

EREPORT

MAC

MACed Fields

ATTRIBUTES

MRENCLAVE

MRSIGNER

ISVPRODID

ISVSVN

REPORTDATA

CPUSVN

KEYID

Equal?

Yes → Trust Report

No → Reject Report

AES-CMAC

Report Key

KEYREQUEST

ATTRIBUTEMASK

KEYNAME

CPUSVN

KEYID

ISVSVN

KEYPOLICY

MRENCLAVE

MRSIGNER

SECS

PADDING

ATTRIBUTES

BASEADDR

SIZE

ISVPRODID

ISVSVN

MRENCLAVE

MRSIGNER

SSAFRAME

SIZE

EGETKEY

Current  
CPUSVN

PADDING

zero

MRENCLAVE

zero

KEYID

zero

MASKEDATTRIBUTES

KEYNAME

CPUSVN

OWNEPOCH

Key Derivation Material

SEAL\_FUSES

OWNEREPOCH  
SGX Register

SEAL\_FUSES

SGX Master  
Derivation Key

AES-CMAC  
Key Derivation

128-bit  
Report key