JEDEC STANDARD

Secure Serial Flash Bus Transactions Version 1.0

JESD254

December 2022

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 2022
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2108

PRICE: Contact JEDEC

Printed in the U.S.A.

This page intentionally left blank

SECURE SERIAL FLASH BUS TRANSACTIONS

Contents

Page

Foreword ii
Introduction ii
1 Scope 1
2 Normative Reference 1
3 Terms and Definitions 2
3.1 Acronyms 3
3.2 Conventions 3
3.3 Keywords 4
4 Key Features 5
4.1 Introduction 5
4.2 Secure Packet Read and Secure Packet Write Transactions 5
4.2.1 Secure Packet Write Transaction 6
4.2.2 Secure Packet Read Transaction 6
4.2.3 SPI Transaction Mapping 7
Annex A — (Informative) Differences between Revisions 8

Figures

Page

Figure 1— Secure Packet Write Transaction 6
Figure 2 — Secure Packet Read Transaction 6

Tables

Page

Table 1 - Packet Read and Packet Write Transaction Characteristics 7

Foreword

This standard is intended for use by both hardware and software developers interested in supporting a packet transfer transaction between a host and SPI memory devices. These Packet Read and Packet Write transactions have become a key requirement for emerging secure flash memories incorporating a SPI interface. Hardware developers must understand the characteristics of the Packet Read and Packet Write transactions. Software developers will need an understanding of how to configure the transactions for proper operation.

This standard was prepared by the JC-42.4_3 Serial Flash task group authorized by the JC-42.4 Non-Volatile Memory subcommittee.

Introduction

This standard defines how packets can be transferred between host and peripheral devices over the Serial Peripheral Interface (SPI). A Packet Write is used to transfer a packet from the host to the SPI peripheral and a Packet Read retrieve a packet from the SPI peripheral back to the host.

The purpose of this specification is to describe the sequencing of the Packet Read and Packet Write transactions. Manufacturer specific details regarding the sequencing (command codes, command modifier lengths and latencies) are described in the device's Serial Flash Discoverable Parameter (SFDP) database (JESD216). The contents of the packet are out of scope of this spec and are manufacturer specific.

While the initial adoption of the Packet Read and Packet Write operations have occurred in Secure Flash products, the packet transactions may be applicable to other applications.

SECURE SERIAL FLASH BUS TRANSACTIONS

(From JEDEC Board Ballot JCB-22-54, formulated under the cognizance of the JC-42.4 Subcommittee on Non-Volatile Memory Devices, item number 1775.77).

1 Scope

This standard describes SPI bus transactions intended to support Secure Flash operation on a serial memory device. The on-chip SFDP database described in JESD216 has been revised to include details about the secure transactions. This ballot does not describe the SFDP revisions or the secure packet structure.

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.

- JEDEC Manual, JM7.01, *Style Manual for Standards and Other Publications of JEDEC*
- JEDEC Standard, JESD88E, *Dictionary of Terms for Solid-State Technology*
- JEDEC Standard, JESD99C, *Terms, Definitions, and Letter Symbols for Microelectronic Devices*
- JEDEC Standard, JESD100B.01, *Terms, Definitions, and Letter Symbols For Microcomputers, Microprocessors, and Memory Integrated Circuits*
- JEDEC Standard, JESD251B, Expanded Serial Peripheral Interface (xSPI) for Non Volatile Memory Devices.
- JEDEC Standard, JESD216F, *Serial Flash Discoverable Parameters (SFDP)*

3 Terms and Definitions

The current version of JESD88, Dictionary of Terms for Solid-State Technology, is the governing document for terms used in this standard. The following terms and definitions are provided for ease of reference:

- **byte (B):** (1) A binary character string operated upon as a unit and usually shorter than a computer word. (Ref. ANSI X3.172.)

NOTE A byte is usually eight bits. Within this standard it is an 8-bit data value with the most significant bit as bit 7 and the least significant bit as bit 0.

- **Controller:** An xSPI device that drives chip select signals to enable one other xSPI device to receive or transmit data on the interface at a given time.

- **Double Data Rate (DDR):** Information (e.g., command, modifier, address, or data) is transferred on each edge of a related clock.
- **Single Data Rate (SDR):** Information (e.g., command, modifier, address, or data) is transferred on one edge of a related clock.

- **host:** The computer system, test system, or other device that writes data to, and reads data from, a memory device. Within this standard it is an xSPI controller**:** An entity or a device with the characteristics of a primary computing device that includes one or more xSPI controllers. The xSPI controller drives out all chip select (CS) signals to xSPI target devices to select one target device at a time to interact with the controller. The controller provides transfer type and address information to target devices.

