

IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices

IEEE Computer Society

Sponsored by the
Information Assurance Committee



IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 1667™-2015
(Revision of
IEEE Std 1667-2009)

IEEE Std 1667™-2015

(Revision of
IEEE Std 1667-2009)

IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices

Sponsor

**Information Assurance Committee
of the
IEEE Computer Society**

Approved 3 September 2015
IEEE-SA Standards Board

This is a Redline Document produced by Techstreet, a business of Thomson Reuters.

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

Redline Processing Notes:

1. ~~Red Text~~ - Red strikethrough text denotes deletions.
2. Blue Text - Blue underlined text denotes modifications and additions.

Abstract: Discovery, authentication, and authorization protocols between hosts and storage devices over multiple transports are defined in this standard. It specifies a new Silo Type Identifier (STID) allocation process that uses the IEEE Registration Authority.

Keywords: authentication, authorization, CF, compactflash, discovery, EMMC, IEEE 1667™, password silo, probe silo, SAS, SATA, SCSI, SCTS, security, SILO, smart card transport silo, STID, storage, TCG storage transport silo, transport independent, trusted computing group, UAS, UFS, USB BOT, USB

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 22 January 2016. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

CF+ and CompactFlash are trademarks of the CompactFlash Association.

Mac is a registered trademark in the U.S. Patent & Trademark Office, owned by Apple Incorporated.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Intel is a registered trademark of Intel Corporation in the U.S. and/or other countries.

Palm OS is a registered trademark in the U.S. Patent & Trademark Office, owned by Palm Trademark Holding Company, LLC.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Ltd.

Print: ISBN 978-0-7381-9869-9 STD20339
PDF: ISBN 978-0-7381-9870-5 STDPD20339

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/expel/standards.jsp> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IOWA's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

The following is a list of participants in the IEEE 1667 Working Group.

Curtis Stevens, *Chair*
Jim Hatfield, *Vice Chair and Editor*
John Geldman, *Secretary*
Patrick Hery, *Treasurer*

David Abzarian
Daniele Balluchi
Kiran Bangalore
Leonid Baryudin
Bart Bombay
James Borden
Gary Calder
Jason Cambria
Jorge Campello
Laurent Castillo
Joseph Chen
Dan Colegrove
Jason Cox
Mike Danielson
Boris Dolgunov
Tom Friend
Michael George
Daniel Goodman
Bill Grace

Cyril Guyot
Aidan Herbert
Michael James
Greg Kazmierczak
Dave Landsman
Kelvin Lee
Duoying Liu
Leo Liu
Jean Lusetti
Grigory Lyakhovitskiy
Dale McNamara
Tim Markey
Gary Moorehead
Jack Nagle
Dmitry Obukhov
Steve Olsson
Hiromichi Oribe
Teruki Orihashi

Lei Poo
Lee Prewitt
Donald Rich
Marco Sanvido
Avraham Shimor
Yoni Shternhell
Heng Tang
Jon Tanguy
Bob Thibadeau
Victor Tsai
Mike Tsang
Ram Valliyappan
Len Veil
Yun Wang
Jim Warino
Ralph Weber
Michael Willett
Danny Ybarra
Jing Zhu

The following members of the entity balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Cadence Design Systems, Inc.
Dell
EDF
Marvell Semiconductor, Inc.
Micron Technology, Inc.

Microsoft Corporation
Nokia
Phison Electronics Corp.
PMC-Sierra, Inc.
SanDisk Corporation
Seagate Technology LLC

Synopsys, Inc.
TOSHIBA Corporation
ULINK Technology, Inc.
Western Digital
Corporation

When the IEEE-SA Standards Board approved this standard on 3 September 2015, it had the following membership:

John D. Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Jean-Philippe Faure
J. Travis Griffith
Gary Hoffman
Michael Janezic

Joseph L. Koepfinger*
David J. Law
Hung Ling
Andrew Myles
T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Annette D. Reilly

Stephen J. Shellhammer
Adrian P. Stephens
Yatin Trivedi
Phillip Winston
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1667™-2015, IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices.

The following are included in this document:

- Front matter
- 12 clauses
- 11 annexes

This is the third published version of IEEE Std 1667, as follows:

- IEEE Std 1667-2006 (superseded by IEEE Std 1667-2009)
- IEEE Std 1667-2009 (superseded by IEEE Std 1667-2015)
- IEEE Std 1667-2015

This standard provides the following:

- Device-type independent protocol for discovering and using multiple interfaces
- Support for multiple applications (silos)
- A mechanism and ground rules for externally defined functional modules

Principal changes from IEEE Std 1667-2009 are as follows:

- Support for the Password, Smart Card Transport, and TCG Storage Transport silos
- Obsoleted support for the Certificate Authentication Silo
- Additional Probe Silo functionality
- General clarifications
- Support for interface transports: Serial ATA, USB BOT, UAS, CompactFlash, e•MMC, and UFS.

Contents

1.	Overview	1
1.1	Scope	1
1.2	Purpose	1
1.3	Conventions	1
2.	Normative references	8
3.	Definitions	10
4.	Special terms, acronyms, and abbreviations	11
4.1	Special terms	11
4.2	Acronyms and abbreviations	15
5.	Model	16
5.1	How to use this standard	16
5.2	Stack	17
5.3	Silo Type Identifier (STID)	18
5.4	Silo interactions	19
5.5	Provisioning	20
5.6	Authentication	20
5.7	Authorization	20
6.	Host requirements	22
6.1	Overview	22
6.2	Host requirements for the Probe Silo	22
6.3	Host requirements for the Password Silo	22
6.4	Host requirements for the Smart Card Transport Silo	22
6.5	Host requirements for the TCG Storage Transport Silo	22
7.	Addressable Command Target requirements	23
7.1	General ACT requirements	23
7.2	IEEE 1667 Reset types	23
8.	Status Codes	25
8.1	Common Status Codes	25
8.2	Success	26
8.3	Failure	26
8.4	Invalid Parameter Combination	26
8.5	Invalid Parameter Length	26
8.6	Inconsistent Payload Content Length	26
8.7	Invalid Silo	26
8.8	Incomplete Command Received	26
8.9	Invalid Parameter	26
8.10	No Probe	26
8.11	Silo Interactions Error	27
8.12	P_OUT/P_IN Sequence Rejection	27
8.13	Invalid Command ID	27

