FDE iTC: Authorization Acquisition (AA) 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

Cryptographic Key Management

User Authorization

The product shall use approved *Cryptographic Operations* to perform user authorization before releasing a BEV to the EE. If the product uses user-supplied authorization factor(s) to directly produce the BEV (e.g. through conditioning), then authorization is implied.

Options include:

- Conditioned password/passphrase
- Simple token containing a raw key
- Simple token containing an encrypted key
- A smartcard using RSA or ECC pairs protected by an external entity

Application Note:

This requirement specifies that the vendor must document the mechanisms by which their product authorizes users to release BEVs to the EE. The mechanisms may include, but not limited to, authorizing the release of keys and/or authorization factors stored in smart cards, USB tokens, and conditioning passwords. The product may then validate the authorization factor(s) prior to releasing BEVs to the EE. Furthermore, the validation method does not compromise the keys or keying material. The means of validation may vary based on the type of authorization factor(s).

Evaluation Activities:

The evaluator shall check the vendor's documentation to verify that it describes how the product releases the BEV. If the product grants access to stored values used as authorization factors based upon the supplied authorization factors, then authorization is required before releasing the BEVs. If the product performs validation, the evaluator shall check that the documentation describes how the product validates the authorization factors prior to releasing the BEVs. The documentation shall describe the process in enough detail so that the evaluator can verify that the method or methods do not inadvertently expose the BEV or any intermediate values in a key chain. "Expose" also includes the notion of weakening the BEV or intermediate keying material. The documentation shall describe if authorization factors are a) conditioned, b) used in generation of BEV, or c) used directly as the BEV. The evaluator shall document his or her analysis of the methods the product uses to validate the authorization factors (if any) in their test report.

The evaluator shall perform the following test:

- Test 1: Ensure the product prompts for the user's authorization factor(s) prior to releasing the BEV to the EE.
- Test 2: [conditional] If the product provides validation, for each supported authorization factor, ensure that when the user provides an incorrect authorization factor, the product indicates that the user provided an incorrect authorization factor and denies access to the BEV, except as noted in the SPD.
- Test 3 [conditional]: If the product provides a bypass or alternate means of authorizing access to the BEV (e.g. a recovery scheme), the evaluator tests it to ensure it also consistently meets all requirements (i.e. the user or the AA must supply the appropriate authorization factors prior to the product granting access to the BEV).

User Authorization Failures

This is an optional requirement, since the product may not provide validation.

If implemented, the AA shall support limiting consecutively failed authorization attempts if it provides authorization validation independent of the EE.

Application Note:

The product validates the authorization factor(s) prior to allowing the user access to the data. In cases where validation of the authorization factor(s) fails, the product will not forward a BEV to EE. 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 valid authorization factors or any keying material that protects keys and authorization factors stored in the AA or in the AA's OE 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 vendor's documentation shall define the dictionary attack protection. If the BEV supports validation, the vendor's product shall allow no more than 300 invalid authorization attempts in a 24 hour period.

The evaluator shall perform the following test:

- Test 1: The evaluator shall determine the limit on the average rate 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.

If the product supports multi factor authorization:

Key Combination

An authorization factor listed above may be combined with one or more other factors in accordance with an exclusive OR (XOR), SHA-256, SHA-384, or SHA-512.

Evaluation Activity

The author shall describe how factors are combined.

Test 1 [conditional]: If there is more than one authorization factor, ensure that failure to supply a required authorization factor does not result in access to the encrypted data.

BEV requirements:

BEV Size

The product shall support BEVs of size 128 and/or 256 bits to match the expected security strength of the DEKs they protect.

Evaluation Activities:

The evaluator shall review vendor documentation to verify that the product supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

This is the method for maintaining cryptographic strength from the Authorization Factor to the BEK.

BEV – Key Chaining

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

- **A chain of one or more intermediary keys from initial Authorization Factor to the BEV in accordance with Cryptographic Operation (Key Wrap) or Cryptographic Key Generation (KEK) – KEK Generation.**

- **The initial authorization value is used as the BEV (Chain of 1)**

Application Note:

Key Chaining is the method of using multiple layers of encryption keys to protect data. The number of intermediate keys will vary – from one (taking the conditioned authorization factor and directly using it as the BEV) to many. This applies to all keys that contribute to the ultimate wrapping or derivation of the BEV, including those in areas of protected storage (e.g. TPM stored keys, comparison values, etc).

Evaluation Activity

The vendor shall provide documentation containing a description of their key hierarchy for all authorizations methods selected in Cryptographic Key Generation (KEK) –Authorization Factors that are used to protect the BEV. 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. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

Cryptographic Key Generation (Intermediate Keys)

This is an optional requirement, since the product may use certain Authorization Factors directly as the BEV and may not use intermediate keys.

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

Application Note:

Products MAY allow two different possibilities for the creation of a KEK used by a storage device:

- The product generates the KEK using one of the approved methods.
- The product receives a KEK from the Operating Environment.

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 BEV 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[1].

