



IEEE Standard for Authentication in Host Attachments of Transient Storage Devices

IEEE Computer Society

Sponsored by the
IEEE Information Assurance Committee



1667TM

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

26 March 2010

IEEE Std 1667TM-2009
(Revision of
IEEE Std 1667-2006)

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.

IEEE Standard for Authentication in Host Attachments of Transient Storage Devices

Sponsor

Information Assurance Committee
of the

IEEE Computer Society

Approved 11 November 2009

IEEE-SA Standards Board

Abstract: A method for host authentication of removable storage devices and an optional method for authentication of hosts by removable storage devices are specified by this standard. Both methods are certificate based and manageable by device owners. In addition, a method for identifying non-storage capabilities of removable storage devices is specified.

Keywords: authentication, certificates, discovery, probe, removable storage, security

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

Copyright © 2010 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 26 March 2010. 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.

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

Microsoft and Windows are either registered trademarks or trademarks in the U.S. Patent & Trademark Office, owned by Microsoft Corporation.

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

RIM is a registered trademark in the U.S. Patent & Trademark Office, owned by Research In Motion Limited.

Symbian OS is a trademark in the U.S. Patent & Trademark Office, owned by Symbian Software Ltd.

PDF: ISBN 978-0-7381-6123-5 STD95998
Print: ISBN 978-0-7381-6124-2 STDPD95998

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.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the 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.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

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. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, 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 publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the 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, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

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

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

Introduction

This introduction is not part of IEEE Std 1667-2009, IEEE Standard for Authentication in Host Attachments of Transient Storage Devices.

The following are included in this document:

- Front matter
- Nine clauses
- Four annexes

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards 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. 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 Standards Association Web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

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 with respect to the existence or validity of any patent rights in connection therewith. 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

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the IEEE 1667 Working Group had the following membership:

James Borden, *Chair*
Daniel Goodman, *Vice Chair*
Donald Rich, *Technical Editor*

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

<i>Organization Represented</i>	<i>Name of Representative</i>
Fujitsu Computer Products of America.....	Darren Lasko
.....	Shotaro Ichimura (<i>Alt.</i>)
Gemalto NV.....	Jean Lusetti
.....	Laurent Castillo (<i>Alt.</i>)
IBM Corporation	Daniel Goodman
Kingston Technology.....	Joel Tang
.....	John Terpening (<i>Alt.</i>)
Lexar Media.....	John Geldman
.....	Michael George (<i>Alt.</i>)
Marvell Technology Group, Ltd.	Heng Teng
.....	Bo Ye (<i>Alt.</i>)
Microsoft Corporation	Kiran Bangalore
.....	Scott Lee (<i>Alt.</i>)
SanDisk Corporation.....	Donald Rich
.....	David Landsman (<i>Alt.</i>)
Seagate Technology, LLC	James C. Hatfield
.....	Michael Danielson (<i>Alt.</i>)
Toshiba	Patrick Hery
.....	Fred Zayas (<i>Alt.</i>)
Western Digital Technologies, Inc.....	Curtis E. Stevens
.....	Danny Ybarra (<i>Alt.</i>)

Sponsoring Committee Chairs:

John L. (Jack) Cole (Lead), Information Assurance Standards Committee
Curtis Anderson, Storage Systems Standards Committee

Additional Contributors

David Abzarian	Bill Grace	Dmitry Obukhov
Robin Alexander	Zvi Gutterman	Manuel Offenberg
Curtis Anderson	Cyril Guyot	Hideaki Okubo
Kiran Bangalore	Thomas Hardjono	Teng Pin Poo
Jerome Barthelemy	Yehuda Hahn	Lakshmi Ramasubramanian
Vladimir Beker	James C. Hatfield	Donald Rich
Mark Benedikt	G. Scott Henderson	Juha Risikko
Sharon Besser	Patrick Hery	Avner Rosenen
James Borden	Eric Hibbard	Vlad Sadovsky
Eyal Bychkov	Emily Hill	Daniel Schreiber
Gary Calder	Shotaro Ichimura	Rotem Sela
Jason Cambria	Dean Jenkins	Paul Shew
Jorge Campello	Richard Kanadjian	Avraham Shimor
Laurent Castillo	Louis Kaneshiro	Yoni Shternhel
Abon Chen	Nataly Kremer	Ariel Sobelman
Howard Chen	Mike Kuppinger	Curtis Stevens
Jerry Chen	Max Lam	Pasi Suikonen
Joseph Chen	Dave Landsman	Heng Tang
John L. (Jack) Cole	Darren Lasko	Joel Tang
Jason Cox	Pat Lavarre	Keiichi Tsutsui
Cameron Crandall	Scott Lee	Jerry Walker
Paul Crew	Jack Lin	Yun Wang
Michael Danielson	Diyong Liu	Micheal Willet
Boris Dolgunov	Duoling Liu	Albert Yang
Doron Dreyer	John Loveall	Danny Yberra
Rob Ellis	Jean Lusetti	Bo Ye
Tom Friend	Kevin Marks	Fred Zayas
Martin Furuholm	Scott Marks	Jing Zhu
John Geldman	Gary Moorhead	Dana Zelitzki
Daniel Goodman	Dan Morav	Michael Zunke
	Kenichi Nakanishi	

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Howard L. Wolfman, *TAB Representative*
Michael Janezic, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Michael D. Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 Conventions	2
2. Normative references	2
3. Definitions, acronyms, and abbreviations	3
3.1 Definitions	3
3.2 Acronyms and abbreviations	5
4. Authentication layer	6
4.1 Stack	6
5. Host requirements	7
5.1 Probe Silo	7
5.2 Certificate Authentication Silo	7
6. Addressable Command Target requirements	8
6.1 General ACT requirements	8
6.2 Probe Silo requirements	9
6.3 Certificate Authentication Silo requirements	9
7. Status Codes	13
7.1 Common Status Codes	13
8. Probe Silo	15
8.1 Process of Probing	15
8.2 Probe Silo Status Codes	16
8.3 Probe Silo commands	16
9. Certificate Authentication Silo	17
9.1 Certificate names and types	17

9.2 Certificate chains	19
9.3 Certificate Authentication Silo state machine	24
9.4 Certificate Authentication Silo Status Codes	30
9.5 Certificate Authentication Silo Commands	33
9.6 Certificate Authentication command sequences.....	44
Annex A (normative) IEEE 1667 over SCSI	51
Annex B (normative) USB transport.....	112
Annex C (informative) Bibliography	114

IEEE Standard ~~Protocol~~ for Authentication in Host Attachments of Transient Storage Devices

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory 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 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

Industry has witnessed explosive private and corporate growth in use of ~~TSDs. These~~ transient and externally attached storage devices. Although these devices often serve much the same functionality that floppy disks once did, ~~but at much higher capacities and with greater reliability~~ the necessity of authentication (one and functionality. Although floppy disks never required authentication before being read or written by a host, TSDs have arrived in the marketplace at a time when security two way) on such devices has become a ~~a much greater issue than before~~ 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. ~~The stakeholders are primarily companies that are chip manufacturers or vendors that incorporate memory chips into memory solutions for mobile~~

1.3 Conventions

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 ~~embedded systems, personal~~ finally the figures.

If a field consists of more than one bit and ~~portable secure data storage, as well as operating system~~ contains a single value (e.g., a number), then the Least Significant Bit (LSB) is shown on the right and ~~enterprise security application vendors~~ 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 unlabeled

Authorized licensed use limited to: Tsinghua University. Downloaded on March 05, 2026 at 18:15:03 UTC from IEEE Xplore. Restrictions apply.

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.

~~FIPS 180-2, (with change notice 1 dated February 25, 2004), “Secure Hash Standard”¹~~

~~IEEE 1667 Silo Type Identifier Tutorial, Available at: <http://grouper.ieee.org/groups/1667/std->~~

~~IETF RFC 2828, Available at: <http://rfc.net/rfc2828.html>~~

~~IETF RFC 2459, Available at: <http://rfc.net/rfc2459.html>~~

[FIPS Publication 180-2, Secure Hash Standard.¹](#)

[IEEE Std 1541™-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.](#)

IETF RFC ~~3280~~: [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 \(4.2.1.3\).](#) ~~Available at: <http://rfc.net/rfc3280.html>~~

~~NIST 800-22 standard (“A Statistical Test Suite For Random And Pseudorandom Number Generators For IETF RFC 3447-2003, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Cryptographic Applications”) from 15 May 2001. Available at: (<http://esr.nist.gov/rng/SP800-22b.pdf>).~~

~~RSA algorithm following the PKCS#1 v2.1 standard (“PKCS #1 v2.1: RSA Cryptography Standard”) from 14 June 2002. Available at: (<ftp://ftp.rsasecurity.com/pub/pkcs/pkes-1/pkes-1v2-1.pdf>).~~

~~Universal Serial Bus Mass Storage Class Specification Overview, Published by the U.S. Version 2.1.~~

[IETF RFC 3629, UTF-8, A Transformation Format of ISO 10646.](#)

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

[INCITS 447, Information Technology—SCSI Architecture Model—4 \(SAM-4\).⁵](#)

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>).

[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 Available at: \[http://www.usb.org/developers/devclass_docs/usb_msc_overview_1.2.pdf\]\(http://www.usb.org/developers/devclass_docs/usb_msc_overview_1.2.pdf\).](#)

[USB Implementers Forum, Universal Serial Bus Mass Storage Class Specification Overview. Beaverton, OR: USB Implementers Forum, 2003.](#)

3. Definitions, acronyms, [and abbreviations](#)

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. [The IEEE Standards Dictionary: Glossary of Terms and Definitions⁹](#) and IETF RFC 2828 should be referenced for terms not defined in this clause.

3.1.1. Addressable Command Target (ACT): A uniquely addressable functional block in a storage device, to which [IEEE 1667 Silo](#) Commands can be routed based on the ~~Transient Storage Device's~~ native communications protocol [of the Transient Storage Device \(TSD\)](#).

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.

~~Administration Signature: A signature generated based upon a value shared between the host and the Authentication Silo that must be presented with each command used to administer the Authentication silo.~~

[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 ~~administration~~ [Administrative](#) Commands to hosts that can complete the Administration Authentication [command](#) sequence.

