Life Cycle of an SGX Enclave

SGX Enclave:

- Intel SGX provides hardware features that creates a form of user level TEE. The enclave is an isolated region of code and data within applications address space.
- Data within an enclave can be accessed by only with code within the same enclave.
- The enclave is able to protect its data using Enclave Page Cache (EPC); a secure storage used by the processor to store pages when they are part of an executing enclave.
- The EPC is built from chunks of 4KB pages; aligned on a 4KB boundary and each page has security attributes in the Enclave Page Cache Map (EPCM), an internal micro-architecture structure that is not accessible by the software. It tracks the content of each EPC page, and enforces access control for accessing the pages.
- A Cryptographic hash of the code and data residing in an enclave at the time of initialization. The measurement is used to verify that the loaded enclave is what the enclave claims it is.
- An enclave is a protected area in the application's address space, which provides confidentiality and integrity even in the presence of privileged malware.
- Attempted accesses to the enclave memory area from software not resident in the enclave are prevented even from privileged software such as virtual machine monitors, BIOS, or operating systems.
- It provides a safe place for code and data in application. Intel provides some special hardware instruction to create and support enclave. Intel SGX enclave memory is protected even from privileged software.

SGX Enclave Instructions and Protected Rings:

The enclave instructions available with SGX are divided under two protections rings.

1. **Ring 0 Instructions:**

   ECREATE, EADD and EINIT are used for EPC management thus executed by privileged software such as OS and VMM

2. **Ring 3 Instructions:**

   EENTER, EEXIT, EGETKEY, EREPORT and ERESUME are used by the user space software to execute functionality within or between enclaves.

Overview of an SGX Enclave Life Cycle:

An enclave's life cycle is deeply intertwined with resource management, specifically the allocation of EPC pages. Therefore, the instructions that transition between different life cycle states can only be executed by the system software.

Following are the major transitions during an SGX enclave's life cycle:

1. Creation (ECREATE)
2. Loading (EADD, EEXTEND)
3. Initialization (EINIT)
4. Enter/Exit the Enclave (EENTER/EEXIT)
5. Teardown (EREMOVE)

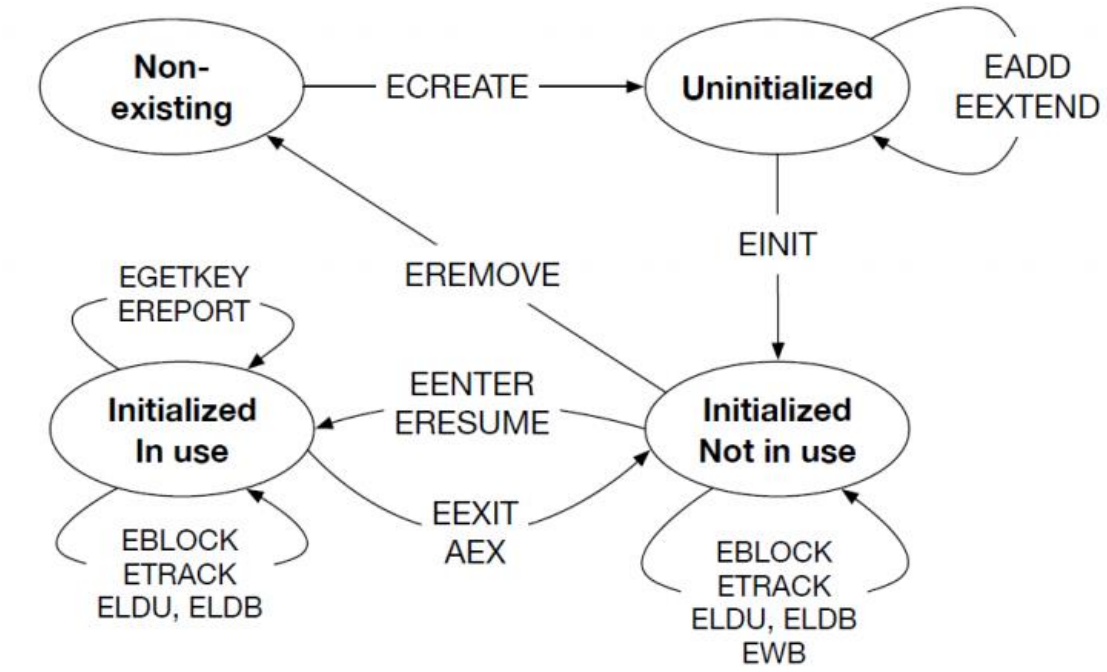

Figure: 1 The SGX enclave life cycle management instructions and state transition diagram

Enclave Creation (ECREATE):

- Creates a unique instance of an enclave, establishes the linear address range, and serves as the enclave's root of trust.
    - Enclave mode of operation (32/64).
    - Processor features that enclave supports.
    - Debug is allowed or not.
- This information stored within a Secure Enclaves Control Structure (SECS) generated by ECREATE.

