TPM Main
Part 2 TPM Structures

Specification version 1.2
Level 2 Revision 116
1 March 2011
TCG Published

Contact: admin@trustedcomputinggroup.com

TCG Published

TCG

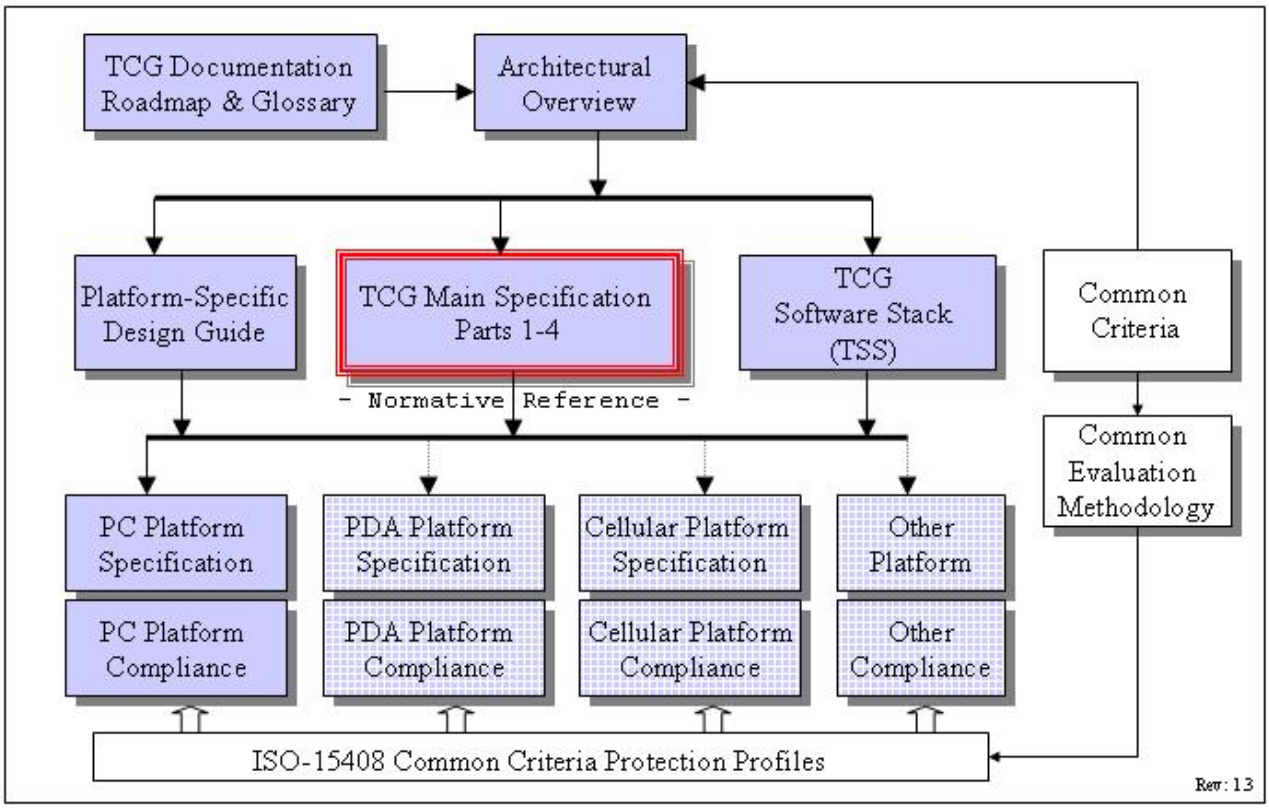
Disclaimers, Notices, and License Terms

57**Revision History**

.10	Started: 1 April 2003. Last Updated: 04/30/01 by David Grawrock
52	Started 15 July 2003 by David Grawrock
53	Started 5 Aug 2003 by David Grawrock
63	Started 2 October 2003 by David Grawrock All change history now listed in Part 1 (DP)
91	Section 19.2 Informative updated by Tasneem Brutch, on Sept. 2005
94	Added the following statement to Section 17 (Ordinals): "The following table is normative, and is the overriding authority in case of discrepancies in other parts of this specification."
94	Added "Physical Presence" column to the table in Section 17 (Ordinals).
100	Add dictionary attack status reporting, clarified CTR mode, deprecated key startup effect, TPM_STRUCT_VER revision ignored on input, clarified TPM_AUTH_NEVER, added deferredPhysicalPresence and its bit map, CMK is optional, added TPM_NV_INDEX_TRIAL, deprecated TPM_CAP_PROP_MAX_NV_AVAILABLE
101	Changed "set to NULL" to "set to zero" in many places. Added rationale for TPM_PAYLOAD_TYPE and TPM_KEY_USAGE distinction. Changed debug PCR from 15 to 16. Clarified what is returned for the Clarified what is returned for the TPM_CAP_NV_LIST and TPM_CAP_NV_INDEX capabilities, specifically when the DIR is being referenced. Clarified that the TPM_CAP_CHECK_LOADED capability requires a TPM_KEY_PARMS structure.
102	Clarified that tickRate is microseconds per tick. Changed optional commands from X to O.
103	Changed TPM_MS_RESTRICT_APPROVE_DOUBLE to TPM_MS_RESTRICT_APPROVE. This rev is errata 2.
104	EK is TPM_ES_RSAESOAEP_SHA1_MGF1. allowMaintenance default state is manufacturer specific if maintenance is not implemented.
105	Indicated that persistent and volatile flags are deprecated. Indicated that tpmDAASeed, daaProof, and daaBlobKey have the same lifetime.
106	For MGF1, the TPM MAY validate encScheme, added permanent flag history, sizeOfSelect rules now defer to platform specification, TPM_PCR_INFO_SHORT localityAtRelease must not be zero, TPM may check localityAtCreation not zero
107	Boolean must be 0 or 1. Removed maxNVBuf. Ordinal table clarified P means sometimes consider physical presence; A means execute when nvLocked is FALSE. TPM_FieldUpgrade is available disabled and deactivated. TPM_KeyControlOwner can be delegated. Explained that TPM_GetCapability returns an error only when a meaningful response cannot be returned, and

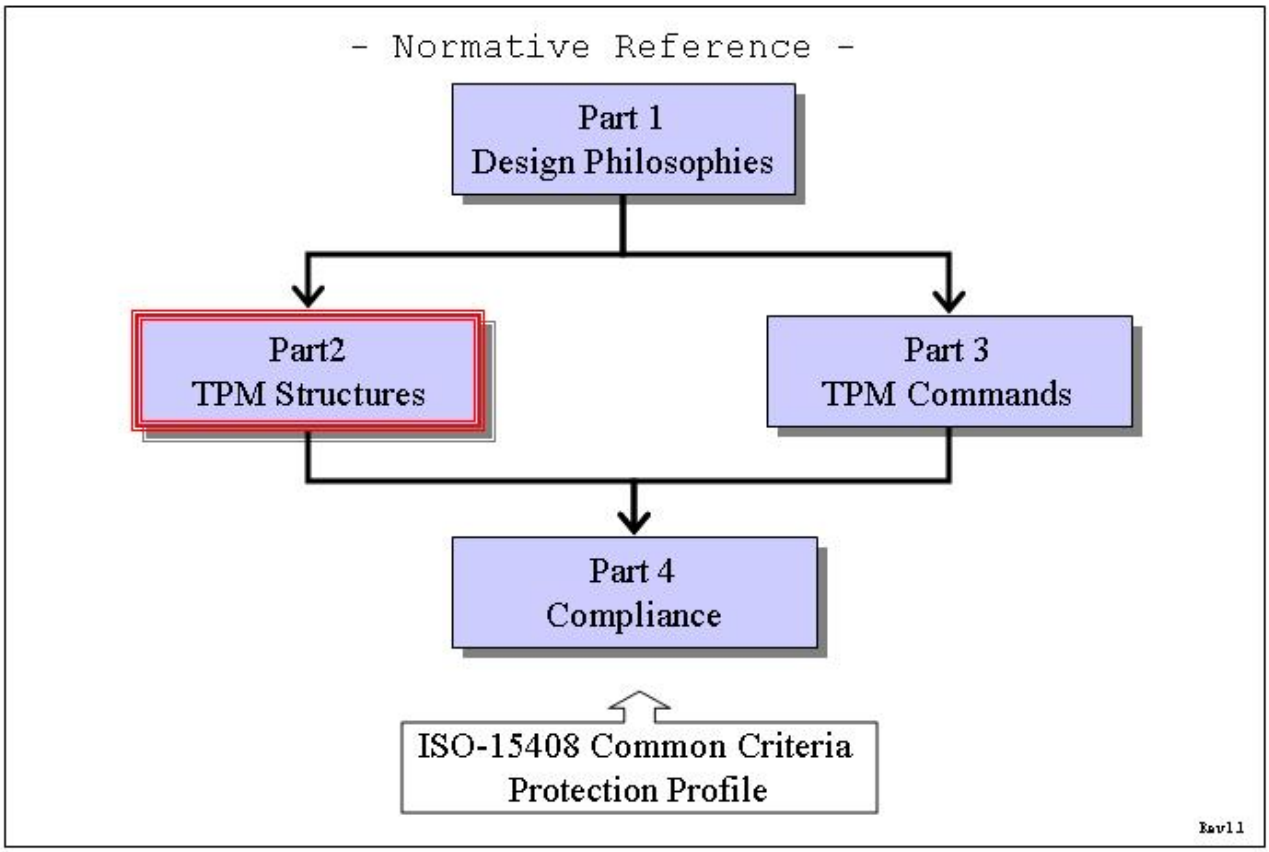
	returns a Boolean FALSE for unused enumerated values.
108	TPM_SetTempDeactivated is available disabled.
109	Clarified that TPM_STCLEAR_FLAGS -> physicalPresence does not reflect the hardware signal. physicalPresenceLock does not affect the hardware signal. Removed bogus normative that physicalPresenceLock is set at manufacture.
110	TPM_AUTH_PRIV_USE_ONLY name change, indication that it refers to reading the public key. pcrIgnoredOnRead MUST ignore for read and MAY ignore for public key use. readSRKPub default changed to TRUE. Indicate that the pcrSelect 0 case sets the digestAtCreation to 0 and ignores digestAtRelease. No minimum number of owner evict keys. Clarified NV index T,P,U,D and resvd bits and purview. Matched reserved indices to ordinal purview. Return of TPM_NV_DATA_PUBLIC digestAtRelease zero changed to MAY.
111	Added BYTE convention and made all structures consistent. Added text for maintenance after field upgrade. tpmProof is TPM_SECRET. Made examples explicit for TPM_PCR_SELECTION. Detailed when sessions are terminated on malformed commands. TPM_EstablishTransport is medium duration.
112	readSRKPub default is vendor specific, ordinal P and C bits reserved
113	Ordinal A bit meaning is deferred to Part 3.
114	readSRKPub SHOULD be FALSE
116	Typo in PCR info structure mapping, updated to specLevel 2 errataRev 3

