

JEDEC STANDARD

Serial NOR Security Hardware Abstraction Layer

JESD261

October 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 22201-2107

JEDEC retains the copyright on this material. By downloading this file the individual agrees not to charge for or resell the resulting material.

PRICE: Contact JEDEC

Printed in the U.S.A.
All rights reserved

PLEASE!

DON'T VIOLATE
THE
LAW!

This document is copyrighted by JEDEC and may not be
reproduced without permission.

For information, contact:

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

or refer to www.jedec.org under Standards-Documents/Copyright Information.

This page intentionally left blank

SERIAL NOR SECURITY HARDWARE ABSTRACTION LAYER

Contents

	Pages
Foreword	iii
Introduction	iii
1 Scope	1
2 Informative Reference	2
3 Terms and Definitions	3
4 Functional Overview	3
4.1 Security Profile Discovery Parameter	5
4.2 Cryptography Attributes	5
4.3 Functional Summary	6
4.4 Performance Expectations	8
5 Device Lifecycle	9
5.1 Security Provisioning	9
5.2 Security Deployment	9
5.3 Security Operation	9
5.3.1 Initialization Phase	10
5.3.2 Cryptographic Session Establishment/Termination Phase	11
5.3.3 Secure Region Management Phase	12
5.3.4 Cryptographic Session Functionality Phase	13
6 Software Interfaces	15
6.1 Application Interface	15
6.1.1 Create Session	16
6.1.2 Terminate Session	17
6.1.3 Secure Erase	18
6.1.4 Secure Program	19
6.1.5 Secure Copy (Optional)	20
6.1.6 Secure Init	22
6.1.7 Secure Uninit	22
6.1.8 Secure Manage Region (Optional)	23
6.1.9 Secure Get Regions Info	26
6.1.10 Secure Read (Optional)	27
7 Implementation	30
7.1 Create Session Sequence Diagram	30

Contents (cont'd)

7.2 Terminate Session Sequence Diagram.....	33
7.3 Secure Manage Region Session Sequence Diagram.....	35
7.4 General Secure Operation Sequence Diagram.....	37
Annex A — (Informative) HAL Download Location.....	38

List of Figures

	Pages
Figure 1 — System Hierarchy	4
Figure 2 — Block Diagram Overview of HAL	5
Figure 3 — HAL API Call Phases.....	6
Figure 4 — Sequence Description	7
Figure 5 — Device Initialization State Diagram	10
Figure 6 — Create Session Sequence Diagram	31
Figure 7 — Create Session Cryptographic Flow Sequence Diagram.....	32
Figure 8 — Terminate Session Sequence Diagram	33
Figure 9 — Terminate Session Cryptographic Flow Sequence Diagram.....	34
Figure 10 — Secure Manage Region Sequence Diagram	35
Figure 11 — Secure Manage Region Cryptographic Flow Sequence Diagram	36
Figure 12 — Secure Operation Sequence Diagram.....	37
Figure 13 — Secure Operation Cryptographic Flow Sequence Diagram.....	38

List of Tables

	Pages
Table 1 — Single versus Multiple Layer Interactions	16

Foreword

This standard has been prepared by the JEDEC TG424_3.4 Serial Flash Task Group. With some exceptions, the general capability of SPI NOR flash devices across the industry are relatively uniform, but the logical cryptographic security functionality within vendors' devices differs widely and may be proprietary.

The purpose of this standard is to provide uniform cryptographic access to a variety of compliant NOR devices. Such devices generally enjoy functional equivalence but lack compatibility at a logical interface level due to varying command structures and implementation differences. Uniformity is achieved using a hardware abstraction layer with a standardized application layer interface. It provides guidelines for software developers and systems designers. The standard also provides sample code that may be used to reduce the design-in effort.

This is the initial revision of this standard and therefore replaces no prior iterations. This standard may be used by system and software designers in conjunction with other related NOR standards such as JESD251B (Expanded Serial Peripheral Interface (xSPI) For Non Volatile Memory Devices) and JESD216F.01 (Serial Flash Discoverable Parameters).

