FDE iTC: Encryption Engine (EE) cPP Functional and Assurance Requirements

BEV (Border Encryption Value) - the key(s) (or secret(s)) that is passed from the AA to the EE

Cryptographic Support

The functional requirements address the primary threats of a brute force attack against the key space and the failure of a cryptographic component.

Cryptographic Key Management

Conformant implementations shall contain at least one key: a Data Encryption Key (DEK). Conformant implementations may also contain other keys, e.g., intermediate keys, Key Encryption Keys (KEKs), which either wrap the DEK, or form a hierarchy of keys in such a way that protects the DEK from unauthorized disclosure. The following sections specify the requirements for the production of the keys.

Cryptographic Key Generation (DEK)

The product may generate a DEK, of sufficient strength, using an approved Random Bit Generator (RBG), or may receive a DEK from a local host (the machine the product is directly connected to, or an encrypted DEK from outside the local host.

Evaluation Activities:

The evaluator shall review the vendor's documentation to determine that it describes how the product obtains a DEK (either generating the DEK or receiving from the environment). If the product received the DEK from the IT environment that is not directly connected to the product, then the documentation states how the DEK is protected when in transit. The documentation, in this case, describes how the product "unwraps" the DEK.

The evaluator uses the description of the interface between the RBG and the product to determine that it requests a key greater than or equal to the required key sizes.

Cryptographic Key Generation (Intermediate Keys)

This is an optional requirement, since the product may use the Border Encryption Value (BEV) to "unwrap" the DEK and may not use intermediate keys.

The product shall generate intermediate keys using an approved Random Bit Generator (RBG), or a Key Derivation Function (KDF). The number of key used is implementation dependent and there are no requirements regarding the number.

The intermediate keys shall be the size of the DEK.

Cryptographic Key and Key Material Protection

The product shall not write keys or keying material to persistent storage (non-volatile) unless they meet one of the following conditions:

- **It is protected by key masking, using an approved algorithm[1];**
- **It is used as a provisioning key that does not provide access to the drive after provisioning;**
- **It is a non-secret value (e.g. salt, IV's)**.

Application Note:

When stored, the DEK is always encrypted (wrapped) and only exists in plaintext form, in volatile memory, when it is being used to encrypt or decrypt data.

Cryptographic Key and Key Material Destruction

The product shall destroy all cryptographic keys and cryptographic security parameters when no longer required using one or more of the approved methods that meet NIST SP800-88.

Keys, including intermediate keys, and key material that are no longer needed are destroyed in volatile memory by using an approved method. When the DEK residing in volatile memory is no longer needed, there is no requirement to destroy the key, since it will be "destroyed" when the machine is powered down.

There may be instances where keys or key material that are contained in persistent storage are no longer needed and require destruction. In these cases, the destruction method conforms to an approved method.

Evaluation Activities:

The evaluator shall review the vendor's documentation for a description of how keys are generated, where the key material resides, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed[2].

---

[1] NIST SP 800-38F contains methods for performing key wrap – Algorithms 1-6 are acceptable as long as AES is used.

[2] The expectation is there will be a lot of details here that will go in an appendix that is not made public.

The product shall support repurposing the storage device by cryptographically erasing the DEK.

For the purposes of this document, *cryptographically erasing* expresses a command (from the AA, or directly from the user) that is meant to destroy the DEK, uses one of the approved destruction methods.

Key Chaining

The product shall maintain a chain of keys with the effective strength of the BEV so that the decryption or derivation of the DEK is not possible without a cryptographic exhaust of the BEV by using one of the following methods:

- **A chain of one or more intermediary keys from BEV to the DEK using the appropriate algorithm from the approved key wrap requirement or the Cryptographic Key Generation (Intermediate Keys).**

Evaluation Activities:

Note: The BEV could be an encrypted DEK.

Note: BEV could be more than one value.

If the product interfaces with the operational environment (OE), then it likely consumes authorization factors and keys provided through those interfaces. In particular, it may have an interface with a separate AA product. The EE product may use certain parameters passed to it from the OE (e.g. an AA product) as authorization factors, keys, or both.

