.3.1.1 Level 0 Discovery Header

See [TCGOpal].

5.3.1.2 TPer Feature (Feature Code = 0x0001)

Devices compliant with this standard are not required to support: ComID management, buffer management, ACK/NACK, Asynchronous protocol.

Table 5-1 is informative and shows Level 0 Discovery - TPer Feature Descriptor content for a device implementing the required features only.

Table 5-1 — Level 0 Discovery - TPer Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB) Feature Code = 0x0001 (LSB)							
1								
2	Version ⁽¹⁾				Reserved			
3	Length = 0x0C							
4	Reserved	ComID Mgmt Supported = 0	Reserved	Streaming Supported = 1	Buffer Mgmt Supported = 0	ACK/NAK Supported = 0	Async Supported = 0	Sync Supported = 1
5 - 15	Reserved							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

5.3.1.3 Locking Feature (Feature Code = 0x0002)

See [TCGOpal].

5.3.1 Level 0 Discovery (cont'd)

5.3.1.4 Geometry Reporting Feature (Feature Code = 0x0003)

This section defines requirements for some parameters of Geometry Reporting Feature Descriptor.

Align

For devices compliant with this specification the value of the AlignmentRequired column of the LockingInfo table shall be equal to TRUE, therefore the ALIGN bit shall be set to one.

LogicalBlockSize

LogicalBlockSize indicates the number of bytes in a logical block (see [TCGOpal]).

The LogicalBlockSize value shall be equal to the bLogicalBlockSize parameter value of the Unit Descriptor corresponding to the logical unit configured as SE Logical Unit (see [UFS]).

AlignmentGranularity

This parameter indicates the number of logical blocks in a group (see [TCGOpal]). AlignmentGranularity value is vendor unique and its value shall be a power of two (2^N , with $N \geq 0$).

LowestAlignedLBA

LowestAlignedLBA indicates the lowest logical block address that is located at the beginning of an alignment granularity group. LowestAlignedLBA shall be set to zero.

Geometry Reporting Feature Descriptor

Table 5-2 is informative and shows Level 0 Discovery - Geometry Descriptor content for a device implementing the required features only.

5.3.1 Level 0 Discovery (cont'd)

5.3.1.4 Geometry Reporting Feature (Feature Code = 0x0003) (cont'd)

Table 5-2 — Level 0 Discovery - Geometry Reporting Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB) _____							
1	Feature Code = 0x0003 _____ (LSB)							
2	Version ⁽¹⁾				Reserved			
3	Length = 0x1C							
4	Reserved							ALIGN = 1
5 - 11	Reserved							
12	(MSB) _____							
...	LogicalBlockSize _____							
15	(LSB)							
16	(MSB) _____							
...	AlignmentGranularity _____							
23	(LSB)							
24	(MSB) _____							
...	LowestAlignedLBA = 0x0000 0000 0000 0000 _____							
31	(LSB)							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

5.3.1.5 Opal SSC V2.01 Feature (Feature Code = 0x0203)

Devices compliant with this standard shall support:

- at least the following two ComID values:
 - 0x0001 (Level 0 Device Discovery)
 - 0x0004 (TPER_RESET command)
- range crossing
 - The device supports commands addressing consecutive LBAs in more than one LBA range if all the LBA ranges addressed are unlocked.
- at least four Locking SP Admin Authorities
- at least eight Locking SP User Authorities

NOTE Support for more than eight Locking SP User Authorities is implementation specific; therefore it may not be provided by all devices in the market.

5.3.1 Level 0 Discovery (cont'd)

5.3.1.5 Opal SSC V2.01 Feature (Feature Code = 0x0203) (cont'd)

In addition to the previous requirements, the “Initial C_PIN_SID PIN Indicator” field and “Behavior of C_PIN_SID PIN upon TPer Revert” field shall be set to zero (see [TCGOpal]).

Table 5-3 is informative and shows Level 0 Discovery - Opal SSC V2.01 Feature Descriptor content for a device implementing the minimum requirements described in this document.