All contents in the Annexes are informative.

Introduction

NOR memory is a relatively small density highly reliable memory capable of storing code and data. It has many system-level uses but is often put in place as a boot memory device within embedded systems. Historically, the NOR memory device is intended to offer the reliability, performance, and storage features required by the computing device while maintaining low power consumption and content integrity. In doing so, NOR memory devices have evolved to where many now offer embedded cryptographic functions that further enhance system level security and data assurance in a computing platform. This enables cryptographically enhanced content transfer into and out of the memory device. This standard unifies disparate chip level cryptographic operation that may be in place from multiple manufacturers by creating a low-level hardware abstraction layer (HAL) interface.

This standard targets NOR SPI devices and may be leveraged for NOR devices with different interface widths which may conform to different standards. The logical and physical communication protocol directly to and from the memory device is not defined as a part of this standard, and as such remains a flexible portion of the overall system design that is expected to conform to the forthcoming JEDEC-standardized secure read and write bus protocol for NOR devices (JEDEC reference TBD).

This standard assumes that the underlying functionality of a targeted NOR device from any vendor can conform to the cryptographic functionality that this standard's interface describes herein. The intent of this standard is therefore to mandate the interface to the secure NOR memory device and not the implementation of the device itself.

As used in this document, "shall", "must", or "will" denotes a normative and therefore mandatory provision of the standard. Other directives such as "Should" denote a provision that is recommended but not mandatory. "May" or "can" denotes a feature whose presence does not preclude compliance, that may or may not be present at the option of the implementer. Any wording in this document that is not strictly defined as normative is instead informative.

This page intentionally left blank

SERIAL NOR SECURITY HARDWARE ABSTRACTION LAYER

(From JEDEC Board Ballot JCB-22-45, formulated under the cognizance of the JC-42.4 Committee on Serial Flash, item 1775.99)

1 Scope

This standard provides a comprehensive definition of the NOR cryptographic security hardware abstraction layer (HAL). It also provides design guidelines and reference software to reduce design-in overhead and facilitate the second sourcing of secure memory devices. It does not attempt to standardize any other interaction to the NOR device that is not related to cryptographic security functionality within the device.

The API definition and functionality described herein require a baseline of symmetric cryptographic capability within supporting memory devices. This architecture does not preclude asymmetric cryptographic functionality in the general sense but does not address asymmetric functionality at the present time.

As with any cryptosystem rooted with symmetric cryptography, a non-ephemeral symmetric secret (key) must be shared between two parties to ensure intended functionality and should be done in a secure manner. This process, typically called key provisioning, is assumed to have already taken place relative to this standard for the targeted computing platform and secure memory device. As such, this standard assumes that a shared secret (nonvolatile root key) already exists between the host and the secure memory device. Initial nonvolatile (pre-shared) key provisioning between a host and memory device will therefore not be addressed by this standard.

2 Informative Reference

The following informative 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 documents indicated below. For undated references, the latest edition of the document referred to applies.

- Eurosmart SECURITY IC PLATFORM AUGMENTATION PACKAGE: EXTERNAL NVM STORAGE: <https://www.eurosmart.com/security-ic-platform-augmentation-package-external-nvm-storage/>
- GlobalPlatform Technology SESIP Profile for Secure External Memories: <https://globalplatform.org/specs-library/globalplatform-technology-sesip-profile-for-secure-external-memories/>
- NIST SP800-56c, Recommendation for Key-Derivation Methods in Key-Establishment Schemes: <https://csrc.nist.gov/publications/detail/sp/800-56c/rev-2/final>
- JESD216F.01, Serial Flash Discoverable Parameters: <https://www.jedec.org/standards-documents/docs/jesd216b>
- JESD251B, Expanded Serial Peripheral Interface (xSPI) For Non Volatile Memory Devices: <https://www.jedec.org/standards-documents/docs/jesd251b>
- FIPS PUB 198-1, The Keyed-Hash Message Authentication Code: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf>

3 Terms and Definitions

For purposes of this standard, the following abbreviations for common terms apply:

API: Application Programming Interface

Cryptoperiod: The lifetime of a cryptographic key when the key is authorized for use.