TCG Doc Roadmap – Main Spec



58

TCG Main Spec Roadmap



59

Table of Contents

252

1. Scope and Audience

The TPM main specification is an industry specification that enables trust in computing platforms in general. The main specification is broken into parts to make the role of each document clear. A version of the specification (like 1.2) requires all parts to be a complete specification.

This is Part 2, the structures that the TPM will use.

This document is an industry specification that enables trust in computing platforms in general.

1.1 Key words

The key words “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in the chapters 2-10 normative statements are to be interpreted as described in [RFC-2119].

1.2 Statement Type

Please note a very important distinction between different sections of text throughout this document. You will encounter two distinctive kinds of text: informative comment and normative statements. Because most of the text in this specification will be of the kind normative statements, the authors have informally defined it as the default and, as such, have specifically called out text of the kind informative comment. They have done this by flagging the beginning and end of each informative comment and highlighting its text in gray. This means that unless text is specifically marked as of the kind informative comment, you can consider it of the kind normative statements.

For example:

Start of informative comment

This is the first paragraph of several paragraphs containing text of the kind **informative comment** …

This is the second paragraph of text of the kind **informative comment** …

This is the nth paragraph of text of the kind **informative comment** …

To understand the TPM specification the user must read the specification. (This use of MUST does not require any action).

End of informative comment

This is the first paragraph of one or more paragraphs (and/or sections) containing the text of the kind normative statements …

To understand the TPM specification the user MUST read the specification. (This use of MUST indicates a keyword usage and requires an action).

2. Basic Definitions

Start of informative comment

The following structures and formats describe the interoperable areas of the specification. There is no requirement that internal storage or memory representations of data must follow these structures. These requirements are in place only during the movement of data from a TPM to some other entity.

End of informative comment

2.1 Representation of Information

2.1.1 Endianness of Structures

Each structure MUST use big endian bit ordering, which follows the Internet standard and requires that the low-order bit appear to the far right of a word, buffer, wire format, or other area and the high-order bit appear to the far left.

2.1.2 Byte Packing

All structures MUST be packed on a byte boundary.

2.1.3 Lengths

The “Byte” is the unit of length when the length of a parameter is specified.

2.1.4 Structure Definitions

This is not a MIDL compatible specification. The syntax of a structure definition is just a hint. It should be used with Description column to determine the nature of a structure member.

In structure definitions and parameter lists, byte arrays are indicated as follows:

1. BYTE is a single byte.
2. BYTE[n] is a fixed array of n bytes.
3. BYTE[] is a self describing variable array of bytes that is always present
4. BYTE* is an array of bytes whose length is specified by a previous structure member. The array is not present if the length is zero.

2.2 Defines

Start of informative comment

These definitions are in use to make a consistent use of values throughout the structure specifications.

End of informative comment

2.2.1 Basic data types

Parameters

Typedef	Name	Description
unsigned char	BYTE	Basic byte used to transmit all character fields.
unsigned char	BOOL	TRUE/FALSE field. TRUE = 0x01, FALSE = 0x00
unsigned short	UINT16	16-bit field. The definition in different architectures may need to specify 16 bits instead of the short definition
unsigned long	UINT32	32-bit field. The definition in different architectures may need to specify 32 bits instead of the long definition

2.2.2 Boolean types

Start of informative comment

Since values other that 0x00 and 0x01 have an implementation specific interpretation, the TSS should send only those two values.

End of informative comment

Name	Value	Description
TRUE	0x01	Assertion
FALSE	0x00	Contradiction

Description

Boolean incoming parameter values other than 0x00 and 0x01 have an implementation specific interpretation. The TPM SHOULD return TPM_BAD_PARAMETER.

2.2.3 Helper redefinitions

The following definitions are to make the definitions more explicit and easier to read.

Parameters

Typedef	Name	Description
BYTE	TPM_AUTH_DATA_USAGE	Indicates the conditions where it is required that authorization be presented.
BYTE	TPM_PAYLOAD_TYPE	The information as to what the payload is in an encrypted structure
BYTE	TPM_VERSION_BYTE	The version info breakdown
BYTE	TPM_DA_STATE	The state of the dictionary attack mitigation logic
UINT16	TPM_TAG	The request or response authorization type.

Typedef	Name	Description
UINT16	TPM_PROTOCOL_ID	The protocol in use.
UINT16	TPM_STARTUP_TYPE	Indicates the start state.
UINT16	TPM_ENC_SCHEME	The definition of the encryption scheme.
UINT16	TPM_SIG_SCHEME	The definition of the signature scheme.
UINT16	TPM_MIGRATE_SCHEME	The definition of the migration scheme
UINT16	TPM_PHYSICAL_PRESENCE	Sets the state of the physical presence mechanism.
UINT16	TPM_ENTITY_TYPE	Indicates the types of entity that are supported by the TPM.
UINT16	TPM_KEY_USAGE	Indicates the permitted usage of the key.
UINT16	TPM_EK_TYPE	The type of asymmetric encrypted structure in use by the endorsement key
UINT16	TPM_STRUCTURE_TAG	The tag for the structure
UINT16	TPM_PLATFORM_SPECIFIC	The platform specific spec to which the information relates to
UINT32	TPM_COMMAND_CODE	The command ordinal.
UINT32	TPM_CAPABILITY_AREA	Identifies a TPM capability area.
UINT32	TPM_KEY_FLAGS	Indicates information regarding a key.
UINT32	TPM_ALGORITHM_ID	Indicates the type of algorithm.
UINT32	TPM_MODIFIER_INDICATOR	The locality modifier
UINT32	TPM_ACTUAL_COUNT	The actual number of a counter.
UINT32	TPM_TRANSPORT_ATTRIBUTES	Attributes that define what options are in use for a transport session
UINT32	TPM_AUTHHANDLE	Handle to an authorization session
UINT32	TPM_DIRINDEX	Index to a DIR register
UINT32	TPM_KEY_HANDLE	The area where a key is held assigned by the TPM.
UINT32	TPM_PCRINDEX	Index to a PCR register
UINT32	TPM_RESULT	The return code from a function
UINT32	TPM_RESOURCE_TYPE	The types of resources that a TPM may have using internal resources
UINT32	TPM_KEY_CONTROL	Allows for controlling of the key when loaded and how to handle TPM_Startup issues
UINT32	TPM_NV_INDEX	The index into the NV storage area
UINT32	TPM_FAMILY_ID	The family ID. Families ID's are automatically assigned a sequence number by the TPM. A trusted process can set the FamilyID value in an individual row to zero, which invalidates that row. The family ID resets to zero on each change of TPM Owner.
UINT32	TPM_FAMILY_VERIFICATION	A value used as a label for the most recent verification of this family. Set to zero when not in use.
UINT32	TPM_STARTUP_EFFECTS	How the TPM handles var
UINT32	TPM_SYM_MODE	The mode of a symmetric encryption
UINT32	TPM_FAMILY_FLAGS	The family flags
UINT32	TPM_DELEGATE_INDEX	The index value for the delegate NV table
UINT32	TPM_CMK_DELEGATE	The restrictions placed on delegation of CMK commands
UINT32	TPM_COUNT_ID	The ID value of a monotonic counter
UINT32	TPM_REDIT_COMMAND	A command to execute
UINT32	TPM_TRANSHANDLE	A transport session handle
UINT32	TPM_HANDLE	A generic handle could be key, transport etc.
UINT32	TPM_FAMILY_OPERATION	What operation is happening

2.2.4 Vendor specific

Start of informative comment

For all items that can specify an individual algorithm, protocol or item the specification allows for vendor specific selections. The mechanism to specify a vendor specific mechanism is to set the high bit of the identifier on.