- **Target:** An xSPI device that receives a chip select signal to enable receive or transmit of data on the interface at a given time.

- **xSPI target:** An entity or a device with the characteristics of peripheral equipment that is selected by an xSPI controller.

NOTE The xSPI target is made active by its chip select (CS#) input to interact with the controller. The target receives transfer type and address information in order to identify which data to receive from or transmit to the xSPI controller.

3.1 Acronyms

DDR	Double Data Rate. Data is transferred on each edge of a related clock.
I/O or IO	Input or Output – A signal port that may receive or drive voltage levels to communicate with other devices.
SDR	Single Data Rate. Data is transferred on one (rising or falling) edge of a related clock.
SPI	Serial Peripheral Interface
xSPI	eXtended Serial Peripheral Interface

3.2 Conventions

This standard follows some conventions used in other JEDEC documents.

A binary number is represented in this standard by any sequence of digits consisting of only the Western- Arabic numerals 0 and 1 immediately followed by a lower-case b (e.g., 0101b). Spaces may be included in binary number representations to increase readability or delineate field boundaries (e.g., 0 0101 1010b).

A hexadecimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 and/or the upper-case English letters A through F immediately followed by a lower-case h (e.g., FA23h). Spaces may be included in hexadecimal number representations to increase readability or delineate field boundaries (e.g., B FD8C FA23h).

A decimal number is represented in this standard by any sequence of digits consisting of only the Western-Arabic numerals 0 through 9 not immediately followed by a lower-case b or lower-case h (e.g., 25).

A range of numeric values is represented in this standard in the form "a to z", where a is the first value included in the range, all values between a and z are included in the range, and z is the last value included in the range (e.g., the representation "0h to 3h" includes the values 0h, 1h, 2h, and 3h).
Other conventions used in this document:

Signals that are considered active when LOW have signal names that end with the hash / pound special character (i.e., have a suffix of #).

3.3 Keywords

Several keywords are used to differentiate levels of requirements and options, as follow:

- **Can** - A keyword used for statements of possibility and capability, whether material, physical, or causal (can equals is able to).
- **Expected** - A keyword used to describe the behavior of the hardware or software in the design models assumed by this standard. Other hardware and software design models may also be implemented.
- **Ignored** - A keyword that describes bits, bytes, or fields whose values are not checked by the recipient.
- **Mandatory** - A keyword that indicates items required to be implemented as defined by this standard.
- **May** - A keyword that indicates a course of action permissible within the limits of the standard (may equals is permitted).
- **Must** - The use of the word must is deprecated and shall not be used when stating mandatory requirements; must is used only to describe unavoidable situations.
- **Obsolete** - A keyword indicating that an item was defined in prior standards but has been removed from this standard.
- **Optional** - A keyword that describes features which are not required to be implemented by this standard. However, if any optional feature defined by the standard is implemented, it shall be implemented as defined by the standard.
- **Preferred** – A keyword used to identify a feature option which is the preferred option to implement for compliance with anticipated future revisions of this standard.
- **Reserved** - A keyword used to describe objects—bits, bytes, and fields—or the code values assigned to these objects in cases where either the object or the code value is set aside for future standardization.

Usage and interpretation may be specified by future extensions to this or other standards. A reserved object shall be zeroed or, upon development of a future standard, set to a value specified by such a standard. The recipient of a reserved object shall not check its value. The recipient of a defined object shall check its value and reject reserved code values.

- **Shall** - A keyword that indicates a mandatory requirement strictly to be followed in order to conform to the standard and from which no deviation is permitted (“shall” equals “is required to”). Designers are required to implement all such mandatory requirements to assure interoperability with other products conforming to this standard.
- **Should** - A keyword used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (“should” equals “is recommended that”).
- **Will** - The use of the word will is deprecated and shall not be used when stating mandatory requirements; will is only used in statements of fact.

4 Key Features

4.1 Introduction

This specification describes the transport layer for a secure packet bus transaction. Command codes to support Secure Packet Read and Secure Packet Write transactions are also described.

There are three transaction protocols that have been proposed within the Task Group that all follow a standard SPI transaction flow:

1. COMMAND (1 byte)
2. COMMAND MODIFIER (traditionally a target address occupying 0, 3, or 4 bytes)
3. LATENCY (traditionally used as bus turn-around time during read operations)
4. PACKET (traditionally the target read data or program data)

This specification describes the extensions to the SFDP database needed to support the secure transactions.

The legacy Replay Protected Monotonic Counter (RPMC) is supported as well as a new Secure Packet transaction format.

4.2 Secure Packet Read and Secure Packet Write Transactions

RPMC transactions and the new Secure Packet (Read and Write) transactions are similar enough to be described in a universal manner in the SFDP database.