[NOTE—The generation and use of the Administration Signatures is defined in ~~Clause 14~~ 9.6.3.1.](#)

~~3.1.3 authentication: The act of checking the identity or integrity of an entity.~~

3.1.4. Administrative Command: A class of Certificate Authentication Silo ~~(AS): A silo Commands~~ that is used to administer the values used in authentication as separate from the class of Certificate Authentication Silo ~~implements the full IEEE 1667 Authentication Command Set.~~**3.1.5 Authentication Silo Key Pair (ASKP):** A pair of public and private keys, associated with an. The private key is stored securely on an ACT and cannot be retrieved by a host using any command including IEEE 1667 commands. However, it can be challenged by encrypting [Commands, which use the](#) data with the public key, which is readily available using the Command Set. ~~Each Authentication Silo must have one and only one ASKP. All ASKPs must be unique within the~~ to authenticate a Transient Storage Device (TSD) or a host. Administrative Commands require the Administration Signature and Admin Sequence Number parameters.

~~3.1.6 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 or device.~~

⁺ ~~FIPS~~² INCITS publications are available from ~~the~~ Sales Department, American National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161—Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (<http://www.ntisansi.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>).

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

¹⁰ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

~~**3.1.7 Command Set:** The protocol that facilitates authentication between a host and an ACT. The Command Set also includes commands that implement security features such as Certificate Store access, cryptography, and device authentication.~~

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

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

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.

3.1.7. 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 or device.

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, ~~depending on authorization~~. 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 a dedicated TCP/IP connection~~), 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.

~~**3.1.9 device:** See: Transient Storage Device.~~

~~**3.1.10 Globally Unique Identifier (GUID):** An immutable globally unique serial number. **descendent:** Certificate A is a descendant of Certificate B when Certificate B appears in the chain of Certificate A. See also: certificate chain.~~

3.1.11. External IEEE 1667 Silo: An IEEE 1667 Silo not defined in this standard.

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

3.1.13. 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.

~~**3.1.12 initialize:** Return a device to its original manufactured state.~~

~~**3.1.13 Mass Storage Class:** USB device class for mass storage devices as defined in Universal Serial Bus Mass Storage Class Specification.~~

~~3.1.14 **Probe Silo (PS):** A silo that implements the 1667 Probe Command. Each ACT must implement a~~
IEEE 1667 Core Silo: An IEEE 1667 Silo required by all Addressable Command Targets (ACTs) (e.g., Probe). ~~Probe Silo at the first silo index.~~

~~3.1.15 **silo:** A uniquely addressable receiver of commands on an ACT that is accessible using the IEEE~~
1667 Defined Silo: An IEEE 1667 Silo that is defined within this standard (e.g., Probe and Certificate Authentication Silos). ~~1667 protocol. One or more silos can exist in an ACT.~~

~~3.1.16 **Silo Type Identifier (STID):** A 4-byte value uniquely identifying the function and version of a~~
silo, IEEE 1667 Silo: A silo that complies with the requirements specified in this standard.

~~3.1.17 **Transient Storage Device (TSD):** A portable device that provides mass storage capabilities to a~~
host, but is not permanently attached to a specific host **IEEE 1667 Silo Command:** Any command sent to an IEEE 1667 Silo using the IEEE 1667 protocol.

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 1541™-2002)

3.1.22. 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*)

3.1.24. 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 taken as a whole, represent a numerical value (e.g., in the number 1000b, the bit that is set to one).

3.1.25. Payload: The parameters attached to an IEEE 1667 Silo Command.

3.1.26. Payload Content Length: The number of bytes of usable data in a payload exclusive of padding. Normally the zero-based index of the last byte defined in the payload structure definition plus 1 unless the payload is truncated by the transport protocol.

3.1.27. provisioning: The act of storing an owner specific credential in the Certificate Authentication Silo to confer ownership and administrative rights to the Certificate Authentication Silo.

3.1.28. Silo: A uniquely addressable receiver of commands with defined behaviors on an Addressable Command Target (ACT) accessible using the protocol defined in this standard.

3.1.29. Silo Type Identifier (STID): A 4-byte value uniquely identifying the function of a Silo.

3.1.30. Transient Storage Device (TSD): A portable device that connects to a host to provides mass storage capabilities but is not permanently attached to a specific host.

3.2 Acronyms and abbreviations

ACT	Addressable Command Target
ASCh	Authentication Silo Certificate
ASCm	Manufacturer chain
ASCS	Authentication Silo Certificate Store
ASKP	Authentication Silo Key Pair
CDB	Command Descriptor Block
GUID	Globally Unique Identifier
HCh	Host Certificate
~~PKI~~	~~Public Key Infrastructure~~
iSCSI	Internet Small Computer System Interface
LSB	Least Significant Bit
MSB	Most Significant Bit
OUI	Organizationally Unique Identifier
OS	operating system
PC	personal computer
PCp	Provisioner Certificate
PHY	physical layer
RNG	Random Number Generator
~~STID~~	~~Silo Type Identifier~~
SCh	Signer Certificate
SCSI	Small Computer System Interface
SPIN	Security Protocol In
SPOUT	Security Protocol Out
STID	Silo Type Identifier
TSD	Transient Storage Device
USB	Universal Serial Bus

3.3 Certificate names

Certificate names are specified in this document according to the KCi structure:

where:

~~K is the public key of the certificate~~

~~i is the issuer of the certificate~~

~~The value X in the K position implies any certificate descended from the issuer i. For example, XCh would refer to any certificate (indicated by the leading X) descendent from the HCh root certificate.~~

4. Authentication layer

4.1 Stack

Figure 1 depicts the area of responsibility of the IEEE 1667 protocol layer in relation to the other services within the host-device relationship.

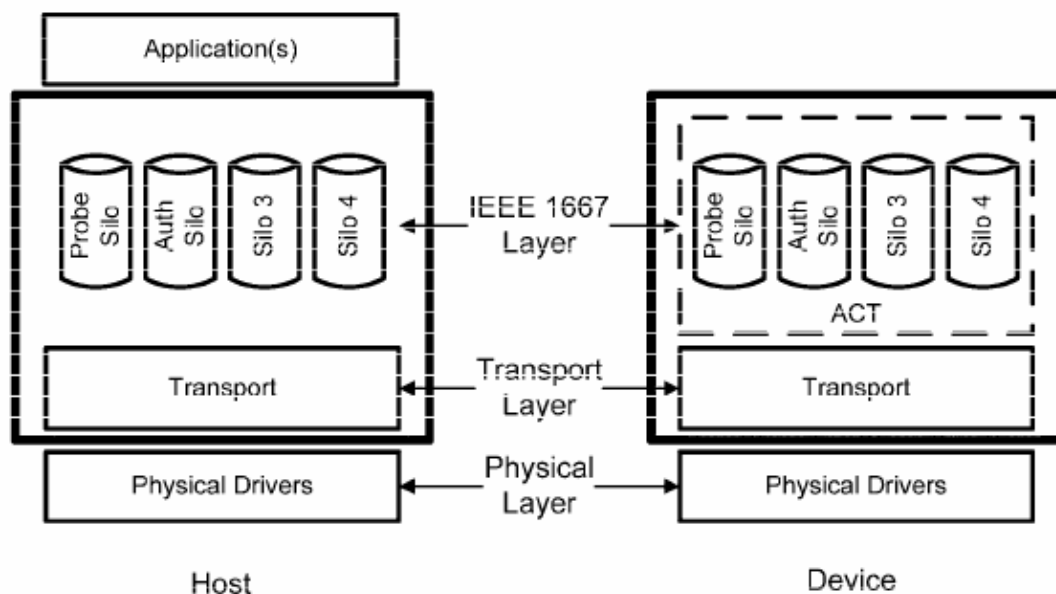


Figure 1—IEEE 1667 stack

NOTE—The components of the IEEE 1667 and Transport layers are defined in this standard.

An example of Addressable Command Target (ACT) and host stacks is depicted in Figure 1. At the base of the stack is the physical (PHY) layer, which may be [the physical implementation of Small Computer System Interface \(SCSI\)](#), [Advanced Technology Attachment \(ATA\)](#), or any other interface that has an IEEE 1667 transport defined for it.

Above the physical layer is the transport layer. The transport layer defines the method used to communicate IEEE 1667 Silo Commands between the host and the device.

NOTE—See the appropriate annex for Transport layer definitions.

Above that is the ACT Driver layer, which represents logical device units. An ACT is represented on the host as a discrete device, and this representation is echoed on the device. [IEEE 1667 Silo](#) Commands using the base protocol are routed from an ACT driver on the host to a corresponding ACT on the device via the physical interface.

Above the ACT [driver](#) layer is the IEEE 1667 layer consisting of ~~silos. A silo is represented as~~ [IEEE 1667 Silos. IEEE 1667 Silos are addressed by](#) an index within the ACT, and each ~~silo may~~ [IEEE 1667 Silo shall](#) contain a separate command processing engine and its own private storage for the command processing engine. Applications reside above the ~~silos~~ [IEEE 1667 Silos](#) and use the silos as a mechanism for transport. ~~A single Authentication Silo (AS) is always present in an ACT that is compliant with IEEE Std~~

The functionality of each IEEE 1667 Silo in each IEEE 1667 ACT is communicated to the host by a Silo Type Identifier (STID). STIDs are assigned by the IEEE 1667 Working Group, and those assignments are documented on the IEEE 1667 Web site [B3].¹¹ Each assignment includes the STID, whether the Silo was defined by the IEEE 1667 Working Group or by another entity (an External IEEE 1667 Silo), and where to find published information about the silo. A Silo Type Identifier Tutorial [B4] is available. For each IEEE 1667 ACT, the host discovers the available silos, their STIDs, and the implemented silo version information with the Probe command (8.3.1) sent to the Probe Silo (8.3).