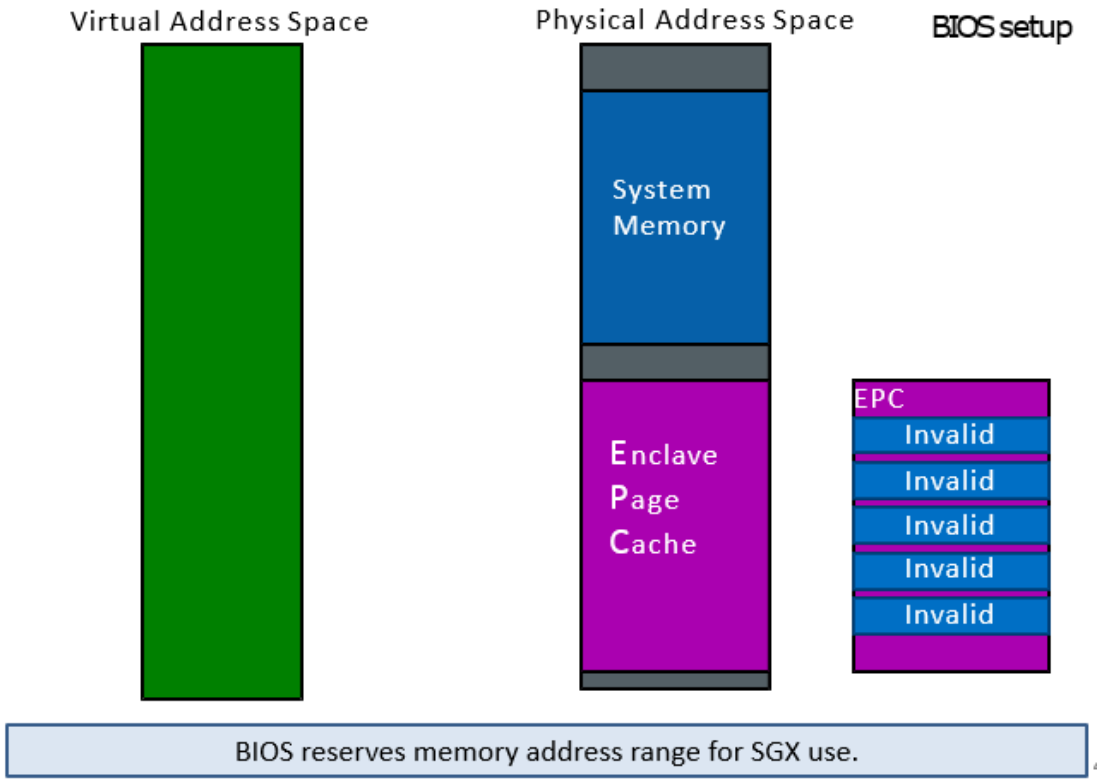

Figure: 2 SGX Enclave Life Cycle – BIOS Memory before ECREATE

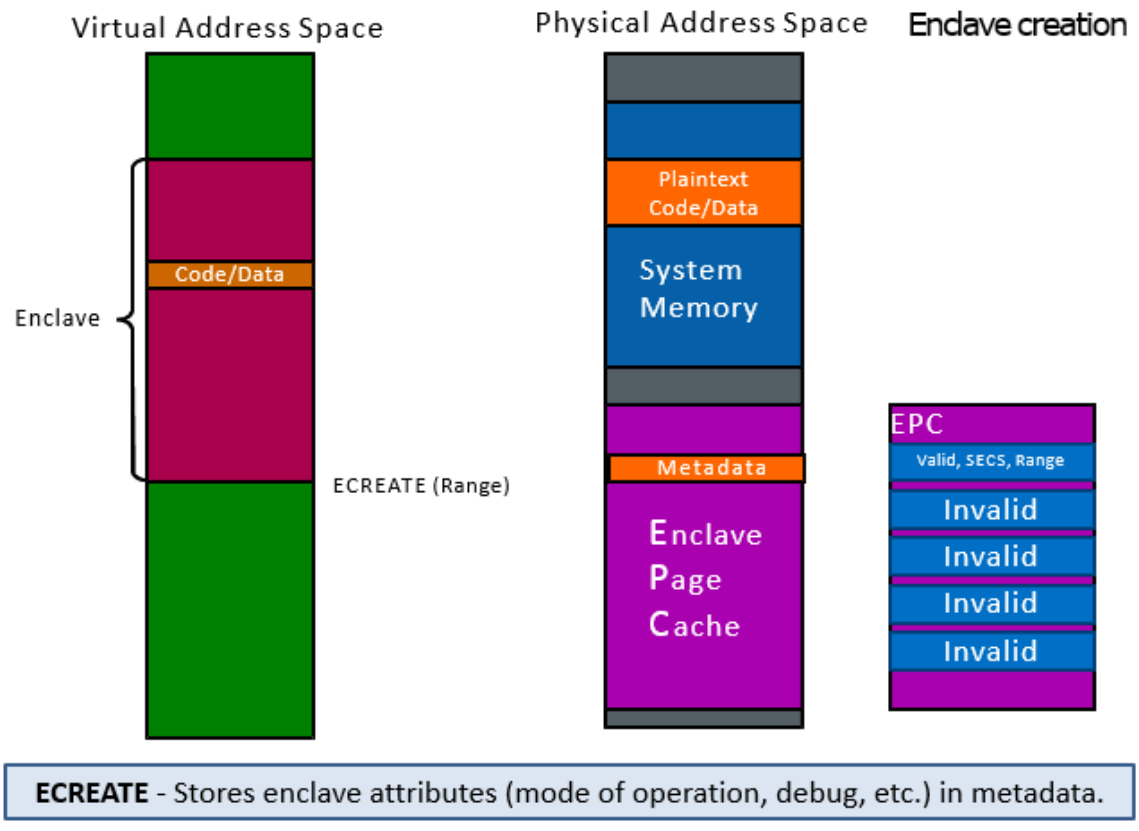

Figure: 3 SGX Enclave Life Cycle – Enclave Creation (ECREATE)

Loading (EADD, EEXTEND):

EADD:

- Add Regular (REG) or Thread Control Structure (TCS) pages into the enclave.