Some of the Secure Packet (Read and Write) transaction characteristics are implied by the manner that legacy Read and Program operations are presented on the SPI bus. Secure Packet Write transaction characteristics are identical to the configured Program Page transaction. For example: Bus Width and SDR/DDR data rate. Secure Packet Read transaction characteristics are identical to the configured Read Fast transaction. For example: Latency, Bus Width, and SDR/DDR data rate.

4.2.1 Secure Packet Write Transaction

The Secure Packet Write transaction consists of a one-byte Command Op-Code followed by a zero, three or four byte Command Modifier field and finally a variable length Secure Packet.

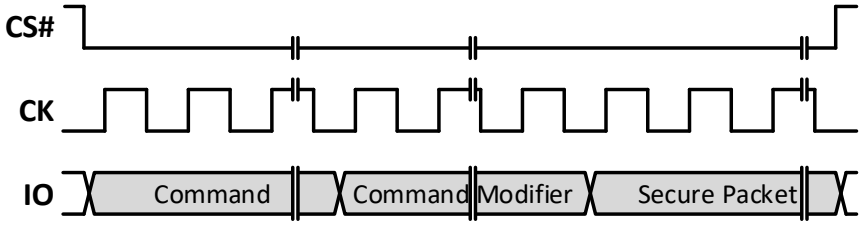

Figure 1— Secure Packet Write Transaction

4.2.2 Secure Packet Read Transaction

The Secure Packet Read transaction consists of a one byte Command Op-Code, a zero, three or four byte Command Modifier field a Latency period that is used to retrieve the target data and finally a variable length Secret Packet.

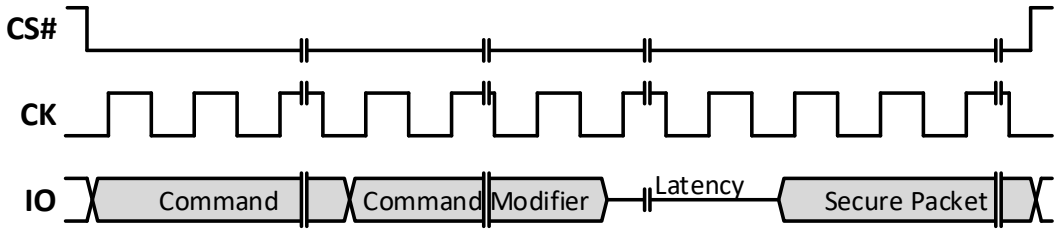

Figure 2 — Secure Packet Read Transaction

4.2.3 SPI Transaction Mapping

The following table describes how the four different transaction proposals compare with regards to Command Code, Command Modifier and Latency. These three characteristics can be applied to both RPMC and also the Secure Packet proposal.

Table 1 - Packet Read and Packet Write Transaction Characteristics

	COMMAND		COMMAND MODIFIER			LATENCY		DATA
								payload *(manufacturer specific)*
	Function	**code**	**Supported?**	**code**	**# bytes**	**Supported?**	**# clocks**	**contents**
RPMC	Packet Write	9Bh	no	-	0	no	0 clocks	CmdType(xxh) … Signature
	Packet Read	96h	no	-	0	yes	***Fixed*** (8 clocks)	ExtendedStatus … Signature
Option 1	Packet Write	F2h	yes	Manufacturer specific	4	no	0 clocks	SecureOp … Signature
	Packet Read	F1h	yes	Manufacturer specific	4	yes	***Configurable*** (Fast Read latency)	Response … Signature
Option 2	Packet Write	2Eh	yes	Manufacturer specific	3 or 4 - density dependent	no	0 clocks	SecureOp … Signature
	Packet Read	2Ah	yes	Manufacturer specific	3 or 4 - density dependent	yes	***Configurable*** (Fast Read latency)	Response … Signature
Option 3	Packet Write	A1h	yes	Manufacturer specific	4	no	0 clocks	SecureOp … Signature
	Packet Read	A2h	no	-	0	yes	***Fixed*** (8 clocks)	Response … Signature

NOTE The values shown in the table are examples provided by the different device manufacturers. The specific values and characteristics for the COMMAND, COMMAND MODIFIER and LATENCY fields are described in each device's SFDP database.

Annex A — (Informative) Differences between Revisions

This annex briefly describes most of the changes made to entries that appear in this standard, JESD**???**, compared to its predecessors. If the change to a concept involves any words added or deleted (excluding deletion of accidentally repeated words), it is included. Some punctuation changes are not included.

This annex is reserved for future revisions to this specification.

Standard Improvement Form **JEDEC Standard No. JESD254**

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®