5. Host requirements

The host may be a personal computer (PC), server, cell phone, or any other device that can support the host-side requirements of IEEE Std 1667. ~~The host includes the following components:~~

- ~~—PKI (Public Key Infrastructure) algorithm (see the RSA algorithm)~~
- ~~—Cryptographic Random Number Generator (see NIST 800-22)~~
- ~~—Certificate Store possibly containing XCh Host Certificate(s) and Root ASCh Device Certificate(s)~~

~~5.1 PKI algorithm~~

~~The PKI algorithm is as described in the RSA algorithm. The minimum key length supported is 1024 bits. The hashing algorithms permitted are the SHA-1 and SHA-256 algorithms as defined in FIPS 180-2, where SHA-1 support is mandatory for all hosts and devices, while SHA-256 is optional.~~

~~PKI algorithm used will be determined from certificate presented to initiate each challenge/response cycle.~~

~~5.2 Random number generator~~

~~The Random Number Generator (RNG) is a random number generator that meets the requirements defined in NIST 800-22. This can be a true RNG or a pseudo-RNG (deterministic RNG).~~

~~5.3 Certificate store~~

~~The Certificate Store is a storage area within the host that can be used to store certificates. The Certificate Store on the host side may include multiple host key pairs. At least one key pair must be stored in the host. The Certificate Store is described in Clause 9.~~

~~5.4 XCh Host Certificate~~

~~XCh host certificates are signed by an HCh, which is stored in the Authentication Silo's Certificate Store.~~

5.1 Probe Silo

The host shall report the version of IEEE Std 1667 implemented by the host to the device using the Probe Silo Probe command.

5.2 Certificate Authentication Silo

The host shall support the following:

- Asymmetric Key Cryptography as defined in 5.2.1.
- Random Number Generator (RNG) as defined in 5.2.2.
- Certificate Store as defined in 5.2.3.
- Credential Store as defined in 5.2.4.

5.2.1 Asymmetric Key Cryptography

The Asymmetric Key Cryptography is as described in IETF RFC 3447-2003.

The signature scheme (with appendix) is either RSASSA-PSS or RSASSA-PKCS1-v1_5 (IETF RFC 3447-2003). The size of the signature data is dependent on the key used.

See Table 4 for a list of supported RSA Key sizes.

¹¹The numbers in brackets correspond to those of the bibliography in Annex C.

5.2.2 Random Number Generator

An Random Number Generator is a device or algorithm that can produce a sequence of random numbers that appears to be from an ideal random distribution. This specification does not have specific requirements on a host's RNG.

NOTE—ANSI X9.82-1:2006 [B1], ANSI X.9.82-3:2007 [B2], and IETF RFC 4086-2005 [B5] provide informative introductions to the art of generating appropriate random numbers.

5.2.3 Host Certificate Store

The Host Certificate Store is a storage area accessible by the host that shall be used to store certificates. The Host Certificate Store may include multiple Host Certificates (HCh), a Provisioner Certificate (PCp), or one or more certificates that are descendents of a HCh or PCp. The Host Certificate Store may also include one or more Signer Certificates (SCh) from an Authentication Silo Certificate (ASCh) chain.

5.2.4 Host Credential Store

The Host Credential Store is a storage area accessible by the host that shall be used to store private data associated with an entity. The Host Credential Store shall contain the Private Key of the key pairs used in the certificates originating from the Host and stored in the Host Certificate Store.

6. Channel

~~The channel is the connection between the host and the ACT. The channel between the host and the ACT is not assumed to be encrypted.~~

~~The channel itself is not protocol dependent.~~

7. TSD requirements

~~A TSD includes one or more ACTs as defined in Clause 8. A TSD must include at least one ACT containing an Authentication Silo.~~

6. Addressable Command Target requirements

~~The ACT includes one or more silos, as defined in 8.8. All ACTs must contain a Probe silo and may contain one Authentication Silo.~~

6.1 Probe siloGeneral Addressable Command Target requirements

~~The Probe Silo is a silo that implements only the IEEE 1667 Probe command. This silo must be able to report the Silo Type Identifiers and version information for all silos implemented in the ACT including itself. Figure 2 shows the structure of an ACT.~~

Authorized licensed use limited to: Tsinghua University. Downloaded on March 05, 2026 at 18:15:03 UTC from IEEE Xplore. Restrictions apply.

The Probe command will include the host operating system type and version as a parameter.

8.2 Authentication silo requirements

The Authentication Silo is a silo that implements all of the commands in the Command Set. The Authentication Silo has the following components:

- ↓ Certificate Store
- ↓ Globally Unique Identifier
- ↓ Authentication Silo Key Pair
- ↓ Authentication Silo Certificate(s)
- ↓ PKI Algorithm
- ↓ Random Number Generator

Authentication Silos will reject all commands until after the probe command is successfully executed on the probe silo in the ACT.

8.3 Certificate Store

The Certificate Store is used to store certificates in an Authentication Silo. The Certificate Store must be protected from user modification and deletion, and may not be accessed except using the commands defined in this protocol specification. The Certificate Store may only be cleared when the device is initialized. The Certificate Store must not be visible to host file systems, and must provide storage for at least four certificates. The Certificate Store is described in Clause 9.

8.4 Globally Unique Identifier

To simplify the creation of access control systems, the Authentication Silo must have an identifier that is globally unique. Globally unique identifiers are assigned using the mechanism defined in Clause 13.

8.5 Authentication Silo Key Pair

The Authentication Silo Key Pair (ASKP) forms the basis of any certificates that are issued by an ACT. The private key is stored securely on the Authentication Silo and cannot be retrieved by any mechanism. However, it can be challenged by encrypting data with the public key, which is available by querying the device. All Authentication Silo Certificates in an Authentication Silo are based on this key pair. This is a minimum requirement; hardware security mechanisms may be implemented beyond this requirement. The security level of the ASKP is attested to by the Manufacturer Certificate.

8.6 Authentication Silo Certificates

Authentication Silo Certificates are stored in the Certificate Store. Certificates used in the protocol are defined in Clause 12. Every Authentication Silo must include an ASCm certificate, as defined in Clause 12.

8.7 PKI algorithm

As defined in 5.1.

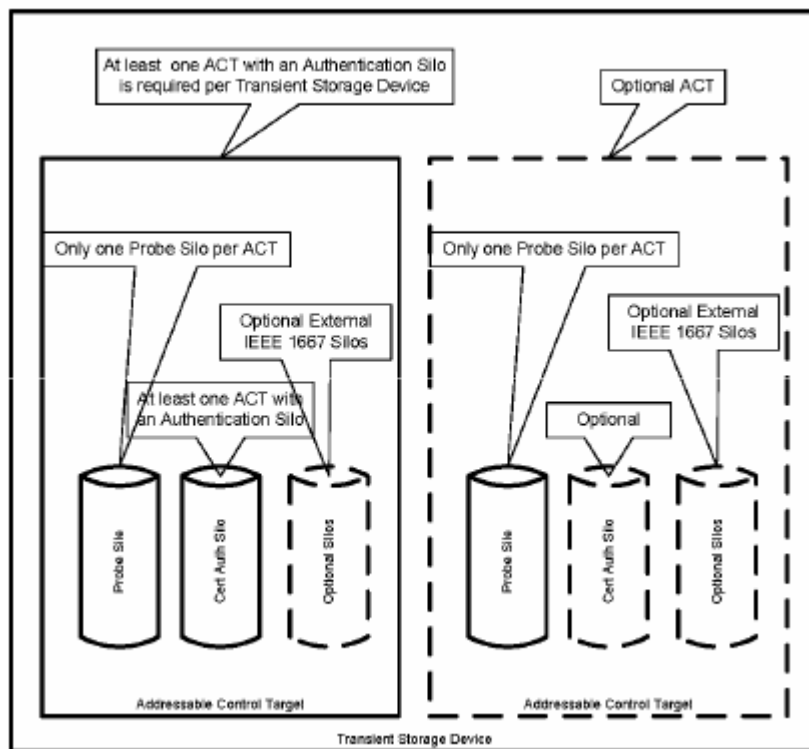
8.8 Random number generator

As defined in 5.2.

8.9 Silo Type Identifier (STID)

Silo Type Identifiers will be 4 bytes long. Each Silo Type Identifier is a unique value with no individual components within the identifier.

Silo Type Identifier allocation and publication are defined in the IEEE 1667 Silo Type Identifier Tutorial.



NOTE—All dashed items in Figure 2 are optional.

Figure 2—IEEE 1667 ACT structure

IEEE 1667 Silos are addressed by a Silo Index.

Each ACT shall contain one and only one Probe Silo.

All Transient Storage Devices shall include at least one ACT containing an Authentication Silo; additional ACTs within the TSD may contain Authentication Silos.

Each ACT may contain zero or more External IEEE 1667 Silos. No Silo shall be addressable in more than one ACT.

6.2 Probe Silo requirements

The Probe Silo is an IEEE 1667 Core Silo that implements all of the commands defined in Clause 8. The Probe Silo shall be addressable at Silo Index 0.

6.3 Certificate Authentication Silo requirements

The Certificate Authentication Silo is an IEEE 1667 Defined Silo that implements all the commands defined in 9.5. The Certificate Authentication Silo shall have the following components:

- Authentication Silo Certificate Store (ASCS) as defined in 6.3.1
- Globally Unique Identifier (GUID) as defined in 6.3.2
- Authentication Silo Key Pair (ASKP) as defined in 6.3.3
- Manufacturer Certificate (ASCm) as defined in 6.3.4
- Asymmetric Key Cryptography as defined in 6.3.5
- Random Number Generator (RNG) as defined in 6.3.6
- Cryptographic Algorithm support as defined in 6.3.7
- Hash Algorithm support as defined in 6.3.8

6.3.1 Authentication Silo Certificate Store

The ASCS is a storage area that is used to store certificates along with their associated Signer Certificate Index, Validation Policy, and Certificate Type (see 9.5.9).

The following certificates and certificate chains are used in authentication and provisioning.

- Manufacturer (ASCm) Chain defined in 9.1.2
- Provisioning Certificate (PCp) defined in 9.1.3
- Authentication Silo Certificate (ASCh) defined in 9.1.4
- Signer Certificate (SCh) defined in 9.1.5
- Host Certificate (HCh) defined in 9.1.6

A zero-based Certificate Index is used to address certificates in the ASCS for store, retrieve, and remove operations.

The following certificates have defined locations:

- The ASCm is stored at Certificate Index equal to zero.
- The PCp is stored at Certificate Index equal to one. Certificate locations shall be indexed by

sequential index values.