9.	Password Silo.....	28
9.1	Overview.....	28
9.2	Model.....	28
9.3	Status Codes.....	52
9.4	IEEE 1667 Reset responses	57
9.5	Commands	57
10.	Probe Silo.....	75
10.1	Overview.....	75
10.2	Model.....	75
10.3	Status Codes.....	76
10.4	IEEE 1667 Reset responses	76
10.5	Commands	76
11.	Smart Card Transport Silo	78
11.1	Overview.....	78
11.2	Model.....	78
11.3	Status Codes.....	81
11.4	IEEE 1667 Reset responses	81
11.5	Commands	86
12.	TCG Storage Transport Silo	88
12.1	Overview.....	88
12.2	Model.....	88
12.3	Status Codes.....	90
12.4	IEEE 1667 Reset responses	91
12.5	Commands	91
	Annex A (informative) Bibliography	94
	Annex B (normative) IEEE 1667 over SCSI and ATA devices	95
	Annex C (normative) SAS transport.....	173
	Annex D (normative) ATA transport.....	177
	Annex E (normative) USB BOT transport	181
	Annex F (normative) USB UASP transport	185
	Annex G (normative) CompactFlash transport.....	190
	Annex H (normative) e•MMC transport.....	191
	Annex I (normative) UFS transport	195
	Annex J (informative) SCTS usage notes and examples of exchanges	199
	Annex K (informative) TCG Storage Transport Silo examples	208

List of tables

Table 1—HEX ASCII conversion	3
Table 2—Acronyms and abbreviations	15
Table 3—Distribution of requirements in this standard	16
Table 4—STID values defined in this standard	18
Table 5—PROBE command interaction pool numbers	19
Table 6—High-level IEEE 1667 reset types	24
Table 7—Common Status Codes	25
Table 8—Password Silo commands	28
Table 9—SHA-256 digest calculation example	32
Table 10—PS commands in state B1: Not PS Blocked	40
Table 11—PS commands in state B2: User PS Blocked	42
Table 12—PS commands in state B3: Admin PS Blocked	43
Table 13—PS commands in state B4: Fully PS Blocked	44
Table 14—PS commands in state S2: Not Provisioned	46
Table 15—PS commands in state S3: Not Authorized	47
Table 16—PS commands in state S4: Authorized	49
Table 17—PS commands in state S5: Failed	49
Table 18—Variable field data format	50
Table 19— FIELD IDENTIFIER values	51
Table 20—Password Silo Status Codes	52
Table 21—Mutual authentication requirements for PS functions	57
Table 22—Reset PS Administrator Authentication Failure Count behavior	61
Table 23— PS USER AUTHENTICATION FAILURE TRACKING field values and behaviors	62
Table 24—ITMS subcommands	67
Table 25— SILO STATE field values	69
Table 26—Probe Silo commands	75
Table 27—Probe Silo Status Codes	76
Table 28—Smart Card Transport Silo commands	78
Table 29—SCTS Status Codes	81
Table 31—SCTS Explicit Reset commands	82
Table 30—Additional SCTS response for IEEE 1667 resets	82
Table 32—APDU command message format	84
Table 33—APDU response message format	85
Table 34—GET SCTS TRANSPORT MODE DESCRIPTION response parameters	86
Table 35—TCG Storage Transport Silo commands	88
Table 36—TCG Storage Transport Silo specific Status Codes	90
Table 37—TCG-SIIS error translations	91
Table 38—TCG Storage Transport Silo reset responses	91
Table B.1—P_IN/P_OUT transports	96
Table B.2—IEEE 1667 major and minor version reporting	100
Table B.3—Common IEEE 1667 Silo Status Code values	101
Table B.4—Common P_OUT payload	102
Table B.5—Common P_IN payload	103
Table B.6—Silo and transport power management interactions	104
Table B.7—Silo and transport reset interactions	105
Table B.8—Password Silo COMMAND ID field values	106
Table B.9—Password Silo Status Codes	106
Table B.10—AUTHORIZE FOR ACT ACCESS command P_OUT payload	108
Table B.11—CHANGE PASSWORD command P_OUT payload	109
Table B.12—CHANGE PASSWORD command P_IN payload	110
Table B.13—CONFIGURE PS ADMINISTRATOR command P_OUT payload	111