    - System software responsible for selecting free EPC page, type, and attributes, content of the page and the enclave to which the page added to.
- Initial EPCM entry to indicate type of page (REG, TCS).
    - Linear address, RWX, associate the page to enclave SECS.

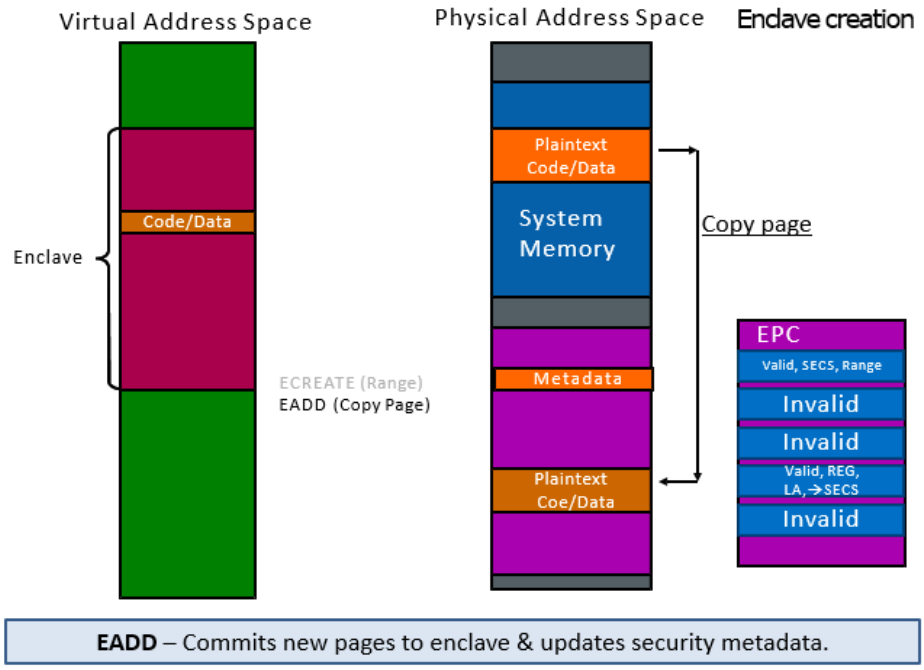

Figure: 4 SGX Enclave Life Cycle – Enclave Loading (EADD)