Certificates stored in the ASCS shall only be accessible to the host through the use of the commands defined in 9.5.

The ASCS shall provide at least five certificate locations in addition to the first location reserved for the ASCm Chain.

The size of each certificate other than ASCm shall be less than or equal to 2 KiB. All certificate locations other than the first location reserved for the ASCm Chain shall store any certificate with a size less than or equal to 2 KiB.

All certificates shall be X.509 Version 3 (IETF RFC 5280) certificates using Distinguished Encoding Rules (DER) (ITU-T X.690-2002).

All certificate fields without requirements specified in this standard shall be determined by the issuing authority.

There shall be no limits to the depth of certificate chains supported in the Certificate Authentication Silo other than the number of certificate locations in the ASCS. Processing of certificate chains is specified in 9.2.1.

The actual structure of the ASCS is implementation dependent.

6.3.2 Globally Unique Identifier

The Certificate Authentication Silo shall have an identifier that is globally unique and is a byte sequence of ASCII characters with the following format:

<Naming Authority><dash><IEEE Organizationally Unique Identifier><dash><Manufacturer Product ID><dash><Product Unique Instance ID><dash><ACT Unique ID>

The Naming Authority shall be a four (4) bit value represented as a single uppercase hexadecimal digit. (See INCITS 1731 NAA Designator Format.)

The IEEE Organizationally Unique Identifier (OUI) shall be a 24-bit OUI value assigned by the IEEE Registration Authority, represented as six (6) uppercase hexadecimal digits.

NOTE—OUI values can be requested from the IEEE Registration Authority using the on-line forms available on the IEEE-RA Web site: <http://standards.ieee.org/regauth/>.

Dash shall be a single character with an ordinal value of 2Dh, based on the ASCII value.

The Manufacturer Product ID shall be a string of 40 bytes. The Manufacturer Product ID is allocated by the manufacturer of the TSD and shall be padded with spaces (ordinal value of 20h) on the right, if necessary.

Product Unique Instance ID shall be an identifier of the TSD unique within the domain of the IEEE OUI and Manufacturer Product ID combination. The Product Unique Instance ID shall be a string of 20 bytes and shall be padded with spaces (ordinal value of 20h) on the right, if necessary.

The ACT Unique ID shall be a 64-bit identifier of the ACT. Each ACT of a TSD shall have a unique ACT Unique ID within the TSD. The ACT Unique ID shall be represented by sixteen (16) uppercase hexadecimal digits.

The organization that has been assigned the IEEE OUI used in creating a GUID, as defined above, shall ensure that no two ACTs share the same GUID.

6.3.3 Authentication Silo Key Pair

The ASKP is the RSA Public/Private Key Pair used by the Certificate Authentication Silo in authentication.

The Public Key of the ASKP shall be included in the ASCm and shall be included in the certificate request returned by the Create Certificate Request command (see 9.5.2).

The Private Key of the ASKP shall not be accessible outside the Certificate Authentication Silo by any mechanism. Storage of the Private Key is not specified in this standard.

All Authentication Silo Certificates (ASCh) in a Certificate Authentication Silo shall be based on this key pair.

The Certificate Authentication Silo shall support the Asymmetric Key Cryptography algorithm and the key length of the ASKP.

Each Certificate Authentication Silo shall have one and only one ASKP. All ASKPs shall be unique within the TSD.

Manufacturers shall generate a new ASKP for each Certificate Authentication Silo. Each ASKP shall be generated using an RNG. See 6.3.6.

6.3.4 Manufacturer Certificate

Every Certificate Authentication Silo shall include an ASCm, as defined in 9.1.2.

6.3.5 Asymmetric Key Cryptography

The Asymmetric Key Cryptography is described in IETF RFC 3447-2003.

The signature scheme (with appendix) is either RSASSA-PSS or RSASSA-PKCS1-v1_5 (IETF RFC 3447-2003).

6.3.6 Random Number Generator

An Random Number Generator is a device or algorithm that can produce a sequence of random numbers that appears to be from an ideal random distribution. This specification does not have specific requirements on the construction of a device's RNG.

NOTE—ANSI X9.82-1:2006 [B1], ANSI X.9.82-3:2007 [B2], and IETF RFC 4086-2005 [B5] provide informative introductions to the art of generating appropriate random numbers.

6.3.7 Cryptographic Algorithm support

Every Certificate Authentication Silo shall support at least one Asymmetric Key Cryptography algorithm and one Signature Algorithm as defined in 9.5.11.

6.3.8 Hash Algorithm support

The Hash algorithm is described in FIPS Publication 180-2.

Every Certificate Authentication Silo shall support at least one Hash algorithm.

7. Status Codes

7.1 Common Status Codes

Each IEEE 1667 silo has unique success and failure Status Codes appropriate to its functionality and commands. Due to the commonality of IEEE 1667 Silo communications and addressing, some success and failure Status Codes are general enough to be defined as common.

Table 1 contains Status Codes that shall be defined for every IEEE 1667 transport and common for every IEEE 1667 Silo and every IEEE 1667 Silo Command.

The following list describes the requirements for the enumeration of Status Codes within each transport:

- IEEE 1667 Status Codes shall be represented as an enumeration of binary values.
- IEEE 1667 Status Codes indicating success shall contain a value with the high-order bit cleared to zero (0).
- IEEE 1667 Status Codes indicating a failure shall contain a value with the high-order bit set to one (1).

NOTE—Table 1 was developed by assigning common Status Codes from the top of the range and assigning from the bottom of the range for silo specific Status Codes.

Errors relating to transports shall be reported as defined in the transport specific annex.

Table 1—Common Status Codes

<u>Status Code</u>	<u>Use</u>	<u>Status type</u>
<u>Success</u>	<u>The command completed without failure.</u>	<u>Success</u>
<u>Failure</u>	<u>General failure condition.</u>	<u>Failure</u>
<u>Invalid Parameter Combination</u>	<u>The combination of command parameters is invalid.</u>	<u>Failure</u>
<u>Invalid Parameter Length</u>	<u>A parameter sent to the IEEE 1667 Silo in the command has an invalid length.</u>	<u>Failure</u>
<u>Inconsistent Payload Content Length</u>	<u>Payload Content Length value does not match the length of the payload expected by the IEEE 1667 Silo.</u>	<u>Failure</u>
<u>Invalid Silo</u>	<u>A command was received for an unimplemented IEEE 1667 Silo.</u>	<u>Failure</u>
<u>Incomplete Command Received</u>	<u>A truncated or incomplete IEEE 1667 Silo Command was received.</u>	<u>Failure</u>
<u>Invalid Parameter</u>	<u>A parameter sent to the IEEE 1667 Silo in the command is invalid.</u>	<u>Failure</u>
<u>No Probe</u>	<u>Non-Probe command received before Probe Silo Probe command successfully completed.</u>	<u>Failure</u>
<u>Reserved Function</u>	<u>The function selection value is reserved.</u>	<u>Failure</u>

Success

Success shall be returned when the command completed without failure and a more specific success Status Code is not defined for the IEEE 1667 Silo and the IEEE 1667 Silo Command.

Failure

Failure shall be returned when the IEEE 1667 Silo Command failed for any reason not specified by another Failure Status Code, either common or silo specific.

Invalid Parameter Combination

Invalid Parameter Combination shall be returned when the combination of IEEE 1667 Silo Command parameters is invalid.

Invalid Parameter Length

Invalid Parameter Length shall be returned when a variable-length parameter sent to the IEEE 1667 Silo in the IEEE 1667 Silo Command has an invalid length.

Inconsistent Payload Content Length

Inconsistent Payload Content Length shall be returned when the Payload Content Length does not match the length of the payload expected by the IEEE 1667 Silo.

Invalid Silo

Invalid Silo shall be returned when the IEEE 1667 Silo Command is addressed to a silo address greater than or equal to the number of IEEE 1667 Silos implemented in the ACT.

Incomplete Command Received

Incomplete Command Received shall be returned when a truncated or incomplete IEEE 1667 Silo Command was received.

Invalid Parameter

Invalid Parameter shall be returned when an IEEE 1667 Silo Command parameter defined in the specification of the addressed IEEE 1667 Silo has an invalid value.

No Probe

No Probe shall be returned when a IEEE 1667 Silo Command that is not a Probe Silo Probe command is received by the ACT before the Probe command of the Probe Silo implemented in that ACT has successfully completed.

Reserved Function

Reserved Function shall be returned for an IEEE 1667 Silo Command where the function identifier is a reserved value.

8. Probe Silo-actions

The Probe command is a mechanism that allows hosts to ~~determine the silos~~ discover the IEEE 1667 Silos implemented in each ACT. The Probe command is implemented by the Probe Silo.

8.1 Process of Probing

Probing begins with a determination that the ACT supports the IEEE 1667 Protocol. This [determination](#) is specific to the underlying protocol as listed in each transport specific annex.

Following this [determination](#), the Probe command is executed on each ACT to determine each ACT's capabilities including the existence of a [Certificate](#) Authentication Silo.

11.2 Probe command

~~Parameters: Host OS version.~~

~~Response: A Silo Type Identifier for each The Probe command allows the ACT to make known its capabilities to the host.~~

~~If any IEEE 1667 Silo Command is sent to any silo implemented by other than the ACT The Probe command is required before executing any other commands in any other silo Probe Silo after the most recent application of power to the ACT. If a command is sent to a silo device and before the successful completion of the Probe command an error condition must, a failure status (No Probe) shall be returned. See Table 1.~~

8.2 Probe Silo Status Codes

[In addition to the Common Status Codes, the Probe Silo defines two additional Status Codes.](#)

Table 2—Probe Silo Specific Status Code values

Condition	Use	Status type
Default Behavior	The Probe command succeeded and the ACT shall not implement any operating system (OS) specific behavior.	Success
Unsupported Host IEEE 1667 Version	The version of IEEE Std 1667 reported by the host is not supported by the ACT.	Failure

[Default Behavior \(Probe\)](#)

[Default Behavior shall be returned when the Probe command completed without failure, and either the Host OS was not specified in the parameters of the Probe command or the ACT has no special behavior defined for the specified Host OS.](#)

[NOTE—If the Probe command completes without failure and Host OS specific behavior is implemented, the Success Status Code is returned.](#)

[Unsupported Host IEEE 1667 Version](#)

[Unsupported Host IEEE 1667 Version shall be returned when the Probe command indicates that the Host IEEE 1667 version is not supported by the ACT. The ACT shall return a description of only the Probe Silo \(see 8.3.1 for returned data\).](#)

8.3 Probe Silo commands

8.3.1 Probe command

Parameters:

- ↓ Host OS version
- ↓ Host IEEE 1667 implementation version
- ↓ Host OS type

Response:

- ↓ A list containing the Silo Type Identifier, implementation version, and supported specification version for each IEEE 1667 Silo implemented by the ACT.

