TRUSTED® COMPUTING GROUP

REFERENCE

Registry of Reserved TPM 2.0 Handles and Localities

Version 1.1
Revision 1.00
February 6, 2019

Contact: admin@trustedcomputinggroup.org

Published

© TCG 2019

DISCLAIMERS, NOTICES, AND LICENSE TERMS

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OaUT OF ANY PROPOSAL, DOCUMENT OR SAMPLE.

Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this document and to the implementation of this document, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this document or any information herein.

This document is copyrighted by Trusted Computing Group (TCG), and no license, express or implied, is granted herein other than as follows: You may not copy or reproduce the document or distribute it to others without written permission from TCG, except that you may freely do so for the purposes of (a) examining or implementing TCG documents or (b) developing, testing, or promoting information technology standards and best practices, so long as you distribute the document with these disclaimers, notices, and license terms.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on document licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

CHANGE HISTORY

REVISION	DATE	DESCRIPTION
1.00/0	January 6, 2013	• Initial Release
1.00/1	April 1, 2015	• The meaning of bits 22 and 23 emphasized 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
1.10/0	Feb 6, 2019	• Added reference to the list of OIDs and Catalog. • Added comment about TPM enforcing some bits of the key handle. • Added requested handles by companies and TCG Workgroups • Added note that organizations are responsible for sub-dividing NV Indices if necessary. • Deprecated certain Platform Classes • Referenced TPM 2 Library specification for numbering format instead of copying it. • NOTE: Will change Revision to 0 when ported to new template and remove this note.

 © TCG 2019

1 Contents

DISCLAIMERS, NOTICES, AND LICENSE TERMS 1
CHANGE HISTORY 2
1 Introduction and Scope 5
1.1 References 5
2 Numbers 6
2 Handles (indices) 7
2.1 PCR Handles 7
2.2 NV Indices 8
2.2.1 TPM Specification Defined 8
2.2.2 TCG Conventional NV Indices Usage 8
2.3 Key Handles 14
2.3.1 Key Handle Assignments 14
2.3.2 Key Handle and Certificate Handle Relationships 15
3 Localities 16
4 Platform Class 17

 © TCG 2019

Table of Tables

Table 1: Reserved Handles for PCR 7
Table 2: Reserved Handles for NV indices 8
Table 3: Example NV Unassigned Usages 9
Table 4: Known NV Index Unassigned Usages 10
Table 5: Endorsement NV Index Usages 10
Table 6: Handles for Global NV indices assigned to Component OEMs 11
Table 7: Handles for Global NV indices assigned to TPM OEMs 11
Table 8: Handles for Global NV indices assigned to Platform OEMs 12
Table 9: NV Indices assigned by TCG for specific usages 13
Table 10: NV Handles for PC Client WG 13
Table 11: Key Handles for Persistent Objects 14
Table 12: Localities Reserved for Platform-Specific Workgroups 16
Table 13: Platform Class Values 17

 © TCG 2019

1 Introduction and Scope

This registry is a companion to the TPM 2.0 library specification [1]. This registry describes TCG's convention for allocating TPM 2.0 handles and localities. Many of the values in this document specify ranges for vendors to use and these ranges are reserved by TCG for those vendors' use.

1.1 References

[1] TPM 2.0 Library Specification

URL: https://trustedcomputinggroup.org/work-groups/trusted-platform-module

 © TCG 2019

2 Numbers

The numbers used in this document are formatted as defined by the TPM Library specification in Section 7.3 Numbers (as of revision 1.46).

 © TCG 2019

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.

2.1 PCR Handles

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 PCR. All handles used by PCR must be within the range stated in Table 1.

Table 1: Reserved Handles for PCR

Handle Type	Entity that further refines the handle type	Refined handle type	Handle Range
PCR indices	TPM workgroup		$00\ 00\ 00\ 00_{16}$ – $00\ FF\ FF\ FF_{16}$

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.

 © TCG 2019

2.2 NV Indices

2.2.1 TPM Specification Defined

The TPM 2.0 library specification Part-II section “NV Storage Structures” defines how a TPM interprets handles for NV indices. The TPM Library Specification defines bits 31-24 as reserved for NV Indices.[1]

2.2.2 TCG Conventional NV Indices Usage

This section defines TCG’s convention for bits 23-00.