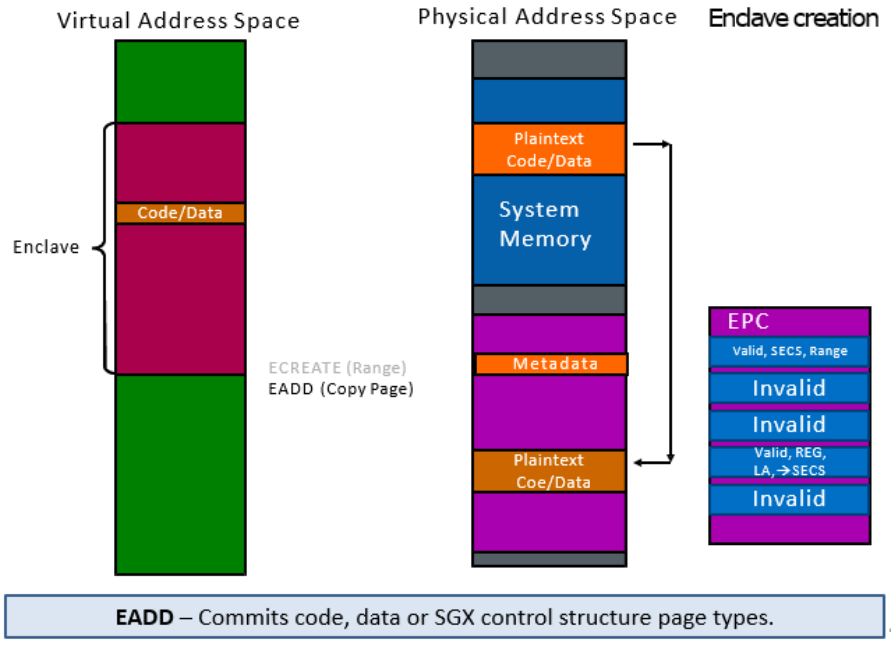

Figure: 5 SGX Enclave Life Cycle – Enclave Loading (EADD)

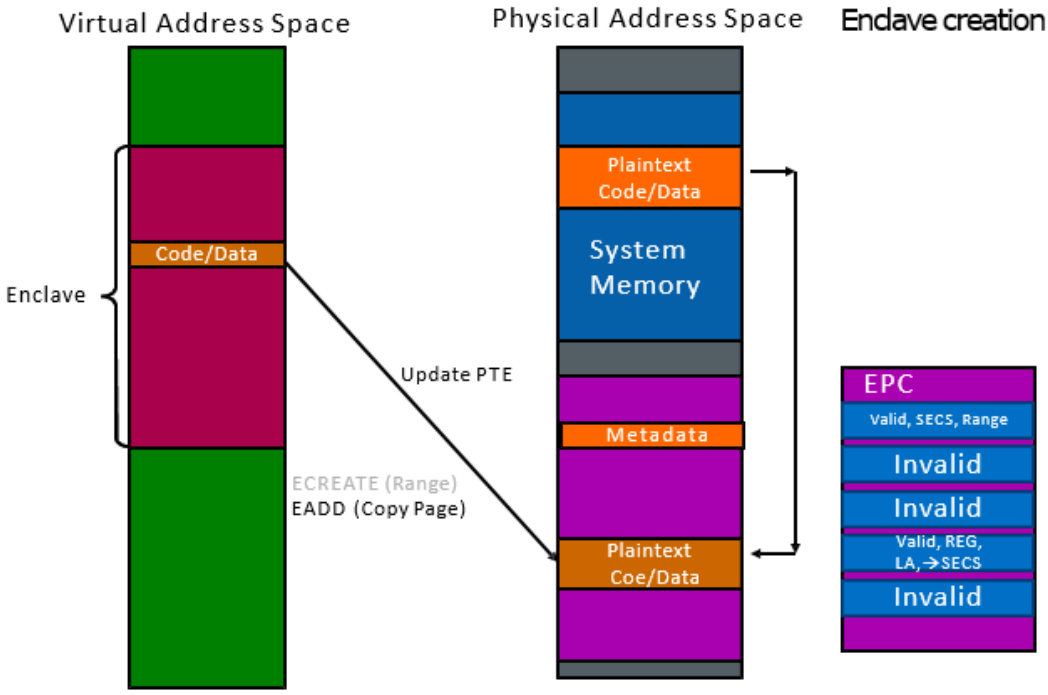

Figure: 6 SGX Enclave Life Cycle – Enclave Loading- EADD copy (EADD)

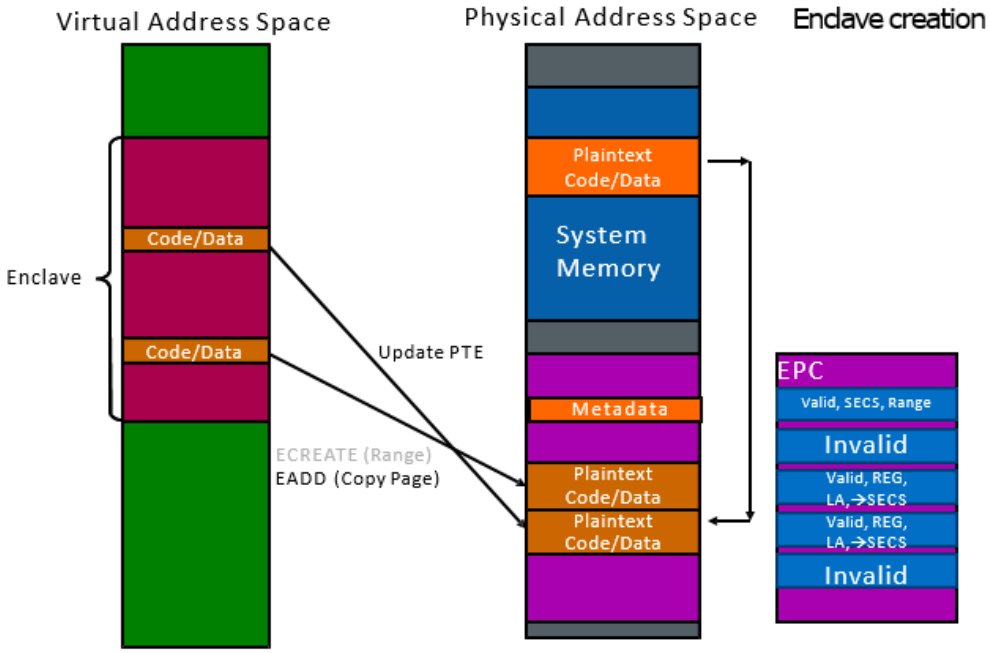

Figure: 7 SGX Enclave Life Cycle – Enclave Loading- EADD copy (EADD)