The Probe command allows the ACT to make known its capabilities to the host and also allows the host to make known its OS type and version to the ACT to enable OS specific operation. The Host OS version format is transport protocol specific.

If the Probe command succeeds, the Probe Silo shall return a list of Silo Type Identifier, silo implementation version, and the supported specification version for each IEEE 1667 Silo implemented by the ACT. If the Probe command fails, the Probe Silo shall return a one-element list containing the Silo Type Identifier, silo implementation version, and supported specification version of the Probe Silo.

The Probe command is required after the most recent application of power to the device and before executing any other IEEE 1667 Silo Commands in any other IEEE 1667 Silo of the ACT. If any IEEE 1667 Silo Command other than the Probe Silo Probe command is sent to any IEEE 1667 Silo after the most recent application of power to the device and before the successful completion of the Probe command, then an error condition shall be returned.

This silo shall report the Silo Type Identifiers and version information for all IEEE 1667 Silos implemented in the ACT including itself.

The Silo Type Identifiers shall be reported in order of ascending Silo Index beginning with the Probe Silo (Silo Index 0) without gaps. The Silo Index of each IEEE 1667 Silo shall be derived from the position of the silo's Silo Type Identifier as returned by the IEEE 1667 Probe command.

9. Certificate Store

~~The Certificate Store is a storage area that is used to store secrets, certificates, and other authentication data.~~

~~The actual structure of the Certificate Store is implementation dependent. However, the store always provides a simplified interface.~~

9.1 Required features

~~The Certificate Store must provide the following functionality:~~

- ~~↓ Store certificate~~

9.2 Authentication Silo Certificate Store

Every Authentication Silo must have a Certificate Store that holds certificates. The following certificates are used in authentication and provisioning. These certificates are referred to as administrative certificates in the Command Set. The device may also store any number of User certificates, which are not defined in this section.

All certificates other than ASCm are limited to 2 KB maximum size.

↓ Manufacturer Certificate (ASCm)

↓ Provisioning Certificate (PCp)

↓ Authentication Silo Certificate (ASCh)

↓ Host Certificate(s) (HCh)

9.2.1 Manufacturer Certificate (ASCm)

This certificate chain is defined by the device manufacturer and is built into each Authentication Silo. The certificate chain is signed by the manufacturer root certificate and is immutable. The fields in this certificate will be as defined in the X.509 Version 1 certificate definition. The ASCm certificate is based on the Authentication Silo's ASKP. An ASCm will contain the unique silo globally unique identifier (GUID).

This certificate chain may exceed the general 2 KB size limit on certificates stored in the Certificate Store.

9.2.2 Provisioning Certificate (PCp)

This certificate is used to provision Authentication Silos. When an Authentication Silo is provisioned, the certificate is written to this location. Only a host that authenticates with PCp can clear PCp by initializing the silo. Any host that can authenticate using a certificate signed by PCp can change HCh and ASCh.

9.2.3 Authentication Silo Certificate(s) (ASCh)

This certificate chain is used to authenticate the silo to a host. It is a certificate chain based on the ASKP and is signed by a root trusted by the host.

Each ASCh certificate chain will be stored as individual certificates in the Certificate Store. The host will be required to read all ASCh certificates and reassemble the certificate chains.

9.2.4 Host Certificate(s) (HCh)

One or more certificate(s) used to authenticate hosts. It is a self-signed root certificate. Any certificate descended from HCh may be used by the silo to authenticate the host.

The main certificate hierarchy is presented in Figure 2.

Host Certificates are validated only by the constraint that these certificates can only be added to the device after Administrative Authentication.

Each time authentication is required the following steps will be executed:

↓ The Authentication Silo will challenge the Host using the relevant ASCh certificate, if needed, for a specified Authentication Silo. (Authenticate Host command)

↓ If authentication is successful, the Authentication Silo will enter the Authenticated state.

↓ The host may authenticate the device before or after the device authenticates the host, but device authentication of the host may not be interleaved with the actions used to authenticate the host. (Challenge Authentication Silo command)

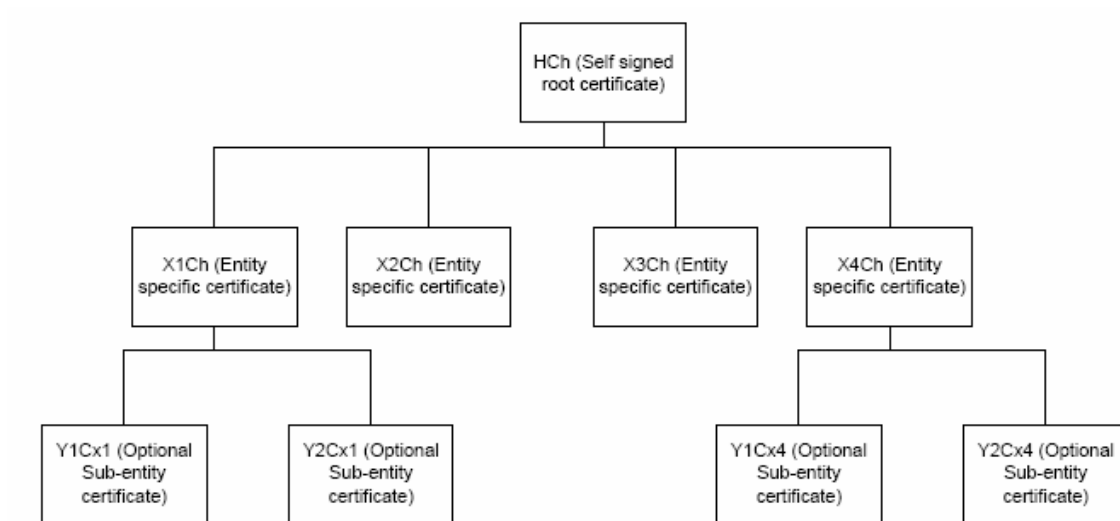


Figure 2—Certificate hierarchy

9.3 Host Certificate Store

The Host Certificate Store may include one or more certificates signed directly or indirectly by a Host

Certificate (HCh). These certificates are presented to the Authentication Silo for host authentication.

9.4 User Certificate Storage

Certificates are stored as X.509 version 3 structures as defined in IETF RFC 2459.

Applications such as access control systems or DRM environments may use standard or extended fields in the certificate to store data relating to specific application rules. The storage limit on this data is defined by the Certificate Store implementation.

User Certificates are processed the same way as Host Certificates including challenge using the Host Authentication/Verify Challenge sequence, except that Verify Challenge does not cause a state change to Authenticated.

9. Certificate Authentication Silo

9.1 Certificate names and types

9.1.1 Certificate names

Certificate names are specified in this document according to the KCi structure, where

K is the Public Key of the certificate i is the issuer of the certificate

The value X in the K position indicates the certificate KCi or any certificate descended from KCi. For example, for certificate HCh, XCh would refer to HCh or any certificate descendent from the HCh certificate.

Values of K:

- X: a certificate or any descendent of the certificate, XCh, XCp
- AS: Authentication Silo, ASCm, ASCh
- S: Signer, SCh
- P: Provisioning, PCp
- H: Host, HCh

Values of i:

- h: host, XCh, HCh, ASCh, SCh
- m: manufacturer, ASCm
- p: provisioner, PCp, XCp

Used values:

- ASCh: Authentication Silo Certificate (see 9.1.4)
- ASCm: Manufacturer Certificate (see 9.1.2)
- HCh: Host Certificate (see 9.1.6)
- PCp: Provisioning Certificate (see 9.1.3)
- SCh: Signer Certificate (see 9.1.5)
- XCh: HCh or any descendant of HCh (see 9.1.6)
- XCp: PCp or any descendant of PCp (see 9.1.3)

9.1.2 Manufacturer certificate (ASCm) chain

This certificate chain shall be defined by the device manufacturer and shall be included in the certificate store of each Certificate Authentication Silo. The ASCm chain shall be signed by the manufacturer certificate authority and shall be immutable.

The fields in the certificates of the ASCm chain shall be as defined in the X.509 Version 3 certificate definition (ITU-T X.690-2002). The ASCm certificate shall have the following properties:

- The subjectPublicKeyInfo shall contain the Public Key of the ASKP.
- The subject field shall contain the ACT Globally Unique Identifier (see 6.3.2) in the RDN “serialNumber.”
- The subject field may contain a display friendly ACT name in the RDN “cn” (common name).
- The KeyUsage extension field shall have the DigitalSignature bit asserted and the extension specified as non-critical.
- The BasicConstraints extension field shall have cA set to FALSE and the extension specified as non-critical.
- If the ASCm certificate is to have no expiration date, the not After field shall be assigned the maximum representable Generalized Time value of 99991231235959Z.

The ASCm chain shall be stored in the first certificate location (Certificate Index 0) of the ASCS.

The ASCm chain may exceed the general 2 KiB size limit on certificates stored in the ASCS.

The ASCm chain shall be stored in PKCS #7 (IETF RFC 2315-PKCS #7) format for certificate chains with DER encoding (ITU-T X690-2002).

9.1.3 Provisioning Certificate (PCp)

This certificate is used in the Administrative Command Sequences (see 9.6.3) to provision and administer Certificate Authentication Silos.

Authentication with a PCp or a certificate chain signed by PCp (XCp) shall be required to clear PCp by initializing the Certificate Authentication Silo.

Authentication with a PCp or a certificate chain signed by PCp (XCp) shall be required to change HCh, ASCh, and SCh certificates.

The PCp shall be stored in the second certificate location (Certificate Index 1) of the ASCS.

Certificates and certificate chains shall be validated as defined in 9.2.2 and 9.2.3.