Table B.14—CONFIGURE PS ADMINISTRATOR command P_IN payload	112
Table B.15—CREATE PS USER command P_OUT payload.....	113
Table B.16—CREATE PS USER command P_IN payload.....	114
Table B.17—DELETE PS USER command P_OUT payload	115
Table B.18—DELETE PS USER command P_IN payload	115
Table B.19—INITIALIZE PS USER PASSWORD command P_OUT payload	116
Table B.20—INITIALIZE PS USER PASSWORD command P_IN payload	117
Table B.21—ITMS command P_OUT payload	117
Table B.22—ITMS command P_IN payload	118
Table B.23—MUTUAL AUTHENTICATION command P_OUT payload	118
Table B.24—MUTUAL AUTHENTICATION command P_IN payload	119
Table B.25—QUERY PASSWORD SILO INFORMATION command P_OUT payload	119
Table B.26—QUERY PASSWORD SILO INFORMATION command P_IN payload	120
Table B.27—REQUEST MUTUAL CHALLENGE command P_OUT payload.....	122
Table B.28—REQUEST MUTUAL CHALLENGE command P_IN payload.....	122
Table B.29—UNAUTHORIZE FOR ACT ACCESS command P_OUT payload	123
Table B.30—UNAUTHORIZE FOR ACT ACCESS command P_IN payload	123
Table B.31—Probe Silo COMMAND ID field values	124
Table B.32—Probe Silo STATUS CODE field values	124
Table B.33—CONFIGURE SILOS command P_OUT payload.....	125
Table B.34— SILO UPDATE ELEMENT FIELD	126
Table B.35—CONFIGURE SILOS command P_IN payload.....	127
Table B.36—PROBE command P_OUT payload.....	128
Table B.37— HOST OS field values.....	129
Table B.38— HOST OS SPEFICATION field for Microsoft Windows OS	130
Table B.39—PROBE command P_IN payload.....	131
Table B.40— SILO LIST ELEMENT field	132
Table B.41—SCTS COMMAND ID field values	134
Table B.42—SCTS STATUS CODE field values	134
Table B.43—SCTS Common P_IN Header for SCTS commands with variable length parameters	136
Table B.44—Command still processing P_IN payload.....	137
Table B.45—SCTS Transport Mode Identifiers.....	137
Table B.46—GET RESULTS command P_OUT payload.....	142
Table B.47—GET RESULTS command P_IN payload (SCTS Command Finished)	143
Table B.48—GET SILO CAPABILITIES command P_OUT payload	144
Table B.49—GET SILO CAPABILITIES command P_IN payload	145
Table B.50—GET SCTS TRANSPORT MODE DESCRIPTION command P_OUT payload	146
Table B.51—GET SCTS TRANSPORT MODE DESCRIPTION command P_IN payload	147
Table B.52—SCTS Transport Mode Description.....	147
Table B.53—CCID Transport Mode Description.....	148
Table B.54—ICCD Transport Mode Description.....	149
Table B.55—MESSAGE EXCHANGE command P_OUT payload	150
Table B.56—MESSAGE EXCHANGE command P_IN payload	151
Table B.57—SCTS RESET command P_OUT payload	152
Table B.58—SCTS RESET command P_IN payload	153
Table B.59—SET SCTS TRANSPORT MODE command P_OUT payload	154
Table B.60—SET SCTS TRANSPORT MODE command P_IN payload	154
Table B.61—TCG Storage Transport Silo COMMAND ID field values.....	155
Table B.62—TCG Storage Transport Silo Status Code Values	155
Table B.63—GET SILO CAPABILITIES command P_OUT payload	158
Table B.64—GET SILO CAPABILITIES command P_IN payload	159
Table B.65—GET TRANSFER RESULTS command P_OUT payload	161
Table C.66—GET TRANSFER RESULTS command P_IN payload	162
Table B.67—STACK RESET command P_OUT payload	164

Table B.68—STACK RESET command P_IN payload	164
Table B.69—TPER RESET command P_OUT payload	166
Table B.70—TPER RESET command P_IN payload	166
Table B.71—TRANSFER command P_OUT payload	168
Table B.72—TRANSFER command P_IN payload	169
Table C.1—SCSI power management transition interactions	174
Table C.2—SAS events mapped to IEEE 1667 Resets	174
Table C.3—IEEE 1667 P_IN and P_OUT CDBs.....	175
Table D.1—ATA power management transition interactions	178
Table D.2—ATA events mapped to IEEE 1667 Resets	178
Table D.3—ATA P_IN/P_OUT command	179
Table E.1—USB events mapped to IEEE 1667 Resets	182
Table E.2—IEEE 1667 P_IN and P_OUT CDBs.....	183
Table F.1—UAS events mapped to IEEE 1667 Resets	187
Table F.2—IEEE 1667 P_IN and P_OUT CDBs	188
Table H.1— <i>e</i> •MMC power management transition interactions	192
Table H.2— <i>e</i> •MMC events mapped to IEEE 1667 Resets	192
Table H.3— <i>e</i> •MMC CMD23 command block.....	193
Table H.4— <i>e</i> •MMC CMD54 and CMD53 structure.....	194
Table I.1—UFS power management transition interactions	196
Table I.2—UFS events mapped to IEEE 1667 resets	197
Table I.3—IEEE 1667 P_IN and P_OUT CDBs	198

List of figures

Figure 1—State diagram convention	6
Figure 2—Sequence figure notation	7
Figure 3—Example of layer relationships for IEEE 1667	17
Figure 4—IEEE 1667 ACT structure(s)	23
Figure 5—Challenge validation flow	34
Figure 6—Digest validation flow	35
Figure 7—Mutual authentication state diagram	37
Figure 8—PS Blocked state transition diagram	39
Figure 9—Password Silo authorization for media access state diagram	45
Figure 10—Examples of Smart Card Transport Silos	79
Figure 11—Examples of TCG Storage Transport Silo configurations	89
Figure B.1—P_OUT/P_IN Command pairing state diagram	98
Figure B.2—SCTS long processing commands state diagram	139
Figure J.1—Example of an SCTS CCID startup sequence	201
Figure J.2—Example of an SCTS APDU startup sequence	203
Figure J.3—Long silo commands P_OUT/P_IN flow (Host)	204
Figure J.4—GET RESULTS fragmentation scheme	205
Figure J.5—Example of a MESSAGE EXCHANGE with a long processing silo command	206
Figure K.1—Example of a typical TRANSFER and GET TRANSFER RESULTS sequence	208
Figure K.2—Example of a long-running command	210
Figure K.3—Example of a P_LENGTH shorter than available results	212
Figure K.4—Example of an error on a TRANSFER command	213

IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of ~~Transient~~ Storage Devices

IMPORTANT NOTICE: ~~IEEE This~~ Standards ~~is~~ documents are not intended to ensure safety, ~~security,~~ health, or environmental protection ~~in all circumstances,~~ or ensure against interference with or from other devices or networks. Implementers of ~~the~~ IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices ~~or~~ and all applicable laws and regulations ~~requirements.~~

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This standard defines discovery, authentication, and authorization protocols between hosts and storage devices over multiple transports. This standard specifies a new Silo Type Identifier (STID) allocation process that uses the IEEE Registration Authority.

