CXL ENGINEERING CHANGE NOTICE

TITLE:	Compliance chapter additions for TSP
DATE:	Introduced date (11/16/2023) Updated date (02/13/2024)
AFFECTED DOCUMENT:	CXL 3.1
SPONSOR:	Chet Douglas, Intel Corporation

Part I

- **Summary of Functional Changes**

  This ECN defines a set of CXL Compliance tests to add basic compliance testing for the Trusted Execution Environment Security Protocol (TSP) that was added to the CXL 3.1 specification. This ECN also includes the addition of a new asynchronous key refresh test for the existing CXL IDE tests.

- **Benefits as a Result of the Changes**
  Allow basic compatibility testing of devices against the basic TSP interfaces to enable use of direct attached HDM-H memory with confidential computing scenarios.

- **Analysis of the Hardware Implications**
  This ECN may have an impact of CXL component hardware depending on the device's implementation.

- **Analysis of the Software Implications**
  Changes to device firmware, System Firmware and OS may be needed to enable these capabilities. When a device is locked through TSP, there will be changes in the device's CCI behavior that may affect existing SW.

- **Analysis of the Compliance and Test Implications**
  This ECN will have compliance and test SW implications

Part II

Detailed Description of the change

Add new CXL IDE test sequence 14.11.3.10 Asynchronous Key Refresh:

14.11.3.9 Asynchronous Key Refresh

This test checks that the device and host are capable of refreshing keys without stopping the host CXL.cachemem transactions that are inflight during the transition to new keys.

Prerequisites:

- Device must support CXL.cachemem IDE security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.3.2/3/4/5 passed (depends on Flit mode operation and topology)

Topologies:

- SHDA

Test Steps:

1. See Test 14.11.3.2/3/4/5 (depends on Flit mode operation and topology) to set up an encrypted link between the host and the device and the initial KEY_EXCHANGE.
2. Host software sets up the Device for Algorithms 1a, 1b, and 2 to initiate traffic (see Section 14.3.6.1).
3. Enable Self-testing for checking validity of data.
4. Host software controls the test execution and test duration.
5. Reconfigure keys with the following steps:
    a. Host Software/CIKMA initiates "CXL_KEY_PROG" for setting up new set of Keys for Tx and Rx of ports.
    b. Host/CIKMA initiates "CXL_K_SET_GO" to Rx, waits for successful response, and then initiates "CXL_K_SET_GO" to Tx ports to indicate/prepare for start of KEY_EXCHANGE.
6. Initiated traffic and test execution continues during and after the key refresh.

Pass Criteria:

- No Failure is reported via the IDE Status register (see Section 8.2.4.22.3) or the CXL IDE Error Status register (see Section 8.2.4.22.4)
- CXL_KP_ACK response with Status=0
- CXL.cachemem transactions continue and are un-heeded by the refresh of the keys.

Fail Conditions:

- IDE reported failures
- CXL_KP_ACK response with Status!=0
- CXL_K_GOSTOP_ACK is not received within the specified timeout period
- CXL.cachemem transactions are interrupted or timeout during the refresh

Add new CXL TSP test sequences to new section 14.11.7 CXL.cachemem TSP with the following content:

14.11.7 CXL.cachemem TSP

14.11.7.1 TSP Support

This test determines whether the CXL device supports CXL TSP.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device

Topologies:
- SHDA

Test Steps:
1) Read the DVSEC CXL Capability register (see Section 8.1.3.1)
2) Verify the TSP Capable bit is set

Pass Criteria:
- TSP Capable bit is set

Fail Conditions:
- Pass criteria is not met

14.11.7.2 Version

This test returns the TSP version of the device.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.1 passed

Topologies:
- SHDA

Test Steps:
1) Host software issues Get Target TSP Version
2) Host software receives Get Target TSP Version Response
3) Verify the TSP Version returned in Get Target TSP Version Response matches the version expected
    a. 1.0 – Initial CXL 3.1 TSP supported

Pass Criteria:
- Get Target TSP Version Response, TSP Version is reported as expected

Fail Conditions:
- Get Target TSP Version Response, TSP Version is not as expected
- Get Target Version results in a TSP Error Response