9.1.4 Authentication Silo Certificate (ASCh)

This certificate is used to authenticate the Certificate Authentication Silo to a Host. This certificate shall contain the Public Key of ASKP and shall be signed by a descendant of a certificate trusted by the Host.

This certificate should be based on the certificate request returned by Create Certificate Request.

Each certificate of the ASCh chain stored by the Certificate Authentication Silo shall be stored as an individual certificate in the ASCS. The host shall read the ASCh certificate and associated SCh certificates and reassemble the certificate chains. Zero or more SCh certificates and an ASCh certificate comprise the ASCh chain.

9.1.5 Signer Certificate (SCh)

These certificate(s) are used to complete the signing chain between an ASCh certificate and a certificate trusted by the Host. The certificate trusted by the host may be stored in the ASCS as an SCh. Zero or more SCh certificates and an ASCh certificate comprise the ASCh chain.

9.1.6 Host Certificate (HCh)

This is a certificate used to authenticate the host to the Certificate Authentication Silo.

Authorized licensed use limited to: Tsinghua University. Downloaded on March 05, 2026 at 18:15:03 UTC from IEEE Xplore. Restrictions apply.

The HCh or a descendant certificate may be used by the Certificate Authentication Silo to authenticate the Host. Certificates and certificate chains shall be validated as defined in 9.2.2 and 9.2.3.

9.2 Certificate chains

9.2.1 Certificate chain requirements

The Certificate Authentication Silo shall support the processing and validation of Host and Admin authentication certificate chains. This shall enable a Host to perform authentication using a descendant certificate (such as XCp and XCh) of certificates stored in the ASCS (such as PCp and HCh, respectively).

As only a certificate in a certificate chain is stored in the ASCS, the Certificate Authentication Silo shall support a certificate chain processing mechanism that shall allow a Host to provide all intermediate certificates, stored on the host, from the certificate stored on the device to the certificate that shall be used for authentication (see 9.6.4 and 9.6.3.3).

Validation Policies define the rules to test that a certificate chain is valid and that the descendant certificate may be used for authentication. The validation policies are None, Basic, and Extended (defined in 9.2.3).

The Certificate Authentication Silo shall support the None and the Basic Validation Policies. The Certificate Authentication Silo may also support the Extended Validation Policy.

ASCh chain validity is verified by the Host. The Host validation policies for the ASCh chain are not defined in this standard. ASCh chains include the ASCh certificate and zero or more SCh intermediate certificates.

ASCh and SCh certificates shall be stored as individual certificates in separate locations in the ASCS.

9.2.2 Certificate chain validation process

Certificate chains are processed by executing one or more Admin Authenticate or Authenticate Host commands in sequence regardless of the Validation Policy.

The certificates in the chain are verified from the top of the certificate chain, starting with the certificate stored in the ASCS, to the final certificate in the chain and shall be presented in this order to the Certificate Authentication Silo.

The four Authenticate Actions of Self, Begin, Continue, and Final shall be used with the Admin Authenticate and Authenticate Host commands to validate certificate chains.

The Authenticate Action of Self shall be used when the host is using the certificate stored in the ASCS to perform authentication.

When certificate chains contain two or more certificates, the Authenticate Action of Begin shall be used for the first certificate. The Authenticate Action of Final shall be used for the last certificate in the chain, which is the certificate that shall be used for authentication. The Authenticate Action of Continue shall be used for each intermediate certificate.

The Validation Policy for a certificate chain is determined by the Validation Policy for the certificate at the Certificate Index Location specified in the Admin Authentication or Authenticate Host command with the Authenticate Action of Begin or Self.

The certificate shall be validated according to validation policy rules specified in 9.2.3.

If the Certificate Authentication Silo failed to parse the certificate, then the silo shall return a Certificate Parsing error.

When any certificate fails the Validation Policy, the Certificate Authentication Silo shall return a Failed Validation Policy error response. Successive Admin Authenticate or Authenticate Host commands shall return the same error until either a different IEEE 1667 Silo Command is executed on the Certificate Authentication Silo or the Admin Authenticate or Authenticate Host command is called with an Authenticate Action of Begin or Self. The Authenticate Action of Self and Begin shall always restart the Certificate Chain Validation process.

9.2.2.1 Self Authenticate Action

The Host may authenticate against the Public Key of the certificate stored in the ASCS using the Self Authenticate Action.

No certificate shall be sent with the Self Authenticate Action.

The Self Authenticate Action shall always reference a certificate index in the ASCS.

For the Admin Authenticate command, the Self Authenticate Action shall specify Certificate Index 1; the location of the PCp certificate.

For the Authenticate Host command, the Self Authenticate Action shall specify the Certificate Index of an HCh certificate.

The validation policy for the certificate shall be determined by the validation policy of the Certificate at the Certificate Index Location specified by the Self Authenticate Action.

Execution of the Admin Authenticate command with a valid certificate and the Self Authenticate Action shall retain the Public Key of the certificate specified by the Certificate Index as the Admin Authentication Certificate (XCp) Public Key for use in the Verify Challenge command.

Execution of the Authenticate Host command with a valid certificate and the Self Authenticate Action shall retain the Public Key of the certificate specified by the Certificate Index as the Host Authentication Certificate (XCh) Public Key for use in the Verify Challenge command.

9.2.2.2 Begin Authenticate Action for certificate chains

For the first certificate in a certificate chain, an Admin Authenticate or Authenticate Host command shall be executed with the Begin Authenticate Action.

No certificate shall be sent with Begin Authentication Action.

The Begin Authenticate Action shall always reference a certificate index in the ASCS.

The validation policy for all certificates in the certificate chain shall be determined by the validation policy of the certificate at the Certificate Index location specified by the Begin Authenticate Action.

For the Admin Authenticate command, the Begin Authenticate Action shall specify Certificate Index 1 as the location of the PCp certificate.

For the Authenticate Host command, the Begin Authenticate Action shall specify the Certificate Index of an HCh certificate.

9.2.2.3 Continue Authenticate Action for certificate chains

The Continue Authenticate Action shall be used for all intermediate certificates in a certificate chain. Intermediate certificates shall be presented one by one in the order specified in 9.2.2.2.

The Intermediate Certificate shall be sent with the command. On each Continue Authenticate Action, the certificate shall be validated using the validation policy determined in the Begin Authenticate Action in 9.2.2.2.

9.2.2.4 Final Authenticate Action for certificate chains

The Final Authenticate Action shall be used when presenting the last certificate in a certificate chain.

The certificate shall be validated using the validation policy determined in the Begin Authenticate Action in 9.2.2.2.

Execution of the Admin Authenticate command with a valid certificate and the Final Authenticate Action shall retain the public key of the certificate used as a parameter in the command as the Admin Authentication Certificate (XCp) Public Key for use in the Verify Challenge command.

Execution of the Authenticate Host command with a valid certificate and the Final Authenticate Action shall retain the public key of the certificate used as a parameter in the command as the Host Authentication Certificate (XCh) Public Key for use in the Verify Challenge command.

9.2.3 Certificate validation policies

9.2.3.1 General requirements

All certificate fields without requirements specified in this standard shall not be validated by the Certificate Authentication Silo.

9.2.3.2 None validation policy

For the Self Authenticate Action, the certificate shall not be inspected. The certificate shall be assumed valid.

The Authenticate Actions of Begin, Continue, and Final shall return an Invalid Validation Policy Operation Status Code.

9.2.3.3 Basic validation policy

Certificates with an Authenticate Action of Self or Begin shall be validated as follows:

- The certificate version shall be 3.
- The Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.

Certificates with an Authenticate Action of Continue or Final shall be validated as follows:

- The certificate version shall be 3.
- The Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- The Subject field of the previous certificate presented shall match the Issuer field of the current certificate.
- The Signature of the current certificate presented shall be successfully verified using the public key of the previously presented certificate and the signing algorithm of the current certificate.

9.2.3.4 Extended validation policy

Certificate Format Requirements

The Extended Validation Policy requires that Begin, Continue, and Final certificates shall have the following fields specified in the certificate. All other fields shall be determined by the issuing authority.

Certificates with an Authenticate Action of Self shall be constructed as follows:

- Certificate Version Number shall be 3.
- Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- Key Usage shall be set as non-critical and shall assert the digital Signature bit. Other bits may be asserted.

Certificates with an Authenticate Action of Begin and Continue shall be constructed as follows:

- Certificate Version Number shall be 3.
- Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- Key Usage shall be set as non-critical and shall assert the keyCertSign bit. Other bits may additionally be asserted.
- Basic Constraints field shall be present and the cA value shall be set to True. The path length constraint may be specified; however, it shall be ignored by the validation policy.

Certificates with an Authenticate Action of Final shall be constructed as follows:

- Certificate Version Number shall be 3.
- Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- Key Usage shall be set as non-critical and shall assert the digital Signature bit. Other bits may additionally be asserted.
- Basic Constraints field shall be present, and the cA value shall be set to False.

Certificate Validation Requirements

Certificates with an Authenticate Action of Self shall be validated as follows:

- The certificate version shall be 3.
- The Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- The Basic Constraints field shall be ignored.
- The digital Signature bit in the Key Usage field shall be asserted.

Certificates with an Authenticate Action of Begin shall be validated as follows:

- The certificate version shall be 3.
- The Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.
- Basic Constraints field shall be present, and the cA value shall be set to True and the path length constraint may be specified; however, it shall be ignored by the validation policy.
- The keyCertSign bit in Key Usage field shall be asserted.

Certificates with an Authenticate Action of Continue shall be validated as follows:

- The certificate version shall be 3.