The vendor shall provide a documentation containing a description of their key hierarchy for all keys between the BEV and the DEK. This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from and that the effective strength of the DEK is maintained throughout the Key Chain. The evaluator shall examine the key hierarchy to ensure that it either passes the BEV directly as the DEK, or appropriately masks the DEK using an approved method.

An Appendix will detail the requirements that have to be included in a document from the vendor for the Key Management Essay.

Cryptographic Operations

This section stipulates the allowed cryptographic operations for use in product functional requirements.

Cryptographic Operation (Data Encryption)

The product shall encrypt and decrypt all user data on the storage device using AES in XTS, CBC, or GCM mode and cryptographic sizes 128 or 256 bits that meet AES as

specified in ISO 18033-3, XTS as specified in IEEE 1619, and CBC as specified in ISO 10116, and GCM as specified in ISO 19772.

Application Note:

This cPP considers both host (or software) encryption and storage device (or hardware) encryption. In software encryption, a general purpose processor on the host platform performs data encryption and decryption. In hardware encryption, dedicated hardware within a general purpose controller or the storage device's SOC or a dedicated (co-)processor performs data encryption and decryption (distinct from the host platform's operating environment).

Evaluation Activities:

- **Software Encryption**

The evaluator SHALL consult the vendor's documentation in performing the evaluation activities for this requirement. The evaluator ensures the comprehensiveness of the description, confirms how the product writes the data to the storage device, and the point at which it applies the encryption function. Since the product implement the encryption/decryption functionality entirely in software on the host platform, the vendor's documentation must make the case that all methods of accessing all the storage devices on the platform will pass through these functions.

In performing their review, the evaluator shall determine that the vendor's documentation covers the initialization of the product and the activities the product performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the product. The documentation shall also describe areas of the disk that it does not encrypt (e.g., portions associated with the Master Boot Records (MBRs), boot loaders, partition tables, etc).

If the product supports multiple disk encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all storage devices on the platform.

The evaluator SHALL review the vendor's documentation to determine that it describes the initial steps needed to enable the FDE function, including any necessary preparatory steps. The documentation shall provide sufficient instructions for all platforms to ensure that when the user enables encryption the product encrypts all hard storage devices.

The evaluators SHALL perform the following test activities:

• Test 1: Ensure that following the product provisioning activities only encrypted data resides on all storage devices. For areas of the storage device unencrypted data, ensure the vendor provides justification in their documentation and that the user cannot write user data or keying material to these areas. The evaluator can perform the examination of the disks in several ways. They may physically remove the storage device and then insert it into another computer. Alternatively, they may boot the platform that contains

the encrypted storage device from an external platform and then directly access the encrypted storage device.

• Test 2: Ensure that product encrypts data (including data stored in page files in the OS) when written to the storage device. The evaluator shall test this in a manner consistent with the previous test; that is, the evaluator may power on the system “normally”, write data to the storage device, and then use the methods mentioned in the previous test to ensure those data do not appear unencrypted on the storage device(s).

• Hardware Encryption

The evaluator SHALL consult the vendor’s documentation and execute tests in performing the evaluation activities for this requirement.

The vendor’s documentation SHALL provide a description of the data encryption engine, its components, and details about its implementation (e.g. integrated within the device’s main SOC or separate co-processor). The vendor’s documentation shall provide a functional (block) diagram showing the main components (such as memories and processors) and the data path between device’s host interface and the device’s persistent media storing the data. The diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine. The vendor documentation shall describe the data flow from the device’s host interface to the device’s persistent media storing the data. The documentation shall provide information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted Master Boot Record area). In its review the evaluator shall ensure that all cases in which data bypasses the encryption engine align with the SPD.

The vendor’s documentation SHALL provide a description of the device’s boot initialization, the encryption engine initialization process, and at what moment the product enables the encryption engine. The evaluator shall validate that the product does not allow for the transfer of user data before it fully initializes the encryption engine.