NOTE: The TPM does not enforce the conventional usage (i.e., bits 23-00) for NV Indices defined in this section.

Table 2 defines the entire range of handles available for NV indices. How each range is used and assigned is defined by the handle type’s assignee. Note that this registry does not assign NV space in a TPM.

Table 2: Reserved Handles for NV indices

Handle Type	Refined Handle Type	Source of Handle Type	Handle Range
NV indices unassigned by TCG See Section 2.2.2.1	TPM	TPM manufacturer	01 00 00 00$_{16}$ – 01 3F FF FF$_{16}$
	Platform	Platform Manufacturer	01 40 00 00$_{16}$ – 01 7F FF FF$_{16}$
	Owner	Owner	01 80 00 00$_{16}$ – 01 BF FF FF$_{16}$
NV indices assigned by TCG per platform component level See Sections 2.2.2.2 and 2.2.2.3	Endorsement	Individual handles are determined by individual workgroups	01 C0 00 00$_{16}$ – 01 C0 7F FF$_{16}$
	Platform	Individual handles are determined by individual workgroups	01 C0 80 00$_{16}$ – 01 C0 FF FF$_{16}$
	Component OEM (See Table 6 of this registry)	Technical Committee	01 C1 00 00$_{16}$ – 01 C1 FF FF$_{16}$
	TPM OEM (See Table 7 of this registry)	Technical Committee	01 C2 00 00$_{16}$ – 01 C2 FF FF$_{16}$

[1] TPM_HT_NV_INDEX = 0x01; HR_SHIFT= 24(decimal); HR_NV_INDEX = (TPM_HT_NV_INDEX << HR_SHIFT)

 © TCG 2019

Handle Type	Refined Handle Type	Source of Handle Type	Handle Range
	Platform OEM (See Table 8 of this registry)	Technical Committee	01 C3 00 00$_{16}$ – 01 C3 FF FF$_{16}$
NV Indices assigned by TCG for specific usages See Section 2.2.2.4	TCG Specifications and Workgroups (See Table 9 and Table 10)	Technical Committee	01 C4 00 00$_{16}$ – 01 FF FF FF$_{16}$

2.2.2.1 NV indices unassigned by TCG

2.2.2.1.1 General Description

An NV index within these ranges are assigned by entities outside TCG. This NV Indices do not have the same meaning across all platform classes. It is anticipated that some of these NV indices will be assigned by firmware or software applications.

1. The indices defined by one individual Owner may or may not be the same as those defined by another individual Owner.
2. The indices defined by one individual platform manufacturer may or may not be the same as those defined by another platform manufacturer.
3. 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.
4. The indices defined by one individual TPM manufacturer may or may not be the same as those defined by another TPM manufacturer.
5. 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.

This range is divided into sub-ranges allocated to the platform component that uses the NV Index. Example usages are in Table 3 below.

Table 3: Example NV Unassigned Usages

Refined Handle Type	Example Usage
TPM	TPM Manufacturer-specific information about the TPM which is not represented by a Capability.
Platform	Platform information which is kept secure using Platform Policies
Owner	OS or application specific usages

2.2.2.1.2 Known Usages

Within these ranges Table 4 identifies known NV Index ranges or specific NV Indices in use. Note these values are informative and are not enforced by TCG. It is possible other uses exist (some may overlap those listed

 © TCG 2019

here) that are not identified. Entities wanting to list their usage should contact TCG admin at: admin@trustedcomputinggroup.org.

Table 4: Known NV Index Unassigned Usages

Refined Handle Type	NV Index or NV Range	Known usage
TPM	<N/A>	
Platform	01 40 00 00 – 01 40 FF FF_{16}	Dell, Inc.
	01 70 00 00 – 01 70 FF FF_{16}	Dell, Inc.
Owner	<N/A>	

2.2.2.2 NV indices assigned by TCG per platform component level

2.2.2.2.1 Endorsement

This range contains NV Indices to support the Endorsement Hierarchy such as Endorsement Certificates, Endorsement Key templates, etc.