End of informative comment

The following defines allow for the quick specification of a vendor specific item.

Parameters

Name	Value
TPM_Vendor_Specific32	0x00000400
TPM_Vendor_Specific8	0x80

339 3. Structure Tags

340 **Start of informative comment**

341 There have been some indications that knowing what structure is in use would be valuable
342 information in each structure. This new tag will be in each new structure that the TPM
343 defines.

344 The upper nibble of the value designates the purview of the structure tag. 0 is used for TPM
345 structures, 1 for platforms, and 2-F are reserved.

346 **End of informative comment**

347 3.1 TPM_STRUCTURE_TAG

348 The upper nibble of the value MUST be 0 for all TPM structures.

349 TPM_ResourceTypes

Name	Value	Structure
TPM_TAG_CONTEXTBLOB	0x0001	TPM_CONTEXT_BLOB
TPM_TAG_CONTEXT_SENSITIVE	0x0002	TPM_CONTEXT_SENSITIVE
TPM_TAG_CONTEXTPOINTER	0x0003	TPM_CONTEXT_POINTER
TPM_TAG_CONTEXTLIST	0x0004	TPM_CONTEXT_LIST
TPM_TAG_SIGNINFO	0x0005	TPM_SIGN_INFO
TPM_TAG_PCR_INFO_LONG	0x0006	TPM_PCR_INFO_LONG
TPM_TAG_PERSISTENT_FLAGS	0x0007	TPM_PERSISTENT_FLAGS (deprecated 1.1 structure)
TPM_TAG_VOLATILE_FLAGS	0x0008	TPM_VOLATILE_FLAGS (deprecated 1.1 structure)
TPM_TAG_PERSISTENT_DATA	0x0009	TPM_PERSISTENT_DATA (deprecated 1.1 structure)
TPM_TAG_VOLATILE_DATA	0x000A	TPM_VOLATILE_DATA (deprecated 1.1 structure)
TPM_TAG_SV_DATA	0x000B	TPM _SV_DATA
TPM_TAG_EK_BLOB	0x000C	TPM_EK_BLOB
TPM_TAG_EK_BLOB_AUTH	0x000D	TPM_EK_BLOB_AUTH
TPM_TAG_COUNTER_VALUE	0x000E	TPM_COUNTER_VALUE
TPM_TAG_TRANSPORT_INTERNAL	0x000F	TPM_TRANSPORT_INTERNAL
TPM_TAG_TRANSPORT_LOG_IN	0x0010	TPM_TRANSPORT_LOG_IN
TPM_TAG_TRANSPORT_LOG_OUT	0x0011	TPM _TRANSPORT_LOG_OUT
TPM_TAG_AUDIT_EVENT_IN	0x0012	TPM_AUDIT_EVENT_IN
TPM_TAG_AUDIT_EVENT_OUT	0X0013	TPM_AUDIT_EVENT_OUT
TPM_TAG_CURRENT_TICKS	0x0014	TPM_CURRENT_TICKS
TPM_TAG_KEY	0x0015	TPM _KEY
TPM_TAG_STORED_DATA12	0x0016	TPM_ STORED_DATA12
TPM_TAG_NV_ATTRIBUTES	0x0017	TPM_ NV_ATTRIBUTES
TPM_TAG_NV_DATA_PUBLIC	0x0018	TPM _NV_DATA_PUBLIC
TPM_TAG_NV_DATA_SENSITIVE	0x0019	TPM _NV_DATA_SENSITIVE
TPM_TAG_DELEGATIONS	0x001A	TPM DELEGATIONS
TPM_TAG_DELEGATE_PUBLIC	0x001B	TPM_ DELEGATE_PUBLIC
TPM_TAG_DELEGATE_TABLE_ROW	0x001C	TPM_DELEGATE_TABLE_ROW
TPM_TAG_TRANSPORT_AUTH	0x001D	TPM_TRANSPORT_AUTH
TPM_TAG_TRANSPORT_PUBLIC	0X001E	TPM_TRANSPORT_PUBLIC
TPM_TAG_PERMANENT_FLAGS	0X001F	TPM_PERMANENT_FLAGS
TPM_TAG_STCLEAR_FLAGS	0X0020	TPM_STCLEAR_FLAGS
TPM_TAG_STANY_FLAGS	0X0021	TPM_STANY_FLAGS
TPM_TAG_PERMANENT_DATA	0X0022	TPM_PERMANENT_DATA
TPM_TAG_STCLEAR_DATA	0X0023	TPM_STCLEAR_DATA

Name	Value	Structure
TPM_TAG_STANY_DATA	0X0024	TPM_STANY_DATA
TPM_TAG_FAMILY_TABLE_ENTRY	0X0025	TPM_FAMILY_TABLE_ENTRY
TPM_TAG_DELEGATE_SENSITIVE	0X0026	TPM_DELEGATE_SENSITIVE
TPM_TAG_DELG_KEY_BLOB	0X0027	TPM_DELG_KEY_BLOB
TPM_TAG_KEY12	0x0028	TPM_KEY12
TPM_TAG_CERTIFY_INFO2	0X0029	TPM_CERTIFY_INFO2
TPM_TAG_DELEGATE_OWNER_BLOB	0X002A	TPM_DELEGATE_OWNER_BLOB
TPM_TAG_EK_BLOB_ACTIVATE	0X002B	TPM_EK_BLOB_ACTIVATE
TPM_TAG_DAA_BLOB	0X002C	TPM_DAA_BLOB
TPM_TAG_DAA_CONTEXT	0X002D	TPM_DAA_CONTEXT
TPM_TAG_DAA_ENFORCE	0X002E	TPM_DAA_ENFORCE
TPM_TAG_DAA_ISSUER	0X002F	TPM_DAA_ISSUER
TPM_TAG_CAP_VERSION_INFO	0X0030	TPM_CAP_VERSION_INFO
TPM_TAG_DAA_SENSITIVE	0X0031	TPM_DAA_SENSITIVE
TPM_TAG_DAA_TPM	0X0032	TPM_DAA_TPM
TPM_TAG_CMK_MIGAUTH	0X0033	TPM_CMK_MIGAUTH
TPM_TAG_CMK_SIGTICKET	0X0034	TPM_CMK_SIGTICKET
TPM_TAG_CMK_MA_APPROVAL	0X0035	TPM_CMK_MA_APPROVAL
TPM_TAG_QUOTE_INFO2	0X0036	TPM_QUOTE_INFO2
TPM_TAG_DA_INFO	0x0037	TPM_DA_INFO
TPM_TAG_DA_INFO_LIMITED	0x0038	TPM_DA_INFO_LIMITED
TPM_TAG_DA_ACTION_TYPE	0x0039	TPM_DA_ACTION_TYPE

350# 4. Types

351## 4.1 TPM_RESOURCE_TYPE

352**TPM_ResourceTypes**

Name	Value	Description
TPM_RT_KEY	0x00000001	The handle is a key handle and is the result of a LoadKey type operation
TPM_RT_AUTH	0x00000002	The handle is an authorization handle. Auth handles come from TPM_OIAP, TPM_OSAP and TPM_DSAP
TPM_RT_HASH	0X00000003	Reserved for hashes
TPM_RT_TRANS	0x00000004	The handle is for a transport session. Transport handles come from TPM_EstablishTransport
TPM_RT_CONTEXT	0x00000005	Resource wrapped and held outside the TPM using the context save/restore commands
TPM_RT_COUNTER	0x00000006	Reserved for counters
TPM_RT_DELEGATE	0x00000007	The handle is for a delegate row. These are the internal rows held in NV storage by the TPM
TPM_RT_DAA_TPM	0x00000008	The value is a DAA TPM specific blob
TPM_RT_DAA_V0	0x00000009	The value is a DAA V0 parameter
TPM_RT_DAA_V1	0x0000000A	The value is a DAA V1 parameter

4.2 TPM_PAYLOAD_TYPE

Start of informative comment

This structure specifies the type of payload in various messages.