EEXTEND:

- Generates a cryptographic hash of the content of the enclave in 256Byte chunks.
    - EEXTEND 16 times for measuring a 4K page

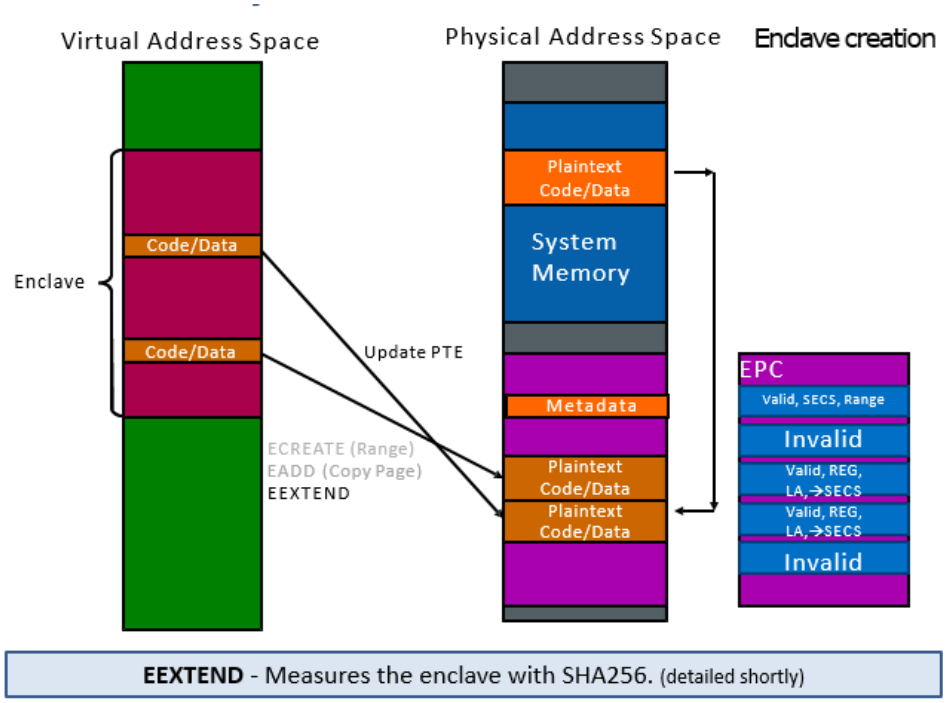

Figure: 8 SGX Enclave Life Cycle – Enclave Loading (EEXTEND)

Initialization (EINIT):

- Verifies the enclave's content against the ISV's signed SIGSTRUCT and initializes the enclave – Mark it ready to be used.
  - Validate SIGSTRUCT is signed using SIGSTRUCT public key.
  - Enclave measurement matches the measurement specified in SIGSTRUCT.
- Enclave attributes compatible with SIGSTRUCT.
- Record sealing identity (sealing authority, product id, SVN) in the SECS