Within the Endorsement Certificate range, the Infrastructure Working Group has defined specific NV Indices to allow EK authorization. See the relevant specification for a description of each NV Index range. The following range is reserved for creating these policies.

Table 5: Endorsement NV Index Usages

Usage	NV Index or NV Range	Description / Specification
EK Policies	01 C0 7F 00_{16} – 01 C0 7F FF_{16}	Policy NV Indices TCG EK Credential Profile

2.2.2.2.2 Platform

This range contains NV Indices to support Certificates to identity the Platform such as Platform Certificates.

 © TCG 2019

2.2.2.3 NV indices Assigned to OEMs

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.

The ranges assigned have a large address space. TCG expects to issue a minimal (ideally only one) range per registrant. For large or complex organizations, each registrant is expected to sub-divide, if necessary, its range amongst its various internal units.

2.2.2.3.1 NV Handles for Component OEM

Table 6 reserves the handles of global NV indices for Component OEMs. They are in the range 01C1 0000-FFFF$_{16}$ stipulated by Table 2 of this registry.

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

Purpose / Registered to	Handle value / Range
Intel, Corp.	01 C1 01 00$_{16}$ – 01 C1 01 3F$_{16}$
Cisco	01 C1 01 40$_{16}$ – 01 C1 01 7F$_{16}$
IBM	01 C1 01 80$_{16}$ – 01 C1 01 BF$_{16}$
Microsoft	01 C1 01 C0$_{16}$ – 01 C1 01 FF$_{16}$
AMD	01 C1 02 00$_{16}$ – 01 C1 02 3F$_{16}$
HP	01 C1 02 40$_{16}$ – 01 C1 02 7F$_{16}$
HPE	01 C1 02 80$_{16}$ – 01 C1 02 BF$_{16}$

2.2.2.3.2 NV Handles for TPM OEMs

Table 7 reserves the handles of global NV indices for TPM OEMs. They are in the range 01C2 0000-FFFF$_{16}$ stipulated by Table 2 of this registry.

Table 7: Handles for Global NV indices assigned to TPM OEMs

Purpose	Handle value
Infineon	01 C2 00 00$_{16}$ – 01 C2 00 7F$_{16}$

 © TCG 2019

2.2.2.3.3 NV Handles for Platform OEMs

Table 8 reserves the handles of global NV indices for Platform OEMs. They are in the range 01C3 0000-FFFF$_{16}$ stipulated by Table 2 of this registry.

Note: Requesters are urged to implement the lowest values within their range. This would allow splitting ranges in the future (with the requestor's permission) if address space becomes scarce.

Table 8: Handles for Global NV indices assigned to Platform OEMs

Purpose	Handle value
Intel	01 C3 01 00$_{16}$ – 01 C3 01 3F$_{16}$
Cisco	01 C3 01 40$_{16}$ – 01 C3 01 7F$_{16}$
HPE	01 C3 01 80$_{16}$ – 01 C3 01 BF$_{16}$
IBM	01 C3 01 C0$_{16}$ – 01 C3 01 FF$_{16}$
Juniper	01 C3 02 00$_{16}$ – 01 C3 02 3F$_{16}$
General Electric	01 C3 02 40$_{16}$ – 01 C3 02 7F$_{16}$
Raytheon, Inc.	01 C3 02 80$_{16}$ – 01 C3 02 BF$_{16}$
HP	01 C3 02 C0$_{16}$ – 01 C3 02 FF$_{16}$
AMD	01 C3 03 00$_{16}$ – 01 C3 03 3F$_{16}$
Qualcomm	01 C3 03 40$_{16}$ – 01 C3 03 7F$_{16}$

2.2.2.4 NV Indices assigned by TCG for specific usages

2.2.2.4.1 General Description

Individual TCG workgroups may assign handles for specific NV Indices within the ranges defined in Table 2. The NV Index for a particular type of object (e.g., a certificate) in one type of platform may be different from the NV Index for the same type of object in another type of platform.