~~This project defines a standard protocol for secure authentication and creation of trust between a secure host and directly attached Transient and other Storage Devices, such as a Universal Serial Bus (USB) flash drive, portable hard drive, or cellular phone. The protocol has only an indirect relationship with data integrity/security, and does not directly address issues of authorization and enforcement. The protocol also does not address devices that are attached using a network connection. However, a device that uses a point to point wireless connection such as wireless USB may comply with this protocol.~~

1.2 Purpose

~~This document does not contain a Purpose statement.~~

~~Industry has witnessed explosive private and corporate growth in use of transient and externally attached storage devices. Although these devices often serve much the same functionality that floppy disks once did, the necessity of authentication (one and two way) on such devices has become paramount.~~

~~Enterprises are now beginning to require authentication of devices before connection by a host is permitted. No standard way of accomplishing that authentication exists for these devices. This standard will act to ensure the security of the enterprise using these devices while allowing a continued robust market and a convenient method of transporting information for the user.~~

1.3 Conventions

1.3.1 Precedence

If a conflict arises among text, tables, or figures, the order of precedence to resolve the conflicts is first the tables, then the text, and finally the figures.

1.3.2 Keywords

1.3.2.1 may

A keyword that indicates flexibility of choice with no implied preference.

1.3.2.2 N/A

A keyword that indicates a field is not applicable, has no defined value, and should not be checked by the host or device.

1.3.2.3 **optional**

A keyword that describes features that are not required by this standard. However, if any optional feature defined by the standard is implemented, the feature shall be implemented in the way defined by the standard.

1.3.2.4 **prohibited**

A keyword indicating that an item shall not be implemented.

1.3.2.5 **reserved**

A keyword indicating reserved bits, bytes, words, fields, and code values that are set aside for future standardization. Their use and interpretation may be specified by future extensions to this or other standards. A reserved bit, byte, word, or field shall be cleared to zero, or in accordance with a future extension to this standard. The recipient shall not check reserved bits, bytes, words, or fields. Receipt of reserved code values in defined fields shall result in the IEEE 1667 Silo command completing with a Status Code value set to Invalid Parameter (see 8.9).

1.3.2.6 shall

A keyword indicating a mandatory requirement. Designers are required to implement all such mandatory requirements to assure interoperability with other products that conform to this standard.

1.3.2.7 should

A keyword indicating flexibility of choice with a strongly preferred alternative. Equivalent to the phrase “it is recommended.”

1.3.3 Field names

Names of fields are referenced in small uppercase (e.g., NAME) followed by the word bit or the word field. Values contained in the field are referenced in small uppercase and are not followed by the word bit or the word field.

1.3.4 LSB and MSB

If a field consists of more than one bit and contains a single value (e.g., a number), then the *least significant bit* (LSB) is shown on the right and the *most significant bit* (MSB) is shown on the left (e.g., in a byte, bit 7 is the MSB and is shown on the left, and bit 0 is the LSB and is shown on the right). The MSB and LSB are not labeled if the field consists of eight or fewer bits.

If a field consists of more than one byte and contains a single value, the byte containing the MSB is stored at the lowest address and the byte containing the LSB is stored at the highest address (i.e., big-endian byte ordering). The MSB and LSB are labeled.

1.3.5 HEX ASCII

Binary values are converted to HEX ASCII strings by converting each byte of the value as defined in Table 1.

For example, the double word value 13579BDFh converted to HEX ASCII is the string “13579BDF” (i.e., 31h, 33h, 35h, 37h, 39h, 43h, 45h, 47h).

Table 1—HEX ASCII conversion

Bits	Value	HEX ASCII first character	Bits	Value	HEX ASCII second character
7:4	0000b	“0” (i.e., 30h)	3:0	0000b	“0” (i.e., 30h)
	0001b	“1” (i.e., 31h)		0001b	“1” (i.e., 31h)
	0010b	“2” (i.e., 32h)		0010b	“2” (i.e., 32h)
	0011b	“3” (i.e., 33h)		0011b	“3” (i.e., 33h)
	0100b	“4” (i.e., 34h)		0100b	“4” (i.e., 34h)
	0101b	“5” (i.e., 35h)		0101b	“5” (i.e., 35h)
	0110b	“6” (i.e., 36h)		0110b	“6” (i.e., 36h)
	0111b	“7” (i.e., 37h)		0111b	“7” (i.e., 37h)
	1000b	“8” (i.e., 38h)		1000b	“8” (i.e., 38h)
	1001b	“9” (i.e., 39h)		1001b	“9” (i.e., 39h)
	1010b	“A” (i.e., 41h)		1010b	“A” (i.e., 41h)
	1011b	“B” (i.e., 42h)		1011b	“B” (i.e., 42h)
	1100b	“C” (i.e., 43h)		1100b	“C” (i.e., 43h)
	1101b	“D” (i.e., 44h)		1101b	“D” (i.e., 44h)
	1110b	“E” (i.e., 45h)		1110b	“E” (i.e., 45h)
	1111b	“F” (i.e., 46h)		1111b	“F” (i.e., 46h)

[\(New\)](#)

1.3.6 **Numbering**

1.3.6.1 **Binary number**

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).

1.3.6.2 **Hexadecimal number**

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 followed by a lowercase h (e.g., FA23h). Underscores or spaces may be included between characters in hexadecimalnumber representations to increase readability or delineate field boundaries (e.g., B FD8C FA23h or B_ FD8C_ FA23h).

1.3.6.3 **Decimal number**

A decimal number is represented in this standard by any sequence of digits consisting of only the 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.

1.3.6.4 Bit conventions

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

n:m, denotes a bit range in a table, where n shall be greater than m.

1.3.6.5 Number range convention

p..q, represents a range of hexadecimal or decimal numbers, where p is less than q (e.g., 100..103 represents the values 100, 101, 102, and 103).

1.3.7 Lists

1.3.7.1 Lists overview

Lists shall be introduced by a complete grammatical proposition followed by a colon and completed by the items in the list. Each item in a list shall be 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, then the first word in the item shall not be capitalized. If the item in a list is a complete sentence, then the first word in the item shall be capitalized. Each item in a list shall end with a semicolon, except the last item, which shall end in a period. The next to the last entry in the list shall end 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.