Table 5-3 — Level 0 Discovery - Opal SSC V2.01 Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB) _____							
1	Feature Code =0x0203 _____ (LSB)							
2	Version ⁽¹⁾				Reserved			
3	Length = 0x10							
4	(MSB) _____							
5	Base ComID = VU _____ (LSB)							
6	(MSB) _____							
7	Number of ComIDs = 0x0001 _____ (LSB)							
8	Reserved for future common SSC parameters							Range Crossing Behavior = 0
9	(MSB) _____							
10	Number of Locking SP Admin Authorities Supported = 0x0004 _____ (LSB)							
11	(MSB) _____							
12	Number of Locking SP User Authorities Supported 0x0008 _____ (LSB)							
13	Initial C_PIN_SID PIN Indicator = 0x00							
14	Behavior of C_PIN_SID PIN upon TPer Revert = 0x00							
15 -19	Reserved for future common SSC parameters							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

5.3.2 Properties Requirements

The requirements for support of the various properties, and the requirements for their values, are shown in Table 5-4.

Table 5-4 — Property Requirements

Property Name	Property Requirements and Values Reported
MaxComPacketSize	16384 (minimum)
MaxResponseComPacketSize	16384 (minimum)
MaxPacketSize	16364 (minimum)
MaxIndTokenSize	16328 (minimum)
MaxPackets	1
MaxSubpackets	1
MaxMethods	1
MaxSessions	1
MaxAuthentications	2
MaxTransactionLimit	1
DefSessionTimeout	

5.4 Requirements for the TCG Storage DataStore Tables feature set in the UFS security extension

An UFS device which supports the UFS Security Extension shall support the “TCG Storage Opal SSC Feature Set: Additional DataStore Tables” specification [TCGAddDST] with the following requirements:

- the number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Opal SSC V2.01 Feature Descriptor;
- the total size of the DataStore Tables shall be at least 10MByte.

5.4.1 DataStore Table Feature Descriptor (Feature Code = 0202h)

This descriptor shall be returned by devices compliant with this standard.

The maximum number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Opal SSC V2.01 Feature Descriptor (see 5.3.1.5).

As required by [TCGOpal], the maximum total size of DataStore tables shall be at least 10MByte.

Table 5-5 is informative and shows Level 0 Discovery - DataStore Table Feature Descriptor content for a device implementing the minimum requirements described in this document.

Table 5-5 — Level 0 Discovery - DataStore Table Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code =0x0202						(LSB)
1								
2	Version ⁽¹⁾				Reserved			
3	Length = 0x0C							
4								
5	Reserved							
6	(MSB)	Maximum number of DataStore tables						(LSB)
7	= 0x0008							
8	(MSB)	Maximum total size of DataStore tables						(LSB)
...	= 0x 0000 0000 00A0 0000							
11								
12	(MSB)	DataStore table size alignment						(LSB)
...	= 1 or above							
15								

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

5.5 Requirements for the TCG Storage Support Single User Mode feature set in the UFS security extension

An UFS device which supports the UFS security extension shall support the “TCG Storage Opal SSC Feature Set: Single User Mode Specification” [TCGSUM].

5.6 Requirements for security characteristics for UFS devices that support the security extension

An UFS device which supports the UFS security extension shall support the following encryption methods:

- AES encryption with at least 128 bit keys;
- AES encryption with either the CBC block cipher mode or the XTX block cipher mode;
- support range crossing (Range Crossing = 0 in 5.3.1.5) ; and
- support Secret Protect.

6 UFS Security Data Transport

6.1 SECURITY PROTOCOL IN/OUT Commands

For UFS devices, IEEE 1667 specifies that the P_OUT and P_IN Silos commands are transported by SECURITY PROTOCOL OUT and SECURITY PROTOCOL IN SCSI commands respectively.

6.1.1 SECURITY PROTOCOL IN command

The SECURITY PROTOCOL IN command (see Table 6-1) is used to retrieve security protocol information or the results of one or more SECURITY PROTOCOL OUT commands (see [SPC]). In particular, SECURITY PROTOCOL IN is used to transport P_IN Silos command defined in IEEE 1667.