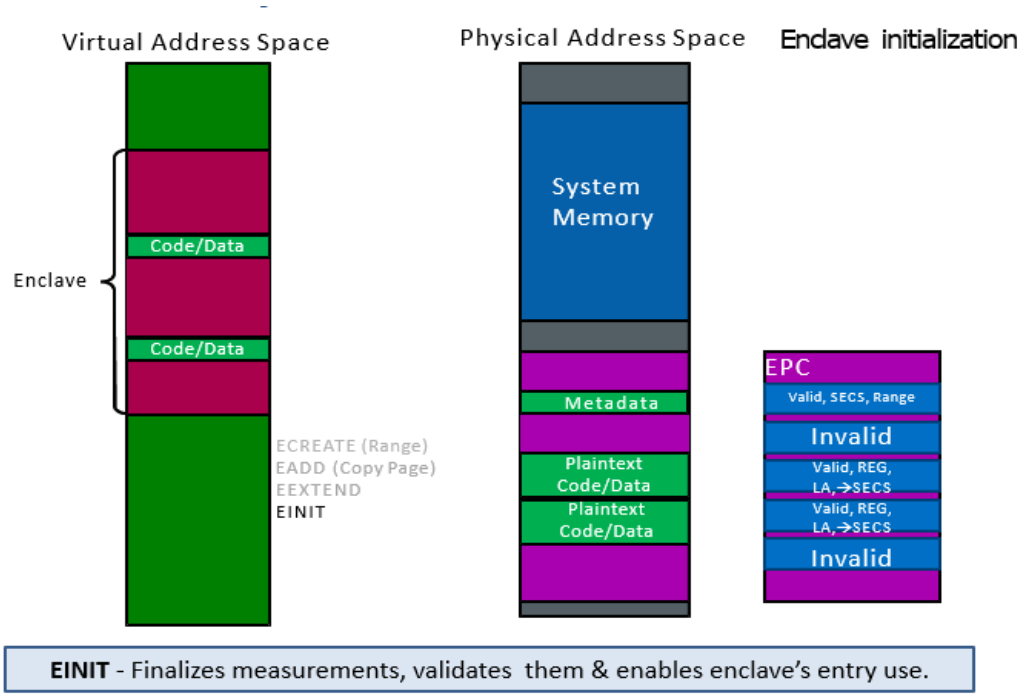

Figure: 9 SGX Enclave Life Cycle – Enclave Initialization (EINIT)

Enter/Exit the Enclave (EENTER/EEXIT):

EENTER (Synchronous Enclave Entry):

- Check that TCS is not busy and flush TLB entries for enclave addresses.
- Transfer control from outside enclave to pre-determined location inside the enclave.
- Change the mode of operation to be in enclave mode.
- Save RSP/RBP for later restore on enclave asynchronous exit.
- Save XCR0 and replace it with enclave XFRM value.
- If debug enclave and software wishes to debug allows traps, breakpoints, single step, Else, set HW so the enclave appears as a single instruction.

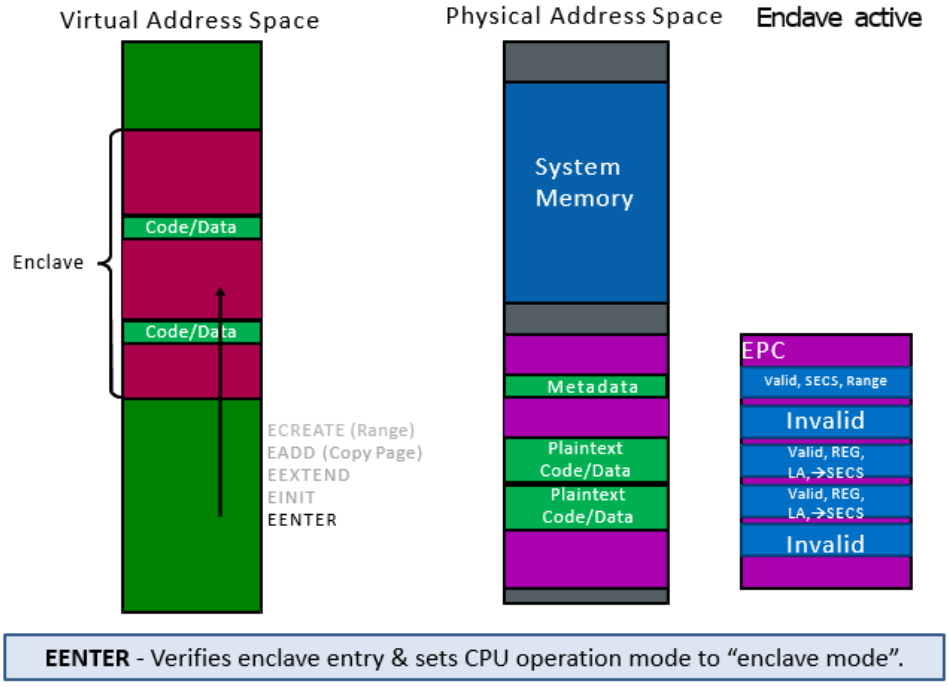

Figure: 10 SGX Enclave Life Cycle – Enclave Enter (EENTER)