1.3.7.2 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 lower case letter followed by a right parenthesis (for level 1), a period (for level 2) or “>” (for level 3). Each list level shall be indented from the previous level.

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

The following are the items for the assembly:

a) a box containing:

a) a bolt, with:

(a) a head with indentation for a Phillips head screwdriver

(b) 2.5 cm length; and

(c) 10 threads per cm;

b) a nut, with

(a) a hexagonal shape;

(b) 0.125 cm height;

(c) 10 threads per cm; and

c) a washer;

b) a screwdriver; and

c) a wrench.

1.3.7.3 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 an Western-Arabic numeral followed by a close parenthesis. Each list level shall be indented from the previous level.

The following is an example of an ordered list with two levels of nested ordered lists:

The following are the instructions for the assembly:

- 1) remove the contents from the box;
- 2) assemble the item;
 - i] use a screwdriver to tighten the screws;
 - ii] align matching edges of part A with part B
 - iii] install:
 - (1) the top bolt; and
 - (2) the bottom bolt;

and

iv] use a wrench to tighten the bolts;

and

3) take a break.

1.3.7.4 Mixed lists

If it is necessary to subdivide an ordered 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 adhere to the unordered list convention (see 1.3.7.2).

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

The following are the instructions for the assembly:

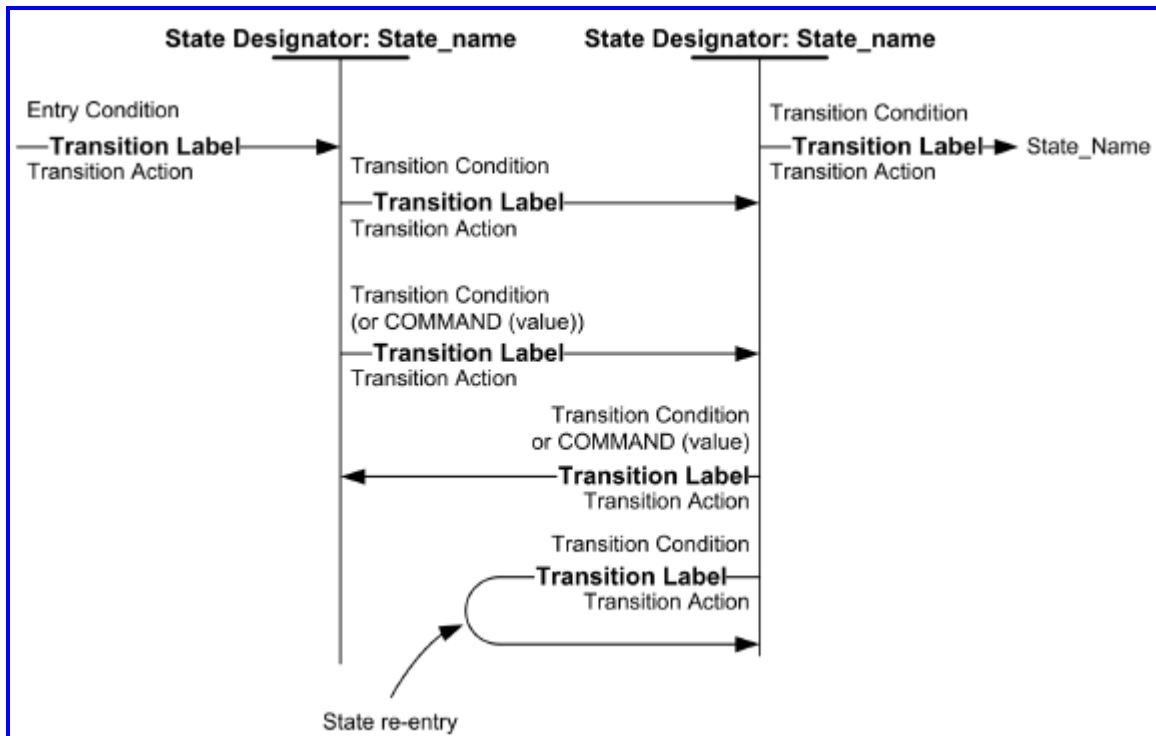
1) remove the contents from the box;

2) assemble the item;

- a] [install the screws;](#)
 - b] [install the bolts and nuts; and](#)
 - c] [paint part A and part B;](#)
-
- 3) [use a wrench to tighten the bolts; and](#)
 - 4) [take a break.](#)

1.3.8 State diagrams

[All state diagrams use the notation shown in Figure 1.](#)



(New)

Figure 1—State diagram convention

Each state is identified by a state designator and a state name. The state designator is unique among all states in all state diagrams in this standard. The state designator consists of a set of letters that are capitalized in the title of the figure containing the state diagram followed by a unique number. The state name is a brief description of the primary action taken during the state, and the same state name may appear in other state diagrams. If the same primary function occurs in other states in the same state diagram, then the primary functions are designated with a unique letter at the end of the name. Additional actions may be taken while in a state, and these actions are described in the state description text.

Each transition is identified by a transition label, a transition condition, and optionally by a transition action. The transition label consists of the state designator of the state from which the transition is being made followed by the state designator of the state to which the transition is being made. The transition to enter or exit a state diagram may come from or go to a number of state diagrams, depending on the command being processed. In this case, the state designator is labeled State name. The transition condition is a brief description of the event or condition that causes the transition to occur. A transition action may be included, indicated in italics, that is taken when the transition occurs. This action is described in the transition description text.

Upon entry to a state, all actions to be processed in that state are processed. If a state is reentered from itself, all actions to be processed in the state are processed again.

Each state diagram is instantiated based on the Entry Conditions. An Entry Condition is a transition based on an action occurring outside of the state diagram.

All transitions shall be instantaneous.

The notation COMMAND (value), as a transition condition, refers to the device processing an otherwise valid command with a specific value or values.