Table 6-1 — SECURITY PROTOCOL IN Command Descriptor Block

Table 6-1 — SECURITY PROTOCOL IN Command Descriptor Block								
Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (A2h)							
1	SECURITY PROTOCOL							
2	SECURITY PROTOCOL SPECIFIC							
3								
4	INC_512	Reserved						
5	Reserved							
6	(MSB)	ALLOCATION LENGTH						(LSB)
9								
10	Reserved							
11	CONTROL = 00h							

The SECURITY PROTOCOL field specifies which security protocol is being used. UFS device that implements security extension shall support EEh value (see Table 6-2).

Table 6-2 — SECURITY PROTOCOL field value

Code	Description	Reference
EEh	Authentication in Host Attachments of Transient Storage Devices	IEEE 1667

The contents of the SECURITY PROTOCOL SPECIFIC field depend on the protocol specified by the SECURITY PROTOCOL field .

The first byte of SECURITY PROTOCOL SPECIFIC field shall be set to the SILO_INDEX value, while the second byte of this field shall be set to FUNCTION_ID value (see [IEEE1667]).

6.1.2 SECURITY PROTOCOL OUT command

The SECURITY PROTOCOL OUT command (see

Table 6-3) is used to send data to the logical unit (see [SPC]).

In particular in this specification the SECURITY PROTOCOL OUT is used to transport P_OUT Silos command defined in IEEE 1667.

As described in [IEEE1667], the application client will use the SECURITY PROTOCOL IN command to retrieve data related to operations initiated by a previous SECURITY PROTOCOL OUT.

Table 6-3 — SECURITY PROTOCOL OUT Command Descriptor Block

Bit Byte	7	6	5	4	3	2	1	0
0	OPERATION CODE (B5h)							
1	SECURITY PROTOCOL							
2	SECURITY PROTOCOL SPECIFIC							
3								
4	INC_512	Reserved						
5	Reserved							
6	(MSB)	TRANSFER LENGTH						
9	(LSB)							
10	Reserved							
11	CONTROL = 00h							

The SECURITY PROTOCOL field specifies which security protocol is being used. UFS device that implements this standard shall support the value shown in Table 6-2.

The first byte of SECURITY PROTOCOL SPECIFIC field shall be set to the SILO_INDEX value, while the second byte of this field shall be set to FUNCTION_ID value (see [IEEE1667]).

6.2 Discovery of IEEE 1667 protocol support

The host may verify if the UFS device supports IEEE 1667 protocol issuing the INQUIRY command, and checking if one of VERSION DESCRIPTOR field included Standard INQUIRY data is equal to any IEEE 1667 version descriptors defined in [SP4].

If IEEE 1667 is supported, then the host may discover which logical unit supports SECURITY PROTOCOL IN/OUT command reading Unit Descriptors: bLUWriteProtect shall be set to 03h.

And then check the Silo list retrieving Silo Type Identifier (STID), the Silo Type Specification and the Silo Type Implementation. See [IEEE1667] for details.

7 Security Interactions with UFS Operations

7.1 Security Support Restrictions on Logical Unit

The user can enable the extended security functionality only in one logical unit. The logical unit on which the extended security functionality is enabled is named “SE Logical Unit” (see 9.1).

The logical unit on which the extended security functionality is enabled can be set during device configuration.

In addition to SCSI commands described in UFS specification (see [UFS]), the SE Logical Unit shall support SECURITY PROTOCOL IN command and SECURITY PROTOCOL OUT command.

This standard does not define any new functionality for all other logical units, which will behave as described in [UFS].

7.2 Authentication and Access Control Management on Logical Unit

If the IEEE 1667/TCG security feature is implemented, user authentication and access control to the logical unit is managed per IEEE 1667 and TCG security.

8 Error Handling

8.1 IEEE 1667 errors (Informative)

The Status Code field in the SECURITY_PROTOCOL_IN payload indicates status information and errors at IEEE 1667 level. Some Status Codes are in common to both Probe and TCG Silos whereas some others are silo-specific. Note that error conditions defined in [TCGSIIS] are mapped into TCG Silo Status Codes.

See [IEEE1667] for more information.

