



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

IEEE Computer Society

Sponsored by the
Information Assurance Committee

1667™

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
6 June 2007

IEEE Std 1667™-2006

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

Sponsor
Information Assurance Committee
of the
IEEE Computer Society

Approved 6 December 2006
IEEE-SA Standards Board

Abstract: This document defines a standard protocol for secure authentication and creation of trust between a secure host and a directly attached Transient Storage Device (TSD), such as a 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 WUSB may comply with this protocol.

Keywords: secure authentication, Transient Storage Device

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

Copyright © 2007 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 6 June 2007. 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 of Apple Computer Inc., registered in the U.S. and other countries.

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

Palm OS is a registered trademark of Palm Trademark Holding Company, LLC.

RIM is a trademark of Research in Motion Limited. RIM is registered with the U.S. Patent and Trademark office and may be pending or registered in other countries.

Symbian OS is a trademark of Symbian Software Ltd.

Print: ISBN 0-7381-5314-1 SH95613
PDF: ISBN 0-7381-5315-X SS95613

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 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 the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards must 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 addressed to:

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 1667-2006, IEEE Standard Protocol for Authentication in Host Attachments of Transient Storage Devices.

IEEE Std 1667 defines bidirectional authentication of Transient Storage Devices (TSDs) such as USB Flash Drives (UFDs), memory cards, and portable hard disks. Not only can the host authenticate the identity of the TSD, but the TSD can also authenticate the identity of the host.

IEEE Std 1667 defines authentication of the host and/or the device based on generic actions in the body of the standard. Protocol specific implementations of these actions are defined separately in annexes to the standard allowing the extension of the specification to more protocols over time. Usually, each protocol-specific implementation will be published as an informative annex and then made a normative part of the specification after widespread review and comment.

Each TSD is defined as containing one or more storage areas. The storage areas are individually authenticated, allowing the standard to address the need for authentication below the device level, e.g., to allow host specific access to the different storage areas on the device. The term Addressable Command Target (ACT) is used to avoid linking the specification to any given protocol. Each protocol-specific annex will identify the equivalence between an ACT and some portion of the device.

Notice to users

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 must not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

At the time this standard was completed, the P1667 Working Group had the following membership:

Ariel Sobelman, *Chair*
Daniel Goodman, *Vice-chair*
Moshe Raines, *Vice-chair*
Donald Rich, *Technical editor*
Yehuda Hahn, *Technical editor*

John Goodman
G. Scott Henderson

Emily Hill
Henry Hutton

Mike Kuppinger

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

Hagai Bar-El
Christopher Fitzgerald
John Geldman

Daniel Goodman
G. Scott Henderson
Emily Hill

Henry Hutton
Mike Kuppinger
Donald Rich

Sponsoring Committee Chairs:

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

When the IEEE-SA Standards Board approved this application guide on 6 December 2006, it had the following membership:

Steve M. Mills, *Chair*
Richard H. Hulett, *Vice Chair*
Judith Gorman, *Secretary*

Mark D. Bowman
Dennis B. Brophy
Joseph Bruder
Richard Cox
Bob Davis
Julian Forster*
Joanna N. Guenin
Mark S. Halpin
Raymond Hapeman

William B. Hopf
Lowell G. Johnson
Herman Koch
Joseph L. Koepfinger*
David J. Law
Daleep C. Mohla
Paul Nikolich

T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Richard L. Townsend
Joe D. Watson
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan H. Cookson, *NIST Representative*

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
2. Normative references.....	1
3. Definitions and acronyms	2
3.1 Definitions	2
3.2 Acronyms	3
3.3 Certificate names	3
4. Authentication layer	4
4.1 Stack	4
5. Host requirements.....	4
5.1 PKI algorithm	5
5.2 Random number generator	5
5.3 Certificate store.....	5
5.4 XCh Host Certificate	5
6. Channel.....	5
7. TSD requirements.....	5
8. ACT requirements	5
8.1 Probe silo requirements	5
8.2 Authentication silo requirements	6
8.3 Certificate Store.....	6
8.4 Globally Unique Identifier.....	6
8.5 Authentication Silo Key Pair	6
8.6 Authentication Silo Certificates.....	6
8.7 PKI algorithm	7
8.8 Random number generator	7
8.9 Silo Type Identifier (STID)	7
9. Certificate Store.....	7
9.1 Required features.....	7
9.2 Authentication Silo Certificate Store	7
9.3 Host Certificate Store	9
9.4 User Certificate Storage.....	9

