

Trusted Update Requirements

Natural language input for SFRs

Failure by the Security Administrator to verify that updates to the system can be trusted may lead to compromise of the entire system. To establish trust in the source of the updates, the system can provide cryptographic mechanisms and procedures to procure the update, check the update cryptographically through the TOE-provided digital signature mechanism, and install the update on the system. While there is no requirement that this process be completely automated, administrative guidance documentation will detail any procedures that must be performed manually, as well as the manner in which the administrator ensures that the signature on the update is valid.

Proposed SFRs

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the currently executed version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software.

Application Note:

The version currently running (being executed) may not be the version most recently installed. For instance, maybe the update was installed but the system requires a reboot before this update will run. Therefore, it needs to be clear that the query should indicate both the most recently executed version as well as the most recently installed update.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to manually initiate updates to TOE firmware/software and [selection: support automatic updates, no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

Application Note:

The digital signature mechanism referenced in FPT_TUD_EXT.1.3 is one of the algorithms specified in FCS_COP.1(2).

Application Note:

“Update” in the context of this SFR refers to the process of replacing a non-volatile, system resident software component with another. The former is referred to as the NV image, and the latter is the update image. While the update image is typically newer than the NV image, this is not a requirement. There are

legitimate cases where the system owner may want to rollback a component to an older version (e.g. when the component manufacturer releases a faulty update, or when the system relies on an undocumented feature no longer present in the update). Likewise, the owner may want to update with the same version as the NV image to recover from faulty storage.

All discrete software components (e.g. applications, drivers, kernel, firmware) of the TSF, should be digitally signed by the corresponding manufacturer and subsequently verified by the mechanism performing the update. Since it is recognized that components may be signed by different manufacturers, it is essential that the update process verify that both the update and NV images were produced by the same manufacturer (e.g. by comparing public keys).

Assurance Activities:

Updates to the TOE are signed by an authorized source. The definition of an authorized source is contained in the TSS. If certificates are used the TSS shall contain a description of how the certificates used by the update verification mechanism are contained on the device. The evaluator ensures this information is contained in the TSS. The evaluator also ensures that the TSS (or the operational guidance) describes how the candidate updates are obtained; the processing associated with verifying the digital signature of the updates; and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The evaluator shall perform the following tests:

- Test 1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it is successfully installed on the TOE. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update.
- Test 2: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:
 - A modified version (e.g. using a hex editor) of a legitimately signed update
 - An image that has not been signed
 - An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature)

If the TOE supports both, manual and automated update, the evaluator shall perform the Tests 1 and 2 for both methods.

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1(1)/Trusted Update: The TSF shall restrict the ability to *enable* of the functions *perform manual update* to *authorized administrators*.

FMT_MOF.1(2)/Trusted Update: The TSF shall restrict the ability to *enable*, *disable* of the functions *automatic update* to *authorized administrators*.

Application note:

FMT_MOF.1(1)/Trusted Update restricts the initiation of manual updates to authorized administrators.

FMT_MOF.1(2)/Trusted Update is only applicable if the TOE supports automatic updates and allows to enable and disable them. Enable and disable of automatic updates is restricted to authorized administrators.

Assurance Activities:

FMT_MOF.1(1)/Trusted Update: The evaluator shall try to perform the update without prior authentication as administrator using a legitimate update image. This test should fail.

The evaluator shall try to perform the update with prior authentication as administrator using a legitimate update image. This test should pass. The good case test should be covered by the tests for FPT_TUD_EXT.1 already.

FMT_MOF.1(2)/Trusted Update: The evaluator shall try to enable and disable automatic updates without prior authentication as administrator. This test should fail.

The evaluator shall try to enable and disable automatic updates with prior authentication as administrator. This test should pass.

FMT_SMF.1 Specification of Management Functions (taken from NDPP V1.1 with only minor changes)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- Ability to administer the TOE locally and remotely;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;
- [selection:
 - Ability to configure the list of TOE-provided services available

before an entity is identified and authenticated, as specified in

FIA_UIA_EXT.1;

- Ability to configure the cryptographic functionality;
- No other capabilities.]

Application Note: The TOE must provide functionality for both local and remote administration, as well as the capability for the administrator to verify that updates received came from a trusted source. They must be capable of performing this action using digital signatures. If the TOE offers the ability for the administrator to configure the services available prior to identification or authentication, or if any of the cryptographic functionality on the TOE can be configured, then the ST author makes the appropriate choice or choices in the second selection, otherwise select "no other capabilities."

Assurance Activity:

The security management functions for FMT_SMF.1 are distributed throughout the cPP and are included as part of the requirements in FMT_MTD, FPT_TST_EXT, and any cryptographic management functions specified in the reference standards. Compliance to these requirements satisfies compliance with FMT_SMF.1.

FMT_SMR.2 Restrictions on Security Roles (taken from NDPP V1.1 with only minor changes)

Hierarchical to: FMT_SMR.1 Security Roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.2.1 The TSF shall maintain the roles:

- Authorized Administrator.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- Authorized Administrator role shall be able to administer the TOE locally;
- Authorized Administrator role shall be able to administer the TOE remotely;

are satisfied.

Application Note:

FMT_SMR.2.2 requires that user accounts be associated with only one role.

However, note that multiple users may have the same role, and the TOE is not required to restrict roles to a single person.

FMT_SMR.2.3 requires that an authorized administrator be able to administer the TOE through the local console and through a remote mechanism (IPsec, SSH, TLS, TLS/HTTPS). For multiple component TOEs, only the TOE components providing the management control and configuration of the other TOE components require a local administration interface.

Assurance Activity:

The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.