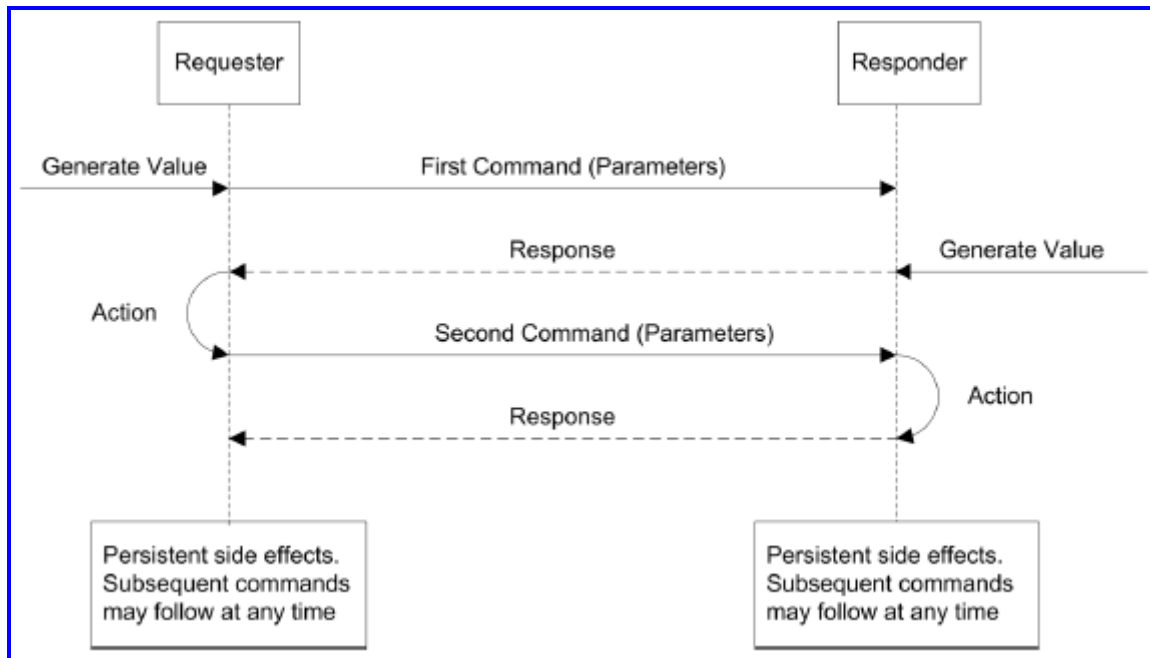
If a state has a transition condition that specifies native max, then any other set max conditions imply a value less than the native max value. If a state has a transition condition that specifies neither volatile nor nonvolatile, then both are implied. If the (value) notation is not present on a transition, then the transition occurs for any parameter combination of the command.

1.3.9 Sequence figure notation

A sequence figure describes sequences of communication between a requestor and a responder. Figure 2 is an example sequence figure. A line with an arrowhead that points to the responder represents a communication from the requestor to the responder. A line with an arrowhead that points to the requestor represents a communication from the responder to the requestor.

Each line with an arrowhead has a label. The label describes the communication between the requestor and the responder.

Communications that appear near the top of a sequence figure occur earlier in time than communications that appear below them.



(New)

Figure 2—Sequence figure notation

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

[ANSI INCITS 457-2010, Information Technology—Serial Attached SCSI-2 \(SAS-2\).](#)¹

[ANSI INCITS 465-2010, Information Technology—SCSI/ATA Translation-2 \(SAT-2\).](#)

[ANSI INCITS 471-2010, USB Attached SCSI \(UAS\).](#)

[ANSI INCITS 482-2012, Information Technology—ATA ATAPI Command Set-2 \(ACS-2\).](#)

[eMMC, Embedded Multimedia Card \(eMMC\), Electrical Standard 4.51, JESD84-B451, June 2012.](#)²

[eMMC.SECEXT, eMMC Security Extension Specification v1.0.](#)

[FIPS Publication 140-2, Security Requirements for Cryptographic Modules, May 25, 2001 \(with change notices 12-03-2002\).](#)³

[FIPS Publication 140-3, Security Requirements for Cryptographic Modules \(revised draft 09/11/09\).](#)

¹ [ANSI publications are available from the American National Standards Institute \(http://www.ansi.org/\).](http://www.ansi.org/)

² [eMMC documents are available from JEDEC at http://www.jedec.org.](http://www.jedec.org)

³ [FIPS publications are available at http://www.csrc.nist.gov/.](http://www.csrc.nist.gov/)

FIPS Publication 180-2, Secure Hash Standard.¹

[IETF RFC 1994, PPP Challenge Handshake Authentication Protocol \(CHAP\).](#)⁴

~~IEEE Std 1541TM-2002, IEEE Standard for Prefixes for Binary Multiples.~~^{2,3}

~~IETF RFC 2315 PKCS #7, Cryptographic Message Syntax Version 1.5.~~⁴

~~IETF RFC 2828, Internet Security Glossary.~~

⁴ [IETF documents \(i.e., RFCs\) are available for download at http://www.rfc-archive.org/.](http://www.rfc-archive.org/)

¹ ~~FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (<http://www.ntis.org/>).~~

² ~~IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org/>).~~

³ ~~The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.~~

⁴ ~~IETF publications are available from the Internet Engineering Task Force, IETF Secretariat, c/o Association Management Solutions, LLC (AMS), 48377 Fremont Boulevard, Suite 117, Fremont, CA 94538 (<http://www.ietf.org>).~~

~~IETF RFC 2986 PKCS #10, Certification Request Syntax Specification Version 1.7.~~

IETF RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

~~IETF RFC 3447-2003, Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.~~

IETF RFC 3629, UTF-8, A Transformation Format of ISO 10646.

