SanDisk Corporation

TrustedFlash v1.0 – microSD

(Firmware Version: 1.0; Hardware Versions: HermonS2TM 256MB, HermonS2TM 512MB, HermonS2TM 1GB, and HermonS2TM 2GB)

FIPS 140-2
Non-Proprietary Security Policy

Level 3 Validation

Document Version 2.1

Prepared for:

SanDisk Corporation
601 McCarthy Boulevard
Milpitas, CA 95035
Phone: (408) 801-1000
Fax: (408) 801-8657
http://www.sandisk.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2005-05-31	Rumman Mahmud	Initial draft.
0.2	2007-02-03	Xiaoyu Ruan	New draft based on HermonS2T.
0.3	2007-07-25	Xiaoyu Ruan	Updated Table 6.
0.4	2007-08-01	Xiaoyu Ruan	Updated Table 6 and Section 2.6.4.
0.5	2007-08-09	Xiaoyu Ruan	Updated Section 2.3.
0.6	2007-08-22	Xiaoyu Ruan	Addressed Lab's comments.
0.7	2007-08-24	Xiaoyu Ruan	Addressed Lab's comments.
0.8	2007-08-27	Xiaoyu Ruan	Addressed Lab's comments.
0.9	2007-09-04	Xiaoyu Ruan	Addressed Lab's comments.
1.0	2007-10-01	Xiaoyu Ruan	Addressed Lab's comments.
1.1	2007-11-15	Xiaoyu Ruan	Addressed Lab's comments.
1.2	2007-11-21	Xiaoyu Ruan	Addressed Lab's comments.
1.3	2007-11-25	Xiaoyu Ruan	Minor changes.
1.4	2007-11-28	Xiaoyu Ruan	Minor changes.
1.5	2007-11-30	Xiaoyu Ruan	Release for CMVP.
1.6	2008-01-29	Xiaoyu Ruan	Addressed CMVP comments.
1.7	2008-01-31	Xiaoyu Ruan	Addressed CMVP comments.
1.8	2008-05-07	Xiaoyu Ruan	Addressed CMVP comments.
1.9	2009-06-17	Darryl Johnson	Updates to reflect changes in power-up self-test execution, zeroization mechanism and FIPS mode indicator
2.0	2009-07-02	Darryl Johnson	Additional information regarding zeroization mechanism
2.1	2009-09-01	Darryl Johnson	Final CMVP comments

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the TrustedFlash v1.0 – microSD (firmware version: v1.0; hardware versions: HermonS2TM 256MB, HermonS2TM 512MB, HermonS2TM 1GB, and HermonS2TM 2GB) from SanDisk Corporation. This Security Policy describes how the TrustedFlash v1.0 – microSD meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/cryptval/.

In this document, the TrustedFlash v1.0 – microSD is referred to as the card or the module.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor evidence
- Finite state machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to SanDisk. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to SanDisk and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact SanDisk.

2 TrustedFlash v1.0 – microSD

2.1 Overview

SanDisk Corporation is the original inventor of flash storage cards and is the world's largest supplier of flash data storage card products using its patented, high-density flash memory and controller technology. Announced on September 27, 2005, the TrustedFlash v1.0 – microSD is a mass-storage device developed and produced by SanDisk Corporation. The TrustedFlash is a new technology that enables consumers to buy premium music, movies, and games on flash memory cards for use interchangeably in mobile phones, laptop computers, Personal Digital Assistants (PDAs), and other portable devices. For example, with the TrustedFlash v1.0 – microSD, music producers and movie studios are able to release premium content on TrustedFlash products because they provide the superior security and digital rights management (DRM) solutions that are required by these providers. Consumers are able to download premium content from online digital music services through their mobile phones or personal computers.

The TrustedFlash v1.0 – microSD empowers consumers to use their purchased content in a multitude of supported devices. This is in contrast with today's closed, proprietary systems that bind content to a particular host device, such as a specific cell phone or MP3 player. The TrustedFlash technology empowers the card itself to be the manager of digital rights. It provides independence from the host, thus giving consumers the freedom to transfer the card and its content to other supported devices without compromising its content protection system. The TrustedFlash v1.0 – microSD also function as mass-storage devices in non-secure host devices.

The cards with TrustedFlash v1.0 – microSD embedded are highly secure. This is due to an on-board processor, a high-performance cryptographic engine, and tamper-resistant technology. They are designed to provide a much higher level of security than has previously existed on memory cards and on most consumer electronics devices. Cards built on the TrustedFlash platform will provide full DRM capabilities and support industry security standards including both symmetric and asymmetric cryptographic algorithms. TrustedFlash cards can be customized to meet any Original Equipment Manufacturer (OEM) customer's specific security and DRM solutions, including integrating their own chosen DRM solution and rights portability across many devices.

TrustedFlash cards are available immediately to OEM customers in the miniSD, microSD, and Secure Digital (SD) card formats.

The TrustedFlash v1.0 – microSD supports an Approved mode of operation and a non-Approved mode of operation. The TrustedFlash v1.0 – microSD is validated at the following FIPS 140-2 Section levels (when operating in the Approved mode of operation).

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-tests	3

Section	Section Title	Level
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

In Table 1, N/A indicates "Not Applicable". EMC and EMI refer to Electromagnetic Compatibility and Electromagnetic Interference, respectively.

2.2 Interface

The cryptographic boundary of each model of the TrustedFlash v1.0 – microSD is defined by its microSD compatible enclosure. The module is shipped in a TrustedFlash form factor as depicted in Figure 1. The cryptographic boundary is the whole microSD card.

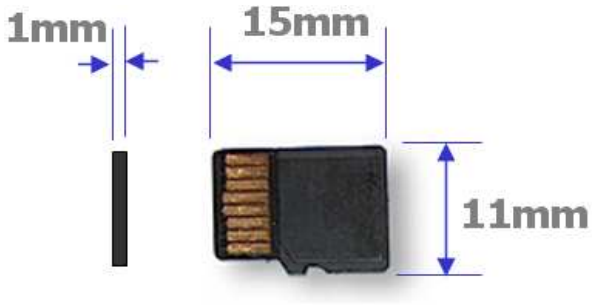

Figure 1 – TrustedFlash Form Factor

The module's physical interfaces are composed of a set of contact pins providing data input, output, power, and clock. No manual control interface is included in the module. The contact pad exposes eight pins as depicted in Figure 2.

