JEDEC STANDARD

Embedded Multimediacard *(e*•MMC) Security Extension

JESD227

NOVEMBER 2016

JEDEC SOLID STATE TECHNOLOGY ASSOCIATION

NOTICE

JEDEC standards and publications contain material that has been prepared, reviewed, and approved through the JEDEC Board of Directors level and subsequently reviewed and approved by the JEDEC legal counsel.

JEDEC standards and publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for use by those other than JEDEC members, whether the standard is to be used either domestically or internationally.

JEDEC standards and publications are adopted without regard to whether or not their adoption may involve patents or articles, materials, or processes. By such action JEDEC does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the JEDEC standards or publications.

The information included in JEDEC standards and publications represents a sound approach to product specification and application, principally from the solid state device manufacturer viewpoint. Within the JEDEC organization there are procedures whereby a JEDEC standard or publication may be further processed and ultimately become an ANSI standard.

No claims to be in conformance with this standard may be made unless all requirements stated in the standard are met.

Inquiries, comments, and suggestions relative to the content of this JEDEC standard or publication should be addressed to JEDEC at the address below, or refer to www.jedec.org under Standards and Documents for alternative contact information.

Published by
©JEDEC Solid State Technology Association 2016
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

PRICE: Contact JEDEC

Printed in the U.S.A.

EMBEDDED MULTIMEDIACARD (*e*•MMC) SECURITY EXTENSION

Contents

Foreword

This *e*•MMC Security Extension Standard has been prepared by JEDEC as an extension to the *e*•MMC Electrical Standard, JESD84-B51.

Introduction

The *e*•MMC Electrical Standard, JESD84-B51, defines a managed memory device capable of storing code and data. *e*•MMC devices are intended to offer the performance and features required by mobile devices while maintaining low power consumption. The *e*•MMC device contains features that support high throughput for large data transfers and performance for small random data accesses more commonly found in code usage. It also contains many desirable features for mobile applications.

This *e*•MMC Security Extension Standard describes the requirements to implement security functionality described in [IEEE1667], [TCGCore], [TCGOpal], [TCGAddDST], [TCGAddDST] and [TCGSIIS] in an *e*•MMC device. The document is considered an extension of the *e*•MMC Electrical Standard, JESD84-B51, [*e*•MMC] used as transport protocol for the security functionalities.

There are three external sets of requirements on the class of *e*•MMC device that support this security extension: IEEE 1667 layer requirements, TCG layer requirements, and requirements related to *e*•MMC security data transport and interaction with *e*•MMC functionality.

EMBEDDED MULTIMEDIACARD (*e*•MMC) SECURITY EXTENSION

(From JEDEC Board Ballot JCB-12-59, formulated under the cognizance of the JC-64.1 Subcommittee on Electrical Specifications and Command Protocols.)

1 Scope

This document provides a comprehensive definition of the *e*•MMC Security requirements for implementation of IEEE 1667 and TCG Opal security functionality. It also provides design guidelines and defines a tool box of macro functions and algorithms intended to reduce design-in overhead.

2 Normative reference

The following normative documents contain provisions that, through reference in this text, constitute provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated. For undated references, the latest edition of the normative document referred to applies.

IEEE 1667 [IEEE1667], *IEEE P1667™ 2015 Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices.*.

Trusted Computing Group [TCGCore], *TCG Storage Architecture Core Specification*, Version 2.01, Revision 1.00

Trusted Computing Group [TCGOpal], *TCG Storage Security Subsystem Class: Opal Specification*, Version 2.01, Revision 1.00

Trusted Computing Group [TCGAddDST], *TCG Storage Opal SSC Feature Set: Additional DataStore Tables Specification*, Version 1.00, Revision 1.00

Trusted Computing Group [TCGSUM], *TCG Storage Opal SSC Feature Set: Single User Mode Specification*, Version 1.00, Revision 2.00

Trusted Computing Group [TCGSIIS], *TCG Storage Interface Interactions Specification (SIIS)*, Version 1.05, Revision 1.00

JEDEC JESD84-B51 [*e*•MMC], *Embedded Multi-Media Card (e•MMC), Electrical Standard (5.0).*

3 IEEE 1667 Functional Requirements

3.1 IEEE 1667 Overview

IEEE 1667 was designed to support native security protocols and tunneling of externally defined security protocols (e.g., TCG and Smart Cards) across multiple transports (e.g., SCSI, USB, ATA).

