JEDEC STANDARD

Universal Flash Storage (UFS) Security Extension

JESD225

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.

UNIVERSAL FLASH STORAGE (UFS) SECURITY EXTENSION

Contents

Contents (cont'd)

Tables

Foreword

This UFS Security Extension Standard is an extension to the UFS Standards, JESD220.

Introduction

The UFS Standard, JESD220, defines a managed memory device capable of storing code and data. UFS devices are intended to offer the performance and features required by mobile devices while maintaining low power consumption. The UFS 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 document describes the requirements to implement security functionality described in [IEEE1667], [TCGCore], [TCGOpal], [TCGAddDST], [TCGSUM] and [TCGSIIS] in an UFS device.

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

UNIVERSAL FLASH STORAGE (UFS) SECURITY EXTENSION

(From JEDEC Board Ballot JCB-12-60, 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 UFS 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, constitutes 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.

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SAM], *SCSI 30 Architecture Model – 5 (SAM-5)*, Revision 05, 19 May 2010

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SPC], *SCSI Primary Commands – 4 (SPC-4)*, Revision 27, 11 October 2010

InterNational Committee on Information Technology Standards (INCITS), T10 Technical Committee [SBC], *SCSI Block Commands - 3 (SBC-3)*, Revision 24, 05 August 2010

IEEE 1667, *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 JESD220A [UFS], *Universal Flash Storage (UFS 2.0)*