FDE Interpretation # 201908

Status: ☒ *Active* □ *Inactive*

Date: 10-24-2019

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *FDE iTC Interpretations Team* □ *FDE iTC*

Affected Document(s): FDE EE cPP v2.0

Affected Section(s): FPT_PWR_EXT.1.1

Superseded Interpretation(s):

Issue:

As a selection in FPT_PWR_EXT.1.1, D0 is listed as a selectable compliant power saving state. While D0 is not being defined as a power saving state by ACPI and just a power state of a device, it is not secure and an unauthorized user will potentially have access to plaintext data if the device or TOE is left unattended. Because D0 does not ensure a device is secure if lost, it does not meet the intent of the compliant power saving states, and should not be a selectable power state within FPT_PWR_EXT.1.1.

The ACPI standard defines D0(Fully-On) in section 2.3 as follows: “This state is assumed to be the highest level of power consumption. The device is completely active and responsive, and is expected to remember all relevant context continuously”.

Proposed Solution:

The CCTL proposes that as D0 does not meet the intent of a Compliant power saving state, it should be removed from the selectable list of Compliant power saving states within FPT_PWR_EXT.1.1 in CPP_FDE_EE to match as follows:

“FPT_PWR_EXT.1.1 The TSF shall define the following Compliant power saving states: [selection: choose at least one of: S3, S4, G2(S5), G3, D1, D2, D3 [assignment: other power saving states]].”

The CCTL also proposes that the application note for FPT_PWR_EXT.1.1 add clarity on the definition and criteria of a compliant power saving state, as well as explicitly state D0 is not an acceptable assignment. The application note should be modified as follows:

"Compliant power saving states are power states that encrypt or destroy all keying material when entered by various conditions and ensure a device is secure if lost in a compliant power saving state. Power saving states S3, S4, G2(S5), G3, D1, D2, D3 are defined by the Advanced Configuration and Power Interface (ACPI) standard. D0 is not an acceptable assignment for a compliant power saving state as D0 does not completely ensure a device is secure if lost."

Resolution:

The FIT acknowledges the issues described in the 'Issue' section above.

The SFR will be altered as proposed, removing D0:

"FPT_PWR_EXT.1.1 The TSF shall define the following Compliant power saving states: [selection: choose at least one of: S3, S4, G2(S5), G3, D1, D2, D3 [assignment: other power saving states]]."

Rationale:

The FIT acknowledges that D0 is not in line with the other listed states so it should be removed. However, the suggested application note will not be included as we permit any power data that complies with the SRFs to be included as indicated with the assignment.

Further Action:

None.

Action by FDE iTC:

None.