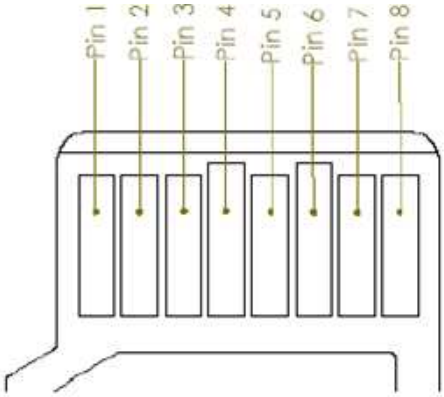

Figure 2 – Pin Assignment on the Contact Pad

The SD and the Serial Peripheral Interface (SPI) are the two alternative communication protocols used by SD cards. Applications can choose either mode. Mode selection is transparent to the host.

Pin assignments for the module are listed in Table 2 (for the SD mode). The contact pins, connected to the internal bond wires, can be mapped into the five FIPS 140-2 logical interfaces. The following is a list of the FIPS 140-2 logical interfaces implemented in the module:

1. Data Input
2. Data Output
3. Control Input
4. Status Output

The rightmost columns of Table 2 map the physical interface of the module to the FIPS 140-2 interfaces.

Table 2 – Physical and FIPS 140-2 Interface Mappings for SD Mode

Pin	Name	Bond Wire Pin Assignment	FIPS 140-2 Interface
1	DAT2	Data line [bit 2]	Data input, data output
2	CD/DAT3	Card detect/Data line [bit 3]	Data input, data output
3	CMD	Command response	Control input, status output
4	VDD	Supply voltage	Power
5	CLK	Clock	Control input
6	VSS	Supply voltage ground	Power
7	DAT0	Data line [bit 0]	Data input, data output
8	DAT1	Data line [bit 1]	Data input, data output

All data is passed to the cryptographic module using standard write and read commands to a buffer. Therefore, from the host's point of view, sending a command means writing data to a special file on the memory device, which is used as the buffer file. Getting information from the module is done via reading data from the buffer file.

2.3 Roles and Services

The module supports two roles: a Crypto-Officer role and a User role. A Crypto-Officer as an operator can log into the system Access Control Records (ACRs) and/or root ACR Group (AGP) that can access all services. Any entity attempting to use the TrustedFlash commands is required to login to the TrustedFlash system through an ACR. An ACR can be considered a user account. Different ACRs may share common interests and privileges within the system, such as secured domains from which to read and write data. ACRs with attributes in common are grouped in ACR groups called AGPs. AGPs and the ACRs are organized in hierarchical trees. The AGP tree structure enables the module to handle multiple applications. This is where each application comprises a collection of identifiable entities represented as an ACR on the tree. Mutual exclusion between the applications is achieved by ensuring there is no cross-talk or cross-communication between the tree branches.

A tree of the Approved mode is a tree with the root AGP configured with the authentication and key establishment method defined as one of the FIPS-Approved schemes shown in Table 7. New ACRs created on a tree of the Approved mode are also working in the Approved mode because the "Tree Authentication Restrictions" command has been executed to the tree during the tree creation process. See Section 3 "Secure Operation" of this document for more information.

Non-Approved mode trees are not supported when the module has been configured to operate in the Approved mode of operation. After FIPS-Approved trees are created and configured according to security policy instructions, the module must then be locked to prevent any additional trees from being created. The procedures to create trees and to lock the card can be found below in Section 3 "Secure Operation" of this document.

All services of the module are provided via TrustedFlash commands. The TrustedFlash commands are passed to the module using standard SD Write and Read commands. Therefore, from the host point of view, sending a TrustedFlash command means writing data to a special file on the memory device used as the buffer file. Getting

information from the module is done via reading data from the buffer file. Generally speaking, TrustedFlash commands are sent and received using SD messages as depicted in Figure 3 – Sample SSA Command Using Trailing Dummy Sectors. SSA means Security Storage Application.

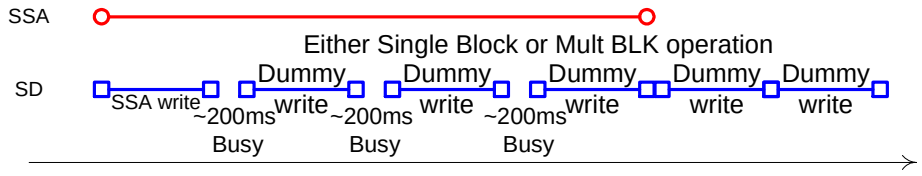

Figure 3 – Sample SSA Command Using Trailing Dummy Sectors

In order to access the encrypted contents of the module, the Crypto-Officer or User has to authenticate to ACRs. Appropriate TrustedFlash commands have to be sent to the module in order to access desired encrypted contents. See [5] for details.

2.3.1 Authentication

The module identifies individual operators using ACR identifiers as described in the previous section. The module authenticates individual operators using the authentication mechanism that has been configured for the ACR or AGP that the operator is attempting to log into, also as described in the previous section. A tree configured to the Approved mode of operation supports one of the following four authentication schemes.

1. One-way symmetric authentication. The module and the host own the same symmetric key, which is used to authenticate the host to the module. An optional Personal Identification Number (PIN) can be configured for use in this scheme.

2. Two-way symmetric authentication. The module and the host own the same symmetric key, which is used for mutual authentication. An optional PIN can be configured for use in this scheme.

3. One-way asymmetric authentication. The host presents its certificate to the module for authentication. The module has the host's root certificate and uses it to verify the signature on host's certificate. The module builds and verifies certificate paths using provided certificates. An optional PIN can be configured for use in this scheme.

4. Two-way asymmetric authentication. The host and the module present their certificates to each other for mutual authentication. The host and the module have each other's root certificate for signature verification. The module builds and verifies certificate paths using provided certificates. An optional PIN can be configured for use in this scheme.

While a TrustedFlash command is in progress, no other SD commands will be send by the Host, that the host application needs to lock device driver for duration of every TrustedFlash command in order to be able to communicate with the card, and that TrustedFlash commands need trailing dummy sectors, i.e. SD dummy writes performed after the SSA write. 200ms is required between SD writes, so assuming even just one dummy write, it would take 400ms for the host to send one command to the card. Since there will always be at least two commands, one to attempt to login, and one to determine if the operation was successful, one login attempt will take 800ms. If each attempt takes about one second, only roughly 75 attempts can be made in a one-minute period. Since the probability that a single random attempt will succeed is 1 in 2^{80}, which is less than 1 in 10^6, since the weakest authentication schemes provide 80 bits of security, the probability that during a 1 minute period a random attempt will succeed is 75 in 2^{80}, which is less than 1 in 10^5.

