IEEE P1667™/D2

February 20, 2006

Draft For Information Only

Selected Extracts from the

Standard Protocol for Authentication in Host Attachments of Transient Storage Devices

Prepared for INCITS/T10

Sponsored by the
Information Assurance Committee
of the
IEEE Computer Society

Piscataway, NJ 08855-1331, USA

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. Definitions

For the purposes of this standard, the following terms and definitions apply. [IETF1] should be referenced for terms not defined in this clause.

1 Authentication: The act of checking the identity or integrity of an entity.

2 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 Command Set: The Command Set is a protocol that facilitates authentication between a host and a TSD. The Command Set also includes commands that implement security features such as Certificate Store access, cryptography, and device authentication.

4 Connect: The process of establishing a connection between a host and a device, allowing the use of functionality in the TSD by the host, or allowing the use of functionality in the host by the TSD, depending on authorization. Generally, a device is connected to a host via a standard connector such as USB, FireWire, WUSB, 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.

5 Consume: To use licensed content in a DRM environment. Consumed content may not be reused outside of the scope of the DRM environment.

6 Cryptographic Processor: The Cryptographic Processor is a co-processor on the TSD that includes functionality for cryptographic algorithms. At minimum the Cryptographic Processor must support the RSA public-key infrastructure algorithms (using the DKP or a user-supplied key) and secure random number generation. (Algorithms are as defined in [FIPS1].) The Cryptographic Processor is controlled using the Command Set.

7 Device Key Pair: A DKP is a pair of public and private keys, associated with a TSD. The private key is stored securely on a TSD and cannot be retrieved by a host using any command. However, it can be challenged by encrypting data with the public key, which is readily available using the Command Set. There may be more than one DKP in a TSD.

8 Globally Unique ID: A GUID is an immutable globally unique device serial number. This serial number is associated with a device at manufacturing time and cannot be changed.

9 Device: *see* Transient Storage Device

10 Host: A computer, server, or other provider of services to a user that has a client-server relationship with a TSD in which the user primarily interacts with the host.

11 Mass Storage Class: USB device class for mass storage devices as defined in [USB2].

12 Policy: A policy is a series of rules that defines security for a connection, device, or host. Policies define access control lists, usage rules, and audit rules.

13 Transient Storage Device: A TSD is a portable device that provides mass storage capabilities to a host, but is not permanently attached to a specific host. In this specification, the term “device” may refer to a physical device or a virtual engine. **TSDs in the initial specification will not have additional authentication requirements other than storage authentication.**

14 User: A physical human user of a device and/or host. Users can be authenticated. In a corporate environment, users correspond to network users. In a commercial environment, users are licensees of specific content, applications, or entities. Typically, a device has a user associated with it.

15 **Virtual Engine**: A uniquely addressable instance of a 1667 device interface. One or more virtual engines can exist in a Transient Storage Device – each instance has all of the properties of the device interface as defined in this specification.

16 **Initialize**: Return a device to its original manufactured state

2.1 Acronyms

DC	Device Certificate
DKP	Device Key Pair
DRM	Digital Rights Management
GUID	Globally Unique Identifier
HC	Host Certificate
HKP	Host Key Pair
MSC	Mass Storage Class
ORC	Owner Root Certificate
PKI	Public Key Infrastructure
RNG	Random Number Generator
TSD	Transient Storage Device

TPM	Trusted Platform Module, as defined in [TCG1]
VE	Virtual Engine
WUSB	Wireless USB

3. References

[FIPS1], Federal Information Processing Standards Publication 196: Entity Authentication Using Public Key Cryptography. Available at http://csrc.nist.gov/publications/fips/fips196/fips196.pdf.

[IEEE1] IEEE P1363, Standard Specifications for Public Key Cryptography.

[IEEE2] IEEE P1363a, Addendum to the Standard Specifications for Public Key Cryptography.

[IETF1] IETF RFC 2828, Available from http://www.ietf.org/rfc/rfc2828.txt?number=2828.

[IETF2] IETF RFC 2459, Available from http://www.faqs.org/rfcs/rfc2459.html.

[ISO1] ISO/IEC 9594-8.

[RSA1], RSA Security Public-Key Cryptography Standards #11, Available at ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf.

[TCG1], Trusted Computing Platform Alliance Main Specification, version 1.1b. Published by the Trusted Computing Group. Available from http://www.trustedcomputinggroup.com.

[USB1], Universal Serial Bus Specification, Version 2.0. Published by the USB Implementers Forum. Available at http://www.usb.org.

[USB2], Universal Serial Bus Mass Storage Class Specification Overview. Published by the USB Implementers Forum. Available at http://www.usb.org.

5. Host Requirements

The host may be a PC, server, cell phone, or any other device that can support the host-side requirements of P1667. The host includes the following components:

— PKI algorithm
— Cryptographic Random Number Generator
— Certificate Store
— Host Certificate(s)

7. Transient Storage Device Requirements

The device itself includes one or more VEs, as defined in 7.7. Each VE has the following components:

— Certificate Store
— Globally Unique Identifier
— Device Key Pair

— Device Certificate(s)
— PKI Algorithm
— Random Number Generator

8. Command Set

The Command Set is a series of commands that define functionality on the device level for security functionality. The Command Set includes cryptographic functions, Certificate Store access, and authentication functionality

8.2 Transport Protocols

This Specification defines a generic set of functional extensions required for all the supported interface protocols and Commands Sets for authenticating TSDs. The following sections list and describe the various physical and logical attachment interface types addressed within the scope of this Specification, with specific adaptation/integration requirements for each type.

8.2.1 SCSI

SCSI devices include the following device types:
— Parallel SCSI
— USB Mass Storage Class
— IEEE 1394 (FireWire)
— Wireless USB

Each of these device types implements different subsets of the SCSI command set and uses a different protocol to channel these commands. This chapter will discuss relevant implementation notes for each device class.

8.2.1.2 USB Mass Storage Class

1667 support will be indicated by the use of a USB interface descriptor as described in [USB1, USB2]. The descriptor will include, at minimum, the version of the standard supported.

The 1667 Command Set is implemented as SCSI commands above the USB Mass Storage Class and extends the state machine implemented for Mass Storage.

10. 1667 State Machine

The following states are described:

— Enumerated
— Initialized
— Not Provisioned
— Not Authenticated
— Authenticated

— Administration Mode

11. Probe

The Probe command allows the device and host to exchange capabilities and version information to determine if 1667 is supported. The Probe may also identify alternative authentication mechanisms.

11.1 Process of Probing

Probing begins with a determination that the device supports the Probe command. This is specific to the underlying protocol as listed in section 8.2. Protocols that have discovery mechanisms may use them in place of the Probe command to accomplish the same goal.

The Probe command is required before executing any other commands.

12. Commands

The 1667 Command Set is to be implemented as a flexible and extensible collection. The actual set of commands and capabilities supported by a certain device/host instance is determined using the Probing mechanism (see 11 above) The following is a representative (incomplete) list of commands currently being specified, included herein as an example:

- Provision
- Initialize (Reset to Manufacturing State)
- Create Certificate Request (DC)
- Admin Authenticate
- Host Authentication by Device
- Challenge Device
- Verify Challenge
- Get Certificate from Store
- Get Current State
- Set Certificate
- Get DC Count
- Get Certificate Type
-