The product under evaluation may contain an area with unencrypted data used for system initialization; this area is outside the scope of for remainder of this assurance activity.

The evaluator SHALL perform the following tests:

1. Write data to random locations, erase, and compare:
    - Ensure device is initialized and encryption engine is ready;
    - Determine a random character pattern of at least 64 KB;

- Retrieve information on what the device's lowest and highest logical address is for which encryption is enabled;
- Randomly select several logical address locations within the device's lowest to highest address range;
- Write the character pattern at the selected locations;
- Engage device's functionality for generating a new encryption key;
- Read from the same locations at which the data was written;
- Compare the retrieved data to the written data and ensure they do not match

2. Repeat "write data to random locations, erase, and compare" (test 1) several times using different data patterns (ensure that prior written locations are avoided).

If the product supports multiple logical regions each using a dedicated encryption key then the evaluator SHALL execute the following test:

3. Write data to random locations, erase, and compare

- Ensure device is initialized and encryption engine is ready;
- Determine a random character pattern of at least 64 KB;
- Retrieve information on how many logical regions the device supports and ensure these regions are configured such that they each hold at least 64 KB of data;
- For each logical region, write the character pattern at a random offset ensuring successful write of all 64 KB of data;
- Engage device's functionality for generating new encryption keys for all logical regions;
- Read from all locations at which the data was written;
- Compare the retrieved data to the written data and ensure they do not match (TBD: at bit level and how often they are allowed to match);
- Compare the retrieved data of one logical region to all the other logical regions and ensure they do not match;
    i. Repeat for all logical regions to which it writes data.

Cryptographic Operation (Cryptographic Hashing)

The product shall perform cryptographic hashing in accordance with SHA-256, SHA-384, SHA-512] that meets FIPS PUB 202 or ISO/IEC 10118-3:2004.

Cryptographic Operation (Random Bit Generation)

This requirement is optional and may be performed by the IT environment.

The product shall perform deterministic random bit generation services using approved algorithms.

Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)

The product shall generate all salts using approved Random Bit Generators (RBG).

The product shall generate unique nonces.

The product shall create IVs in the following manner:

> **CBC: IVs shall be unpredictable. Repeating IVs leak information about whether the first one or more blocks are shared between two messages, so IVs should be non-repeating in such situations.**
>
> **XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer.**

Cryptographic Operation (Key Wrap)

The product shall perform key wrapping in accordance with an approved authenticated-encryption mode of operation of the AES algorithm shall be used (per NIST SP 800-38F) for wrapping the DEK; either KW (as defined in NIST SP 800-38F, with CIPH = AES), KWP (as defined in NIST SP 800-38F, with CIPH = AES), AES-GCM (as defined in NIST SP 800-38D) or AES-CCM (as defined in NIST SP 800-38C) shall be used as the authenticated-encryption mode.
The product shall perform asymmetric key unwrapping with the approved algorithms.

Validation

This class of requirements stipulates how the product validates the BEV, an intermediate key, or DEK.

The product shall have the ability to validate the BEV, an intermediate key, or DEK using a comparison or trial decryption or through approved key wrap.

The product shall have the ability to limit an administrator configurable consecutively failed authorization attempts.

Application Note:

The product validates the authorization factor(s) prior to allowing the user access to the data. In cases with validation of the authorization factor(s) fails, the product will not attempt to unlock the storage device by forming an incorrect KEK, intermediate keys,

and/or DEKS, and presenting gibberish to the user. The product validates the authorization factor(s) in such a way that does not allow the attacker to circumvent the other requirements such as performing side channel analysis to gain knowledge about the DEK or other keying material that protects the DEK from inadvertent exposure.

Evaluation Activities:

The evaluator shall check the vendor's documentation to verify that it describes the methods the product employs to limit the number of consecutively failed authorization attempts. The evaluator SHALL document his or her analysis of the methods to limit consecutive failed authorization attempts.

If the methods employed require an administrator to manually unlock authorization after a failure limit is reached, the evaluator SHALL check the guidance documentation to ensure warnings concerning this situation are provided to administrators.