2.3.2 Crypto-Officer Role

Table 3 shows the services for the Crypto-Officer role[1]. For details of the commands please refer to Section 4 of [5]. The purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). CSP stands for Critical Security Parameter. User services defined in Table 5 are also available to a Crypto-Officer. Certain TrustedFlash commands can be called by Users if the ACR that they log into has been configured by a Crypto-Officer with the necessary permission. There are two types of permissions: ACR Management (ACAM) permissions and Domain permissions. See [5] for additional information about the Crypto-Officer services listed in the table below, including whether or not Crypto-Officers can grant a corresponding ACAM or Domain permission that would allow a User to execute the command.

Table 3 – Crypto-Officer Services

Service	Description	Input	Output	Keys/CSPs and Type of Access
Password Credentials	Provides password protection for an ACR requiring a password during login	Tree name, AGP name, ACR name, password, command	Status	Password – read
Symmetric Credentials	Provides symmetric cryptography protection for an ACR requiring a symmetric key during login	Tree name, AGP name, ACR name, key type, key, command	Status	Symmetric key – read
Import RSA key pair	Imports RSA key pair from the host application to the module for asymmetric authentication	Tree name, AGP name, ACR name, Distinguished Encoding Rules (DER) structure size, DER structure, command	Status	RSA key pair – write
Import Certificate	Adds certificate credentials during ACR creation	Tree name, AGP name, ACR name, certificate size, certificate type, certificate, command	Status	RSA public key – write
Generate RSA key pair	Generates an RSA key pair	Tree name, AGP name, ACR name, RSA key size, command	RSA key pair, status	RSA key pair – write
Root AGP Creation Done	Locks the root AGP so no additional ACRs may be created	Tree name, command	Status	None
Disable System ACR Creation	Disables the create system ACR feature	Command	Status	None
Set Root AGP Creation Mode	Configures the root AGP creation mode setting	One of following modes: open, controlled, locked, command	Status	None
Disable Root AGP Change Mode	Disables the change root AGP creation feature	Command	Status	None
Restrict Tree Authentication Capabilities	Defines which authentication algorithms are restricted for use for all ACRs which belong to the Tree	A 4-byte value indicating which algorithms are allowed, command	Status	None

[1] The module enables access to the public partition through standard SD read and write commands or through the use of TrustedFlash commands. The module enables ACRs to create domains within the public partition and encrypt individual files. Accessing encrypted files within the public partition, as well as setting the access rights to the partitions, is accomplished using TrustedFlash system commands.

Service	Description	Input	Output	Keys/CSPs and Type of Access
Create ACR	Creates ACRs and AGPs	AGP name, ACR name, authentication algorithm, unblocked ACR name, management permissions, maximum number of consecutive authentication failures allowed, command	Status	Password, Symmetric key, RSA public key – write
Create ACR Done	Activates an ACR. The new ACR must be a new (child) ACR of the AGP that the requesting ACR resides within. If a new ACR is created, it will be created as a child of the AGP that the requesting ACR resides within	Tree name, AGP name, ACR name, command	Status	None
Delete ACR	Deletes an ACR. Only sent by a creator ACR to delete a new (child) ACR it has created	Tree name, AGP name, ACR name, command	Status	Password, Symmetric key, RSA public key – delete
Unblock ACR	Unblocks a specific ACR. Only sent by an ACR that has explicit permission to unblock a specific ACR	Tree name, AGP name, ACR name, command	Status	None
Create Partition	Creates a partition. Only sent by an ACR residing in a root AGP	New partition name, new partition size, decreased partition name, command	Status	None
Update Partition	Only sent by an ACR residing in a root AGP. The command is limited to the repartition of two adjacent partitions only	First partition name, new partition size, second partition name, command	Status	None
Delete Partition	Deletes a partition. Only sent by an ACR residing in a root AGP	Deleted Partition Name, Increased partition name, command	Status	None
Restrict Public Partition Access	Restricts the regular read and write commands to and from the public partition, which is also known as the user area. This restriction applies to read and write commands sent by the host and are not part of the TrustedFlash command protocol	Restriction Code: one of the following restrictions: write, read, read_write, command	Status	None
Create Domain	Executes the Create Domain command only if it has the permission granted by ACAM_CREATE_DOMAIN	Domain name, domain encryption type, source for domain Content Encryption Key (CEK), application identification (ID), domain CEK, command	Status	Symmetric key - write
Delete Domain	Only a domain owner may send the Delete Domain command to delete a domain	Domain name, command	Status	None
Export Domain Key	Exports a domain key from the module to a host	Domain name, application ID, command	128-bit AES Domain CEK, status	Symmetric key - read
Delegate Domain Permissions	Delegates Domain Permissions	Domain name, tree name, AGP name, ACR name, permission type, command	Status	None
Delegate Partition Permissions	Delegates Partition Permissions	Partition name, tree name, AGP name, ACR name, permission type, command	Status	None

Service	Description	Input	Output	Keys/CSPs and Type of Access
Retract Domain Permissions	Retracts Domain Permissions	Domain name, tree name, AGP name, ACR name, permission type, command	Status	None
Retract Partition Permissions	Retracts Partition Permissions	Partition name, tree name, AGP name, ACR name, permission type	Status	None
System Login	Issued when a host attempts to use the module through one of the ACRs. The command starts the login/authentication process	Tree name, AGP name, ACR name, command	Status	None
ACR Query	Reads TrustedFlash information that is within the scope of the currently logged-in ACR	Query type, group index, command	Session ID, group index, number of objects in the list, maximum number of objects in sector, object list, status.	None
Open Stream	Sets up the module for data stream transfers to read or write data. This command will determine the characteristics of the data stream, and whether to read or write data with or without domain information along with other required data	Partition name, flash storage domain name, stream direction, transfer type, command	Tree name, AGP name, ACR name, error, stream ID, status, status.	None
Close Stream	Closes a stream	Stream ID, command	Status	None
Change ACR Name	In the case of a root ACR name change, the root ACR must be logged-in and the name change accomplished through the root ACR session. However, when a regular ACR name warrants a change, it must be made only by the creator (father) ACR	Tree name, AGP name, Old ACR name, New ACR name, command	Status	None
System Query	Outputs general module information such as version support and current configuration regarding the visible Root ACRs and TrustedFlash applications	Query type, group index, command	TrustedFlash version number, Command size, number of objects in the list, maximum number of objects in sector, object list, status.	None
Send Password to TrustedFlash Card	Sends the actual ACR password to be verified by the TrustedFlash system located on the memory card. After sending the Command Status command, the host will be able to read the command status. Upon command completion, the host will also be able to read the PASS/FAIL status of the authentication process	Password, command	Pass/Fail, status.	Password - read