For a full description of IEEE 1667 see http://www.ieee1667.com and http://standards.ieee.org.

3.2 IEEE 1667's split command structure

IEEE 1667 uses an output and input transport specific command pair to execute a single IEEE 1667 command. This command pairing only affects the security protocols, and not the transport's normal user data access commands.

The output transport command consists of a transport specific command data block (CDB) and an associated output payload. Together, these include the IEEE 1667 command, any IEEE 1667 output parameters and any tunneled command/data.

This is followed by an input transport command with a transport specific CDB and an associated input payload. Together, these carry the same IEEE 1667 command, any IEEE 1667 input parameters, an IEEE 1667 status response, any tunneled input data, and any tunneled status information.

In this split command process, the command is not executed in the output phase, but is executed in the input phase (i.e., after receipt of the input transport command) where status can be reported in the command payload. This split command structure was designed to enable two desirable features:

- the transport status, the IEEE 1667 command status and the tunneled protocol status are reported such that each can be processed by the appropriate driver layer; and
- the host OS can support a single security communication protocol that supports multiple transports and does not have to implement multiple security-application-specific protocols in multiple transport drivers.

3.3 IEEE 1667 structure

IEEE 1667 functionality is contained by a device in one or more IEEE 1667 Addressable Command Targets (ACT). Each ACT consists of one or more addressable IEEE 1667 command processing blocks called silos. Each IEEE 1667 ACT is required to include one IEEE 1667 Probe silo which provides discovery of additional IEEE 1667 silos. Additional IEEE 1667 silos are optional in IEEE 1667.

The IEEE 1667 TCG silo was designed to enable wrapping of the TCG Storage communications protocol within the IEEE 1667 communications protocol. The IEEE 1667 TCG silo provides an interface for capability discovery and communication with the underlying TCG Storage compliant security subsystem, a Trusted Peripheral (TPer). The IEEE 1667 TCG silo allows a host TCG application to communicate through any transport supported by IEEE 1667 to a TPer without requiring native support of the TCG Storage communication protocols in the transport driver. Note that the while a TPer typically contains cryptographic functionality, the IEEE 1667 TCG silo does not; the 1667 TCG silo is a conduit to TCG functionality.

3.4 Requirements for IEEE 1667 functionality in the *e*•MMC security extension

An *e*•MMC device which supports the *e*•MMC security extension shall contain exactly one IEEE 1667 ACT which shall contain:

- exactly one IEEE 1667 Probe silo;
- exactly one IEEE 1667 TCG silo; and
- no additional IEEE 1667 silos

The IEEE 1667 Probe silo of an *e*•MMC device which supports the *e*•MMC security extension shall return a status of Default Behavior upon successfully processing an IEEE 1667 Probe command

The IEEE 1667 TCG silo of an *e*•MMC device which supports the *e*•MMC security extension shall support all defined TCG Storage Silo commands and not only the Get Silo Capabilities command (see [IEEE1667]).

4 TCG Storage Security Functional Requirements

4.1 TCG Storage Security overview

The TCG Storage Security specifications define an architecture that puts storage devices under the policy control of a trusted platform host.

- The TCG Storage Core specification [TCGCore] provides a general security framework
- The TCG Storage Security Subclass Opal [TCGOpal] provides a specific functional security set
- The TCG Storage Additional DataStore Tables feature set [TCGAddDST] adds specific functionality to the Opal SSC
- The TCG Storage Single User Mode feature set [TCGSUM] adds specific functionality to the Opal SSC
- The TCG Storage Interface Interaction specification [TCGSIIS] provides a description of the functional interactions between the security subsystem and the external interface (e.g., *e*•MMC) functionality.

4.2 Requirements for the TCG Storage Core in the *e*•MMC security extension

An *e*•MMC device, compliant with this standard, shall implement TPer functionalities defined in [TCGCore] required to support: [TCGOpal] , [TCGAddDST] and [TCGAddDST]. In particular, it shall support:

- the Locking Feature (0x0002);
- the TCG Stack reset; and
- the following Session Manager methods:
  - TPer Properties Method;
  - Start Session Method;
  - Close Session Method.