14.11.7.3 Capabilities

This test verifies the returned TSP capabilities of the device. The specific TSP features that a target supports are almost all optional from a CXL specification perspective. The table of TSP features below outlines what is required for confidential computing and what is optional. Optional support depends on the host or device implementation and specific security requirements of the TEE and the device. The rest of the TSP compliance tests depend on the capabilities reported here.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.2 passed

Topologies:

- SHDA

Test Steps:

1) Host software issues Get Target Capabilities
2) Host software receives Get Target Capabilities Response
3) Verify the capabilities returned in Get Target Capabilities Response supports the required and optional device expected security features for confidential computing

Pass Criteria:

- The Get Target Capabilities Response payload will indicate what features are supported and can be tested. Required confidential computing features must be supported by the device. The following table outlines the basic TSP features, whether they are required for confidential computing and which compliance test applies to each feature.

Get Target Capabilities Response			**Confidential Computing Requirement**	**Additional Compliance Tests**
Memory Encryption Features Supported	Encryption		Optional – Target or Initiator based encryption required	**14.11.7.8**
	CKID-based Encryption	Number of CKIDs		**14.11.7.10** **14.11.7.11** **14.11.7.12**
	Range-based Encryption	Memory Encryption Number of Range Based Keys		**14.11.7.13** **14.11.7.14** **14.11.7.15**
	CKID Base Required			**14.11.7.9**
TE State Change and Access Control Features Supported	Write Access Control		Optional	**14.11.7.6** **14.11.7.7**
	Read Access Control			**14.11.7.5** **14.11.7.6** **14.11.7.7**
	Implicit TE State Change		Required – At least one method of TE State Change shall be supported	**14.11.7.4** **14.11.7.5**
	Explicit Out-of-band TE State Change	Supported Explicit Out-of-band TE State Granularity		**14.11.7.7**
	Explicit In-band TE State Change	Supported Explicit In-band TE State Granularity		**14.11.7.6**

Fail Conditions:

- Get Target Capabilities Response payload does not support required confidential computing security features
- Get Target Capabilities Response payload does not support expected optional confidential computing security features
- Get Target Capabilities results in a TSP Error Response

14.11.7.4 Implicit TE State Changes

This test verifies basic optional Implicit TE State Change functionality of the target device. Specifically, this covers the case with no Read Access Control enabled, where the target is expected to simply return the current TE State saved for the address being accessed. This tests the TSP table: Target Behavior for Implicit TE State Changes.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for Implicit TE State Changes

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to enable Implicit TE State Changes
    a. TE State Change and Access Control Enable, Implicit TE State Change shall be set
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable and to enable receiving TEE Opcodes
4) Host software receives Lock Target Configuration Response
5) Host untrusted (VM) software generates a memory read request for the test address with non-TEE opcode
6) Host software verifies read returned non-TEE Opcode but data is undefined
7) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern A
8) Host software verifies write returned TEE Opcode in the response
9) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
10) Host software verifies read returned TEE Opcode and expected data pattern A
11) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern B
12) Host software verifies write returned non-TEE Opcode in the response
13) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
14) Host software verifies read returned non-TEE Opcode and expected data pattern B
15) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern A
16) Host software verifies write returned non-TEE Opcode in the response
17) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
18) Host software verifies read returned non-TEE Opcode and expected data pattern A
19) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern B
20) Host software verifies write returned TEE Opcode in the response
21) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
22) Host software verifies read returned TEE Opcode and expected data pattern B

Pass Criteria:

- TE/non-TEE opcode returned is correct for all reads
- Read data returned for all reads is expected

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Pass criteria is not met

14.11.7.5 Implicit TE State Changes w Read Access Control

This test verifies basic optional Implicit TE State Change functionality of the target device. Specifically, this covers the case with Read Access Control enabled, where the target is expected to check the TE State and return all 1's data pattern and opposite TE State in the read response. This tests the TSP table: Target Behavior for Implicit TE State Changes and Target Behavior for Read Access Control.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for Implicit TE State Changes and Read Access Control

Topologies:
- SHDA

Test Steps:
1) Host software issues Set Target Configuration to enable Implicit TE State Changes and Read Access Control
    a. TE State Change and Access Control Enable, Implicit TE State Change shall be set & Read Access Control shall be set
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable and to enable receiving TEE Opcodes
4) Host software receives Lock Target Configuration Response
5) Host trusted TEE (TVM) software generates a full cache-line memory write request to the test address with a TEE opcode and known data pattern
6) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
7) Host software verifies read returned TEE Opcode and expected data pattern
8) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
9) Host software verifies read returned TEE Opcode and all 1's for the data
10) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern
11) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
12) Host software verifies read returned non-TEE Opcode and expected data pattern
13) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
14) Host software verifies read returned non-TEE Opcode and all 1's for the data