The payload may indicate whether the key is a CMK, and the CMK type. The distinction was put here rather than in TPM_KEY_USAGE:

- for backward compatibility
- because some commands only see the TPM_STORE_ASYMKEY, not the entire TPM_KEY

End of informative comment

TPM_PAYLOAD_TYPE Values

Value	Name	Comments
0x01	TPM_PT_ASYM	The entity is an asymmetric key
0x02	TPM_PT_BIND	The entity is bound data
0x03	TPM_PT_MIGRATE	The entity is a migration blob
0x04	TPM_PT_MAINT	The entity is a maintenance blob
0x05	TPM_PT_SEAL	The entity is sealed data
0x06	TPM_PT_MIGRATE_RESTRICTED	The entity is a restricted-migration asymmetric key
0x07	TPM_PT_MIGRATE_EXTERNAL	The entity is a external migratable key
0x08	TPM_PT_CMK_MIGRATE	The entity is a CMK migratable blob
0x09 – 0x7F		Reserved for future use by TPM
0x80 – 0xFF		Vendor specific payloads

4.3 TPM_ENTITY_TYPE

Start of informative comment

This specifies the types of entity and ADIP encryption schemes that are supported by the TPM. TPM entities are objects with authorization, such as the owner, a key, NV defined space, etc.

The LSB is used to indicate the entity type. The MSB is used to indicate the ADIP encryption scheme when applicable.

For compatibility with TPM 1.1, this mapping is maintained:

0x0001 specifies a keyHandle entity with XOR encryption

0x0002 specifies an owner entity with XOR encryption

0x0003 specifies some data entity with XOR encryption

0x0004 specifies the SRK entity with XOR encryption

0x0005 specifies a key entity with XOR encryption

The method of incrementing the symmetric key counter value is different from that used by some standard crypto libraries (e.g. openSSL, Java JCE) that increment the entire counter value. TPM users should be aware of this to avoid errors when the counter wraps.

End of informative comment

When the entity is not being used for ADIP encryption, the MSB MUST be 0x00.

TPM_ENTITY_TYPE LSB Values

Value	Entity Name	Key Handle	Comments
0x01	TPM_ET_KEYHANDLE		The entity is a keyHandle or key
0x02	TPM_ET_OWNER	0x40000001	The entity is the TPM Owner
0x03	TPM_ET_DATA		The entity is some data
0x04	TPM_ET_SRK	0x40000000	The entity is the SRK
0x05	TPM_ET_KEY		The entity is a key or keyHandle
0x06	TPM_ET_REVOKE	0x40000002	The entity is the RevokeTrust value
0x07	TPM_ET_DEL_OWNER_BLOB		The entity is a delegate owner blob
0x08	TPM_ET_DEL_ROW		The entity is a delegate row
0x09	TPM_ET_DEL_KEY_BLOB		The entity is a delegate key blob
0x0A	TPM_ET_COUNTER		The entity is a counter
0x0B	TPM_ET_NV		The entity is a NV index
0x0C	TPM_ET_OPERATOR		The entity is the operator
0x40	TPM_ET_RESERVED_HANDLE		Reserved. This value avoids collisions with the handle MSB setting.

TPM_ENTITY_TYPE MSB Values

Value	Algorithm	ADIP encryption scheme

0x00	TPM_ET_XOR	XOR
0x06	TPM_ET_AES128_CTR	AES 128 bits in CTR mode

4.4 Handles

Start of informative comment

Handles provides pointers to TPM internal resources. Handles should provide the ability to locate an entity without collision. When handles are used, the TPM must be able to unambiguously determine the entity type.

Handles are 32 bit values. To enable ease of use in handles and to assist in internal use of handles the TPM will use the following rules when creating the handle.

The three least significant bytes (LSB) of the handle contain whatever entropy the TPM needs to provide collision avoidance. The most significant byte (MSB) may also be included.

Counter handles need not provide collision avoidance.

Reserved key handles

Certain TPM entities have handles that point specifically to them, like the SRK. These values always use the MSB of 0x40. This is a reserved key handle value and all special handles will use the 0x40 prefix.

Handle collisions

The TPM provides good, but not foolproof protection against handle collisions. If system or application software detects a collision that is problematic, the software should evict the resource, and re-submit the command.

End of informative comment

1. The TPM MUST generate key, authorization session, transport session, and daa handles and MAY generate counter handles as follows:
    a. The three LSB of the handle MUST and the MSB MAY contain the collision resistance values. The TPM MUST provide protection against handle collision. The TPM MUST implement one of the following:
        i. The three LSB of the handle MUST and the MSB MAY be generated randomly. The TPM MUST ensure that no currently loaded entity of the same type has the same handle.
        ii. The three LSB of the handle MUST be generated from a monotonic counter. The monotonic counter value MUST NOT reset on TPM startup, but may wrap over the life of the TPM.
    b. The MSB MAY be a value that does not contribute to collision resistance.
2. A key handle MUST NOT have the reserved value 0x40 in the MSB.
3. The TPM MAY use the counter index as the monotonic counter handle.
4. Handles are not required to be globally unique between entity groups (key, authorization session, transport session, and daa).
    a. For example, a newly generated authorization handle MAY have the same value as a loaded key handle.

4.4.1 Reserved Key Handles

Start of informative comment

The reserved key handles. These values specify specific keys or specific actions for the TPM.

TPM_KH_TRANSPORT indicates to TPM_EstablishTransport that there is no encryption key, and that the "secret" wrapped parameters are actually passed unencrypted.

End of informative comment

1. All reserved key handles MUST start with 0x40.
2. By default, when an ordinal input parameter specifies a TPM_KEY_HANDLE, a TPM generated key handle or TPM_KH_SRK can be used, but a reserved key handle other than TPM_KH_SRK can never be used.
   a. The actions may further restrict use of any key. For example, TPM_KH_SRK cannot be used for TPM_Sign because it is not a signing key.
3. When an ordinal input parameter specifies a TPM_KEY_HANDLE, a reserved key handle can be used if explicitly allowed by the ordinal actions.
   a. For example, TPM_CreateWrapKey or TPM_GetPubKey can use TPM_KH_SRK but not TPM_KH_EK by default.
   b. For example, TPM_OwnerReadInternalPub can use TPM_KH_EK because it is explicitly allowed by the actions.

Key Handle Values

Key Handle	Handle Name	Comments
0x40000000	TPM_KH_SRK	The handle points to the SRK
0x40000001	TPM_KH_OWNER	The handle points to the TPM Owner
0x40000002	TPM_KH_REVOKE	The handle points to the RevokeTrust value
0x40000003	TPM_KH_TRANSPORT	The handle points to the TPM_EstablishTransport static authorization
0x40000004	TPM_KH_OPERATOR	The handle points to the Operator auth
0x40000005	TPM_KH_ADMIN	The handle points to the delegation administration auth
0x40000006	TPM_KH_EK	The handle points to the PUBEK, only usable with TPM_OwnerReadInternalPub

440 4.5 TPM_STARTUP_TYPE

441**Start of informative comment**

442To specify what type of startup is occurring.

443**End of informative comment**

444TPM_STARTUP_TYPE Values

Value	Event Name	Comments
0x0001	TPM_ST_CLEAR	The TPM is starting up from a clean state
0x0002	TPM_ST_STATE	The TPM is starting up from a saved state
0x0003	TPM_ST_DEACTIVATED	The TPM is to startup and set the deactivated flag to TRUE

4454.6 TPM_STARTUP_EFFECTS

446**Start of Informative comment**

447This structure lists for the various resources and sessions on a TPM the affect that
448TPM_Startup has on the values.

449There are three ST_STATE options for keys (restore all, restore non-volatile, or restore none)
450and two ST_CLEAR options (restore non-volatile or restore none). As bit 4 was insufficient
451to describe the possibilities, it is deprecated. Software should use TPM_CAP_KEY_HANDLE
452to determine which keys are loaded after TPM_Startup.

453**End of informative comment**

454Types of Startup

Bit position	Name	Description
31-9		No information and MUST be FALSE
8		TPM_RT_DAA_TPM resources are initialized by TPM_Startup(ST_STATE)
7		TPM_Startup has no effect on auditDigest
6		auditDigest is set to all zeros on TPM_Startup(ST_CLEAR) but not on other types of TPM_Startup
5		auditDigest is set to all zeros on TPM_Startup(any)
4		Deprecated, as the meaning was subject to interpretation. (Was:TPM_RT_KEY resources are initialized by TPM_Startup(ST_ANY))
3		TPM_RT_AUTH resources are initialized by TPM_Startup(ST_STATE)
2		TPM_RT_HASH resources are initialized by TPM_Startup(ST_STATE)
1		TPM_RT_TRANS resources are initialized by TPM_Startup(ST_STATE)
0		TPM_RT_CONTEXT session (but not key) resources are initialized by TPM_Startup(ST_STATE)

4554.7 TPM_PROTOCOL_ID

456**Start of informative comment**

457This value identifies the protocol in use.