Service	Description	Input	Output	Keys/CSPs and Type of Access
Get Challenge from TrustedFlash Card	Acquires a symmetric challenge from the card	Command	Symmetric challenge, status.	None
Send Challenge to TrustedFlash Card	Sends the host challenge to the card	Symmetric challenge, command	Status	None
Get Challenge Response from TrustedFlash Card	Acquires card's response to the host challenge	Command	Card response, status.	None
Send Challenge Response from TrustedFlash Card	Sends the host response to the card challenge	Host response, command	Status	None
Get TrustedFlash Pre-Master Secret	A step in the symmetric authentication protocol. This command reads the random number generated for the session key by the module	Command	Pre-Master secret, status	None
Send Host Pre-Master Secret to TrustedFlash Card	A step in the symmetric authentication protocol. This command sends the random number generated for the session key by the host	Symmetric challenge, command	Status	ACR Symmetric Credential – read
Send Start Session Message	Send "Start Session" string to host	"Start Session" string, PIN, command	Status	PIN – read
Get Authentication Complete Message	Get "Authentication Complete" phrase from host	Command	"Authenticati on Complete" phrase, ACR PIN, status	PIN – read
Get Asymmetric Device Public Key	Exports the ACR public key	Command	"E" and "N" values of the RSA public key, key size, status	RSA public key – read
Set Asymmetric Host Public Key	Sends the host/application public key to the module	RSA public key, key size, command	Status	RSA public key – write
Set Asymmetric Host Random Challenge	Sends the host/application challenge number to module for signing with the ACRs private key	RSA key size, random challenge, command	Status	None
Verify Asymmetric Device Public Key	Commands the host/application to read the module signed challenge to verify the ACR's public key	Command	Signed random challenge, status	RSA private key – read
Get Asymmetric Device Random Challenge	Commands the host/application to read the module challenge that will be signed with its private key	Command	RSA key size, random challenge, status	None

Service	Description	Input	Output	Keys/CSPs and Type of Access
Verify Host Public Key	Host/application signs the module challenge data and returns it to the module for verification	RSA key size, signed challenge, command	Pass/Fail, status	RSA public key – read
Set Asymmetric Host Secret Number	The host/application sends the module a number signed by the host private key	RSA key size, host secret number, command	Status	None
Get Asymmetric Device Secret Number	The module sends a number signed by its private key to the host/application	Command	RSA key size, ACR generated secret number, status	RSA private key – read
Set Host Certificate Chain	The host sends a certificate chain to the TrustedFlash card. The certificate buffer will follow the command sector	Certificate size, if this certificate is the last in the chain, certificates revoke list size, command	Status	None
Get Device Certificate Chain	The host reads the TrustedFlash card certificate chain	Certificate size, if this certificate is the last in the chain, command	Status	None
Change Password	Changes an ACR's password	Tree name, AGP name, ACR name, old password, new password, command	Status	Password – delete, write
Change Symmetric Key	Changes an ACR's symmetric key	Tree name, AGP name, ACR name, symmetric key type, symmetric key, command	Status	Symmetric key – delete, write
Get Zeroizing Entity	Returns the name of the Zeroizing entity	Command	Entity name	None
Set Zeroizing Entity	Sets the name of the Zeroizing entity to the System ACR	Zeroizing entity name	Status	None
Zeroize TrustedFlash System	Zeroizes the System ACR and all ACRs (and their objects) in the system	Command	Status	Zeroize
Write	Evokes a write transfer stream from the module to the host/device-application. Data is sent after a write-stream has been opened	Stream ID, start Logical Block Address (LBA), sector count, data buffer pointer, command	Status	Session key – read
Read	Evokes a read transfer stream from the module to the host/device-application. Data is sent after a read-stream has been opened	Stream ID, start LBA, sector count, data buffer pointer, command	Status	Session key – read
Write Public Partition	Write data to the public partition	Command	Status	None
Read Public Partition	Read data from the public partition	Command	Status	None

2.3.3 User Role

Table 5 shows the services for the User role. Similar to Table 3, the purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). The only services defined for the User role are to logs in/out the module and obtain command status. For details of the commands please refer to Section 4 of [5].

Table 4 – User Services

Service	Description	Input	Output	Keys/CSP and Type of Access
System Login	Issued when a host attempts to use the module through one of the ACRs. The command starts the login/authentication process.	Tree name, AGP name, ACR name, command.	Status	None
Get Login Status	After sending the system login command, the host/device application is required to send the Get Login Status command and receive the status of the login process along with the session ID. This command must follow the ACR login command to proceed with the login sequence. If the host fails to send this command after the ACR login command the login sequence will fail and the host will need to restart it.	Tree name, AGP name, ACR name, command	Tree name, AGP name, ACR name, ACR login status, error code, session ID, status	None
System Logout	Issued when a host attempts to terminate a session. The command ends all activities in the session. After this command is issued, the host must restart the login process in order to be able to execute further actions with the module.	Command	Status	None
Additional TrustedFlash commands	1. TrustedFlash commands that require ACAM permissions 2. TrustedFlash commands that require Domain permissions	Command	Status	See Crypto-Officer role service descriptions

2.3.4 Unauthenticated Services

The services listed in Table 5 – Unauthenticated Services are not authenticated and are not specific to either Crypto-Officer or User role.

Table 5 – Unauthenticated Services

Service	Description	Input	Output	Keys/CSP and Type of Access
Vendor Query	Enables the host to request vendor or product information about the card that is housing the TrustedFlash system	Command	Vendor specific data, status	None
Command Status	Sent to the system to prompt a return status message from the previously sent command.	Command	Last command, session ID, command status, ACR login status, application specific status, tree authentication capability, status.	Session key – read
Get Login Status	After sending the system login command, the host/device application is required to send the Get Login Status command and receive the status of the login process along with the session ID. This command must follow the ACR login command to proceed with the login sequence. If the host fails to send this command after the ACR login command the login sequence will fail and the host will need to restart it	Tree name, AGP name, ACR name, command	Tree name, AGP name, ACR name, ACR login status, error code, session ID, status	None

Service	Description	Input	Output	Keys/CSP and Type of Access
SD Commands	SD write and read commands used to send TrustedFlash commands from the host to the card or access public partitions.	See [4]	See [4]	None
SPI Commands	SPI write and read commands used to send TrustedFlash commands from the host to the card or access public partitions..	See [4]	See [4]	None

2.4 Physical Security

The TrustedFlash v1.0 – microSD cards are multi-chip embedded modules that use a tamper-evident enclosure as a physical security mechanism. The enclosure uses a tamper-evident epoxy covering and a tamper-evident microSD plastic enclosure as physical security mechanisms. All card models are constructed identically in terms of locations of types of components, including physical security mechanisms.

