**Unified Extensible Firmware Interface  
Engineering Change Request (ECR)**

**Draft for Review**

**Title:**

**Digest Algorithm flexibility in Authenticated Variable signatures**

**Document:**

**Divneil Rai Wadhawan (Intel)**

**Submission Date for Review: 8/5/2020**

# **Summary**

## **Summary of Change**

EFI\_VARIABLE\_AUTHENTICATION\_2 specifies the SignedData.digestAlgorithms to be always SHA256. The implication is that the signing algorithm can use RSA keys greater than 2048 bits, but the digest algorithm remains SHA256. The proposed change is to allow digest algorithm to be greater than SHA256.

## **Benefits of Change**

This brings agility to the signing mechanism of Authenticated variables by allowing it to sign a larger digest.

## **Impact of Change**

There is no impact on the existing Authenticated variables.

## **References**

UEFI Specification 2.8

# **Detailed Description of the change**

Text formats below:

Existing text: may include “…” to indicate an area to skip

inserted or replaced text

~~deleted text~~

8.2.2 Using the EFI\_VARIABLE\_AUTHENTICATION\_2 descriptor

When the attribute **EFI\_VARIABLE\_TIME\_BASED\_AUTHENTICATED\_WRITE\_ACCESS** is set, then the Data buffer shall begin with an instance of a complete (and serialized) ….

Construct a DER-encoded PKCS #7 version 1.5 SignedData (see [RFC2315]) with the signed content as follows:

1. SignedData.version shall be set to 1
2. SignedData.digestAlgorithms shall contain the digest algorithm used when preparing the signature. Only a digest algorithm ~~of~~ greater than or equal to SHA-256 is accepted.