The device is not required to support the following features:

- Asynchronous protocol communication
- Creation or deletion of tables, and creation or deletion of table rows post-manufacturing

4.3 Requirements for the TCG Storage Opal SSC in the *e*•MMC security extension

An *e*•MMC device which supports the *e*•MMC security extension shall support the TCG Storage Opal SSC specification (see [TCGOpal]) and in particular:

- Geometry Reporting Feature in level 0 Discovery
- ability to disable SID authority in the Admin SP;
- the Locking SP shall be created by the device manufacturer

The device is not required to support the following features:

- Dynamic ComID Management
- RestrictedCommands (Object Table)

4.3.1 Level 0 Discovery

e•MMC devices, compliant with this standard, shall return the following elements in the Level 0 response as defined in [TCGOpal]:

- Level 0 Discovery Header
- TPer Feature Descriptor
- Locking Feature Descriptor
- Opal SSC Feature Descriptor
- Geometry Reporting

4.3.1.1 Level 0 Discovery Header

See [TCGOpal].

4.3.1 Level 0 Discovery (cont'd)

4.3.1.2 TPer Feature (Feature Code = 0x0001)

e•MMC devices, compliant with this standard, are not required to support: ComID management, buffer management, ACK/NACK, Asynchronous protocol.

Table 0-1 is informative and shows Level 0 Discovery - TPer Feature Descriptor content for a device implementing the required features only.

Table 0-1 — Level 0 Discovery - TPer Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code = 0x0001						
1								(LSB)
2	Version (1)				Reserved			
3	Length = 0x0C							
4	Reserved	ComID Mgmt Supported = 0	Reserved	Streaming Supported = 1	Buffer Mgmt Supported = 0	ACK/NAK Supported = 0	Async Supported = 0	Sync Supported = 1
5 - 15	Reserved							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

4.3.1.3 Locking Feature (Feature Code = 0x0002)

See [TCGOpal].

4.3.1 Level 0 Discovery (cont'd)

4.3.1.4 Geometry Reporting Feature (Feature Code = 0x0003)

This section defines requirements for some parameters of Geometry Reporting Feature Descriptor.

Align

For *e*•MMC devices, compliant with this standard, the value of the AlignmentRequired column of the LockingInfo table shall be equal to TRUE, therefore the ALIGN bit shall be set to one.

LogicalBlockSize

LogicalBlockSize indicates the number of bytes in a logical block.

LogicalBlockSize shall be set according to Table 0-2.

Table 0-2 — LogicalBlockSize and AlignmentGranularity

Device Density Range	eMMC spec		Geometry Reporting Feature Fields	
	Native Sector size	Address mode	LogicalBlockSize	AlignmentGranularity
Density ≤ 2 GByte	N.A.	Byte (1)	1	$512 * 2^N$, with $N \geq 0$
Density > 2 GByte	512 Byte	512 Byte	512	2^N, with $N \geq 0$
Density > 2 GByte	4 KByte	512 Byte (2)	512	$8 * 2^N$, with $N \geq 0$

NOTE 1 For density not greater than 2 GByte, the address shall be aligned to 512-Byte even though the device is byte addressable.

NOTE 2 For density greater than 2 GByte, the address shall be aligned to 8 512-Byte sector, and the data transfer shall be a multiple of 8 512-Byte sector.

READ_BL_PARTIAL field and WRITE_BL_PARTIAL field of the device CSD register shall be set to zero.

AlignmentGranularity

See [TCGOpal]. Please note that the term "physical block" referenced in [TCGOpal] is not to be confused with the "erase group" definition in JESD84-B51. Instead, it refers to a physical property of the storage medium specific to the manufacturer for the purpose of logical to physical mapping optimization.

This parameter is vendor unique and its value shall set as defined in Table 0-2.

LowestAlignedLBA

LowestAlignedLBA indicates the lowest logical block address that is located at the beginning of an alignment granularity group. For *e*•MMC devices compliant with this standard LowestAlignedLBA shall be set to zero.

4.3.1 Level 0 Discovery (cont'd)

4.3.1.4 Geometry Reporting Feature (Feature Code = 0x0003) (cont'd)

Geometry Reporting Feature Descriptor

Table 0-3 is informative and shows Level 0 Discovery - Geometry Descriptor content for a device implementing the required features only.