- [Basic Constraints field shall be present, and the cA value shall be set to True and the path length constraint may be specified; however, it shall be ignored by the validation policy.](#)
- [The keyCertSign bit in Key Usage field shall be asserted.](#)
- [The Subject field of previous certificate presented shall match the Issuer field of the current certificate.](#)
- [The Signature of current certificate presented shall be successfully verified using the Public Key of the previously presented certificate and the signing algorithm of the current certificate.](#)

[Certificates with an Authenticate Action of Final shall be validated as follows:](#)

- [The certificate version shall be 3.](#)
- [The Signature Algorithm shall be one of the supported signing algorithms listed in 9.5.11.](#)
- [Basic Constraints field shall be present, and the cA value shall be set to False.](#)
- [The digital Signature bit in the Key Usage field shall be asserted.](#)
- [The Subject field of previous certificate presented shall match the Issuer field of the current certificate.](#)
- [The Signature of the current certificate presented shall be successfully verified using the Public Key of the previously presented certificate and the signing algorithm of the current certificate.](#)

[9.3 Certificate Authentication Silo state machine](#)

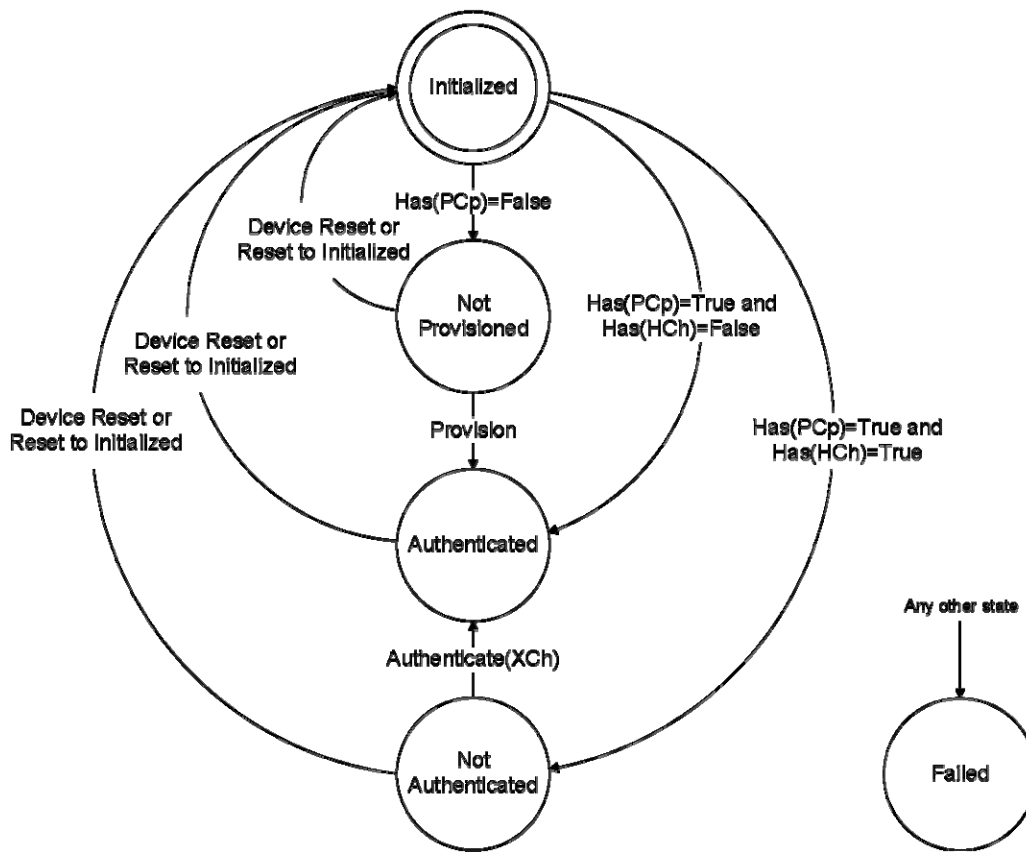
Figure 3 describes [the states of a Certificate Authentication Silo](#). The following state machine documents the states and state transitions of the ~~device~~[Certificate Authentication Silo](#) and therefore reflects the authentication of the Host by the Certificate Authentication Silo and not the authentication of the Certificate Authentication Silo by the Host.

The following states are defined:

- ↓ Initialized
- ↓ Not Provisioned
- ↓ Not Authenticated
- ↓ Authenticated
- ↓ [Failed](#)

Each [Certificate Authentication Silo](#) shall maintain a single state ~~and therefore states distinguished by the host are not supported.~~

When the TSD is powered OFF, disconnected, reset, or initialized, the Certificate Authentication Silos in all ACT on the device shall return to the Initialized state.



NOTE—The Failed state can be reached from any other state on detection of a failure in the Certificate Authentication Silo.

Figure 3—Certificate Authentication Silo state machine

9.3.1 Initialized

The Initialized state determines the operating state based on the certificates present within the [Authentication Silo](#) Certificate Store, regardless of the content of the certificates ~~(see Figure 4)~~. This state is a ~~temporary decision~~ transitory state only, and shall place the [Certificate Authentication Silo](#) in one of ~~two~~ the following states: Not Provisioned ~~or Not~~, Authenticated, Not Authenticated, or the optional Failed state. While in the Initialized state, all commands other than the Query Certificate Authentication Silo shall respond with the Invalid State Status Code value. The Query Certificate Authentication Silo may be used to determine when the Certificate Authentication Silo has exited the Initialized state allowing execution of other commands.

The Initialized State is entered on application of power, reset, or execution of the Reset to Initialized command (Figure 4).

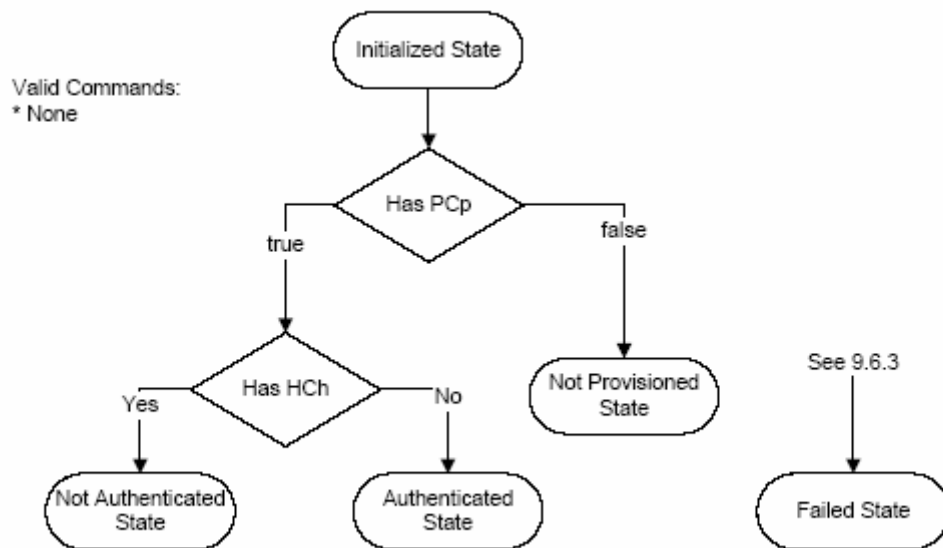


Figure 4—Initialized State

~~The Initialized State does not allow communications with the host and does not accept any commands.~~

If the certificate store contains a PCp and no Host Certificates, the Certificate Authentication Silo shall transition into the Authenticated state before any Certificate Authentication Silo Commands can be executed.

9.3.2 Not Provisioned

The Not Provisioned state (Figure 5) is reached when the Certificate Authentication Silo has not been provisioned using the Set Certificate command. ~~This state allows the Provisioning~~ The Set Certificate (PCp) command to be set. Optionally, the PCp is only accepted when the host may authenticate the Certificate Authentication Silo is in this state by challenging the manufacturer certificate ASCm ~~the Not Provisioned state.~~

After provisioning, the ~~silo, it~~ Certificate Authentication Silo shall transition automatically ~~transitions~~ to the Authenticated state. This removes the need for a reset event to transition after the provisioning process.

The Reset to Initialized command or a reset event transitions the Certificate Authentication Silo from the Not Provisioned state to the Initialized state.

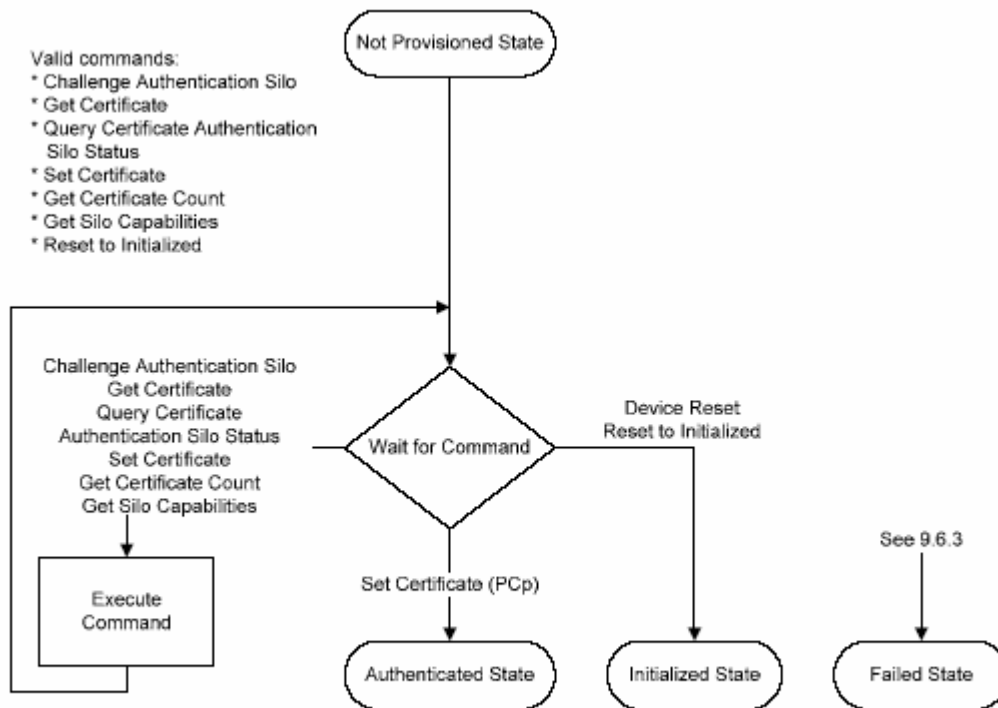


Figure 5—Not Provisioned State

9.3.3 Not Authenticated

The Not Authenticated state (Figure 6) allows for authentication of the host by the Certificate Authentication Silo, if required. The host may also authenticate the Certificate Authentication Silo in this state; or request administrative authentication.

