**# Title:**

Disambiguate the meaning of the values in the EFI\_IMAGE\_EXECUTION\_INFO.Action field.

**# Status:**

Draft

**# Document:**

UEFI Spec 2.10

**# License:**

SPDX-License-Identifier: CC-BY-4.0

**# Submitter:**

·         Arm LTD (Joseph Hemann, Samer El-Haj-Mahmoud, Stuart Yoder, Jose Marinho)

**# Summary of the change**

Clarify the conditions for the values of EFI\_IMAGE\_EXECUTION\_INFO.Action to be set.

**# Benefits of the change**

Clarifies UEFI spec, creates consistency with reference implementation.

 **# Impact of the change**

N/A

**# Detailed description of the change [normative updates]**

·         Insertions in yellow highlight

·         Removals in red highlight

32.4.2 Image Execution Information Table…Additionally for every image, an element will be created in the table for every EFI\_CERT\_SHAXXX that is  
supported by the platform. The contents of **Action** for each element are determined by comparing that  
specific element’s *Signature* (which will contain exactly 1 **EFI\_SIGNATURE\_DATA**) to the currently configured image security databases and policies, and shall be either  
**EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_PASSED**, **EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FAILED**, EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_NOT\_FOUND, EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FOUND, or **EFI\_IMAGE\_EXECUTION\_POLICY\_FAILED**.

…

Description…  
First, this field describes the results of the firmware’s attempt to authenticate the image.  
1. If EFI\_IMAGE\_EXECUTION\_AUTH\_UNTESTED is set, then no authentication attempt was  
made.  
2. If EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FAILED is set, then the image had at least one digital  
signature and the check of the digital signatures failed..

3. If EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_PASSED is set, then the image had at least one valid  
digital signature and a check of that digital signature passed.  
4. If EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_NOT\_FOUND is set, then the image’s signatures could not be found in the signature database.

5. If EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FOUND is set, then the image’s signature was found in the signature database,  
6. If EFI\_IMAGE\_EXECUTION\_POLICY\_FAILED is set, then authentication failed because of  
(unspecified) firmware security policy.

|  |  |
| --- | --- |
| Authentication attempt status | Condition met |
| EFI\_IMAGE\_EXECUTION\_AUTH\_UNTESTED | Either:   * The image is not a valid PE/COFF. * The image contains 0 certificates. |
| EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FAILED | The image has at least one certificate, and either:   * An image certificate is in the forbidden database, **or** * A digest of an image certificate is in the forbidden database. |
| EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_PASSED | The image has at least one certificate, and either:   * An image certificate is in authorized database. * The image digest is in the authorized database. |
| EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_NOT\_FOUND | The image has at least one certificate, and:   * no image certificate is found in the authorized database, **and** * the image digest is not in the authorized database. |
| EFI\_IMAGE\_EXECUTION\_AUTH\_SIG\_FOUND | The image has at least one certificate, and  the image digest is in the forbidden database. |
| EFI\_IMAGE\_EXECUTION\_POLICY\_FAILED | Authentication failed because of (unspecified) firmware security policy. |

Second, this field describes whether the image was initialized or not.