Table 0-3 — Level 0 Discovery - Geometry Reporting Feature Descriptor

Bit / Byte	7	6	5	4	3	2	1	0
0	(MSB)			Feature Code =0x0003				
1								(LSB)
2	Version (1)				Reserved			
3	Length = 0x1C							
4	Reserved							ALIGN = 1
5 - 11	Reserved							
12	(MSB)			LogicalBlockSize				
…								
15								(LSB)
16	(MSB)			AlignmentGranularity				
…								
23								(LSB)
24	(MSB)			LowestAlignedLBA = 0x0000 0000 0000 0000				
…								
31								(LSB)

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

4.3.1 Level 0 Discovery (cont'd)

4.3.1.5 Opal SSC V2.01 Feature (Feature Code = 0x0203)

Devices compliant with this standard shall support:

- at least the following two ComID values:
  - 0x0001 (Level 0 Device Discovery)
  - 0x0004 (TPER_RESET command)
- range crossing
  - The device supports commands addressing consecutive LBAs in more than one LBA range if all the LBA ranges addressed are unlocked.
- at least four Locking SP Admin Authorities
- at least eight Locking SP User Authorities

NOTE Support for more than eight Locking SP User Authorities is implementation specific; therefore it may not be provided by all devices in the market.

In addition to the previous requirements, the "Initial C_PIN_SID PIN Indicator" field and "Behavior of C_PIN_SID PIN upon TPer Revert" field shall be set to zero (see [TCGOpal)].

Table 0-4 is informative and shows Level 0 Discovery - Opal SSC V2.01 Feature Descriptor content for a device implementing the minimum requirements described in this standard.

Table 0-4 — Level 0 Discovery - Opal SSC V2.01 Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)	Feature Code =0x0203						
1								(LSB)
2	Version (1)				Reserved			
3	Length = 0x10							
4	(MSB)	Base ComID = VU						
5								(LSB)
6	(MSB)	Number of ComIDs = 0x0001						
7								(LSB)
8	Reserved for future common SSC parameters							Range Crossing Behavior = 0
9	(MSB)	Number of Locking SP Admin Authorities Supported = 0x0004						
10								(LSB)
11	(MSB)	Number of Locking SP User Authorities Supported 0x0008						
12								(LSB)
13	Initial C_PIN_SID PIN Indicator = 0x00							
14	Behavior of C_PIN_SID PIN upon TPer Revert = 0x00							
15 -19	Reserved for future common SSC parameters							

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

4.3.2 Properties Requirements

The requirements for support of the various properties, and the requirements for their values, are shown in Table 0-5.

Table 0-5 — Property Requirements

Property Name	Property Requirements and Values Reported
MaxComPacketSize	16384 (minimum)
MaxResponseComPacketSize	16384 (minimum)
MaxPacketSize	16364 (minimum)
MaxIndTokenSize	16328 (minimum)
MaxPackets	1
MaxSubpackets	1
MaxMethods	1
MaxSessions	1
MaxAuthentications	2
MaxTransactionLimit	1
DefSessionTimeout	

4.4 Requirements for the TCG Storage DataStore Tables feature set in the *e*•MMC security extension

An *e*•MMC device which supports the *e*•MMC security extension shall support the "TCG Storage Opal SSC Feature Set: Additional DataStore Tables" specification [TCGAddDST] with the following requirements:

- the number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Opal SSC V2.01 Feature Descriptor;
- the total size of the DataStore Tables shall be at least 10MByte.

4.4.1 DataStore Table Feature Descriptor (Feature Code = 0202h)

This descriptor shall be returned by devices compliant with this standard.

The maximum number of the DataStore Tables shall be equal to or greater than the number of Locking SP User Authorities reported in the Opal SSC V2.01 Feature Descriptor (see 4.3.1.5).

As required by [TCGOpal], the maximum total size of DataStore tables shall be at least 10MByte.

Table 0-6 is informative and shows Level 0 Discovery - DataStore Table Feature Descriptor content for a device implementing the minimum requirements described in this standard.