~~If the Certificate Store contains no Host Certificates the Authentication Silo will immediately transition into the~~ The Reset to Initialized command or a reset event transitions the Certificate Authentication Silo from the Not Authenticated state to the Initialized state.

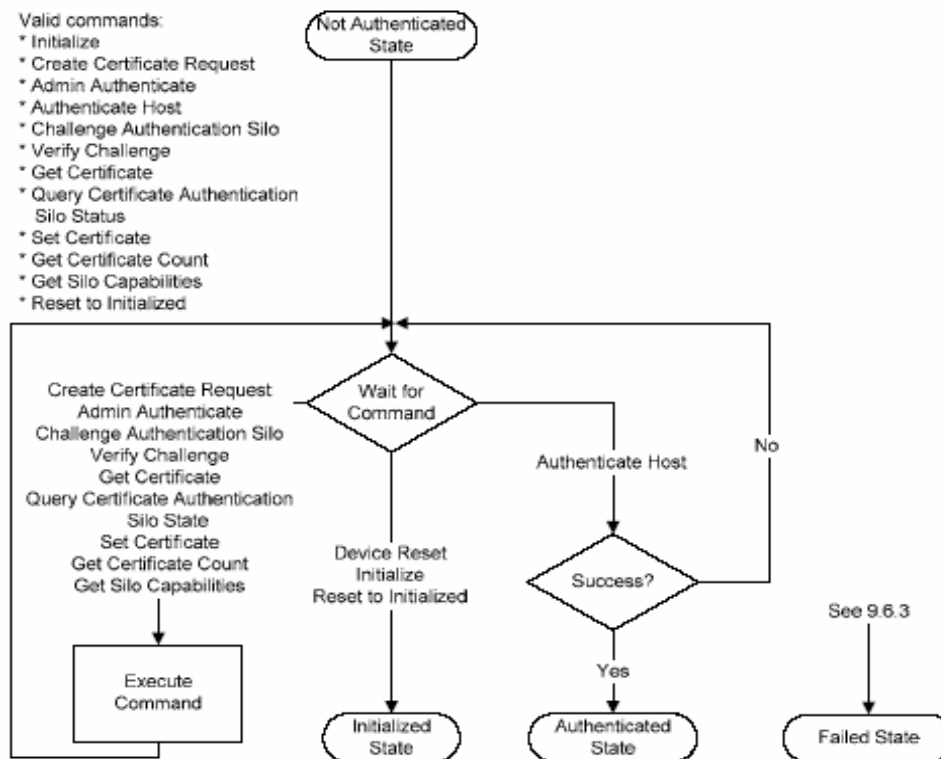


Figure 6—Not Authenticated State

9.3.4 Authenticated

The Authenticated state (Figure 7) is the ~~operational~~ state of the [Certificate](#) Authentication Silo; in which the silo has authenticated the host. ~~In this state, user access to the Certificate Store and media access are enabled. The host may authenticate the silo~~ [The host may authenticate the Certificate Authentication Silo](#) at any time in this state.

[The Reset to Initialized command or a reset event transitions the Certificate Authentication Silo from the Authenticated state to the Initialized state.](#)

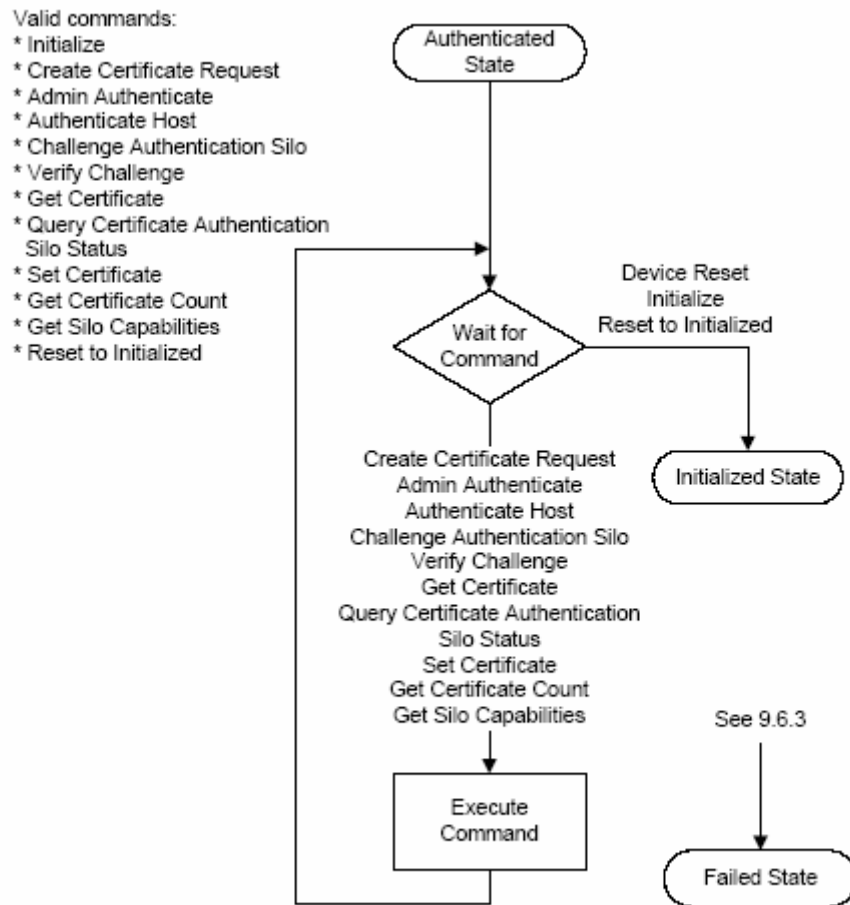


Figure 7—Authenticated State

9.3.5 Always Authenticated Configuration

The Always Authenticated Configuration is when the Certificate Authentication Silo is provisioned (has a PCp) but has no HCh stored in the ASCS. When the Certificate Authentication Silo is set in this manner, it shall transition from the Initialized state to the Authenticated state and shall not require any IEEE 1667 Silo Commands to transition to the Authenticated state. This allows an ACT to reach the Authenticated state without dependence on host support for IEEE Std 1667.

9.3.6 Failed

The optional Failed state (Figure 8) is entered when any failure inhibiting the Certificate Authentication Silo functionality is detected (e.g., a cryptographic self-test). The only exit from this volatile state shall be reset by application of power.

When a Failed state is reported in the Query Certificate Authentication Silo Status command, an optional informative, vendor specific, variable-length Failure Response can be returned.

Commands not executable in the Failed state shall return the Invalid State Status Code.



Figure 8—Failed State

9.4 Certificate Authentication Silo Status Codes

In addition to the Common Status Codes, the Certificate Authentication Silo defines 15 additional Status Codes (Table 3).

Table 3—Certificate Authentication Silo specific Status Code values

Condition	Use	Status type
Valid Certificate	Certificate presented for authentication is valid.	Success
Invalid Admin Signature	An Administration Signature is required, but the value supplied is not valid.	Failure
Invalid Cert Index	The supplied Certificate Index is not valid for the command.	Failure
Invalid Cert Type	The Certificate at the Certificate Index is not valid for the command.	Failure
Occupied Cert Index	Failed attempt to set a Certificate at an occupied Certificate Index.	Failure
Certificate Parsing Error	The Certificate Authentication Silo failed to parse the certificate.	Failure
Invalid Algorithm	Certificate presented for authentication requires the use of an unsupported algorithm or key size.	Failure
Invalid Certificate Size	The certificate presented is larger than the supported certificate size.	Failure
Invalid State	The command is not supported in the current state.	Failure
Invalid Capability Type	The Capability Type requested in the Get Silo Capabilities command is reserved.	Failure
Invalid Signer Certificate Index	The certificate store location indicated by the Signer Certificate Index is empty, does not contain an ASCh or SCh certificate, or the index is greater than the maximum certificate store index implemented in the Certificate Authentication Silo.	Failure
Maximum Sequence Number	The Admin Sequence Number has reached its maximum value.	Failure
Failed Validation Policy	The certificate does not pass the required validation policy.	Failure
Unsupported Validation Policy	This silo does not support the specified validation policy test.	Failure
Invalid Validation Policy Operation	The specified validation policy operation is not valid for the current Certificate Authentication Silo Command.	Failure

Valid Certificate (Admin Authenticate, Authenticate Host)

Valid Certificate shall be returned when executing a Certificate Authentication Silo Command with an Authenticate Action of Begin or Continue and the Certificate is determined to be valid.

Invalid Admin Signature (Initialize, Set Certificate)

Invalid Admin Signature shall be returned when the Certificate Authentication Silo Command requires Administration Authentication and the Administration Signature is determined to be invalid. The state and contents of the Certificate Authentication Silo shall remain unchanged.

Invalid Cert Index (Set Certificate, Get Certificate, Authenticate Host, Challenge Authentication Silo)

Invalid Cert Index shall be returned under the following conditions for the Set Certificate command:

↓ The Certificate Index is zero (00h) or greater than or equal to the number of allowed certificates.

Invalid Cert Index shall be returned under the following conditions for the Get Certificate command:

↓ The Certificate Index is greater than or equal to the number of allowed certificates.

Invalid Cert Index shall be returned under the following conditions for the Authenticate Host command:

↓ The Certificate Index is less than two (2) or greater than or equal to the number of allowed certificates.

Invalid Cert Index shall be returned under the following conditions for the Challenge Authentication Silo command:

↓ The Certificate Index is not set to indicate a challenge against the Manufacturer certificate or a valid Authentication Silo Certificate.

Invalid Cert Type (Set Certificate, Authenticate Host)

Invalid Cert Type shall be returned under the following conditions for the Set Certificate command:

↓ The certificate type is a reserved value.

Invalid Cert Type shall be returned under the following conditions for the Authenticate Host command:

↓ The certificate at the specified certificate index is not a Host certificate.

Occupied Cert Index (Set Certificate)

Occupied Cert Index shall be returned when:

- a) A Set Certificate command is received
- b) An S certificate already exists at the specified index
- c) The Certificate type does not equal No Certificate

Certificate Parsing Error (Admin Authenticate, Authenticate Host, Challenge Authentication Silo)

Certificate Parsing Error shall be returned when the Certificate Authentication Silo encounters an error when attempting to parse a certificate used in the command.