There are two chips that are covered on one side by epoxy and on the other by substrate. A non-removable, tamper evident plastic cover that is compatible with microSD card readers surrounds the substrate underneath the chips and the epoxy on top of the chips. The plastic cover exposes two sets of contact pins. One set of contact pins is covered by epoxy. There are two separate epoxy coverings in other words.

The epoxy that covers the otherwise exposed contact pins surrounds the pins. The plastic cover cannot be removed without damaging the epoxy that covers the otherwise exposed contact pins. The epoxy that covers the otherwise exposed contact pins must be inspected periodically to ensure that physical security is maintained.

- The plastic cover on the same side as the covered pins must also be inspected periodically to determine if there is visible evidence of tampering or if the substrate underneath the two chips has been exposed to ensure that physical security is maintained.
- The plastic cover on the opposite side must also be inspected periodically to determine if there is visible evidence of tampering or if the epoxy covering the top of the two chips has been exposed to ensure that physical security is maintained.

All card modules have been tested for and meets applicable Federal Communications Commission (FCC) EMI and EMC requirements for home use as defined in Subpart B of FCC Part 15.

2.5 Operational Environment

The operational environment of the module is non-modifiable. The firmware included in the module cannot be upgraded or modified after the card leaves the factory. The module is capable of executing only certain commands from host applications. The command set is stored within the module and cannot be modified. The FIPS 140-2 requirements for operational environment are not applicable to the TrustedFlash v1.0 – microSD.

2.6 Cryptographic Key Management

The module implements the following Approved cryptographic algorithms:

- Advanced Encryption Standard (AES) – 128-bit, Cipher-Block Chaining (CBC), and Electronic Codebook (ECB) modes (Certificate #643)
- Triple Data Encryption Standard (Triple-DES) – 112- and 168-bits, CBC and ECB modes (Certificate #595)
- RSA Public Key Cryptography Standards (PKCS) #1 v2.1 and v1.5 signature generation/verification – 1024- and 2048-bit (Certificate #294)
- Secure Hash Algorithm -1 (SHA-1) (Certificate #678)

- American National Standards Institute (ANSI) X9.31 Appendix A.2.4 Random Number Generator (RNG) with 128-bit AES (Certificate #366)

The module implements the following non-Approved cryptographic algorithms:

- DES
- A non-Approved RNG for seeding the ANSI X9.31 Appendix A.2.4 RNG
- RSA PKCS#1 v2.1 and v1.5 (key wrapping; key establishment methodology provides 80 bits or 112 bits of encryption strength; non-compliant less than 80 bits of encryption strength)
- AES CBC MAC (used in firmware integrity test)

The following table gives a list all cryptographic keys, cryptographic key components, and CSPs used by the module in the Approved mode of operation.

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/ Key Component	Type	Generation / Input	Output	Storage	Zeroization	Use
Secret CryptoKey	AES symmetric key (128 bits)	Generated and installed during manufacturing	No	Plaintext in non-volatile memory on controller chip	Not zeroized	Compute AES CBC MAC for firmware integrity test Not a CSP of the module
CEK	AES symmetric key (128 bits)	1. During ACR creation, input from host in ciphertext encrypted with session key 2. Generated internally by ANSI X9.31 Appendix A.2.4 RNG	Ciphertext encrypted with session key	Plaintext in flash memory	By "Zeroize TrustedFlash System" command	Encrypt a domain on the flash memory
ACR Symmetric Credential	AES/Triple-DES symmetric keys	During ACR creation, input from host in ciphertext encrypted with session key	No	Plaintext in flash memory	By "Zeroize TrustedFlash System" command	Authentication
ACR Asymmetric Credential	RSA key pair	1. During ACR creation, input from host in ciphertext encrypted with session key 2. Generated internally by ANSI X9.31 Appendix A.2.4 RNG	RSA public key is output in plaintext or ciphertext encrypted with session key	Plaintext in flash memory	By "Zeroize TrustedFlash System" command	Authentication

Key/ Key Component	Type	Generation / Input	Output	Storage	Zeroization	Use
PIN	User PIN for two-factor authentication	1. During ACR creation, input from host in ciphertext 2. During authentication, input from host in ciphertext encrypted by Session Key	No	Plaintext in flash memory	By "Zeroize TrustedFlash System" command	Two-factor authentication
Session Key	AES/Triple-DES symmetric keys	1. Generated internally by ANSI RNG[2] 2. Input from host in encrypted form using the ACR Credential[3]	1. RSA-encryption form[2] 2. Not output[3]	Plaintext in volatile memory	When session is over	Encrypt/decrypt session transmissions between host and card
ANSI X9.31 Appendix A.2.4 RNG seed	RNG seed (128 bits)	Generated internally by a hardware RNG	No	Plaintext in volatile memory	When a random number is generated by ANSI X9.31 Appendix A.2.4 RNG	Initialize ANSI X9.31 Appendix A.2.4 RNG
ANSI X9.31 Appendix A.2.4 RNG seed key	AES key (128 bits)	Generated internally by a hardware RNG	No	Plaintext in volatile memory	When a random number is generated by ANSI X9.31 Appendix A.2.4 RNG	Initialize ANSI X9.31 Appendix A.2.4 RNG

2.6.1 Key Generation

The module uses ANSI X9.31 Appendix A.2.4 RNG to generate cryptographic keys. This RNG is Approved as indicated by Annex C to FIPS PUB 140-2. The seeds of the ANSI X9.31 Appendix A.2.4 RNG are provided by a non-Approved hardware RNG, which collects system contexts from the card. This non-Approved hardware RNG is implemented in hardware and does not have an external interface.

2.6.2 Key Input/Output

Host RSA public keys can be imported in plaintext. The module's RSA public key can be exported to the host in plaintext. CEKs are input into or output from the card ciphertext encrypted with session keys. ACR credentials are input into the card in ciphertext encrypted with session keys. Other keys and CSPs are not input into or output from the module.

2.6.3 Key Storage

There exists a special section of the flash memory called the Security Storage (SST). The SST is used for the storage of security-critical information such as user and device key-pairs, permanent symmetric keys, configuration

[2] For the one-way asymmetric authentication.
[3] For the one-way symmetric authentication, two-way symmetric authentication, and the two-way asymmetric authentication schemes.

information, PINs, root certificates, and a key table used to support the secure application data storage areas on the flash memory.

2.6.4 Key Zeroization

A session key between the host and the module is stored only in the volatile memory and is zeroized when the session is over or when it is closed. The symmetric, asymmetric, or password credentials of an ACR are zeroized when their associated ACR is deleted. All key information of an ACR is AES-encrypted with a CEK. CEKs are stored in the SST. A CEK is zeroized when the domain it encrypts is deleted. The "Delete ACR" command, when called by the Crypto-Officer to delete the last ACR in the root AGP, will immediately zeroize all FIPS-Approved tree CEKs and ACR CSPs (keys, certificates, PINs) and associated encrypted content. Authorized Crypto-Officers can also use the "Zeroize System ACR" command, which will zeroize the System ACR and all other ACRs in the system.