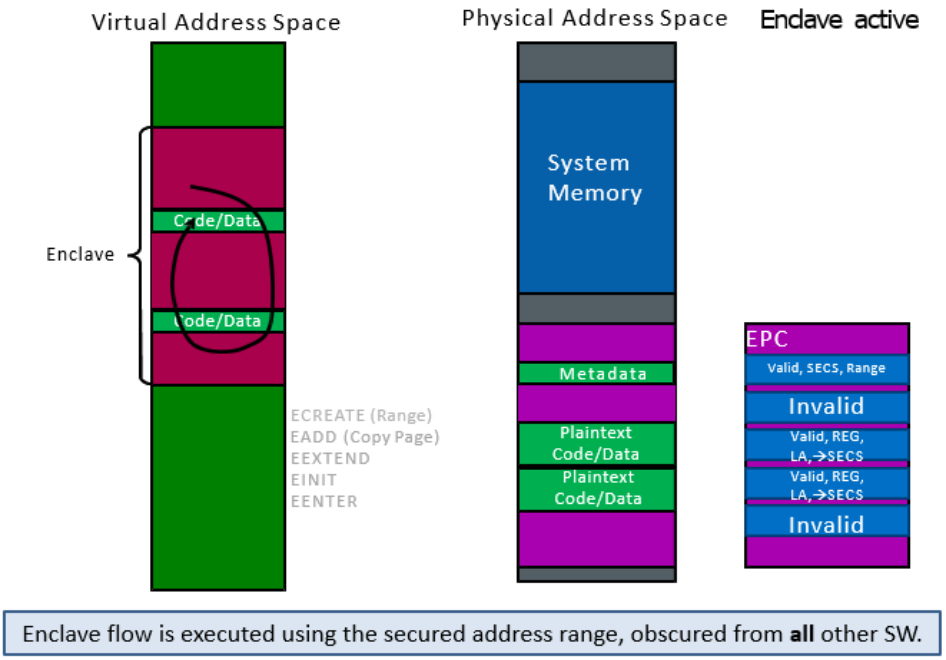

Figure: 11 SGX Enclave Life Cycle – Enclave Enter (EENTER)

EEXIT (Synchronous Enclave Exit):

- Clear enclave mode and TLB entries for enclave addresses.
- Transfer control from inside enclave to a location outside specified by RBX.
    - Mark TCS as not busy.
- Responsibility to clear register state is on enclave writer (run time system)

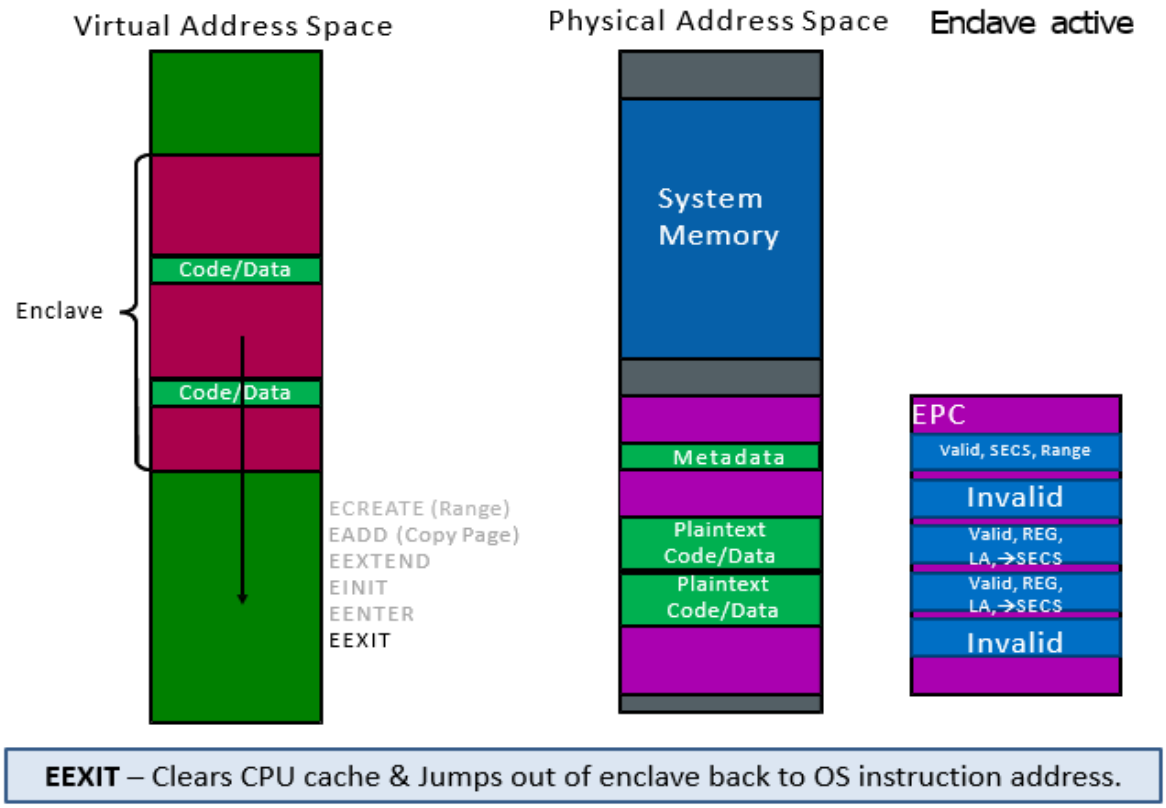

Figure: 12 SGX Enclave Life Cycle – Enclave Exit (EEXIT)

Teardown (EREMOVE):

- EREMOVE deallocates/removes a 4KByte page permanently from the EPC.
- A page cannot be removed until there is no thread executing code inside this enclave.
- A SECS page cannot be removed until all the regular pages of this enclave are removed.
- The SECS page is removed at the very last, and this also destroys the Enclave.

