Registry of reserved TPM 2.0 handles and localities

Version 1.0

11th October 2013

Revision 1

Contact: admin@trustedcomputinggroup.org

TCG Published

TCG

Disclaimer

Revision History

Version	Revision	Description
1.0	0	First version
	1	No changes to normative information, just clarification of existing information • The meaning of bits 22 and 23 emphasised in a new table (Table 2) • Specific values of bits 22 and 23 incorporated into specific handle values in Table 3. • New Tables 4, 5, and 6 inserted in anticipation of future values of “Component OEM“, “TPM OEM“ and “Platform OEM” NV handles

CONTENTS

Registry of reserved TPM 2.0 handles and localities

1 Introduction and Scope

This registry is a companion to the TPM 2.0 library specification. This registry describes TCG's convention for allocating TPM 2.0 handles and localities.

2 Handles (indices)

A handle is a 32-bit value. Its most significant octet identifies the type of resource. At any given instant, a handle's low-order bits identify a unique resource. The actual resource identified by the low-order bits may change with time.

Platform-specific workgroups choose the resources whose handles they wish to register, and define those handles in their individual TCG specifications. However, all TPM 2.0 handle definitions must be consistent with the TPM 2.0 specification and the definitions in this registry.

Table 1 of this registry states the range that is assigned by TCG to PCR handles. Note that Table 1 reserves the entire range of handles that is available for PCRs. All handles used by PCRs must be within the range stated in Table 1.

Table 1: reserved handles for PCRs

Handle type	Entity that further refines the handle type	Refined handle type	Handle value (bits)			
			31-24	23-16	15-8	7-0
PCR indices	TPM workgroup		00	00-FF	00-FF	00-FF

The proper interpretation of Table 1 is that the lower 24 bits of a PCR handle have the same value as the PCR's number. For example, the handle of PCR-0 is 00 00 00 00_{16}, the handle of PCR-2 is 00 00 00 02_{16}. The handle for the same PCR (PCR-0, PCR-1, etc) is always the same, irrespective of workgroup, although the integrity metrics recorded in a PCR may vary with workgroup.

The TPM 2.0 library specification Part-II section "NV Storage Structures" defines how a TPM interprets handles for NV indices. Tables 2 and 3 of this registry states the TCG's convention for the entities that assign NV handles. In particular, bits 23-22 of an NV index identify the entity with the authority to define the NV index.

Table 2 : Entity that determines the refined handle type

Entity with authority to define the NV index	Bits 23-22 of handle value
TPM manufacturer	00
Platform Manufacturer	01
Owner	10
TCG	11

When bits 23-22 equal 3, individual NV indices are assigned by TCG and the assigning entities are further refined.

Table 3 reserves the entire range of handles that is available for NV indices, but does not dictate how an entity may further refine its allocated range. The handle values are written in radix-16 (each "digit" represents four bits of the value in hex notation). Note that this registry doesn't assign NV space in a TPM.

Table 3: Reserved handles for NV indices

Handle type	Refined handle type	Entity that determines the refined handle type	Handle value			
			Bit 31-24	Bit 23-16	Bit 15-8	Bit 7-0
NV indices for entities outside TCG	TPM	TPM manufacturer	01	00-3F	00-FF	00-FF
	Platform	Platform Manufacturer		40-7F	00-FF	00-FF
	Owner	Owner		80-BF	00-FF	00-FF
Global NV indices for OEMs, assigned by TCG	Endorsement certificate	Individual handles are determined by individual workgroups		C0	00-7F	00-FF
	Platform certificate	Individual handles are determined by individual workgroups			80-FF	00-FF
	Component OEM (See Table 4 of this registry)	Technical Committee		C1	00-FF	00-FF
	TPM OEM (See Table 5 of this registry)	Technical Committee		C2	00-FF	00-FF
	Platform OEM (See Table 6 of this registry)	Technical Committee		C3	00-FF	00-FF
NV Indices for individual TCG workgroups, assigned by TCG	PC-Client	PC-Client workgroup		C4	00-FF	00-FF
	Server	Server workgroup		C5	00-FF	00-FF
	Virtualized Platform	Virtualized Platform workgroup		C6	00-FF	00-FF
	MPWG	MPWG		C7	00-FF	00-FF

	Embedded	Embedded workgroup		C8	00-FF	00-FF
<reserved NV indices >	<reserved >	<reserved >		C9 - FF	00-FF	00-FF

An NV index assigned by an entity outside TCG does not have the same meaning in all platforms. It is anticipated that some of these NV indices will be assigned by firmware or software applications.

- The indices defined by one individual Owner may or may not be the same as those defined by another individual Owner.
- The indices defined by one individual platform manufacturer may or may not be the same as those defined by another platform manufacturer.
- The indices defined by a platform manufacturer for one type of platform may or may not be the same as those defined by the same manufacturer for another type of platform.
- The indices defined by one individual TPM manufacturer may or may not be the same as those defined by another TPM manufacturer.
- The indices defined by a TPM manufacturer for one type of TPM may or may not be the same as those defined by the same manufacturer for another type of TPM.

In contrast a global NV range or specific index is one that has the same meaning in all platforms, irrespective of manufacturer or type.