The evaluator SHALL perform the following test:

> Test 1: The evaluator shall determine the limit of the number of consecutive failed authorization attempts. He or she will test the product by entering that number of incorrect authorization factors in consecutive attempts to access user data. If the limit mechanism includes any "lockout" period, the time period tested should include at least one such period. Then the evaluator will verify that the product behaves as described in the vendor's documentation.

Security Management Functions

This class of requirements call out critical activities the must be performed by an administrator to prevent putting the storage device in an insecure state.

Cryptographic Support

This section calls out critical cryptographic requirements for security management functions.

Generate DEK

The product shall support management functions that generate a DEK or receive a DEK from the local host or receive an encrypted DEK from outside the product.

Evaluation Activities:

The evaluator shall review the vendor's documents and confirm that the instructions for generating or importing a DEK exist. The instructions must cover all environments on which the vendor claims conformance, and include any preconditions that must exist in order to successfully generate or re-generate the DEK. The evaluator shall also confirm

the documents describe the processing (if any) that occurs for existing data when a user generates and installs a new DEK. The evaluator shall also perform the following tests:

• Test 1: On a "clean" installation, the evaluator shall generate the DEK.

[Need more evaluation activities here.]

Configure Cryptography

The product MAY support management functions that allow the administrator to configure the cryptographic algorithms selection.

Key Escrow, Archiving, and Recovery

This section calls out critical key escrow, archiving, and recovery requirements for security management functions.

Disable key recovery

The product SHALL support disabling key escrow, archiving, and recovery features when supported.

Application Note:

Escrow implies a regimented procedure that automates the process of storing, managing, and retrieving keying material for contingency planning and/or disaster recovery. The term has a connotation of implying that one must authorize the retrieval of keying material at a later date. Archiving implies a process of merely copying or aging off key material and keeping them around for historical purposes, with little consideration for retrieving them in case of an emergency. The term has a connotation of copying keying material to a USB token in plaintext and locking it in a file cabinet with no expectation of authorization for retrieving them. Nonetheless, many people seem to use the two terms interchangeably. In either case, the product shall support the disablement of these features so that neither users nor administrators can recover their data in case of the loss of authorization factors, or a catastrophic failure, or for any reason.

Evaluation Activities:

The evaluator shall review the vendor's documentation to confirm the product contains a method to disable key escrow/recovery. The evaluator shall verify that the vendor's operational guidance (AGD) contains explicit steps to configure this option.

The evaluator shall review the vendor's documentation to verify the presence of authorization factor escrow/recovery. If present, the evaluator shall verify that the vendor's operational guidance (AGD) contains explicit steps to configure this option.

The evaluator should verify that when the key escrow feature is disabled, that the recovery process does not function as described and that no data exits the ToE boundary.

Protection of the Product

The section calls out the requirements for protecting the product integrity, both powered down and in a powered state.

Trusted Update

The product provides authorized user the ability to initiate signed updates using a digital mechanism.

Evaluation Activities:

The evaluator shall confirm the vendor's documents contain information stating that an authorized source signs product updates and will have an associated signed hash. The documentation contains a definition of an authorized source along with a description of how the product uses public keys for the update verification mechanism in the Operational Environment. The evaluator ensures the vendor's documentation contains this information and details any instructions dealing with the installation of the update credentials. The evaluator also ensures that the operational guidance describes how the product obtains candidate updates; the processing associated with verifying the digital signature of the updates; and the actions that take place for successful and unsuccessful cases. If the Operational Environment performs the digital hashing and signature verification, then the evaluator shall check the vendor's documentation to ensure it describes--for each platform identified in the vendor's documentation--the interface(s) used by the product to invoke this cryptographic functionality.

The evaluators shall verify the location of the software that performs the processing as described in the vendor's documentation. The evaluators shall perform the following tests (if the products supports an optional hash, then the evaluator performs tests 2 and 3 for different combinations of valid and invalid digital signatures and hashes, as well as for digital signature alone):

• Test 1: The evaluator performs the version verification activity to determine the current version of the product. After the update tests described in the following tests, the evaluator performs this activity again to verify that the version correctly corresponds to that of the update.

