[Public]



In-Field Structural Test
ASP Host Interface
IFST Programming Model Specification

Publication # **69413** Revision: **0.90**
Issue Date: **October 2026**

Advanced Micro Devices 

[Public]

© 2026 Advanced Micro Devices, Inc. All rights reserved.

The information contained herein is for informational purposes only, and is subject to change without notice. While every precaution has been taken in the preparation of this document, it may contain technical inaccuracies, omissions and typographical errors, and AMD is under no obligation to update or otherwise correct this information. Advanced Micro Devices, Inc. makes no representations or warranties with respect to the accuracy or completeness of the contents of this document, and assumes no liability of any kind, including the implied warranties of noninfringement, merchantability or fitness for particular purposes, with respect to the operation or use of AMD hardware, software or other products described herein. No license, including implied or arising by estoppel, to any intellectual property rights is granted by this document. Terms and limitations applicable to the purchase or use of AMD’s products are as set forth in a signed agreement between the parties or in AMD's Standard Terms and Conditions of Sale.

Trademarks

AMD, the AMD Arrow logo, AMD EPYC, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other product names used in this publication are for identification purposes only and may be trademarks of their respective companies.

Linux is a registered trademark of Linus Torvalds.

[Public]

Contents

Chapter 1 Introduction 7

1.1 Scope 7

1.2 ASP IFST Package 7

Chapter 2 Interface 8

2.1 IFST Command ID 8

2.2 IFST DRAM Command Buffer Layout 8

2.3 EXECUTE Command Error Codes 9

[Public]

List of Figures

Figure 1. IFST EXECUTE COMMAND DRAM Command Buffer..... 9

[Public]

List of Tables

Table 1. Mailbox Registers (C2PMSG_173..175) 8
Table 2. EXECUTE Command Error Codes 9

[Public]

Revision History

Date	Revision	Description
October 2026	0.90	Initial public release.

[Public]

Chapter 1 Introduction

This document describes the AMD Security Processor (ASP) interface used for the In-Field Structural Test (IFST) feature.

1.1 Scope

This document covers only the Software Programming Interface to the ASP trusted application to manage In-Field Structural Test.

This document does not cover the IFST architecture in detail or any implementation details.

1.2 ASP IFST Package

An IFST package contains:

- Test pattern payload

For security reasons, the whole IFST package will be cryptographically signed:

- IFST-trusted firmware and test pattern payload – signed by AMD / customer.

[Public]

Chapter 2 Interface

IFST commands are processed via dedicated C2PMSG registers 173, 174, and 175. IFST uses a new standalone command dispatched directly through these registers. The IFST command is processed by the ASP interface.

Table 1. Mailbox Registers (C2PMSG_173..175)

Register	Bit	Description
C2PMSG_173	31	Ready (1=done, 0=busy)
	30	Recovery
	29:24	Reserved
	23:16	Command ID (host writes)
	15:0	Status (firmware writes)
C2PMSG_174	31:0	cmd_buf phys addr [31:0]
C2PMSG_175	31:0	cmd_buf phys addr [63:32]


(phys addr of cmd_buf in DRAM)

2.1 IFST Command ID

IFST uses a new command ID written to MPASP_C2PMSG_173[23:16]:

```
  #define IFST_CMD_EXECUTE  0x01  /*!< Execute IFST – command via
C2PMSG 173-175 */
```

2.2 IFST DRAM Command Buffer Layout

The 64-bit DRAM address written to MPASP_C2PMSG_174 (low) and MPASP_C2PMSG_175 (high) points to the IFST command buffer in DRAM. This buffer contains pointers to the IFST package and output fields for the test result region – the IFST package is at a separate DRAM address, not attached to this buffer.

```
struct ifst_cmd_buf (__packed, 120 bytes)
```

[Public]

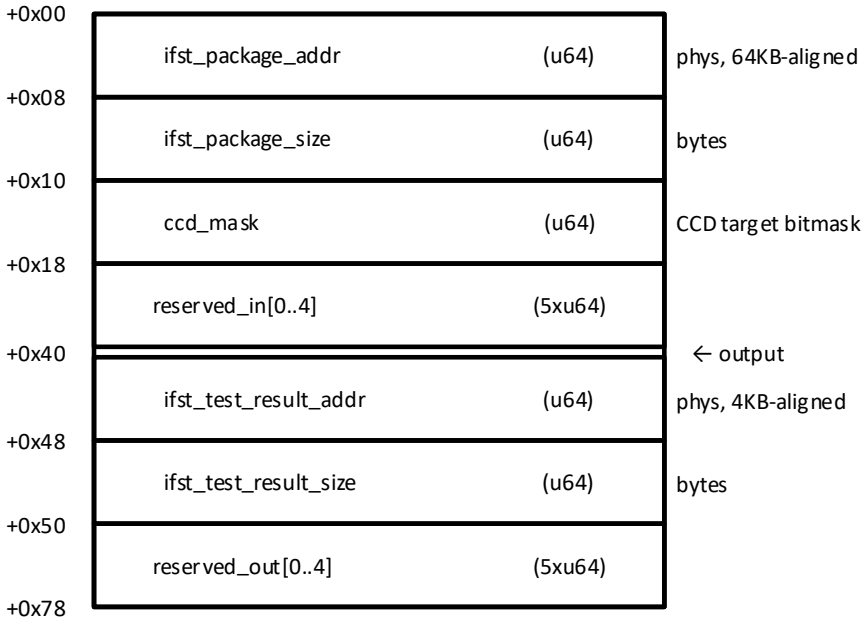


Figure 1. IFST EXECUTE COMMAND DRAM Command Buffer

2.3 EXECUTE Command Error Codes

Firmware reports the TEE_ERROR_AMD_IFST_* values in C2PMSG_173 bits [15:0] when it completes the command. It sets bits [15:8] to the fixed value 0x1f and indicates the error code in bits [7:0], as shown in *Table 2 below*.

Table 2. EXECUTE Command Error Codes

Value	Name	Description
0x01	INVALID_PACKAGE_ADDRESS	Package address is invalid (misaligned or out of bounds)
0x02	INVALID_PKG_SIZE	IFST package size is invalid (too small/large, or inconsistent with header)
0x03	RUNNING_NOT_ALLOWED	IFST execution is not allowed (security state, policy, or hardware lockout)
0x04	INVALID_CUSTOMER_SIGNATURE	Customer signature is invalid (signature check failed)
0x05	CUSTOMER_SIGNING_NOT_ALLOWED	Customer signing is not allowed (policy restriction)

[Public]

Value	Name	Description
0x06	INVALID_PACKAGE	Package is invalid (corrupt, malformed, or fails validation)
0x07	VALIDATE_DRIVER	TEE IFST driver validation failed (signature or integrity check)
0x08	DRIVER_LOAD_FAIL	TEE IFST driver load failed (load error, memory, or dependency)
0x09	VALIDATE_TA	IFST TA firmware validation failed (signature or integrity check)
0x0A	TA_LOAD_FAIL	IFST TA firmware load failed (load error, memory, or dependency)
0x0B	VALIDATE_PAYLOAD	IFST payload validation failed (signature or integrity check)
0x0C	INVALID_PAYLOAD	Payload is invalid (malformed or corrupt)
0x0D	BUSY	IFST execution already in progress (concurrent command not allowed)