Ephemeral key: a key that may become a session-based shared secret between host and memory device and has a cryptoperiod of no longer than the memory device's valid session span. An ephemeral key may be volatile or nonvolatile as determined by the memory vendor.

HAL: Hardware Abstraction Layer

Hash: A hash function is a one-way **cryptographic** algorithm that takes an input of any size and generates an output of a fixed length

HMAC: Hashed-based Message Authentication Code, a type of message authentication code involving a cryptographic hash function as described in FIPS Publication 198-1 dated July, 2008

FIPS: Federal Information Processing Standards

Root key: nonvolatile key that becomes a shared secret between host and memory device. The updateability of the root key is up to the memory vendor and outside the scope of this document.

Session: the sequence of operations spanning a time in which a key is utilized between host and memory device

SHA: Secure Hash Algorithm

SHA-2: Secure Hash Algorithm 2, a set of cryptographic hash functions designed by the United States National Security Agency described in FIPS Publication 180-4 dated August, 2015

Tuple: An immutable sequence of ordered elements, such as items associated with and defining a session

4 Functional Overview

The JEDEC cryptographic HAL is a software component that enables manufacturer-neutral communication with secure functionality with NOR flash memory devices. The HAL can be compiled for use within user space, kernel space, and bare metal applications. The protocols supported by the HAL assume nonvolatile key provisioning operations have previously been put in place so the HAL can also be compiled to run in a trusted execution environment. Shown below are possible locations for the HAL in relation to an operating system (or the absence thereof).

4 Functional Overview (cont'd)

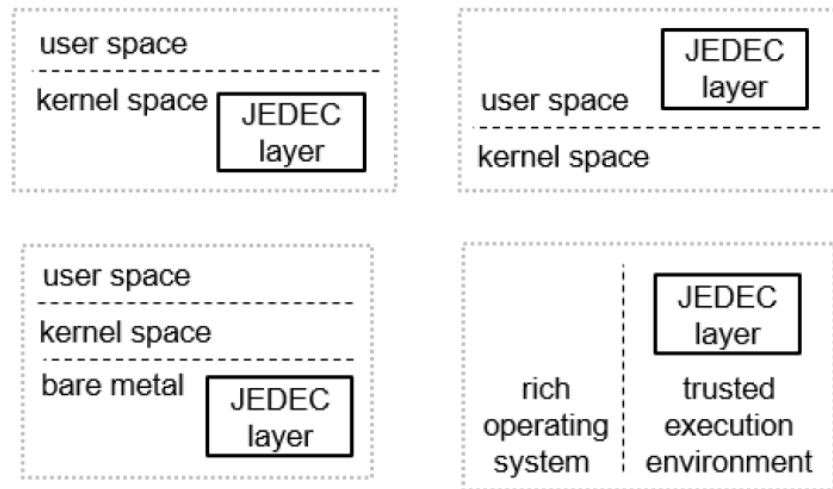


Figure 1 — System Hierarchy

The JEDEC layer enables manufacturer-neutral communication with secure flash devices by exposing a common application interface. Through the JEDEC layer, this application interface is integrated with two other interfaces for communicating with a crypto service and vendor drivers. Considering crypto library variants on different platforms, a specific wrapper for each crypto library may be needed to unify the interface for the crypto function calls made by the JEDEC layer.

In addition, this standard targets NOR SPI devices by leveraging the existing SPI Flash protocol and enveloping security communication into a packet. In addition to the NOR-specific secure packet protocol defined by the forthcoming JEDEC standard, some security Flash vendors also have their own proprietary packet format. This standard also accommodates the variety of packet types through vendor specific implementations.