• Test 2: The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it an update successfully installs it on the product. The evaluator shall perform a subset of other assurance activity tests to demonstrate that the update functions as expected.

• Test 3: The evaluator obtains or produces an illegitimate update, and attempts to install it on the product. The evaluator verifies that the product rejects the update.

Authorized Updates

The product shall allow only the authorized user to initiate updates to the product.

Evaluation Activities:

The evaluator shall confirm the vendor's documents contain information stating that the product authorizes only an administrator to initiate an update of itself. The evaluator shall attempt to make an update to the device using a trusted update, but providing a user authentication different from the administrator authorization. He shall confirm that the attempt fails. He shall then attempt to make an update of the trusted update to the device without any authorization at all and confirm that that also fails. Finally the evaluator shall attempt to directly copy data to the firmware without going through the update mechanism and confirm that also fails.

Power-On Self Tests

The product runs a suite of self-tests during initial start-up (power on) to demonstrate its correct operation. The product shall run Known Answer Tests of the cryptographic algorithms and verify correct answers before their use.

Application Note:

This requirement is optional for now.

Evaluation Activities:

The vendor's documents shall describe the known-answer self-tests for cryptographic functions.

The evaluator shall verify that the vendor's documents describe, for some set of non-cryptographic functions affecting the correct operation of the product, the method by which the product tests those functions. The vendor's documentation will describe, for each of these functions, the method by which the product verifies the correct operation of the function. The evaluator shall determine that the product adequately tests all of the identified functions on start-up.

Power Management

This section calls out the requirements for protecting user data and sensitive keying material during various low power states.

Power State

The vendor shall identify system "sleeping" states for all supported operating environments and for each environment, provide administrative guidance on how to disable the sleep state.

Application Note:

The Unified Extensible Firmware Interface (EFI) Forums' Advanced Configuration and Power Interface (ACPI) Specification defines Global 1 (G1) "sleeping" state. The G1 state defines up to four system sleeping states S1, S2, S3, or S4; each sleeping state has different characteristics for power and exit latencies. The intent of this requirement is to allow an administrator the ability to configure a system to disable the sleep state – resulting in only two power states:

- power on – The ACPI specification identifies this state as Global 0 (G0) or "working" state.
- power off – The ACPI specification identifies this state as either Global 2 (G2) or "soft off" (a normal operating environment initiated shutdown) or Global 3 (G3) "mechanical off" (power loss).

The aim here is to prevent the writing of user or system context to non-volatile memory as could potentially occur during a sleeping state.

Evaluation Activities:

For the operating environments supported by the product, follow the administrative guidance provided to disable the system sleep state(s). Using the information provided on how to identify the sleep states, verify that the operating environment does not enter into any sleep state.

Idle State

The vendor shall provide administrative guidance on how to configure the operational environments it supports to shut down after an administratively defined period of inactivity.

Application Note:

Either the Operational Environment or the product SHOULD keep track of its period of inactivity. Once the product reaches the administratively defined limit it SHOULD initiate a "soft-off" shutdown of the storage device.

Evaluation Activities:

For the operating environments supported by the product, follow the administrative guidance provided to set a period of inactivity for shutdown. Verify that after the period of inactivity limit is reached that the device shutdowns. Upon restart, confirm the

product prompts for authorization factors before resuming operation. Confirm providing an incorrect authorization factor does not allow access to encrypted data, and then confirm providing the correct authorization factor does allow access to encrypted data.

Power Failure

Upon loss of power to the storage device, the product shall require reauthorization before allowing user access to the data.

Evaluation Activities:

For the operating environments supported by the product, place the device into a "mechanical off" state (i.e., remove power). Upon power restoration, confirm the product prompts for authorization factors before resuming operation. Confirm providing an incorrect authorization factor does not allow access to encrypted data, and then confirm providing the correct authorization factor does allow access to encrypted data.