[INCITS 513-2015, Information Technology—SCSI Primary Commands-4 \(SPC-4\).](#)⁵

[ISO/IEC 7816-3:2006, Identification cards—Integrated circuit cards—Part 3: Cards with contacts—Electrical interface and transmission protocols.](#)⁶

[ISO/IEC 7816-4:2005, Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange.](#)

⁵ [This document is available from T10 at http://www.t10.org.](http://www.t10.org)

⁶ [ISO/IEC publications are available from the ISO Central Secretariat \(http://www.iso.org/\). ISO publications are also available in the United States from the American National Standards Institute \(http://www.ansi.org/\).](http://www.iso.org/)

[OSVERSIONINFOEX Structure Documentation, Microsoft® Corporation.](#)⁷

[PC/SC Specification Version 2.01.09, Interoperability Specification for ICCs and Personal Computer Systems—Part 3. Requirements for PC-Connected Interface Devices, June 2007.](#)⁸

[TCG-CoreSpec, TCG Storage Architecture Core Specification, Version 2.00, Revision 1.00.](#)⁹

[TCG-Opal2, TCG Storage Security Subsystem Class: Opal Specification, Version 2.00, Revision 1.00.](#)

[TCG-SIIS, TCG Storage—Interface Interactions Specification, Version 1.02, Revision 1.00.](#)

[UFS 1.1, Universal Flash Storage, JESD220A, June 2012.](#)¹⁰

⁷ [This document is available from Microsoft at http://www.msdn.microsoft.com.](http://www.msdn.microsoft.com)

⁸ [This document is available from the PC/SC Workgroup at http://www.pcscworkgroup.com.](http://www.pcscworkgroup.com)

⁹ [Trusted Computing Group \(TCG\) documents are available at http://www.trustedcomputinggroup.org.](http://www.trustedcomputinggroup.org)

¹⁰ [USF documents are available from JEDEC at http://www.jedec.org.](http://www.jedec.org)

[UFS.SECEXT, Security Extension Specification v1.0.](#)

[USB BOT, Bulk-Only Transport, Revision 1.0, Sept. 31, 1999.¹¹](#)

[USB CCID, Smart Card CCID, Specification for Integrated Circuit\(s\) Cards Interface Devices, Revision 1.1 April 22, 2005.](#)

[USB ICCD, Smart Card ICCD, Specification for USB Integrated Circuit\(s\) Cards Devices, Revision 1.0. April 22, 2005.](#)

[USB MSC, Mass Storage Class Specification Overview. Revision 1.4, Feb. 19, 2010.](#)

[USB Revision 2, Universal Serial Bus Specification, Revision 2.0, April 27, 2000.](#)

[USB Revision 3, Universal Serial Bus 3.0 Specification, Revision 1.0, June 6, 2011.](#)

[USB UASP, USB Attached SCSI Protocol \(UASP\), Revision 1.0, June 24, 2009.](#)

~~[IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List \(CRL\) Profile.](#)~~

¹¹ [USB documents are available from the USB Implementers Forum web site at <http://www.usb.org>.](#)

~~INCITS 447, Information Technology—SCSI Architecture Model—4 (SAM-4).⁵~~

~~INCITS 1731, SCSI (Small Computer System Interface) Primary Command Set—4, SPC-4.~~

~~ITU-T X.690-2002, Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).⁶~~

~~Microsoft Corporation, OSVERSIONINFOEX Structure Documentation. Redmond, WA: Microsoft Corporation.⁷~~

~~USB Implementers Forum, Universal Serial Bus Revision 2. Beaverton, OR: USB Implementers Forum.⁸~~

~~USB Implementers Forum, Universal Serial Bus Mass Storage Class Specification Overview. Beaverton, OR: USB Implementers Forum, 2003.~~

⁵ ~~INCITS publications are available from Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (<http://www.ansi.org/>) or from the INCITS Standards Store (<http://www.techstreet.com/ncitsgate.html>).~~

⁶ ~~ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva-20, Switzerland/Suisse (<http://www.itu.int/>).~~

⁷ ~~Microsoft publications are available from Microsoft Corporation, 1 Microsoft Way, Redmond, WA 98052 (msdn2.microsoft.com).~~

⁸ ~~USB publications are available from the USB Implementers Forum, 3855 SW 153rd Drive, Beaverton, OR 97006 (<http://www.usb.org>).~~

3. Definitions

For the purposes of this document, the *IEEE Standards Dictionary Online* [B5] should be consulted for terms not defined in Clause 4.^{12, 13}

This standard does not define any additional terms for the *IEEE Standards Dictionary Online*.

See Clause 4 for the definition of special terms used in this standard.

4. Special terms, ~~Definitions~~, acronyms, and abbreviations

4.1 Special terms ~~Definitions~~

For the purposes of this ~~document~~ standard, the following terms and definitions apply. ~~The *IEEE Standards Dictionary: Glossary of Terms and Definitions*⁹ and IETF RFC 2828 should be referenced for terms not defined in this clause.~~

¹² *IEEE Standards Dictionary Online* is available at: <http://ieeexplore.ieee.org/xpls/dictionary.jsp>.

~~¹⁴~~¹³ The numbers in brackets correspond to those of the bibliography in Annex A.

⁹ ~~The *IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.~~

4.1.1 Addressable Command Target (ACT)

A uniquely addressable functional block in a storage device, to which IEEE 1667 Silo ~~Commands~~ [functions](#) can be routed based on the native communications protocol of the ~~Transient~~ storage device (~~TSD~~).

4.1.2 [administrative command](#)

[A Password Silo command that requires authentication as PS Administrator \(see Table 21\).](#)

4.1.3 [Application Protocol Data Unit \(APDU\)](#)

[A command/response pair sent to an embedded secure object that follows smart card specifications \(see ISO/IEC 7816-4:2005\).](#)

4.1.4 [APDU Processing Entity](#)

[The hardware or software components in the smart card or secure element responsible for processing the APDUs received through the Smart Card Transport Silo \(SCTS\). The implementation of the APDU Processing Entity is vendor specific.](#)

~~3.1.2. Admin Sequence Number:~~ A value in a nonrepeating sequence included in all Certificate Authentication Silo Commands that include an Administration Signature to prevent replay attacks.