The Secret CryptoKey is not zeroized; however, physically destroying the card will effectively render the Secret CryptoKey unusable. See Section 3.6 of this document for details about key zeroization.

2.7 Self-Tests

The card performs a firmware integrity self-test at power-up. The integrity self-test uses the 128-bit AES CBC Message Authentication Code (MAC) algorithm. The signing operation was done during manufacturing.

The card performs the following cryptographic algorithm self-tests during power-up:

- Known Answer Test (KAT) on Triple-DES.
- KAT on AES.
- KAT on SHA-1 (this test is performed as part of the RSA signature generation/verification KAT).
- KAT on RSA encryption/decryption.
- KAT on RSA signature generation/verification.
- KAT on ANSI X9.31 Appendix A.2.4 RNG.

Conditional self-tests are performed when an applicable security function or operation is invoked. The module implements three conditional self-tests.

- Pair-wise consistency test for RSA keys.
- Continuous RNG test for the non-Approved RNG that seeds the ANSI X9.31 Appendix A.2.4 RNG.
- Continuous RNG test for the ANSI X9.31 Appendix A.2.4 RNG.

If the power-up integrity self-test fails, neither SD/SPI commands nor TrustedFlash commands are accepted by the card. If either a power-up cryptographic algorithm KAT or conditional self-test fails, no TrustedFlash are accepted by the card, with the following exceptions:

1. "Get Login Status" command
2. "Command Status" command
3. "Vendor Query" command

See Section 3.5 of this document for more information about how to identify FIPS self-test errors.

3 Secure Operation

The TrustedFlash v1.0 – microSD cards meet Level 3 requirements of FIPS 140-2. The sections below describe how to install and configure cards such that they operate in the Approved mode of operation.

3.1 Initial Setup

Setup described in Sections 3.1.2, 3.1.3, and 3.1.4 are required by either the Crypto-Officer or the User each time the card is used, regardless of Crypto-Officer configuration.

3.1.1 Secure Delivery

The operator is not authenticated upon accessing the module for the first time. Secure delivery procedures are relied on to control access to the module before it is accessed by an operator for the first time. Trusted couriers are relied on to maintain the security of the module when distributing it to a Crypto-Officer's site.

3.1.2 Installing the Card Reader and Drivers

The module is accessed by what is called a "Host Controller" in SD terminology. Host Controller refers to either a computer or device that is interoperable with [4]. Host Controllers access the module using Host Drivers (OS-specific drivers for Host Controllers) and Card Drivers (OS drivers for the module). The module is compatible with microSD readers that are interoperable with [3].

3.1.3 Configuring the Card Reader and Drivers

All card models are accessed using compatible drivers and calling applications. Configuration of drivers and calling applications should be according instructions provided with compatible drivers and calling applications. Drivers and calling applications must be configured to support the following card requirements:

- Voltage: 2.6 – 2.7 V or 1.65 – 1.95 V (requires a special Field-Programmable Gate Array (FPGA) for the low range)
- Timeout: Initialization: 0 – 0xFFFF milliseconds. Write: 0 – 300,000 milliseconds. 0 means infinite.

3.1.4 Installing the Card in a Card Reader

All card models must be physically installed into a compatible card reader in order to access card services. Cards may be first installed into compatible adapters to support a wider range of card reader types.

3.2 Module Initialization and Configuration

All card models require initial setup by the Crypto-Officer. Each time cards are accessed after they have been installed into a reader, either a SD or SPI session must first be established before sending TrustedFlash commands to the card, regardless of whether Crypto-Officers or Users are accessing the cards as depicted in Figure 4 – Crypto-Officer and User Operation. See Section 3 of [5] for details.

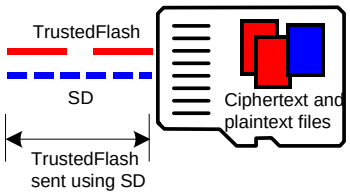

Figure 4 – Crypto-Officer and User Operation

At the first time the card is used, the Crypto-Officer should send TrustedFlash commands to the card to create the system ACR and to configure access to the public partition. The first ACR created is the system ACR. The system ACR can be created by executing the "Create ACR" command. Several parameters, including Tree name, AGP name, ACR name, and login algorithm need to be configured for the "Create ACR" command. The system ACR is not removable or reconfigurable.

3.3 Creating Trees that are Configured to Operate in an Approved Mode

Trees are configured as part of their creation using TrustedFlash commands. Trees (root AGPs) can only be created by Crypto-Officers during the card's initial secure installation and configuration. See also Section 2.3 for a description of permission mechanisms.

3.3.1 Sending TrustedFlash Commands to the Card to Create One or More Root AGPs

Section 3 of [5] gives detailed procedures of communicating with the module via standard SD interface and commands. The Crypto-Officer is able to create trees of either the Approved mode or the non-Approved mode. The following step-by-step instructions provide details of creating a tree in an Approved mode. See section 2.3.1 of this document for a list of the authentication configurations that are supported in the Approved mode of operation.

1. Creating the first root ACRs of the targeted tree by executing the "Create ACR" command. In the "Create ACR" command, the Crypto-Officer should set the AUTH_ALGORITHM argument to one of the values that represent FIPS-Approved login algorithms, which are marked with "Y" in the leftmost column of Table 7.

Table 7 – ACR Login Algorithms

FIPS	Symbol	Value	Description
N	NONE	0	No authentication is required. The session is opened as soon as the "System Login" command is issued for this ACR.
N	PASSWORD	0x1	Password based authentication
Y	AES_HOST_AUTH	0x2	One-way symmetric authentication using AES. Card is authenticating the user.
Y	AES_HOST_AUTH_SEC	0x82	One-way symmetric authentication using AES. Card is authenticating the user. Secure channel is established and used for this ACR.
Y	AES_HOST_AUTH_SEC_PIN	0xC2	One-way symmetric authentication using AES. Card authenticates the user. Secure channel is established and used for this ACR. Authentication is completed after an additional PIN is provided.
Y	AES_MUTUAL_AUTH	0x22	Two-way symmetric authentication using AES. Card and host authenticate each other.
Y	AES_MUTUAL_AUTH_SEC	0xA2	Two-way symmetric authentication using AES. Card and host authenticate each other. Secure channel is established and used for this ACR.
Y	AES_MUTUAL_AUTH_SEC_PIN	0xE2	A two-factor authentication using AES. Card and host authenticate each other. Secure channel is established and used for this ACR. Authentication is complete after an additional PIN is provided.
N	DES_HOST_AUTH	0x3	One-way symmetric authentication using DES. Card is authenticating the user.
N	DES_HOST_AUTH_SEC	0x83	One-way symmetric authentication using DES. Card is authenticating the user. Secure channel is established and used for this ACR.

