Platform Trust Technology (PTT) API Vendor Specific Properties

Author: Igor Slutsker

PTT supports a set of vendor specific properties. They are used to get PTT specific information. The TPM2_GetCapability command is used to access to the properties. The capability must be equal to the TPM_CAP_VENDOR_PROPERTY (0x00000100). The property shall be equal to the to the vendor specific property value (INTEL_PROP). The property value must be equal to one of the possible values listed in the table below.

Table 1 — Definition of (UINT32) INTEL_PROP Constants

Property Name	Value	Return Type
INTEL_PROP_INTC_FLAGS	0x00000003	INTEL_PROPERTY
INTEL_PROP_INTC_EK_REKEY_SUPPORT	0x00000007	INTEL_PROPERTY

The returned value is represented in the format of INTEL_PROPERTY structure.

Table 2 — Definition of INTEL_PROPERTY Structure

Name	Type	Description
count	UINT32	Number of values returned for the property. A value of zero is allowed.
property	INTEL_PROP_VALUE	An array of values

The INTEL_PROP_VALUE is defined as a UINT32 type.

INTEL_PROP_INTC_FLAGS

The request of the INTEL_PROP_INTC_FLAGS property returns information about special behavior of PTT. The returned value is a set of flags (TPM_CAP_INTC_FLAGS). If the flag is set, the special behavior is enabled.

The list of the flags is represented in the table below.

Table 3 — Definition of (UINT32) TPM_CAP_INTC_FLAGS Bits

Bit	Name	Description
0	TPM_CAP_INTC_FLAGS_NO_AR	**SET (1):** AntiReplay is not supported in the platform. **CLEAR (0):** AntiReplay is supported in the platform.
1	TPM_CAP_INTC_FLAGS_LOCKOUT_POLICY_SUPPORT	**SET (1):** Lockout Policy is supported in the platform. **CLEAR (0):** Lockout Policy is supported in the platform.
2-31	Reserved	Shall be zero Reserved for future use

INTEL_PROP_INTC_EK_REKEY_SUPPORT

The request of the INTEL_PROP_INTC_EK_REKEY_SUPPORT property returns information about recertification support for different Endorsement Keys (EK) types. The returned values is represented as a bitmask with possible values represented below.

Table 4 — Definition of (UINT32) TPM_CAP_INTC_REKEY_SUPPORT_BITMASK Bits

Bit	Name	Description
0	INTC_REKEY_SUPPORT_RSA_256	**SET (1):** RSA 256 recertification is supported in the platform. **CLEAR (0):** RSA 256 recertification is not supported in the platform.
1	INTC_REKEY_SUPPORT_ECC_256	**SET (1):** ECC 256 recertification is supported in the platform. **CLEAR (0):** ECC 256 recertification is not supported in the platform.
2	INTC_REKEY_SUPPORT_ECC_384	**SET (1):** ECC 384 recertification is supported in the platform. **CLEAR (0):** ECC 384 recertification is not supported in the platform.
3-31	Reserved	Shall be zero Reserved for future use

®2017 Intel Corporation