- Individual TCG workgroups may assign handles for specific certificates within the global ranges defined in Table 3. The handle for a particular type of certificate in one type of platform may therefore be different to the handle for the same type of certificate in another type of platform. This is to facilitate contiguous certificate handles with disparate sets of algorithms. If certificates comprise large amounts of data and a TPM's bandwidth is low, TCG workgroups should design certificate formats so that the type of a certificate may be read without reading the entire certificate.
- Component OEMs (such as chipset manufacturers), TPM OEMs, and platform OEMs, may request the TCG Technical Committee to assign global handles for resources. The only such global handles are those defined in this registry.

  Table 4 reserves the handles of global NV indices for Component OEMs. The handle values are written in radix-16 (each "digit" represents four bits of the value in hex notation). They are in the range 01C1 0000-FFFF stipulated by Table 3 of this registry.

Table 4: Handles for Global NV indices assigned to Component OEMs

Purpose	Handle value
<no handles are currently assigned>	

  Table 5 reserves the handles of global NV indices for TPM OEMs. The handle values are written in radix-16 (each "digit" represents four bits of the value in hex notation). They are in the range 01C2 0000-FFFF stipulated by Table 3 of this registry.

Table 5: Handles for Global NV indices assigned to TPM OEMs

Purpose	Handle value
<no handles are currently assigned>	

Table 6 reserves the handles of global NV indices for Platform OEMs. The handle values are written in radix-16 (each ”digit” represents four bits of the value in hex notation). They are in the range 01C3 0000-FFFF stipulated by Table 3 of this registry.

Table 6: Handles for Global NV indices assigned to Platform OEMs

Purpose	Handle value
<no handles are currently assigned>	

The TPM 2.0 library specification Part-III section “TPM 2.0_evictControl” defines handles for persistent objects:

- If auth is TPM_RH_OWNER, the handle for persistent objects is in the inclusive range of 81 00 00 00_{16} to 81 7F FF FF_{16}.
- If auth is TPM_RH_PLATFORM, the handle for persistent objects is in the inclusive range of 81 80 00 00_{16} to 81 FF FF FF_{16}.

Table 7 of this registry states the TCG’s convention for handles of keys that have been rendered persistent via the command TPM 2.0_EvictControl. Note that Table 7 reserves just part of the entire range of handles that is available for persistent keys, and reserves just the ranges for persistent primary keys. The remainder of the range of handles for persistent keys is available for persistent non-primary keys. The handle values are written in radix-16 (each ”digit” represents four bits of the value in hex notation).

Table 7: reserved handles for persistent objects

Handle type	Entity that further refines the handle type	Refined handle type	Handle value (bits)			
			31-24	23-16	15-8	7-0
Primary keys	Hypervisor/ Operating system	Storage primary keys	81	00	00-FF	00-FF
		Endorsement primary keys		01	00-FF	00-FF
	Platform	Platform primary keys		80	00-FF	00-FF

This registry assigns handle ranges for just 2^{16} “Storage primary keys”, 2^{16} “Endorsement primary keys”, and 2^{16} “Platform primary keys”. The handle for a particular primary key in one platform may be different to the handle for the same type of primary key in another platform. This is because a workgroup may choose to define handles for persistently stored primary keys that use just the cryptographic algorithms that are mandatory in that workgroup’s specifications, for example.

3 Localities

Platform-specific workgroups request localities for stated purposes. The values of localities for those purposes are assigned by the Technical Committee, and recorded in this registry.

Localities are a scarce resource. Therefore all assigned values must be actually used: ranges with unused values cannot be preassigned to individual platform-specific workgroups.

The locality value is represented as a byte. Locality values have two separate interpretations.

- Localities 0 through 4 are interpreted as bits in the byte with $0000\ 0001_2$ representing locality 0 and $0001\ 0000_2$ representing locality 4. This representation allows multiple localities to be represented in a single byte as long as the localities are in the range of 0-4.
- A second interpretation applies to localities above 4. These are called extended localities. For extended localities, the locality byte is an integer value representing the locality. Because of the format for localities 0-4, the first extended locality is 32. The range of extended localities is 32-255. An extended locality value may indicate only one locality at a time.

Table 8 of this registry states the assignment of locality values to TCG workgroups, and the interpretation of a locality value. Table 8 reserves all possible locality values.

Table 8: localities reserved for platform-specific workgroups

Workgroup that defines the meaning of the locality	Locality value	Description of the locality
PC-Client	0	The Static RTM, its chain of trust and its environment
	1	An environment for use by the Dynamic OS
	2	Dynamically Launched OS (Dynamic OS) “runtime” environment
	3	Auxiliary components
	4	Trusted hardware component
unallocated	5-31	It is impossible to implement these localities because of legacy constraints and the representation of locality as a Byte
MPWG	32	L_TEE: a locality indicating access from code within the same TEE as the receiving TPM Mobile
	33	L_ATPM: a locality indicating access from an Application TPM Mobile residing in the same TEE as a Platform TPM Mobile. Used for attestation.
Virtualized Platform Workgroup	34	unknown
	35	unknown

	36	unknown
<reserved values>	37-255	Reserved by the Technical Committee