Pass Criteria:
- TE/non-TEE opcode returned is correct for all reads
- Read data returned for all reads is expected
- Data pattern of all 1's returned for reads with TE State mismatch

Fail Conditions:
- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Pass criteria is not met

14.11.7.6 Explicit In-band TE State Changes w Read and Write Access Control

This test verifies basic optional Explicit In-band TE State Change functionality of the target device. Specifically, this covers the case with Read and Write Access Control both enabled, where the target is expected to a) check the TE State for writes and drop the write and return the current TE State in the write response if there is a TE State mismatch, b) check the TE State for reads and return current TE State in the read response and return all 1's data pattern if there is a TE State mismatch. Utilizing in-band memory transactions this tests the following TSP tables: Target Behavior for Explicit In-band TE State Changes, Target Behavior for Read Access Control and Target Behavior for Write Access Control.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for Explicit In-band TE State Changes and Read Access Control and Write Access Control

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to enable Explicit In-band TE State Changes, Read Access Control and Write Access Control
    a. TE State Change and Access Control Enable, Explicit In-band TE State Change & Read Access Control & Write Access Control shall all be set
    b. Explicit In-band TE State Granularity Entry 0 shall have a valid TE State Granularity and valid Length Index supported by the target, all other Granularity Entries are set to invalid
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable and to enable receiving TEE Opcodes
4) Host software receives Lock Target Configuration Response
5) Host software generates TEUpdate memory request to set TE State to 1 for the test memory address
6) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern A
7) Host software verifies write returned TEE Opcode in the response
8) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
9) Host software verifies read returned TEE Opcode in the response and expected data pattern A
10) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern B
11) Host software verifies write returned TEE Opcode in the response
12) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
13) Host software verifies read returned TEE Opcode in the response and all 1's for the data
14) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
15) Host software verifies read returned TEE Opcode in the response and expected data pattern A
16) Host software generates TEUpdate memory request to set TE State to 0 for the test memory address
17) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern A
18) Host software verifies write returned non-TEE Opcode in the response
19) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
20) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
21) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern B
22) Host software verifies write returned non-TEE Opcode in the response
23) Host trusted TEE (TVM) software generates a memory read request to the same address with TEE opcode
24) Host software verifies read returned non-TEE Opcode in the response and all 1's for the data
25) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
26) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A

Pass Criteria:

- TE/non-TEE opcode returned is correct for all writes & reads
- Read data returned for all reads is expected
- Data pattern of all 1’s returned for reads with TE State mismatch

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Pass criteria is not met

14.11.7.7 Explicit Out-of-band TE State Changes w Read and Write Access Control

This test verifies basic optional Explicit Out-of-band TE State Change functionality of the target device. Specifically, this covers the case with Read and Write Access Control both enabled, where the target is expected to a) check the TE State for writes and drop the write and return the current TE State in the write response if there is a TE State mismatch, b) check the TE State for reads and return current TE State in the read response and return all 1's data pattern if there is a TE State mismatch. Utilizing out-of-band TSP TE State change request and response, this tests the following TSP tables: Target Behavior for Read Access Control and Target Behavior for Write Access Control.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for Explicit Out-of-band TE State Changes and Read Access Control and Write Access Control

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to enable Explicit Out-of-band TE State Changes, Read Access Control and Write Access Control
    a. TE State Change and Access Control Enable, Explicit Out-of-band TE State Change & Read Access Control & Write Access Control shall all be set
    b. One Explicit Out-of-band TE State Granularity bit is set.
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable and to enable receiving TEE Opcodes
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target TE State to set TE State to 1 for the test memory address

6) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern A
7) Host software verifies write returned TEE Opcode in the response
8) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
9) Host software verifies read returned TEE Opcode in the response and expected data pattern A
10) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern B
11) Host software verifies write returned TEE Opcode in the response
12) Host untrusted (VM) software generates a memory read request to the same address with non-TEE opcode
13) Host software verifies read returned TEE Opcode in the response and all 1's for the data
14) Host trusted TEE (TVM) software generates a memory read request to the same address with a TEE opcode
15) Host software verifies read returned TEE Opcode in the response and expected data pattern A
16) Host software issues Set Target TE State to set TE State to 0 for the test memory address

17) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and known data pattern A
18) Host software verifies write returned non-TEE Opcode in the response
19) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
20) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
21) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with a TEE opcode and known data pattern B
22) Host software verifies write returned non-TEE Opcode in the response
23) Host trusted TEE (TVM) software generates a memory read request to the same address with TEE opcode
24) Host software verifies read returned non-TEE Opcode in the response and all 1's for the data
25) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
26) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A

Pass Criteria:

- TE/non-TEE opcode returned is correct for all writes & reads
- Read data returned for all reads is expected
- Data pattern of all 1's returned for reads with TE State mismatch

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Pass criteria is not met

14.11.7.8 Initiator-based memory encryption

This test verifies basic optional initiator-based memory encryption by disabling target based encryption.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for Explicit Out-of-band TE State Changes and Read Access Control and Write Access Control

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to disable target encryption
    a. Memory Encryption Features Enable flags, all bits is set to 0
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable and to enable receiving TEE Opcodes
4) Host software receives Lock Target Configuration Response
5) Host software encrypts data before writing
6) Host software writes encrypted data to the locked target device with known data pattern
7) Host software reads encrypted data from the target
8) Host software decrypts the data and verifies it matches the known data pattern

Pass Criteria:

- Data does not match expected pattern after the decrypt by the host

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Pass criteria is not met

14.11.7.9 Target-based CKID-based memory encryption invalid CKID range

This test verifies basic invalid CKID range handling for optional target-based CKID-based memory encryption when the target supports a limited number of CKID. This tests the following TSP tables: Target Behavior for Invalid CKID Ranges.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for target-based CKID-based Encryption and the target limits the CKID range that is supported (CKID Base Required is set in Test 14.11.7.3 is set)

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to enable target-based CKID-based memory encryption
    a. Memory Encryption Features Enable flags, Encryption set, CKID-based Encryption set
    b. Memory Encryption Algorithm Select has a single algorithm selected that the target will utilize for data at rest security. Shall be one of the algorithms supported by the target as reported by Get Target Capabilities.
    c. CKID Base = the base the target supports
    d. Number of CKIDs = Number of CKIDs the target supports – 1, so that CKID Base + Number of CKIDs is out of range.
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target CKID Specific Key to associate a key with a CKID
    a. CKID assigned in valid range supported by the target
    b. CKID Type = OSCKID
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key to utilize for the CKID
6) Host software receives Set Target CKID Specific Key Response
7) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode, CKID assigned and known data pattern A
8) Host software verifies write returned non-TEE Opcode in the response
9) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode and the assigned CKID
10) Host software verifies read returned non-TEE opcode in the response and the data matches the known data pattern A

    // Attempt to write with CKID out of range
11) Host untrusted (VM) software generates a full cache-line memory write request to the same address with a non-TEE opcode and the CKID = CKID Base + Number of CKIDs, programmed in step 1 above using a known data pattern B

    // Verify write was dropped
12) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode using the assigned CKID
13) Host software verifies read returned non-TEE opcode in the response and the data matches the known data pattern A

    // Attempt to read with CKID out of range
14) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode with the CKID = CKID Base + Number of CKIDs programmed in step 1 above
15) Host software verifies read returned non-TEE opcode in the response and the data returns an all 1's pattern

Pass Criteria:

- Read data returned for all reads is expected

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Set Target CKID Specific Key results in a TSP Error Response
- Pass criteria is not me

14.11.7.10 Target-based CKID-based memory encryption invalid CKID Type

This test verifies basic invalid CKID Type handling for optional target-based CKID-based memory encryption. This tests the following TSP tables: Target Behavior for Verifying CKID Type.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for target-based CKID-based Encryption