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;**
- **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)**.

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

Cryptographic Operations

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

Cryptographic Operation (Password Conditioning)

A password/passphrase shall support up to 64 or more characters consisting of all of the ASCII printable characters and shall perform PBKDF in accordance with HMAC-SHA (256, 384, 512) and at least 1,000 iterations.

Evaluation Activities:

Support for minimum length: *The evaluator shall also perform the following tests:*

- *Test 1: Ensure that the TOE supports passwords/passphrases of 64 characters.*
- *Test 2: Try entering a password/passphrase less than 64 characters.*
- *Test 3: If the TOE supports a password/passphrase length up to a maximum number of characters, n (which would be greater than 64), then ensure that the TOE will not accept more*

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

than n characters.

- *Test 4: Ensure that the TOE supports passwords/passphrases consisting of all of the ASCII printable characters.*

Support for PBKDF: *The evaluator shall examine the password hierarchy TSS to ensure that the formation of the DEK and intermediary keys is described and that the key sizes match that described by the ST author.*

The evaluator shall check that the TSS describes the method by which the password/passphrase is first encoded and then fed to the SHA algorithm. The settings for the algorithm (padding, blocking, etc.) shall be described, and the evaluator shall verify that these are supported by the selections in this component as well as the selections concerning the hash function itself. The evaluator shall verify that the TSS contains a description of how the output of the hash function is used to form the submask that will be input into the function and is the same length as the KEK as specified above.

For the NIST SP 800-132-based conditioning of the password/passphrase, the required assurance activities will be performed when doing the assurance activities for the appropriate requirements. If any manipulation of the key is performed in forming the submask that will be used to form an intermediary key, that process shall be described in the TSS.

No explicit testing of the formation of the submask from the input password is required.

Cryptographic Operation (Cryptographic Hashing)

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

Application Note:

The hash selection should be consistent with the overall strength of the algorithm used for **Error! Reference source not found.**.

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 AA 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 MEK; 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.

or

- **RSA using the KTS-OAP-basic scheme,**
- **RSA using KTS-OAEP-confirmation scheme,**
- **ECC CDH using key sizes 128 bits (AES), 256 bits (AES), 2048 (RSA), 4096 (RSA), 256-bit prime modulus (ECC CDH), 384-bit prime modulus (ECC CDH)**

User Data Protection

This class of requirements stipulates the encryption of all stored data, except as noted in the SPD.

Key Interface

- **The AA shall provision the Boundary Encryption Value(BEV) with the EE.**
- **If the BEV requires authorization, the AA shall associate specific authorization values or secrets with the release of the BEV to the EE.**
- **If the BEV requires authorization, the AA shall protect the release of the BEV against dictionary attacks.**
- **The AA shall provide the Boundary Encryption Value (BEV) to the EE.**

Evaluation Activity

The evaluator shall review the vendor’s documentation to verify the requirements for the Key Interface. The vendor’s documentation shall detail the types of BEV supported in their product. The vendor’s documentation shall define the provisioning process for associating the BEV with an EE. The vendor’s documentation shall define what authorization factors may be associated with the BEV. The vendor’s documentation shall define the process by which the authorization factors may be associated with the BEV.

Security Management Functions

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

Cryptographic Support

- **The AA shall support forwarding requests for changing the DEK to the EE.**
- **The AA shall support changing authorization factors.**
- **The AA shall support forwarding requests to cryptographically erase the DEK to the EE.**

Evaluation Activities:

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.

Changing Authorization Factors:

The evaluator shall initialize the product such that it requires the user to input an authorization factor in order to access encrypted data. The evaluator shall also provision administrative factors distinct from the user authorization factors for privileged functions during provisioning. The evaluator shall examine the vendor's documents and verify it clearly describes the methods by which users may change their authorization factors and by which administrators may change their authorization factors and by which administrators may change users' authorization factors.

- Test 1: The evaluator shall first provision user authorization factors, and then verify the authorization factors allow the user access to the encrypted data. Then the evaluator shall exercise the management functions to change a user's authorization factor to a new one. Then he or she will verify that the product denies access to the user's encrypted data when he or she uses the old or original authorization factor to gain access.

- Test 2: The evaluator shall exercise the management functions to change an administrator's authorization factor. Then he or she will verify that the product denies access to administrative functions when he or she uses the old authorization factor to gain access. Then he or she will verify that the product grants access to the administrative function when provided the new authorization factor.

Key Escrow, Archiving, and Recovery

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

Disable key recovery

The AA shall support disabling key and authorization factor escrow, archiving, and recovery features.

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 Drive

The section calls out the requirements for protecting the drive 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.

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 Failure

Upon loss of power to the drive, the AA shall require reauthorization to unlock it.

Evaluation Activities:

Test 1: Power on the AA host device that is configured to operate with the encrypted drive and authenticate successfully to unlock the drive. Power off the AA. Power on the AA. Do not provide any authentication factors. Confirm the AA remains in the locked state (for example displaying a pre-boot authentication message). Confirm the native OS does not boot.