FIPS	Symbol	Value	Description
N	DES_HOST_AUTH_SEC_PIN	0xC3	One-way symmetric authentication using DES. Card authenticates the user. Secure channel is established and used for this ACR. Authentication is completed after an additional PIN is provided.
N	DES_MUTUAL_AUTH	0x23	Two-way symmetric authentication using DES. Card and host authenticate each other.
N	DES_MUTUAL_AUTH_SEC	0xA3	Two-way symmetric authentication using DES. Card and host authenticate each other. Secure channel is established and used for this ACR.
N	DES_MUTUAL_AUTH_SEC_PIN	0xE3	A two-factor authentication using DES. Card and host authenticate each other. Secure channel is established and used for this ACR. Authentication is complete after an additional PIN is provided.
Y	Triple-DES_K2_HOST_ AUTH	0x4	One-way symmetric authentication using 2-key Triple-DES. Card is authenticating the user.
Y	Triple-DES_K2_HOST_ AUTH_SEC	0x84	One-way symmetric authentication using 2-key Triple-DES. Card is authenticating the user. Secure channel is established and used for this ACR.
Y	Triple-DES_K2_HOST_ AUTH_SEC_PIN	0xC4	One-way symmetric authentication using 2-key Triple-DES. Card authenticates the user. Secure channel is established and used for this ACR. Authentication is completed after an additional PIN is provided.
Y	Triple-DES_K2_ MUTUAL_AUTH	0x24	Two-way symmetric authentication using 2-key Triple-DES. Card and host authenticate each other.
Y	Triple-DES_K2_ MUTUAL_AUTH_SEC	0xA4	Two-way symmetric authentication using 2-key Triple-DES. Card and host authenticate each other. Secure channel is established and used for this ACR.
Y	Triple-DES_K2_ MUTUAL_AUTH_SEC_PIN	0xE4	A two-factor authentication using 2-key Triple-DES. Card and host authenticate each other. Secure channel is established and used for this ACR. Authentication is complete after an additional PIN is provided.
Y	Triple-DES_K3_HOST_ AUTH	0x5	One-way symmetric authentication using 3-key Triple-DES. Card is authenticating the user.
Y	Triple-DES_K3_HOST_ AUTH_SEC	0x85	One-way symmetric authentication using 3-key Triple-DES. Card is authenticating the user. Secure channel is established and used for this ACR.
Y	Triple-DES_K3_HOST_ AUTH_SEC_PIN	0xC5	One-way symmetric authentication using 3-key Triple-DES. Card authenticates the user. Secure channel is established and used for this ACR. Authentication is completed after an additional PIN is provided.
Y	Triple-DES_K3_ MUTUAL_AUTH	0x25	Two-way symmetric authentication using 3-key Triple-DES. Card and host authenticate each other.
Y	Triple-DES_K3_ MUTUAL_AUTH_SEC	0xA5	Two-way symmetric authentication using 3-key Triple-DES. Card and host authenticate each other. Secure channel is established and used for this ACR.
Y	Triple-DES_K3_ MUTUAL_AUTH_SEC_PIN	0xE5	A two-factor authentication using 3-key Triple-DES. Card and host authenticate each other. Secure channel is established and used for this ACR. Authentication is complete after an additional PIN is provided.
N	RSA_PRIM_MUTUAL_AUTH	0x06	Two-way asymmetric RSA primitives key exchange method.

FIPS	Symbol	Value	Description
Y	RSA_V15_HOST_AUTH	0x66	PKCS#1_V1.5 One-way asymmetric authentication, TrustedFlash authenticates the user, using public key. Asymmetric authentication always uses a secure channel.
Y	RSA_V21_HOST_AUTH	0xA6	PKCS#1_V2.1 One-way asymmetric authentication, TrustedFlash authenticates the user, using public key. Asymmetric authentication always uses a secure channel.
Y	RSA_V15_HOST_AUTH_PIN	0x76	PKCS#1_V1.5 One-way asymmetric authentication, TrustedFlash authenticates the user, using public key. Asymmetric authentication always uses a secure channel with PIN option.
Y	RSA_V21_HOST_AUTH_PIN	0xB6	PKCS#1_V2.1 One-way asymmetric authentication, TrustedFlash authenticates the user, using public key. Asymmetric authentication always uses a secure channel with PIN option.
Y	RSA_V15_MUTUAL_AUTH	0x46	PKCS#1_V1.5 Two-way asymmetric RSA authentication method.
Y	RSA_V21_MUTUAL_AUTH	0x86	PKCS#1_V2.1 Two-way asymmetric RSA authentication method.
Y	RSA_V15_MUTUAL_AUTH_PIN	0x56	PKCS#1_V1.5 Two-way asymmetric RSA authentication method with PIN option.
Y	RSA_V21_MUTUAL_AUTH_PIN	0x96	PKCS#1_V2.1 Two-way asymmetric RSA authentication method with PIN option.

2. Restricting the algorithms that are allowed in the targeted tree by executing the "Restrict Tree Authentication Capabilities" command. The command specifies a tree and the authentication limitations applied to the tree. This command accepts a four-byte Tree Authentication Capability bitmask as an argument (see Table 8 for a breakdown of the bitmask). It is possible to restrict a combination of several algorithms by calculating a binary OR among the values in the second column.

Table 8 – Tree Authentication Capability Bitmask

FIPS	Symbol	Value	Description
N	Enable all	0x00	None of the algorithms are disabled in the AGP
N	None	0x01	An ACR with no credentials is disabled for the AGP
N	Password	0x02	Password authentication is disabled for the AGP
N	DES 64	0x04	DES with key size of 64 bits is disabled for the AGP
Y	Triple-DES128	0x08	Triple-DES with key size of 128 bits is disabled for the AGP
Y	Triple-DES192	0x10	Triple-DES with key size of 192 bits is disabled for the AGP
Y	AES128	0x20	AES with key size of 128 bits is disabled for the AGP
N	RSA512	0x40	RSA with key size of up to 512 bits is disabled for the AGP
Y	RSA1024	0x80	RSA with key size of up to 1024 bits is disabled for the AGP
Y	RSA2048	0x100	RSA with key size of up to 2048 bits is disabled for the AGP
N	All other values	Reserved	Reserved modes for future use, must be disabled

Only Approved algorithms (Triple-DES128, Triple-DES192, AES128, RSA1024, and RSA2048) shall be used. For details of how to set the bitmask argument so that the ACR uses Approved algorithms, please refer to Section 4 of [5]. An ACR that is created in a FIPS-Approved tree employs only Approved cryptographic algorithms and authentication mechanisms. See Section 2.3.1 of this document for a list of the authentication configurations that are supported in the Approved mode of operation.