Topologies:
- SHDA

Test Steps:
1) Host software issues Set Target Configuration to enable target-based CKID-based memory encryption
    a. Memory Encryption Features Enable flags, Encryption set, CKID-based Encryption set
    b. Memory Encryption Algorithm Select has a single algorithm selected that the target will utilize for data at rest security. Shall be one of the algorithms supported by the target as reported by Get Target Capabilities.
    c. For targets that limit the CKID range (CKID Base Required is set in Test 14.11.7.3 is set) CKID Base Required is set and CKID Base and Number of CKIDs is set to a range the target supports
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target CKID Specific Key to associate a key with a CKID
    a. CKID assigned in valid range supported by the target
    b. CKID Type = OSCKID
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key to utilize for the CKID
6) Host software receives Set Target CKID Specific Key Response
7) Host untrusted (VM) software generates a full cache-line memory write request to the test address with the CKID assigned with a non-TEE opcode using a known data pattern A
8) Host software verifies write returned non-TEE Opcode in the response
9) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
10) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
11) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with the CKID assigned with a TEE opcode using a known data pattern B
12) Host software verifies write returned non-TEE Opcode in the response
13) Host trusted TEE (TVM) software generates a memory read request to the same address with the CKID assigned with a TEE opcode
14) Host software verifies read returned non-TEE Opcode in the response and fixed all 1's data pattern
15) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
16) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
17) Host software issues Set Target CKID Specific Key to associate a key with a CKID
    a. CKID assigned in valid range supported by the target
    b. CKID Type = TVMCKID
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key to utilize for the CKID
18) Host software receives Set Target CKID Specific Key Response
19) Host trusted TEE (TVM) software generates a full cache-line memory write request to the same address with the CKID assigned with a TEE opcode using a known data pattern A
20) Host software verifies write returned TEE Opcode in the response
21) Host trusted TEE (TVM) software generates a memory read request to the same address with the CKID assigned with a TEE opcode
22) Host software verifies read returned TEE Opcode in the response and expected data pattern A
23) Host untrusted (VM) software generates a full cache-line memory write request to the same address with the CKID assigned with a non-TEE opcode using a known data pattern B
24) Host software verifies write returned TEE Opcode in the response
25) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
26) Host software verifies read returned TEE Opcode in the response and fixed all 1's data pattern

27) Host trusted TEE (TVM) software generates a memory read request to the same address with the CKID assigned with a TEE opcode
28) Host software verifies read returned TEE Opcode in the response and expected data pattern A

Pass Criteria:

- TE/non-TEE opcode returned is correct for all writes & reads
- Read data returned for all reads is expected

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Set Target CKID Specific Key results in a TSP Error Response
- Pass criteria is not met

14.11.7.11 Target-based CKID-based memory encryption clearing keys

This test verifies basic clear key handling for optional target-based CKID-based memory encryption.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for target-based CKID-based Encryption

Topologies:
- SHDA

Test Steps:
1) Host software issues Set Target Configuration to enable target-based CKID-based memory encryption
    a. Memory Encryption Features Enable flags, Encryption set, CKID-based Encryption set
    b. Memory Encryption Algorithm Select has a single algorithm selected that the target will utilize for data at rest security. Shall be one of the algorithms supported by the target as reported by Get Target Capabilities.
    c. For targets that limit the CKID range (CKID Base Required is set in Test 14.11.7.3 is set) CKID Base Required is set and CKID Base and Number of CKIDs is set to a range the target supports
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target CKID Random Key to associate a key with a CKID
    a. CKID assigned in valid range supported by the target
    b. CKID Type = OSCKID
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key Entropy X to utilize for the CKID
6) Host software receives Set Target CKID Random Key Response
7) Host untrusted (VM) software generates a full cache-line memory write request to the test address with the CKID assigned with a non-TEE opcode using a known data pattern A
8) Host software verifies write returned non-TEE Opcode in the response
9) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
10) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
11) Host software issues Clear Target CKID Key to disassociate a key with a CKID
    a. CKID assigned in valid range supported by the target
12) Host software receives Clear Target CKID Key Response
13) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
14) Host software verifies read returned non-TEE Opcode in the response and expected data pattern is NOT A
15) Host software issues Set Target CKID Random Key to associate a key with a CKID
    a. CKID assigned in valid range supported by the target
    b. CKID Type = OSCKID
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key Entropy X to utilize for the CKID
16) Host software receives Set Target CKID Random Key Response
17) Host untrusted (VM) software generates a memory read request to the same address with the CKID assigned with a non-TEE opcode
18) Host software verifies read returned non-TEE Opcode in the response and expected data pattern is NOT A

Pass Criteria:
- TE/non-TEE opcode returned is correct for all writes & reads
- Read data returned for all reads is expected

Fail Conditions:
- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Set Target CKID Specific Key results in a TSP Error Response
- Clear Target CKID Key results in a TSP Error Response
- Pass criteria is not met

14.11.7.12 Target-based range-based memory encryption

This test verifies basic setting and clearing of encryption keys for optional target-based range-based memory encryption.