4.4.1 DataStore Table Feature Descriptor (Feature Code = 0202h) (cont'd)

Table 0-6 — Level 0 Discovery - DataStore Table Feature Descriptor

Bit Byte	7	6	5	4	3	2	1	0
0	(MSB)			Feature Code =0x0202				
1								(LSB)
2		Version [1]				Reserved		
3				Length = 0x0C				
4				Reserved				
5								
6	(MSB)			Maximum number of DataStore tables = 0x0008				
7								(LSB)
8	(MSB)			Maximum total size of DataStore tables = 0x 0000 0000 00A0 0000				
…								
11								(LSB)
12	(MSB)			DataStore table size alignment = 1 or above				
…								
15								(LSB)

NOTE 1 Version = 0x1 or any version that supports the defined features in [TCGOpal].

4.5 Requirements for the TCG Storage Support Single User Mode feature set in the *e*•MMC security extension

An *e*•MMC device which supports the *e*•MMC security extension shall support the "TCG Storage Opal SSC Feature Set: Single User Mode Specification" [TCGSUM].

4.6 Requirements for security characteristics for *e*•MMC devices that support the security extension

An *e*•MMC device which supports the *e*•MMC security extension shall support the following encryption methods:

- AES encryption with at least 128 bit keys;
- AES encryption with either the CBC block cipher mode or the XTS block cipher mode;
- support range crossing (Range Crossing = 0 in 4.3.1.5); and
- support Secret Protect.

5 *e*•MMC Security Data Transport

5.1 Extended Security Commands

Command Class 10 has been defined in JESD84-B51 for security data transport between the host and *e*•MMC device that supports the IEEE 1667 security protocol.

Command Class 10 defines CMD53 (PROTOCOL_RD) and CMD54 (PROTOCOL_WR) which are mapped to the P_IN and P_OUT command functions required by the IEEE 1667 security protocol.

Command Class 10 is mandatory to support the *e*•MMC security extension as specified in this document.

Refer to JESD84-B51 [*e*•MMC] or later releases.

5.2 Discovery of Extended Security Commands Support

The host issues CMD9 SEND_CSD to obtain the Device Specific Data in the CSD register. Bit 10 of CCC[95:84] field shall return a value of '1' to indicate Command Class 10 support.

5.3 Atomicity of Extended Security Commands

CMD53 PROTOCOL_RD and CMD54 PROTOCOL_WR commands are required to be preceded by CMD23 SET_BLOCK_COUNT command in JESD84-B51. Each CMD23/CMD53 or CMD23/CMD54 combination shall be considered as atomic, similar to pre-defined block count Read and Write commands.

A CMD23/CMD53 or CMD23/CMD54 combination is necessary to transmit the information corresponding to the Security Protocol, Security Protocol Specific, and Allocation Length fields of a SCSI or ATA CDB as required in IEEE 1667. CMD53 or CMD54 without a preceding CMD23 shall result in a SEC_INVALID_COMMAND_PARAMETERS error as defined in JESD84-B51.

IEEE 1667 requires a pairing of a PROTOCOL_WR command and a PROTOCOL_RD command for IEEE 1667 command processing (see 5.2), therefore a complete IEEE 1667 command pairing includes both a COM23/CMD54 combination and a CMD23/53 combination.

5.4 Data transport requirements specific to this Security Extension Specification

The data transport payload sizes are limited by JESD84-B51 to increments of 512 bytes (e.g., a block count value of one means 512 bytes, two means 1024 bytes, etc.). If additional bytes are required to meet these size requirements, then pad bytes shall be appended to meet this length. Pad bytes shall have a value of 00h.

6 Security Interactions with *e*•MMC Operations

6.1 Security Support Restrictions on Partitions

The extended security functionality described in this document shall have effects on the User Partition only. All other partitions shall operate as in an *e*•MMC without extended security functions.

CMD53 PROTOCOL_RD and CMD54 PROTOCOL_WR commands are accepted while the device is operating in User Partition mode only. CMD53 and CMD54 issued while the device is in different partition mode shall be considered as illegal command.

6.2 Authentication and Access Control Management on User Partition

If the IEEE 1667/TCG security feature is implemented, user authentication and access control to the User Partition is managed per IEEE 1667 and TCG security (see References)

6.3 Dynamic Capacity

Dynamic Capacity functionality shall be disabled once the Manufactured SP's have transitioned from Manufactured-Inactive to Manufactured state.