3. Executing the “Create ACR Done” command for the first root ACR.

A tree working in the Approved mode of operation has been created after the above three steps are successfully performed.

3.3.2 Sending TrustedFlash Commands to the Card to Prevent the Creation of New Trees

To prevent the creation of any additional trees, the card must be configured to operate in “Disabled mode” (also called “Locked mode”) using the following TrustedFlash commands:

1. Configure root ACR creation for disabled mode using the “Set Root AGP Creation Mode” command, setting the mode to “LOCKED” (no root AGP may be created).

2. Disable the method configuration command using the “Disable Root AGP Change Mode” command.

3.3.3 Sending TrustedFlash Commands to the Card to Create One or More Non-Root ACRs

To create an ACR on a tree working in the Approved mode of operation, in the “Create ACR” command, the Crypto-Officer shall set the AUTH_ALGORITHM argument to one of the values that represent Approved algorithms, which are marked with “Y” in the leftmost column of Table 7. Notice that setting the AUTH_ALGORITHM argument to values with marking “N” will result in error (TF_ERR_TREE_AUTH_RESTRICTION_CONFLICT) because the corresponding algorithms have been disabled by the “Restrict Tree Authentication Capabilities” command. Users are expected to protect their PINs, authentication credential, and exported CEKs.

3.4 FIPS Mode Status Indicator

Operators can determine whether or not a card is operating in the Approved mode by accessing the Tree Authentication Capabilities bitmask. This is a four-byte bitmask in which each bit identifies the specific algorithms used by the module. When operating in FIPS mode, the non-Approved algorithms will be disabled. Thus, when operating in FIPS mode, the Tree Authentication Capability bitmask will read:

“1000 0000 0000 0000 0000 0000 xx1x xx11”

The bit positions marked with an “x” represent each of the Approved algorithms supported. When least one of those designated bit positions is set to “0”, this indicates that the module is running in its Approved mode and that the corresponding algorithm is enabled. In all other cases, the module is not considered to be in an Approved state

Any operator can read the bitmask by calling the “Command Status” command.

3.5 Identifying the Error State

3.5.1 Identifying Power-up Integrity Self-Test Errors

Power-up integrity self-test errors are identified by attempting to send SD commands. When the power-up integrity self-test fails, neither SD/SPI commands nor TrustedFlash commands are accepted by the card. For example, a typical card initialization sequence consists of issuing SD commands CMD0, CMD55, ACMD41, CMD2, and then CMD3. When the power-up integrity self-test fails, none of these commands will receive a response from the card. For example, SD command responses generally include response tokens that include bits used as error indicators. When the power-up integrity self-test fails, not even response tokens are sent by the card.

3.5.2 Identifying Power-up Cryptographic Algorithm KAT Errors

Power-up cryptographic algorithm KAT errors are identified by TrustedFlash commands. The “Command Status” command must be used to figure out whether or not the card has entered its error state as the result of a power-up

cryptographic algorithm KAT error. When a power-up cryptographic algorithm KAT fails, error code 4121 will be returned.

3.5.3 Identifying Conditional Self-Test Errors

Conditional self-test errors are identified by TrustedFlash commands. The "Command Status" and "Get Login Status" commands must be used to figure out whether or not the card has entered its error state as the result of a conditional cryptographic algorithm self-test error. When a conditional self-test error occurs during login, specifically when a continuous random number generator test fails during key establishment, error code 4107 will be returned by the "Get Login Status" command. When a conditional self-test error occurs during card operation after login, error code 4121 will be returned by the "Command Status" command.

3.5.4 Recovering from FIPS Self-Test Errors

When a FIPS self-test error has occurred, the only way to attempt to recover is to reboot the module. This can be done by either cycling the power or sending a SD/SPI command (CMD0) to the card.

3.6 Module Zeroization

Zeroizing the card requires two steps. First use TrustedFlash commands, and then use physical force to destroy the module.

3.6.1 Zeroizing a Tree

All CSPs, including CEKs and authentication credentials of ACRs, involved in a tree can be zeroized by deleting the root AGP of the tree. Deleting the root AGP is done by deleting all ACRs (using the "Delete ACR" command) within the root AGP. Deleting an ACR zeroizes all CEKs and authentication credentials associate with the ACR and its child ACRs. Deleting a domain (using the "Delete Domain" command) zeroizes the CEK of the domain.

3.7 Command Reference and Communication Requirements

3.7.1 SD Command Compatibility

TrustedFlash commands are sent using lower-level SD/SPI commands. The module is interoperable with host controllers that are compliant with [1] and [2].

3.7.2 SD Command Usage

Instructions about how to send TrustedFlash commands to the module using SD commands can be found in Section 3 "Communicating with the SSA System" in [5].

3.7.3 TrustedFlash Command Reference

Instructions about TrustedFlash command structures can be found in Section 4 "The TrustedFlash Commands – Command Structure" in [5]. Instructions about how to use TrustedFlash commands can be found in Section 4 "The TrustedFlash Commands – Command Sequences" in [5]. Complete TrustedFlash command descriptions can be found in Section 4 "The TrustedFlash Commands – Detailed Command Description" in [5]. TrustedFlash command error code information can be found in Section 4 "The TrustedFlash Commands – Detailed Command Description – Command Status" and in Section 4 "The TrustedFlash Commands – Detailed Command Description – Get Login Status" in [5].

4 References

[1] SD Association, “Physical Layer Specification”, version 1.00

[2] SD Association, “File System Specification”, version 1.01

[3] SD Association, “microSD Addendum”, version 1.10

[4] SD Association, “Host Controller Specification”, version 1.0

[5] SanDisk Corporation, “TrustedFlash – SD Product Reference Spec”, revision 1.0

5 Acronyms

Table 9 – Acronyms

Acronym	Definition
ACAM	ACR Management
ACR	Access Control Record
AES	Advanced Encryption Standard
AGP	ACR Group
ANSI	American National Standards Institute
CBC	Cipher-Block Chaining
CEK	Content Encryption Key
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DRM	Digital Rights Management
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
ID	Identification
KAT	Known Answer Test
LBA	Logical Block Address
MAC	Message Authentication Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
OS	Operating System
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SD	Secure Digital
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface

Acronym	Definition
SSA	Security Storage Application
SST	Security Storage