Prerequisites:

- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for target-based Range-based Encryption

Topologies:

- SHDA

Test Steps:

1) Host software issues Set Target Configuration to enable target-based range-based memory encryption
    a. Memory Encryption Features Enable flags, Encryption set, Range-based Encryption set
    b. Memory Encryption Algorithm Select has a single algorithm selected that the target will utilize for data-at-rest security. Shall be one of the algorithms supported by the target as reported by Get Target Capabilities.
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target Range Specific Key to associate a key with the first memory range
    a. Range ID = 0
    b. Range Start and Range End describe the test address range on the host
    c. Validity Flags, Bit[0] set
    d. Data Encryption Key to utilize for the memory Range ID
6) Host software receives Set Target Range Specific Key Response
7) Host software generates a full cache-line memory write request for the test address range using a known data pattern
8) Host software generates a memory read request to the same address
9) Host software verifies the data matches the known data pattern
10) Host software issues Clear Target Range Specific Key to remove the association of a key with the memory range
    a. Range ID = 0
11) Host software receives Clear Target Range Specific Key Response
12) Host software generates a full cache-line memory write request for the test address range using a known data pattern
13) Host software generates a memory read request to the same address
14) Host software verifies the data matches the known data pattern

Pass Criteria:

- Data does not match expected pattern after any reads

Fail Conditions:

- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Set Target Range Specific Key results in a TSP Error Response
- Clear Target Range Key results in a TSP Error Response
- Pass criteria is not met

14.11.7.13 Target-based range-based memory encryption clearing keys

This test verifies basic clear key handling for optional target-based range-based memory encryption.

Prerequisites:
- Device must support CXL.cachemem TSP security
- Device must support Compliance Mode DOE and SPDM over DOE
- Host software has established a secure SPDM link to the device
- Test 14.11.7.3 passed AND the target reports support for target-based range-based Encryption

Topologies:
- SHDA

Test Steps:
1) Host software issues Set Target Configuration to enable target-based range-based memory encryption
    a. Memory Encryption Features Enable flags, Encryption set, Range-based Encryption set
    b. Memory Encryption Algorithm Select has a single algorithm selected that the target will utilize for data at rest security. Shall be one of the algorithms supported by the target as reported by Get Target Capabilities.
2) Host software receives Set Target Configuration Response
3) Host software issues Lock Target Configuration to make the configuration immutable
4) Host software receives Lock Target Configuration Response
5) Host software issues Set Target Range Random Key to associate a key with a memory range
    a. RangeID = 0
    b. Range Start/Range End = valid 4k HDM memory range containing the test address
6) Host software receives Set Target Range Random Key Response
7) Host untrusted (VM) software generates a full cache-line memory write request to the test address with an address within the range the key was set for with a non-TEE opcode using a known data pattern A
8) Host software verifies write returned non-TEE Opcode in the response
9) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
10) Host software verifies read returned non-TEE Opcode in the response and expected data pattern A
11) Host software issues Clear Target Range Key to disassociate the test address from the key
    a. RangeID = 0
12) Host software receives Clear Target Range Key Response
13) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
14) Host software verifies read returned non-TEE Opcode in the response and expected data pattern is NOT A
15) Host software issues Set Target Range Random Key to associate a key with a memory range
    a. RangeID = 0
    b. Range Start/Range End = valid 4k HDM memory range containing the test address
16) Host software receives Set Target Range Random Key Response
17) Host untrusted (VM) software generates a memory read request to the same address with a non-TEE opcode
18) Host software verifies read returned non-TEE Opcode in the response and expected data pattern is NOT A

Pass Criteria:
- TE/non-TEE opcode returned is correct for all writes & reads
- Read data returned for all reads is expected

Fail Conditions:
- Set Target Configuration results in a TSP Error Response
- Lock Target Configuration results in a TSP Error Response
- Set Target Range Specific Key results in a TSP Error Response
- Clear Target Range Key results in a TSP Error Response
- Pass criteria is not met