8.1.1 Command Out of Sequence

An IEEE 1667 command is initiated by a SECURITY PROTOCOL OUT command and it is completed by the following SECURITY PROTOCOL IN command.

Each IEEE 1667 Silo retains the last received SECURITY PROTOCOL OUT command for which a SECURITY PROTOCOL OUT command with the same FUNCTIONAL_ID has not been received (pending command).

Receipt of a SECURITY PROTOCOL IN command when the IEEE 1667 Silo holds no pending command will not change the state of the Silo and will return a specific Status Code value.

Receipt of a SECURITY PROTOCOL OUT command when the IEEE 1667 Silo holds a pending command will result in replacement of the pending.

See IEEE 1667 for more information.

8.1.2 Silo Index mismatch in SECURITY_PROTOCOL_IN, SECURITY_PROTOCOL_OUT

If the Silo Index of the SECURITY_PROTOCOL_OUT is set to an unsupported value, the payload shall be dropped and no error shall be generated at UFS Transport level.

If the Silo Index of the SECURITY_PROTOCOL_IN is set to an unsupported value, the Status Code shall return Invalid Silo Error and no error shall be generated at UFS Transport level.

8.1.3 Transport Specific Error

The Invalid Security Protocol ID Parameter error is defined in IEEE 1667 to report the condition that the IEEE 1667 TCG Storage silo is not communicating correctly with the tPER.

See IEEE 1667 for more information.

8.2 UFS Transport Errors

8.2.1 SECURITY PROTOCOL IN/OUT Specific Error

If the logical unit does not support EEh value for SECURITY PROTOCOL field, then the command shall be terminated with CHECK CONDITION status, with the sense key set to ILLEGAL REQUEST, and the additional sense code set to INVALID FIELD IN CDB.

8.2.2 Unauthorized Access

Unauthorized access is an application error defined and reported in JESD220. The application relationship is described in the TCG SIIS specification. No data shall be written to or read from the medium.

Restrictions and device behaviors for access across secure LBA ranges are described in the TCG Opal specification. Unauthorized access is reported as Data Protection Error.

In particular, READ and WRITE commands shall be terminated with CHECK CONDITION status, with the sense key set to DATA PROTECT, the additional sense code set to ACCESS DENIED–NO ACCESS RIGHTS, and no data shall be transferred.

9 Configuration

9.1 SE Logical Unit Configuration

The user can enable the extended security functionality only in one logical unit. The logical unit on which the extended security functionality is enabled is named “SE Logical Unit”.

The logical unit on which the extended security functionality is enabled may be selected during device configuration setting bLUWriteProtect to 03h (SE Logical Unit).

Table 9-1 — bLUWriteProtect parameter

UNIT DESCRIPTOR					
Offset	Size	Name	MDV ⁽¹⁾	User Conf. ⁽²⁾	Description
05h	1	bLUWriteProtect	00h	Yes	Logical Unit Write Protect 00h: LU not write protected 01h: LU write protected when fPowerOnWPEn =1 02h: LU permanently write protected when fPermanentWPEn =1 03h: SE Logical Unit Others: Reserved

The storage TPer shall contain Manufactured SP’s (Admin SP and Locking SP) in Manufactured-Inactive state as shipped from the device manufacturer.



Standard Improvement Form**JEDEC** _____

The purpose of this form is to provide the Technical Committees of JEDEC with input from the industry regarding usage of the subject standard. Individuals or companies are invited to submit comments to JEDEC. All comments will be collected and dispersed to the appropriate committee(s).

If you can provide input, please complete this form and return to:

JEDEC
Attn: Publications Department
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

Fax: 703.907.7583

1. I recommend changes to the following:

☐ Requirement, clause number _____

☐ Test method number _____ Clause number _____

The referenced clause number has proven to be:

☐ Unclear ☐ Too Rigid ☐ In Error

☐ Other _____

2. Recommendations for correction:

3. Other suggestions for document improvement:

Submitted by

Name: _____

Phone: _____

Company: _____

E-mail: _____

Address: _____

City/State/Zip: _____

Date: _____