458**End of informative comment**

459TPM_PROTOCOL_ID Values

Value	Event Name	Comments
0x0001	TPM_PID_OIAP	The OIAP protocol.
0x0002	TPM_PID_OSAP	The OSAP protocol.
0x0003	TPM_PID_ADIP	The ADIP protocol.
0X0004	TPM_PID_ADCP	The ADCP protocol.
0X0005	TPM_PID_OWNER	The protocol for taking ownership of a TPM.
0x0006	TPM_PID_DSAP	The DSAP protocol
0x0007	TPM_PID_TRANSPORT	The transport protocol

4604.8 TPM_ALGORITHM_ID

461**Start of informative comment**

462This table defines the types of algorithms that may be supported by the TPM.

463TPM_ALG_AESxxx is used to represent any of TPM_ALG_AES128, TPM_ALG_AES192, or
464TPM_ALG_AES256.

465**End of informative comment**

466TPM_ALGORITHM_ID values

Value	Name	Description
0x00000001	TPM_ALG_RSA	The RSA algorithm.
0x00000002	reserved	(was the DES algorithm)
0X00000003	reserved	(was the 3DES algorithm in EDE mode)
0x00000004	TPM_ALG_SHA	The SHA1 algorithm
0x00000005	TPM_ALG_HMAC	The RFC 2104 HMAC algorithm
0x00000006	TPM_ALG_AES128	The AES algorithm, key size 128
0x00000007	TPM_ALG_MGF1	The XOR algorithm using MGF1 to create a string the size of the encrypted block
0x00000008	TPM_ALG_AES192	AES, key size 192
0x00000009	TPM_ALG_AES256	AES, key size 256
0x0000000A	TPM_ALG_XOR	XOR using the rolling nonces

467Description

468The TPM MUST support the algorithms TPM_ALG_RSA, TPM_ALG_SHA, TPM_ALG_HMAC,
469and TPM_ALG_MGF1

4704.9 TPM_PHYSICAL_PRESENCE

Name	Value	Description
TPM_PHYSICAL_PRESENCE_HW_DISABLE	0x0200h	Sets the physicalPresenceHWEnable to FALSE
TPM_PHYSICAL_PRESENCE_CMD_DISABLE	0x0100h	Sets the physicalPresenceCMDEnable to FALSE
TPM_PHYSICAL_PRESENCE_LIFETIME_LOCK	0x0080h	Sets the physicalPresenceLifetimeLock to TRUE
TPM_PHYSICAL_PRESENCE_HW_ENABLE	0x0040h	Sets the physicalPresenceHWEnable to TRUE
TPM_PHYSICAL_PRESENCE_CMD_ENABLE	0x0020h	Sets the physicalPresenceCMDEnable to TRUE
TPM_PHYSICAL_PRESENCE_NOTPRESENT	0x0010h	Sets PhysicalPresence = FALSE
TPM_PHYSICAL_PRESENCE_PRESENT	0x0008h	Sets PhysicalPresence = TRUE
TPM_PHYSICAL_PRESENCE_LOCK	0x0004h	Sets PhysicalPresenceLock = TRUE

4714.10 TPM_MIGRATE_SCHEME

472**Start of informative comment**

473The scheme indicates how the StartMigrate command should handle the migration of the
474encrypted blob.

475**End of informative comment**

476TPM_MIGRATE_SCHEME values

Name	Value	Description
TPM_MS_MIGRATE	0x0001	A public key that can be used with all TPM migration commands other than 'ReWrap' mode.
TPM_MS_REWRAP	0x0002	A public key that can be used for the ReWrap mode of TPM_CreateMigrationBlob.
TPM_MS_MAINT	0x0003	A public key that can be used for the Maintenance commands
TPM_MS_RESTRICT_MIGRATE	0x0004	The key is to be migrated to a Migration Authority.
TPM_MS_RESTRICT_APPROVE	0x0005	The key is to be migrated to an entity approved by a Migration Authority using double wrapping

4774.11 TPM_EK_TYPE

478**Start of informative comment**

479This structure indicates what type of information that the EK is dealing with.

480**End of informative comment**

Name	Value	Description
TPM_EK_TYPE_ACTIVATE	0x0001	The blob MUST be TPM_EK_BLOB_ACTIVATE
TPM_EK_TYPE_AUTH	0x0002	The blob MUST be TPM_EK_BLOB_AUTH

4814.12 TPM_PLATFORM_SPECIFIC

482**Start of informative comment**

483This enumerated type indicates the platform specific spec that the information relates to.

484**End of informative comment**

Name	Value	Description
TPM_PS_PC_11	0x0001	PC Specific version 1.1
TPM_PS_PC_12	0x0002	PC Specific version 1.2
TPM_PS_PDA_12	0x0003	PDA Specific version 1.2
TPM_PS_Server_12	0x0004	Server Specific version 1.2
TPM_PS_Mobile_12	0x0005	Mobil Specific version 1.2

5. Basic Structures

5.1 TPM_STRUCT_VER

Start of informative comment

This indicates the version of the structure.

Version 1.2 deprecates the use of this structure in all other structures. The structure is not deprecated as many of the structures that contain this structure are not deprecated.

The rationale behind keeping this structure and adding the new version structure is that in version 1.1 this structure was in use for two purposes. The first was to indicate the structure version, and in that mode the revMajor and revMinor were supposed to be set to 0. The second use was in TPM_GetCapability and the structure would then return the correct revMajor and revMinor. This use model caused problems in keeping track of when the revs were or were not set and how software used the information. Version 1.2 went to structure tags. Some structures did not change and the TPM_STRUCT_VER is still in use. To avoid the problems from 1.1, this structure now is a fixed value and only remains for backwards compatibility. Structure versioning comes from the tag on the structure, and the TPM_GetCapability response for TPM versioning uses TPM_VERSION.

End of informative comment

Definition

```
typedef struct tdTPM_STRUCT_VER {
   BYTE major;
   BYTE minor;
   BYTE revMajor;
   BYTE revMinor;
} TPM_STRUCT_VER;
```

Parameters

Type	Name	Description
BYTE	major	This SHALL indicate the major version of the structure. MUST be 0x01
BYTE	minor	This SHALL indicate the minor version of the structure. MUST be 0x01
BYTE	revMajor	This MUST be 0x00 on output, ignored on input
BYTE	revMinor	This MUST be 0x00 on output, ignored on input

Descriptions

1. Provides the version of the structure
2. The TPM SHALL inspect the major and minor fields to determine if the TPM can properly interpret the structure.
   a. On error, the TPM MUST return TPM_BAD_VERSION.
   b. The TPM MUST ignore the revMajor and revMinor fields on input.

5165.2 TPM_VERSION_BYTE

517**Start of Informative comment**

518Allocating a byte for the version information is wasteful of space. The current allocation
519does not provide sufficient resolution to indicate completely the version of the TPM. To allow
520for backwards compatibility the size of the structure does not change from 1.1.

521To enable minor version numbers with 2-digit resolution, the byte representing a version
522splits into two BCD encoded nibbles. The ordering of the low and high order provides
523backwards compatibility with existing numbering.

524An example of an implementation of this is; a version of 1.23 would have the value 2 in bit
525positions 3-0 and the value 3 in bit positions 7-4.

526**End of informative comment**

527TPM_VERSION_BYTE is a byte. The byte is broken up according to the following rule

Bit position	Name	Description
7-4	leastSigVer	Least significant nibble of the minor version. MUST be values within the range of 0000-1001
3-0	mostSigVer	Most significant nibble of the minor version. MUST be values within the range of 0000-1001

5.3 TPM_VERSION

Start of informative comment

This structure provides information relative the version of the TPM. This structure should only be in use by TPM_GetCapability to provide the information relative to the TPM.

End of informative comment

Definition

```
typedef struct tdTPM_VERSION {
  TPM_VERSION_BYTE major;
  TPM_VERSION_BYTE minor;
  BYTE revMajor;
  BYTE revMinor;
} TPM_VERSION;
```

Parameters

Type	Name	Description
TPM_VERSION_BYTE	Major	This SHALL indicate the major version of the TPM, mostSigVer MUST be 0x01, leastSigVer MUST be 0x00
TPM_VERSION_BYTE	Minor	This SHALL indicate the minor version of the TPM, mostSigVer MUST be 0x01 or 0x02, leastSigVer MUST be 0x00
BYTE	revMajor	This SHALL be the value of the TPM_PERMANENT_DATA -> revMajor
BYTE	revMinor	This SHALL be the value of the TPM_PERMANENT_DATA -> revMinor

Descriptions

1. The major and minor fields indicate the specification version the TPM was designed for
2. The revMajor and revMinor fields indicate the manufacturer's revision of the TPM
   a. Most challengers of the TPM MAY ignore the revMajor and revMinor fields

5.4 TPM_DIGEST

Start of informative comment

The digest value reports the result of a hash operation.