The JEDEC layer is designed to provide a set of device agnostic HAL APIs for upper Application API layer for operations such as secure program or secure erase. The JEDEC vendor driver is used to address differences among various security devices manufactured by different vendors. The JEDEC specific implementation described by this standard includes reference source code accompanying the JEDEC common interface layer. Vendors can also have their own implementations fit into this HAL by complying to the function calls required by the JEDEC layer.

This standard defines the JEDEC specific implementation with certain explicit steps that are imposed on the underlying connected security device. The security device accessed through the JEDEC-specific implementation must conform to the minimal security features required by this standard, but other functionality within the actual memory device may be vendor defined. Nevertheless, certain sub-functions may appear in form of object code to offer a measure for vendors for protecting their interest if necessary.

4 Functional Overview (cont'd)

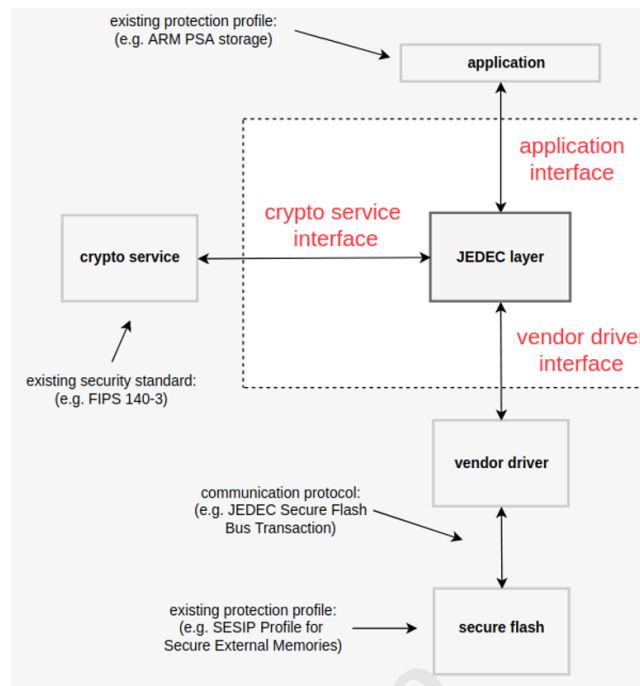


Figure 2 — Block Diagram Overview of HAL

The gray box is the companion cryptosystem and is used this way throughout the rest of the document. For further content related to implementation flows that work within the context of **Figure 2**, see **clause 7**

4.1 Security Profile Discovery Parameter

This HAL standard does not directly reference or require knowledge of specific clauses or parameters within the Serial Flash Discovery Parameter table. But the HAL's underlying abstraction software does make use of the SFDP parameter which describes how to issue secure read and write operations to the memory device. This SFDP clause is therefore informative to hosts who leverage this HAL.

4.2 Cryptography Attributes

Each memory vendor may have one or more unique ways of performing secure operations within their memory device. These can manifest in differences in cryptographic algorithms, key lengths and strengths, whether encryption is used or not, etc. This HAL does not communicate these differences for any particular memory vendor. Rather, users of this HAL must infer this information for a particular memory device based on the root key used and actions taken by the host to pre-share this key with the memory device. As noted in **clause 5.1**, the root key must be pre-shared between host and device during the Provisioning stage of operation which is outside the scope of this standard. It is therefore assumed that all aforementioned attributes that must be associated with that key are also shared during provisioning and/or may be inferred from the root key used.

4.3 Functional Summary

The HAL works with application-layer software by abstracting common security functionality present within supporting memory devices. The application layer software may make API calls that include only a key reference. No cryptographic keys are utilized within the API call but the calling software must be entitled to indirectly use the referenced key.

Once a call is made and the JEDEC specific implementation is bound, the HAL software will sequentially execute an application layer API call in three phases: perform optional pre-processing vendor-unique command functions, perform JEDEC standard command functions, and perform post-processing standard and optional vendor-unique verification functions. These three phases can be seen in **Figure 3**Figure 3 — HAL API Call Phases.