~~NOTE—The generation and use of the Admin Sequence Number is defined in 9.6.3.2.~~¹⁰

~~3.1.3. Administration Signature:~~ A signature generated based on the command parameters, the Admin Sequence Number, and a value shared between the Host and the Certificate Authentication Silo, which is included with each Certificate Authentication Silo Command used to administer the Certificate Authentication Silo. This limits the use of Administrative Commands to hosts that can complete the Administration Authentication command sequence.

~~NOTE—The generation and use of the Administration Signatures is defined in 9.6.3.1.~~

~~3.1.4. Administrative Command:~~ A class of Certificate Authentication Silo Commands that is used to administer the values used in authentication as separate from the class of Certificate Authentication Silo Commands, which use the data to authenticate a Transient Storage Device (TSD) or a host. Administrative Commands require the Administration Signature and Admin Sequence Number parameters.

~~NOTE—Specification of each Certificate Authentication Silo Command as an Administrative Command is made in each subclause in 9.5.~~

4.1.5 authentication

The process of determining whether someone or something is, in fact, who or what it is declared to be.

4.1.6 authenticated silo

A silo that has successfully completed an authentication (see 4.1.5) since the most recent ACT Reset (see 7.2).

4.1.7 authentication silo

An IEEE 1667 silo that performs authentication.

~~3.1.6. Authentication Silo Key Pair (ASKP): A pair of Public and Private Keys associated with a Certificate Authentication Silo.~~

~~NOTE—The ASKP is defined in 6.3.3.~~

4.1.8 authorization

The process of determining, by evaluating applicable access control information, whether an authenticated user, device, or host is allowed access to a particular host, [storage device](#), or [service](#) (e.g., [media access](#)) within that host or storage device.

4.1.9 [cryptographic failure](#)

[A failure of the software or hardware that is used to perform cryptographic commands \[e.g., the random number generator \(see 9.2.4\) is not performing to specification\].](#)

4.1.10 [digest](#)

[A numerical value or a fixed size block of data that is created algorithmically from one or more blocks of data of arbitrary size.](#)

4.1.11 [empty string](#)

[A string whose length is zero.](#)

~~3.1.8. **certificate chain:** A series of certificates, all of which, except the first, are signed by the preceding (higher or earlier) certificate. Note that a single certificate is the reduced case of a certificate chain.~~

~~3.1.9. **connect:** The process of establishing a connection between a host and a device, allowing the use of functionality in the Addressable Command Target (ACT) by the host, or allowing the use of functionality in the host by the ACT. Generally, a device is connected to a host via connections such as Universal Serial Bus (USB), IEEE 1394 (FireWire), wireless USB, Advanced Technology Attachment (ATA), or Internet Small Computer System Interface (iSCSI). The functionality provided by the Transient Storage Device (TSD) and the host may be limited prior to authentication of the TSD and the host.~~

~~3.1.10. **descendent:** Certificate A is a descendant of Certificate B when Certificate B appears in the chain of Certificate A. See also: **certificate chain**.~~

4.1.12 External IEEE 1667 Silo

An IEEE 1667 Silo not defined in this standard. [See B.10.](#)

~~3.1.12. **Globally Unique Identifier (GUID):** An immutable globally unique identifier.~~

4.1.13 host

A computer, server, or other provider of services to a user that has a client-server relationship with an Addressable Command Target (ACT) in which the user primarily interacts with the host.

~~3.1.14. IEEE 1667 Core Silo: An IEEE 1667 Silo required by all Addressable Command Targets (ACTs) (e.g., Probe).~~

4.1.14 IEEE 1667 Defined Silo

An IEEE 1667 Silo that is defined within this standard (e.g., Probe and ~~Certificate Authentication~~ [Password](#) Silos).

4.1.15 IEEE 1667 Silo

A silo that complies with the requirements specified in this standard.

4.1.16 IEEE 1667 Silo command

~~A~~ ~~Any~~ command ~~sent to~~ [defined in this standard for](#) an IEEE 1667 Silo ~~using the IEEE 1667 protocol.~~

4.1.17 ITMS command

[Password Silo command: Initialize to Manufacturer State.](#)

~~3.1.18. **ignored:** A keyword used to describe a conditionally unused bit, byte, word, field, or code value. The contents or value of an ignored bit, byte, word, field, or code value shall not be examined by the receiving device and may be set to any value by the transmitting device.~~

~~3.1.19. **immutable:** Immutable items [Globally Unique Identifier (GUID), Authentication Silo Key Pair (ASKP), and Manufacturer Certificate] persist across software resets, firmware updates, and the Initialize command (see 9.5.1). These items are created in manufacturing and can only be changed by remanufacturing the device.~~

~~3.1.20. **initialize:** Return a device to its original manufactured state.~~

~~3.1.21. **kibibyte (KiB):** 1024 bytes. (IEEE Std 1541TM-2002)~~

4.1.18 least significant bit (LSB)

In a binary code, the bit or bit position with the smallest numerical weighting in a group of bits that, when taken as a whole, represent a numerical value (e.g., in the number 0001b, the bit that is set to one).

~~3.1.23. **Mass Storage Class:** Universal Serial Bus (USB) device class for mass storage devices. (USB Implementers Forum, *Universal Serial Bus Mass Storage Class Specification Overview*)~~

4.1.19 most significant bit (MSB)

In a binary code, the bit or bit position with the largest numerical weighting in a group of bits that, ~~when~~ if taken as a whole, represent a numerical value (e.g., in the number 1000b, the bit that is set to one).

4.1.20 P IN

A command in an transport command set that receives IEEE 1667 response parameters from the device and return status appropriate for the transport command sent to the host.

4.1.21 P LENGTH

A parameter specifying the number of bytes of a payload in a transport command.

4.1.22 P OUT

A command in a transport command set that sends to the device an IEEE 1667 command, IEEE 1667 command parameters, and returns from the device status appropriate for the transport command set.