In version 1 the hash algorithm is SHA-1 with a resulting hash result being 20 bytes or 160 bits.

It is understood that algorithm agility is lost due to fixing the hash at 20 bytes and on SHA-1. The reason for fixing is due to the internal use of the digest. It is the AuthData values, it provides the secrets for the HMAC and the size of 20 bytes determines the values that can be stored and encrypted. For this reason, the size is fixed and any changes to this value require a new version of the specification.

End of informative comment

Definition

```
typedef struct tdTPM_DIGEST{
   BYTE digest[digestSize];
} TPM_DIGEST;
```

Parameters

Type	Name	Description
BYTE[]	digest	This SHALL be the actual digest information

Description

The digestSize parameter MUST indicate the block size of the algorithm and MUST be 20 or greater.

For all TPM v1 hash operations, the hash algorithm MUST be SHA-1 and the digestSize parameter is therefore equal to 20.

Redefinitions

Typedef	Name	Description
TPM_DIGEST	TPM_CHOSENID_HASH	This SHALL be the digest of the chosen identityLabel and privacyCA for a new TPM identity.
TPM_DIGEST	TPM_COMPOSITE_HASH	This SHALL be the hash of a list of PCR indexes and PCR values that a key or data is bound to.
TPM_DIGEST	TPM_DIRVALUE	This SHALL be the value of a DIR register
TPM_DIGEST	TPM_HMAC	This shall be the output of the HMAC algorithm
TPM_DIGEST	TPM_PCRVALUE	The value inside of the PCR
TPM_DIGEST	TPM_AUDITDIGEST	This SHALL be the value of the current internal audit state

568

569**5.4.1 Creating a PCR composite hash**

570The definition specifies the operation necessary to create TPM_COMPOSITE_HASH.

571**Action**

5721. The hashing MUST be done using the SHA-1 algorithm.

5732. The input must be a valid TPM_PCR_SELECTION structure.

5743. The process creates a TPM_PCR_COMPOSITE structure from the TPM_PCR_SELECTION 575 structure and the PCR values to be hashed. If constructed by the TPM the values MUST 576 come from the current PCR registers indicated by the PCR indices in the 577 TPM_PCR_SELECTION structure.

5784. The process then computes a SHA-1 digest of the TPM_PCR_COMPOSITE structure.

5795. The output is the SHA-1 digest just computed.

5.5 TPM_NONCE

Start of informative comment

A nonce is a random value that provides protection from replay and other attacks. Many of the commands and protocols in the specification require a nonce. This structure provides a consistent view of what a nonce is.

End of informative comment

Definition

```
typedef struct tdTPM_NONCE{
  BYTE nonce[20];
  } TPM_NONCE;
```

Parameters

Type	Name	Description
BYTE[20]	Nonce	This SHALL be the 20 bytes of random data. When created by the TPM the value MUST be the next 20 bytes from the RNG.

Redefinitions

Typedef	Name	Description
TPM_NONCE	TPM_DAA_TPM_SEED	This SHALL be a random value generated by a TPM immediately after the EK is installed in that TPM, whenever an EK is installed in that TPM
TPM_NONCE	TPM_DAA_CONTEXT_SEED	This SHALL be a random value

593 5.6 TPM_AUTHDATA

594**Start of informative comment**

595The AuthData data is the information that is saved or passed to provide proof of ownership 596of an entity. For version 1 this area is always 20 bytes.

597**End of informative comment**

598 Definition

599
```
typedef BYTE tdTPM_AUTHDATA[20];
```

600 Descriptions

601When sending AuthData data to the TPM the TPM does not validate the decryption of the 602data. It is the responsibility of the entity owner to validate that the AuthData data was 603properly received by the TPM. This could be done by immediately attempting to open an 604authorization session.

605The owner of the data can select any value for the data

606 Redefinitions

Typedef	Name	Description
TPM_AUTHDATA	TPM_SECRET	A secret plaintext value used in the authorization process.
TPM_AUTHDATA	TPM_ENCAUTH	A ciphertext (encrypted) version of AuthData data. The encryption mechanism depends on the context.

607 5.7 TPM_KEY_HANDLE_LIST

608**Start of informative comment**

609TPM_KEY_HANDLE_LIST is a structure used to describe the handles of all keys currently 610loaded into a TPM.

611**End of informative comment**

612 Definition

```
613typedef struct tdTPM_KEY_HANDLE_LIST {
614   UINT16  loaded;
615   [size_is(loaded)] TPM_KEY_HANDLE    handle[];
616} TPM_KEY_HANDLE_LIST;
```

617 Parameters

Type	Name	Description
UINT16	loaded	The number of keys currently loaded in the TPM.
UINT32	handle	An array of handles, one for each key currently loaded in the TPM

618 Description

619The order in which keys are reported is manufacturer-specific.

620 5.8 TPM_KEY_USAGE values

621**Start of informative comment**

622This table defines the types of keys that are possible. Each value defines for what operation
623the key can be used. Most key usages can be CMKs. See 4.2, TPM_PAYLOAD_TYPE.

624Each key has a setting defining the encryption and signature scheme to use. The selection
625of a key usage value limits the choices of encryption and signature schemes.

626

627**End of informative comment**

Name	Value	Description
TPM_KEY_SIGNING	0x0010	This SHALL indicate a signing key. The [private] key SHALL be used for signing operations, only. This means that it MUST be a leaf of the Protected Storage key hierarchy.
TPM_KEY_STORAGE	0x0011	This SHALL indicate a storage key. The key SHALL be used to wrap and unwrap other keys in the Protected Storage hierarchy
TPM_KEY_IDENTITY	0x0012	This SHALL indicate an identity key. The key SHALL be used for operations that require a TPM identity, only.
TPM_KEY_AUTHCHANGE	0X0013	This SHALL indicate an ephemeral key that is in use during the ChangeAuthAsym process, only.
TPM_KEY_BIND	0x0014	This SHALL indicate a key that can be used for TPM_Bind and TPM_UnBind operations only.
TPM_KEY_LEGACY	0x0015	This SHALL indicate a key that can perform signing and binding operations. The key MAY be used for both signing and binding operations. The TPM_KEY_LEGACY key type is to allow for use by applications where both signing and encryption operations occur with the same key. The use of this key type is not recommended
TPM_KEY_MIGRATE	0x0016	This SHALL indicate a key in use for TPM_MigrateKey

628 5.8.1 TPM_ENC_SCHEME, TPM_SIG_SCHEME

629**Start of Informative comment**

630For a given key usage type there are subset of valid encryption and signature schemes.

631The method of incrementing the symmetric key counter value is different from that used by
632some standard crypto libraries (e.g. openSSL, Java JCE) that increment the entire counter
633value. TPM users should be aware of this to avoid errors when the counter wraps.

634**End of informative comment**

635The key usage value for a key determines the encryption and / or signature schemes which
636MUST be used with that key. The table below maps the schemes defined by this
637specification to the defined key usage values.

Name	Allowed Encryption schemes	Allowed Signature Schemes
TPM_KEY_SIGNING	TPM_ES_NONE	TPM_SS_RSASSAPKCS1v15_SHA1 TPM_SS_RSASSAPKCS1v15_DER TPM_SS_RSASSAPKCS1v15_INFO
TPM_KEY_STORAGE	TPM_ES_RSAESOAEP_SHA1_MGF1	TPM_SS_NONE
TPM_KEY_IDENTITY	TPM_ES_NONE	TPM_SS_RSASSAPKCS1v15_SHA1
TPM_KEY_AUTHCHANGE	TPM_ES_RSAESOAEP_SHA1_MGF1	TPM_SS_NONE
TPM_KEY_BIND	TPM_ES_RSAESOAEP_SHA1_MGF1	TPM_SS_NONE

	TPM_ES_RSAESPKCSV15	
TPM_KEY_LEGACY	TPM_ES_RSAESOAEP_SHA1_MGF1 TPM_ES_RSAESPKCSV15	TPM_SS_RSASSAPKCS1v15_SHA1 TPM_SS_RSASSAPKCS1v15_DER
TPM_KEY_MIGRATE	TPM_ES_RSAESOAEP_SHA1_MGF1	TPM_SS_NONE

638

639The endorsement key is of type TPM_KEY_STORAGE. That is, it is never used for signing, 640and the encryption algorithm is TPM_ES_RSAESOAEP_SHA1_MGF1.