 © TCG 2019

2.2.2.4.2 NV Indices assigned by TCG for specific usages

Table 9: NV Indices assigned by TCG for specific usages

Purpose	Range
PC-Client workgroup	01 C4 00 00_{16} – 01 C4 FF FF_{16}
Server workgroup	01 C5 00 00_{16} – 01 C5 FF FF_{16}
Virtualized Platform workgroup	01 C6 00 00_{16} – 01 C6 FF FF_{16}
MPWG	01 C7 00 00_{16} – 01 C7 FF FF_{16}
Embedded workgroup	01 C8 00 00_{16} – 01 C8 FF FF_{16}
Infrastructure workgroup	01 C9 00 00_{16} – 01 C9 FF FF_{16}
<Reserved>	01 CA 00 00_{16} – 01 CF FF FF_{16}
TPM Workgroup	01 D0 00 00_{16} – 01 D0 FF FF_{16}
<Reserved>	01 D1 00 00_{16} – 01 FF FF FF_{16}

2.2.2.4.3 Workgroup Specific Usages

2.2.2.4.3.1 NV Handles for PC Client WG

Table 10 reserves the handles of global NV indices for PC Client WGs. They are in the range 01C4 0000_{16} – $FFFF_{16}$ stipulated by Table 2 of this registry.

Table 10: NV Handles for PC Client WG

Purpose	Handle value
GPIO	01 C4 00 00_{16} – 01 C4 00 $0F_{16}$
Reserved	01 C4 00 10_{16} – 01 C4 00 FF_{16}
Enhanced Peripheral Interface	01 C4 01 00_{16} – 01 C4 01 FF_{16}

 © TCG 2019

2.3 Key Handles

2.3.1 Key Handle Assignments

The TPM enforces bits 31-24 for all persistent keys, and enforces bit 23 to distinguish platform hierarchy keys from storage/endorsement hierarchy keys. However, bits 22-16, which distinguish storage from endorsement are by convention only and are not enforced by the TPM.

The TPM 2.0 library specification Part-III section “TPM2_EvictControl” defines handles for persistent objects:

1. 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}.
2. 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 11 of this registry states the TCG’s convention for handles of keys that have been rendered persistent via the command TPM2_EvictControl. Note that Table 11 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.

Table 11: Key Handles for Persistent Objects

Scope	Hierarchy	Handle Type	Range
Hypervisor, Operating System or Applications	Storage	Storage Primary Key	81 00 00 00_{16} – 81 00 00 FF_{16}
		Reserved	81 00 01 00_{16} – 81 00 7F FF_{16}
		Available	81 00 80 00_{16} – 81 00 FF FF_{16}
	Endorsement	Endorsement Primary Key	81 01 00 00_{16} – 81 01 00 FF_{16}
		Reserved	81 01 01 00_{16} – 81 01 7F FF_{16}
		Available	81 01 80 00_{16} – 81 01 FF FF_{16}
		Infrastructure WG	81 02 00 00_{16} – 81 02 00 FF_{16}
		Reserved	81 02 01 00_{16} – 81 03 FF FF_{16}
Platform	Platform	Platform Keys (all)	81 80 00 00_{16} – 81 80 00 FF_{16}
	Reserved	Reserved	81 80 01 00_{16} – 81 FF FF FF_{16}

This registry assigns handle ranges for just 256 “Storage primary keys”, 256 “Endorsement primary keys”, and 256 “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.

Handle types marked as Reserved, should not be used as these may be designated later by TCG. Handle Types marked as Available are for use by platform manufacturers, Hypervisor or Operating systems (or applications) but should remain within the ranges designated as Available within the appropriate Hierarchy.

 © TCG 2019

2.3.2 Key Handle and Certificate Handle Relationships

Unlike TPM 1.2, TPM 2.0 does not require persistent endorsement keys. They can be repeatedly created as transient keys on demand, while a persistent EK would consume scarce NV space.

If an EK is made persistent, it may be easier for software if there is a relationship between the EK persistent handle and the EK certificate NV Index. For example, if an Endorsement Certificate within the Endorsement Certificate range in Table 2 has an Endorsement Primary Key within Table 11 the offset of each entity could be the same within each respective range. For example, an Endorsement Certificate at NV Index 01 C0 00 21_{16} (offset 21_{16} starting from the beginning of the assigned NV Index range) could have an Endorsement Primary Key at handle 81 00 00 21_{16} (offset 21_{16} starting from the beginning of the assigned key handle range).