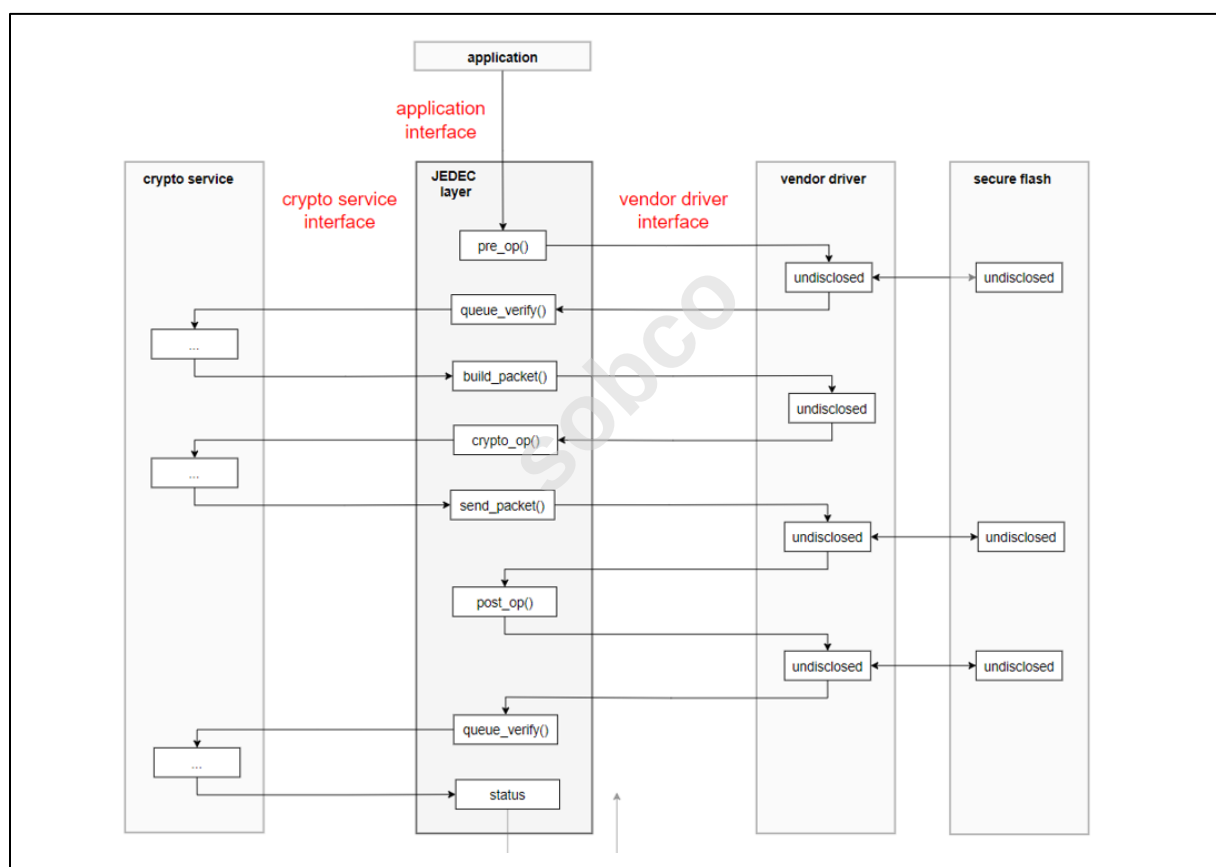


Figure 3 — HAL API Call Phases

All vendor-unique command and verification functions are optional. HAL software within each of the three phases shall be able to communicate with a companion cryptosystem (host cryptographic hardware or software library) through the cryptographic interface by using the key reference received in the application layer API call. The cryptographic interface purpose is to provide access to functionality such as performing cryptographic operations like hashing and key derivation, creating MAC signatures such as HMAC or CMAC, verifying MAC signatures, etc. without exposing the underlying key. Each of the three phases of HAL software execution may invoke cryptographic operations within the companion cryptosystem and receive response status and data.