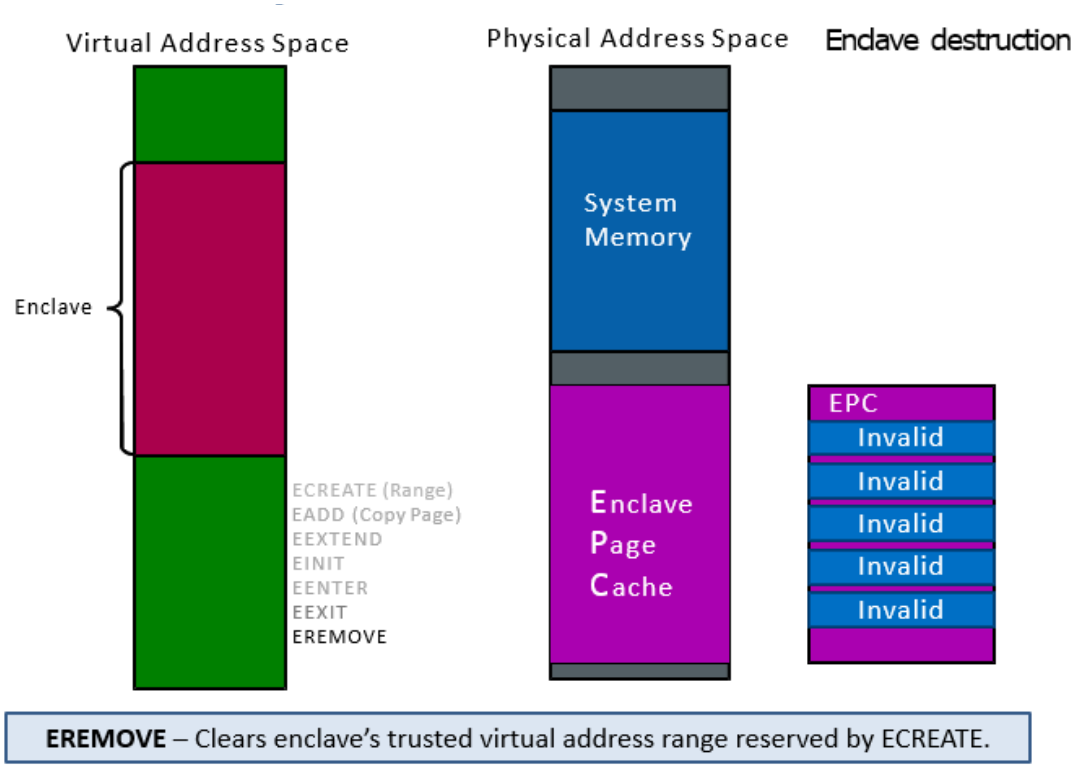

Figure: 13 SGX Enclave Life Cycle – Teardown Enclave (EREMOVE)

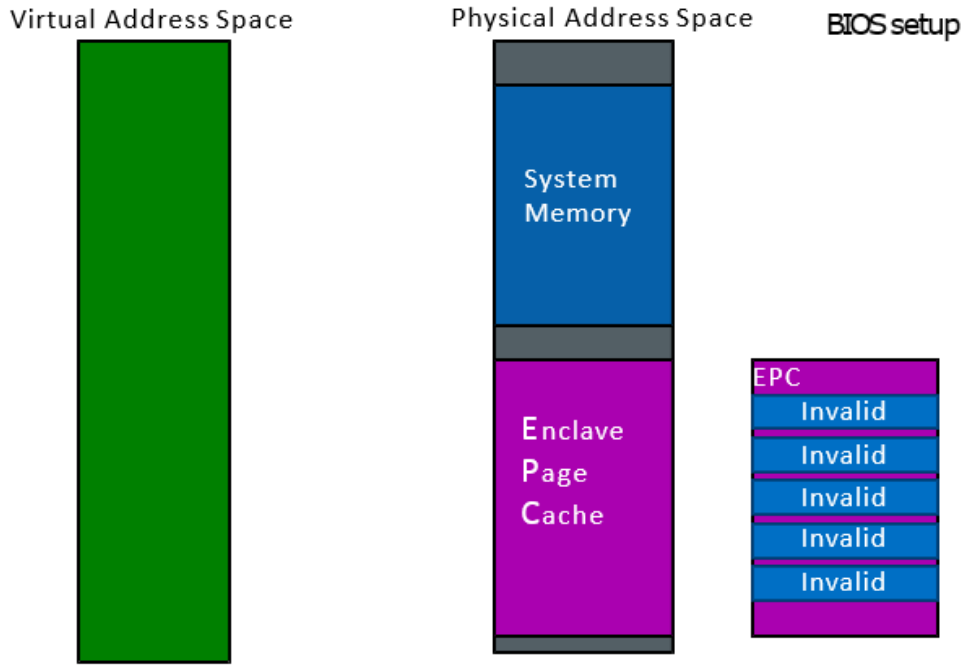

Figure: 14 SGX Enclave Life Cycle – BIOS Memory after EREMOVE