641Where manufacturer specific schemes are used, the strength must be at least that listed in 642the above table for TPM_KEY_STORAGE, TPM_KEY_IDENTITY and 643TPM_KEY_AUTHCHANGE key types.

644

645The TPM MUST check that the encryption scheme defined for use with the key is a valid 646scheme for the key type, as follows:

Key algorithm	Approved encryption schemes	TPM_ENC_SCHEME
TPM_ALG_RSA	TPM_ES_NONE	0x0001
TPM_ALG_RSA	TPM_ES_RSAESPKCSv15	0x0002
TPM_ALG_RSA	TPM_ES_RSAESOAEP_SHA1_MGF1	0x0003
TPM_ALG_AESxxx	TPM_ES_SYM_CTR	0x0004
TPM_ALG_AESxxx	TPM_ES_SYM_OFB	0x0005

647

648For TPM_ALG_MGF1, TPM_ENC_SCHEME is not used. The TPM MAY validate that 649TPM_ENC_SCHEME is TPM_ES_NONE.

650The TPM MUST check that the signature scheme defined for use with the key is a valid 651scheme for the key type, as follows:

Key algorithm	Approved signature schemes	TPM_SIG_SCHEME
TPM_ALG_RSA	TPM_SS_NONE	0x0001
	TPM_SS_RSASSAPKCS1v15_SHA1	0x0002
	TPM_SS_RSASSAPKCS1v15_DER	0x0003
	TPM_SS_RSASSAPKCS1v15_INFO	0x0004

5.9 TPM_AUTH_DATA_USAGE values

Start of informative comment

The indication to the TPM when authorization sessions for an entity are required. Future versions may allow for more complex decisions regarding AuthData checking.

Tag	Ordinal Table	TPM_AUTH_DATA_USAGE	Action
AUTH1_COMMAND	AUTH1	TPM_AUTH_ALWAYS	Authorization HMAC is checked
AUTH1_COMMAND	AUTH1	TPM_AUTH_NEVER	Authorization HMAC is checked
AUTH1_COMMAND	AUTH1,RQU	TPM_AUTH_ALWAYS	Authorization HMAC is checked
AUTH1_COMMAND	AUTH1,RQU	TPM_AUTH_NEVER	Authorization HMAC is checked
RQU_COMMAND	AUTH1		Return TPM_BADTAG
RQU_COMMAND	AUTH1,RQU	TPM_AUTH_ALWAYS	Return TPM_AUTHFAIL
RQU_COMMAND	AUTH1,RQU	TPM_AUTH_NEVER	Allow command with no authorization check

The above table describes various combinations.

Lines 1-4 say that, if an authorization HMAC is present and the ordinal table allows authorization, it is always checked. The TPM_AUTH_DATA_USAGE value is ignored.

Line 4 is often missed. That is, even if the ordinal table says that the command can be run without authorization and TPM_AUTH_DATA_USAGE says TPM_AUTH_NEVER, authorization can be present. If present, it is checked. TPM_AUTH_NEVER means that authorization may not be required for the key. It does not mean that authorization is not allowed.

Line 5 says that, if an authorization HMAC is not present, but the ordinal table says that authorization is required for the ordinal, TPM_BADTAG is returned. The TPM_AUTH_DATA_USAGE value is ignored. For example, TPM_CreateWrapKey always requires authorization, even if the key has TPM_AUTH_NEVER set.

Lines 6 says that, if an authorization HMAC is not present, the ordinal table allows the command without the HMAC, but TPM_AUTH_ALWAYS is set, TPM_AUTHFAIL is returned. Even though the ordinal in general allows no authorization, the key used for this command requires authorization.

Lines 7 says that, if an authorization HMAC is not present, the ordinal table allows the command without the HMAC, and TPM_AUTH_NEVER is set, the command is allowed to execute without authorization. The ordinal in general permits no authorization, and the key also permits no authorization.

End of informative comment

Name	Value	Description
TPM_AUTH_NEVER	0x00	This SHALL indicate that usage of the key without authorization is permitted.
TPM_AUTH_ALWAYS	0x01	This SHALL indicate that on each usage of the key the authorization MUST be performed.
TPM_NO_READ_PUBKEY_AUTH	0x03	This SHALL indicate that on commands that require the TPM to use the the key, the authorization MUST be performed. For commands that cause the TPM to read the public portion of the key, but not to use the key (e.g. TPM_GetPubKey), the authorization may be omitted.
		All other values are reserved for future use.

677 5.10 TPM_KEY_FLAGS

678**Start of informative comment**

679This table defines the meanings of the bits in a TPM_KEY_FLAGS structure, used in 680TPM_KEY and TPM_CERTIFY_INFO.

681**End of informative comment**

682 TPM_KEY_FLAGS Values

Name	Mask Value	Description
redirection	0x00000001	This mask value SHALL indicate the use of redirected output.
migratable	0x00000002	This mask value SHALL indicate that the key is migratable.
isVolatile	0x00000004	This mask value SHALL indicate that the key MUST be unloaded upon execution of the TPM_Startup(ST_Clear). This does not indicate that a nonvolatile key will remain loaded across TPM_Startup(ST_Clear) events.
pcrIgnoredOnRead	0x00000008	When TRUE the TPM MUST NOT check digestAtRelease or localityAtRelease for commands that read the public portion of the key (e.g., TPM_GetPubKey) and MAY NOT check digestAtRelease or localityAtRelease for commands that use the public portion of the key (e.g. TPM_Seal) When FALSE the TPM MUST check digestAtRelease and localityAtRelease for commands that read or use the public portion of the key
migrateAuthority	0x00000010	When set indicates that the key is under control of a migration authority. The TPM MUST only allow the creation of a key with this flag in TPM_CMK_CreateKey

683

684The value of TPM_KEY_FLAGS MUST be decomposed into individual mask values. The 685presence of a mask value SHALL have the effect described in the above table

686On input, all undefined bits MUST be zero. The TPM MUST return an error if any undefined 687bit is set. On output, the TPM MUST set all undefined bits to zero.

688 5.11 TPM_CHANGEAUTH_VALIDATE

689**Start of informative comment**

690This structure provides an area that will stores the new AuthData data and the challenger's
691nonce.

692**End of informative comment**

693 Definition

```
694typedef struct tdTPM_CHANGEAUTH_VALIDATE {
695   TPM_SECRET newAuthSecret;
696   TPM_NONCE n1;
697} TPM_CHANGEAUTH_VALIDATE;
```

698 Parameters

Type	Name	Description
TPM_SECRET	newAuthSecret	This SHALL be the new AuthData data for the target entity
TPM_NONCE	n1	This SHOULD be a nonce, to enable the caller to verify that the target TPM is on-line.

699 5.12 TPM_MIGRATIONKEYAUTH

700 **Start of informative comment**

701 This structure provides the proof that the associated public key has TPM Owner AuthData
702 to be a migration key.

703 **End of informative comment**

704 Definition

```
705 typedef struct tdTPM_MIGRATIONKEYAUTH{
706   TPM_PUBKEY migrationKey;
707   TPM_MIGRATE_SCHEME migrationScheme;
708   TPM_DIGEST digest;
709 } TPM_MIGRATIONKEYAUTH;
```

710 Parameters

Type	Name	Description
TPM_PUBKEY	migrationKey	This SHALL be the public key of the migration facility
TPM_MIGRATE_SCHEME	migrationScheme	This shall be the type of migration operation.
TPM_DIGEST	digest	This SHALL be the digest value of the concatenation of migration key, migration scheme and tpmProof

5.13 TPM_COUNTER_VALUE

Start of informative comment

This structure returns the counter value. For interoperability, the value size should be 4 bytes.