 © TCG 2019

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 pre-assigned to individual platform-specific workgroups.

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

1. 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.
2. 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_{10}. The range of extended localities is 32_{10}-255_{10}. An extended locality value may indicate only one locality at a time.

Table 12 of this registry states the assignment of locality values to TCG workgroups, and the interpretation of a locality value. Table 12 reserves all possible locality values.

Table 12: Localities Reserved for Platform-Specific Workgroups

Workgroup Defining the locality	Locality value	Description of the locality
PC-Client	00_{16}	The Static RTM, its chain of trust and its environment
	01_{16}	An environment for use by the Dynamic OS
	02_{16}	Dynamically Launched OS (Dynamic OS) “runtime” environment
	03_{16}	Auxiliary components
	04_{16}	Trusted hardware component
Unallocated	05_{16} – $1F_{16}$	It is impossible to implement these localities because of legacy constraints and the representation of locality as a Byte
MPWG	20_{16}	L_TEE: a locality indicating access from code within the same TEE as the receiving TPM Mobile
	21_{16}	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	22_{16}	Unknown
	23_{16}	Unknown
	24_{16}	Unknown
<reserved values>	24_{16} – FF_{16}	Reserved by the Technical Committee

 © TCG 2019

4 Platform Class

Table 13 contains values used to assert the class (or type) of platform. These are just canonical numeric values used by TCG specifications to identify a platform's class as defined by that specification.

The values in Table 13 are stated in hexadecimal, however, the actual representation of the values including the number of octets and endianness is not declared in this document. The representation of these values is defined by the specification utilizing them.

Note there are also OIDs defined to designate platform class. Those are listed in the OID registry.

Note to editor: It's likely when Table 13 is modified the OID registry should also be modified to include the new definition.

NOTE: Adding a canonical set of string values representing Platform Class is within scope of this document, however, there are no specific use cases for them therefore none are defined. If a string value (e.g., "pc_client") is needed contact the TCG Technical Committee.

Table 13: Platform Class Values

Platform Class	Value	Comments	Example Use[2]
Unclassified	00_{16}	not platform specific	TPM_PS_MAIN
PC Client	01_{16}	PC Client (see NOTE 1)	TPM_PS_PC
PDA	02_{16}	PDA (includes all mobile devices that are not specifically cell phones)	TPM_PS_PDA
CELL_PHONE	03_{16}	Cell Phone	TPM_PS_CELL_PHONE
SERVER	04_{16}	Server WG (see NOTE 1)	TPM_PS_SERVER
PERIPHERAL	05_{16}	Peripheral WG	TPM_PS_PERIPHERAL
TSS	06_{16}	Deprecated[3]	TPM_PS_TSS
STORAGE	07_{16}	Storage WG	TPM_PS_STORAGE
AUTHENTICATION	08_{16}	Authentication WG	TPM_PS_AUTHENTICATION
EMBEDDED	09_{16}	Embedded WG	TPM_PS_EMBEDDED
HARDCOPY	$0A_{16}$	Hardcopy WG	TPM_PS_HARDCOPY
INFRASTRUCTURE	$0B_{16}$	Deprecated	TPM_PS_INFRASTRUCTURE
VIRTUALIZATION	$0C_{16}$	Virtualization WG	TPM_PS_VIRTUALIZATION
TNC	$0D_{16}$	Deprecated	TPM_PS_TNC
MULTI_TENANT	$0E_{16}$	Deprecated	TPM_PS_MULTI_TENANT

[2] As documented in the TPM 2 Library Specification

[3] While these values indicated as Deprecated are documented in the TPM 2 Library, their use is not anticipated.

 © TCG 2019

Platform Class	Value	Comments	Example Use[2]
TC	$0F_{16}$	Deprecated	TPM_PS_TC

NOTE 1: In the TCG ACPI specification PC Client has a value of 00_{16} and Server has a value of 01_{16}.

END

 © TCG 2019