10. Authentication Silo state machine	9
10.1 Initialized	10
10.2 Not Provisioned	11
10.3 Not Authenticated	12
10.4 Authenticated	12
10.5 Non-IEEE 1667 host support	13
11. Probe Silo actions	13
11.1 Process of probing	13
11.2 Probe command	14
12. Authentication Silo actions	14
12.1 Initialize (reset to manufacturing state)	14
12.2 Create Certificate Request	14
12.3 Admin Authenticate	14
12.4 Authenticate Host	16
12.5 Challenge Authentication Silo	18
12.6 Verify Challenge	19
12.7 Get Certificate	20
12.8 Get State	20
12.9 Set Certificate	20
12.10 Get Certificate count	21
12.11 Get Silo capabilities	21
13. Authentication of ACTs	22
14. Authentication Command sequences	22
14.1 Provisioning	22
14.2 Host Authentication by the Authentication Silo	24
14.3 Authentication Silo Authentication by the host	24
14.4 Authentication Silo Authentication using ASCh	25
Annex A (informative) SCSI Command Set	27
A.1 IEEE 1667 conventions	27
A.2 Non-IEEE 1667 silos	27
A.3 Acronyms	27
A.4 IEEE 1667 commands	27
A.5 Probe Silo commands	28
A.6 Authentication Silo Commands	32

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

1. Overview

1.1 Scope

This project defines a standard protocol for secure authentication and creation of trust between a secure host and a directly attached Transient Storage Device (TSD), such as a 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 WUSB may comply with this protocol.

1.2 Purpose

Industry has witnessed explosive private and corporate growth in use of TSDs. These devices serve much the same functionality that floppy disks once did, but at much higher capacities and with greater reliability 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 has become a much greater issue than before.

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 insure 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 and embedded systems, personal and portable secure data storage, as well as operating system and enterprise security application vendors.

2. Normative references

The following referenced documents are indispensable for the application of this document. 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/stdid>.

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

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

IETF RFC 3280: 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 Cryptographic Applications”) from 15 May 2001. Available at: (<http://csrc.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/pkcs-1/pkcs-1v2-1.pdf>).

Universal Serial Bus Mass Storage Class Specification Overview,. Published by the U.S. Implementers Forum. Available at: http://www.usb.org/developers/devclass_docs/usb_msc_overview_1.2.pdf.

3. Definitions and acronyms

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. IETF RFC 2828 should be referenced for terms not defined in this clause.

3.1.1 Addressable Command Target (ACT): A uniquely addressable area in a storage device, to which commands can be routed based on the Transient Storage Device’s native communications protocol.

3.1.2 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. This limits the use of administration commands to hosts that can complete the Administration Authentication sequence. The generation and use of the Administration Signatures is defined in Clause 14.

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

3.1.4 Authentication Silo (AS): A silo that 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 Authentication Silo. 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 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 Transient Storage Device.

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.

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/>).

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.

3.1.8 connect: The process of establishing a connection between a host and a device, allowing the use of functionality in the 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 a standard connector such as USB, FireWire, WUSB, ATA, or a dedicated TCP/IP connection. The functionality provided by the 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.

3.1.11 host: A computer, server, or other provider of services to a user that has a client-server relationship with an 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 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 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.

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.

3.2 Acronyms

ACT	Addressable Command Target
ASKP	Authentication Silo Key Pair
GUID	Globally Unique Identifier
PKI	Public Key Infrastructure
RNG	Random Number Generator
STID	Silo Type Identifier
TSD	Transient Storage Device

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) descended from the HCh root certificate.

4. Authentication layer

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

4.1 Stack

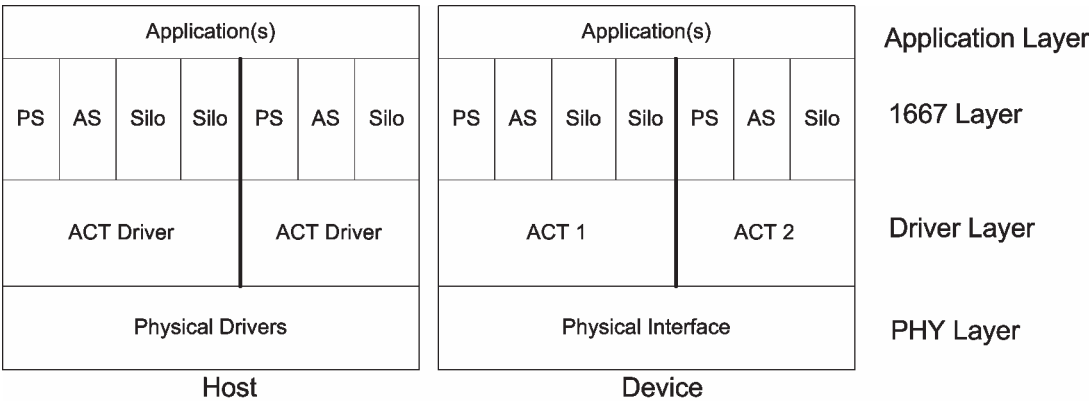


Figure 1—IEEE 1667 stack

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) interface, which can be SCSI, ATA, or any other interface that has an IEEE 1667 transport defined for it.

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. 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 layer is the IEEE 1667 layer consisting of silos. A silo is represented as an index on the device, and each silo may contain a separate command processing engine and its own private storage for the command processing engine. Applications reside above the 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 1667.

5. Host requirements

The host may be a 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.

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.

8. ACT 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.

8.1 Probe silo 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.

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.

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
- Retrieve certificates by index

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)