4.3 Functional Summary (cont'd)

In doing so, each phase of the HAL may utilize this information to construct commands and receive responses to/from memory device using the supporting memory vendor's vendor driver interface.

Both the pre-processing and post-processing vendor-unique phases for any application layer API call are optional for any particular memory vendor. For example, in some cases vendors may implement functions that perform no operations at all. They exist to enable vendor-unique functionality in the supporting memory device that may be outside the scope of the JEDEC HAL standard functionality but are still required to enable functional support of the application layer API call.

All Application layer API calls must result in initiating one of four mandatory JEDEC layer sequences.

Figure 4 shows a summary of all defined Application layer commands and their required sequence classification. For more details about each command, see (**clause 5** and **clause 6**).

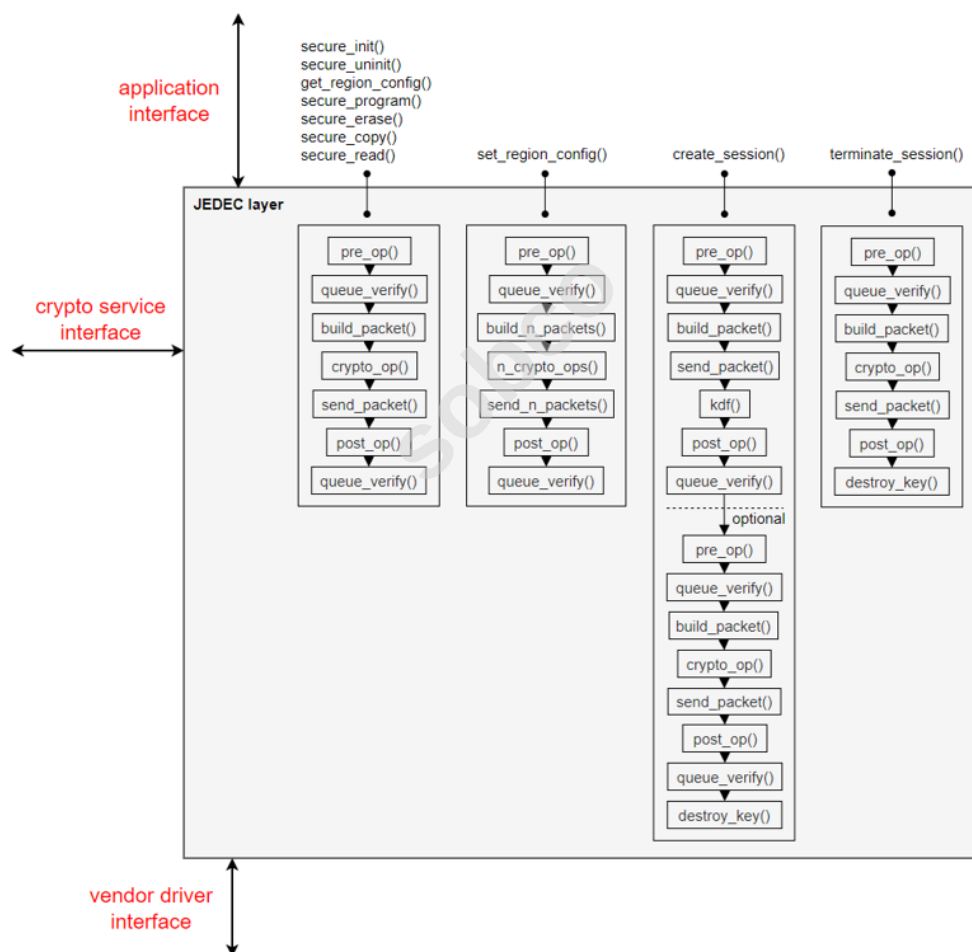


Figure 4 — Sequence Description

In the process of executing either of the first two phases of the HAL software, one or more secure commands may be created and issued to the memory device. Here, a secure command is defined as one, at a minimum, which contains a MAC of the command contents.