7 Error Handling

7.1 IEEE 1667 errors

The Status Code field in the PROTOCOL_RD payload indicates status information and errors at IEEE 1667 level. Some Status Codes are in common to both Probe and TCG Silos whereas some others are silo-specific. Note that error conditions defined in [TCGSIIS] are mapped into TCG Silo Status Codes.

See [IEEE1667] for more information.

7.1.1 PROTOCOL_RD, PROTOCOL_WR Command Out of Sequence

While processing IEEE 1667 commands, if consecutive PROTOCOL_WR's are received by the device, only the most recent PROTOCOL_WR is kept, and earlier PROTOCOL_WR commands are invalidated without notice.

While processing IEEE 1667 commands, if a PROTOCOL_RD is sent without a prior corresponding PROTOCOL_WR, the instructions contained in the PROTOCOL_RD are not to be processed and an error is generated at the IEEE 1667 layer.

See [IEEE1667] for more information.

7.1.2 Silo Index mismatch in PROTOCOL_RD, PROTOCOL_WR

If the Silo Index of the PROTOCOL_WR is set to an unsupported value, the payload shall be dropped and no error shall be generated at *e*•MMC Transport level.

If the Silo Index of the PROTOCOL_RD is set to an unsupported value, the Status Code shall return Invalid Silo Error and no error shall be generated at *e*•MMC Transport level.

7.1.3 PROTOCOL_RD, PROTOCOL_WR Transport Specific Error

The Invalid Security Protocol ID Parameter error is defined in IEEE 1667 to report the condition that the IEEE 1667 TCG Storage silo is not communicating correctly with the tPER.

See [IEEE1667] for more information.

7.2 *e*•MMC Transport Errors

7.2.1 PROTOCOL_RD, PROTOCOL_WR Transport Specific Error

The Invalid Security Protocol ID Parameter error is defined in [TCGSIIS] to report the condition that direct communications with the TPer are not being processed correctly due to invalid Protocol ID field value in PROTOCOL_RD command or PROTOCOL_WR command.

This error is reported in EXTENDED_SECURITY_FAILURE bit of EXCEPTION_EVENTS_STATUS [120] and SEC_INVALID_COMMAND_PARAMETERS bit of EXT_SECURITY_ERR [505] in the EXT_CSD register.

7.2.2 Unauthorized Access

Unauthorized access is an application error defined and reported in JESD84-B51. The application relationship is described in [TCG SIIS]. No data shall be written to or read from the medium.

Restrictions and device behaviors for access across secure LBA ranges are described in [TCGOpal]. Unauthorized access is reported as a Data Protection Error.

For *e*•MMC, the Data Protection Error as defined in [TCG SIIS] is reported in the EXTENDED_SECURITY_FAILURE bit of EXCEPTION_EVENTS_STATUS [120] and ACCESS_DENIED bit of EXT_SECURITY_ERR [505] in the EXT_CSD register.

8 Configuration

8.1 *e*•MMC Partition Configuration

An *e*•MMC secure storage device shall designate the User partition as the TCG Opal-SSC compliant storage device (SD), supporting one TCG secure storage TPer.

The storage TPer shall contain the Manufactured SP's (Admin SP and Locking SP) in the Manufactured-Inactive state as shipped from the device manufacturer. The capacity of the User partition can be changed and re-configured per *e*•MMC partition management procedures in JESD84-B51 while the Manufactured SP's are in the Manufactured-Inactive state. The User partition cannot be re-configured once the Manufactured SP's have transitioned from Manufactured-Inactive to Manufactured state.

Standard Improvement Form **JEDEC** _____

The purpose of this form is to provide the Technical Committees of JEDEC with input from the industry regarding usage of the subject standard. Individuals or companies are invited to submit comments to JEDEC. All comments will be collected and dispersed to the appropriate committee(s).

If you can provide input, please complete this form and return to:

JEDEC
Attn: Publications Department
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2107

Fax: 703.907.7583

1. I recommend changes to the following:

☐ Requirement, clause number _____

☐ Test method number _____ Clause number _____

The referenced clause number has proven to be:

☐ Unclear ☐ Too Rigid ☐ In Error

☐ Other _____

2. Recommendations for correction:

_____

_____

_____

_____

3. Other suggestions for document improvement:

_____

_____

_____

_____

Submitted by

Name: _____ Phone: _____

Company: _____ E-mail: _____

Address: _____

City/State/Zip: _____ Date: _____


JEDEC®