End of informative comment

Definition

```
typedef struct tdTPM_COUNTER_VALUE{
  TPM_STRUCTURE_TAG  tag;
  BYTE label[4];
  TPM_ACTUAL_COUNT counter;
} TPM_COUNTER_VALUE;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_COUNTER_VALUE
BYTE[4]	label	The label for the counter
TPM_ACTUAL_COUNT	counter	The 32-bit counter value.

723 5.14 TPM_SIGN_INFO Structure

724**Start of informative comment**

725This is an addition in 1.2 and is the structure signed for certain commands (e.g., 726TPM_ReleaseTransportSigned). Some commands have a structure specific to that command 727(e.g., TPM_Quote uses TPM_QUOTE_INFO) and do not use TPM_SIGN_INFO.

728TPM_Sign uses this structure when the signature scheme is 729TPM_SS_RSASSAPKCS1v15_INFO.

730**End of informative comment**

731 Definition

```
732typedef struct tdTPM_SIGN_INFO {
733   TPM_STRUCTURE_TAG tag;
734   BYTE fixed[4];
735   TPM_NONCE replay;
736   UINT32 dataLen;
737   [size_is (dataLen)] BYTE* data;
738} TPM_SIGN_INFO;
```

739 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	Set to TPM_TAG_SIGNINFO
BYTE[4]	fixed	The ASCII text that identifies what function was performing the signing operation
TPM_NONCE	replay	Nonce provided by caller to prevent replay attacks
UINT32	dataLen	The length of the data area
BYTE*	data	The data that is being signed

5.15 TPM_MSA_COMPOSITE

Start of informative comment

TPM_MSA_COMPOSITE contains an arbitrary number of digests of public keys belonging to Migration Authorities. An instance of TPM_MSA_COMPOSITE is incorporated into the migrationAuth value of a certified-migration-key (CMK), and any of the Migration Authorities specified in that instance is able to approve the migration of that certified-migration-key.

End of informative comment

Definition

```
typedef struct tdTPM_MSA_COMPOSITE {
   UINT32 MSAlist;
   TPM_DIGEST[] migAuthDigest[];
} TPM_MSA_COMPOSITE;
```

Parameters

Type	Name	Description
UINT32	MSAlist	The number of migAuthDigests. MSAlist MUST be one (1) or greater.
TPM_DIGEST[]	migAuthDigest[]	An arbitrary number of digests of public keys belonging to Migration Authorities.

TPMs MUST support TPM_MSA_COMPOSITE structures with MSAlist of four (4) or less, and MAY support larger values of MSAlist.

757 5.16 TPM_CMK_AUTH

758**Start of informative comment**

759The signed digest of TPM_CMK_AUTH is a ticket to prove that an entity with public key
760"migrationAuthority" has approved the public key "destination Key" as a migration
761destination for the key with public key "sourceKey".

762Normally the digest of TPM_CMK_AUTH is signed by the private key corresponding to
763"migrationAuthority".

764To reduce data size, TPM_CMK_AUTH contains just the digests of "migrationAuthority",
765"destinationKey" and "sourceKey".

766**End of informative comment**

767 Definition

```
768typedef struct tdTPM_CMK_AUTH{
769   TPM_DIGEST migrationAuthorityDigest;
770   TPM_DIGEST destinationKeyDigest;
771   TPM_DIGEST sourceKeyDigest;
772} TPM_CMK_AUTH;
```

773 Parameters

Type	Name	Description
TPM_DIGEST	migrationAuthorityDigest	The digest of a public key belonging to a Migration Authority
TPM_DIGEST	destinationKeyDigest	The digest of a TPM_PUBKEY structure that is an approved destination key for the private key associated with "sourceKey"
TPM_DIGEST	sourceKeyDigest	The digest of a TPM_PUBKEY structure whose corresponding private key is approved by a Migration Authority to be migrated as a child to the destinationKey.

5.17 TPM_CMK_DELEGATE values

Start of informative comment

The bits of TPM_CMK_DELEGATE are flags that determine how the TPM responds to delegated requests to manipulate a certified-migration-key, a loaded key with payload type TPM_PT_MIGRATE_RESTRICTED or TPM_PT_MIGRATE_EXTERNAL.

End of informative comment

Bit	Name	Description
31	TPM_CMK_DELEGATE_SIGNING	When set to 1, this bit SHALL indicate that a delegated command may manipulate a CMK of TPM_KEY_USAGE == TPM_KEY_SIGNING
30	TPM_CMK_DELEGATE_STORAGE	When set to 1, this bit SHALL indicate that a delegated command may manipulate a CMK of TPM_KEY_USAGE == TPM_KEY_STORAGE
29	TPM_CMK_DELEGATE_BIND	When set to 1, this bit SHALL indicate that a delegated command may manipulate a CMK of TPM_KEY_USAGE == TPM_KEY_BIND
28	TPM_CMK_DELEGATE_LEGACY	When set to 1, this bit SHALL indicate that a delegated command may manipulate a CMK of TPM_KEY_USAGE == TPM_KEY_LEGACY
27	TPM_CMK_DELEGATE_MIGRATE	When set to 1, this bit SHALL indicate that a delegated command may manipulate a CMK of TPM_KEY_USAGE == TPM_KEY_MIGRATE
26:0	reserved	MUST be 0

The default value of TPM_CMK_Delegate is zero (0)

781 5.18 TPM_SELECT_SIZE

782**Start of informative comment**

783This structure provides the indication for the version and sizeOfSelect structure in
784TPM_GetCapability. Entities wishing to know if the TPM supports, for a specific version, a
785specific size fills in this structure and requests a TPM_GetCapability response from the
786TPM.

787For instance, the entity would fill in version 1.1 and size 2. As 2 was the default size the
788TPM should return true. Filling in 1.1 and size 3, would return true or false depending on
789the capabilities of the TPM. For 1.2 the default size is 3 so all TPM's should support that
790size.

791The real purpose of this structure is to see if the TPM supports an optional size for previous
792versions.

793**End of informative comment**

794 Definition

```
795typedef struct tdTPM_SELECT_SIZE {
796   BYTE major;
797   BYTE minor;
798   UINT16 reqSize;
799} TPM_SELECT_SIZE;
```

800 Parameters

Type	Name	Description
BYTE	Major	This SHALL indicate the major version of the TPM. This MUST be 0x01
BYTE	Minor	This SHALL indicate the minor version of the TPM. This MAY be 0x01 or 0x02
UINT16	reqSize	This SHALL indicate the value for a sizeOfSelect field in the TPM_SELECTION structure

5.19 TPM_CMK_MIGAUTH

Start of informative comment

Structure to keep track of the CMK migration authorization

End of informative comment

Definition

```
typedef struct tdTPM_CMK_MIGAUTH{
  TPM_STRUCTURE_TAG tag;
  TPM_DIGEST msaDigest;
  TPM_DIGEST pubKeyDigest;
} TPM_CMK_MIGAUTH;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	Set to TPM_TAG_CMK_MIGAUTH
TPM_DIGEST	msaDigest	The digest of a TPM_MSA_COMPOSITE structure containing the migration authority public key and parameters.
TPM_DIGEST	pubKeyDigest	The hash of the associated public key

812 5.20 TPM_CMK_SIGTICKET

813 **Start of informative comment**

814 Structure to keep track of the CMK migration authorization

815 **End of informative comment**

816 Definition

```
817 typedef struct tdTPM_CMK_SIGTICKET{
818    TPM_STRUCTURE_TAG tag;
819    TPM_DIGEST verKeyDigest;
820    TPM_DIGEST signedData;
821 } TPM_CMK_SIGTICKET;
```

822 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	Set to TPM_TAG_CMK_SIGTICKET
TPM_DIGEST	verKeyDigest	The hash of a TPM_PUBKEY structure containing the public key and parameters of the key that can verify the ticket
TPM_DIGEST	signedData	The ticket data

5.21 TPM_CMK_MA_APPROVAL

Start of informative comment

Structure to keep track of the CMK migration authorization

End of informative comment

Definition

```
typedef struct tdTPM_CMK_MA_APPROVAL{
  TPM_STRUCTURE_TAG tag;
  TPM_DIGEST migrationAuthorityDigest;
} TPM_CMK_MA_APPROVAL;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	Set to TPM_TAG_CMK_MA_APPROVAL
TPM_DIGEST	migrationAuthorityDigest	The hash of a TPM_MSA_COMPOSITE structure containing the hash of one or more migration authority public keys and parameters.

833 6. TPM_TAG (Command and Response Tags)

834 **Start of informative comment**

835 These tags indicate to the TPM the construction of the command either as input or as
836 output. The AUTH indicates that there are one or more AuthData values that follow the
837 command parameters.

838 **End of informative comment**

Tag	Name	Description
0x00C1	TPM_TAG_RQU_COMMAND	A command with no authentication.
0x00C2	TPM_TAG_RQU_AUTH1_COMMAND	An authenticated command with one authentication handle
0x00C3	TPM_TAG_RQU_AUTH2_COMMAND	An authenticated command with two authentication handles
0x00C4	TPM_TAG_RSP_COMMAND	A response from a command with no authentication
0x00C5	TPM_TAG_RSP_AUTH1_COMMAND	An authenticated response with one authentication handle
0x00C6	TPM_TAG_RSP_AUTH2_COMMAND	An authenticated response with two authentication handles

7. Internal Data Held By TPM

Start of Informative comment

There are many flags and data fields that the TPM must manage to maintain the current state of the TPM. The areas under TPM control have different lifetimes. Some areas are permanent, some reset upon TPM_Startup(ST_CLEAR) and some reset upon TPM_Startup(ST_STATE).

Previously the data areas were not grouped exactly according to their reset capabilities. It has become necessary to properly group the areas into the three classifications.

Each field has defined mechanisms to allow the control of the field. The mechanism may require authorization or physical presence to properly authorize the management of the field.

End of informative comment

7.1 TPM_PERMANENT_FLAGS

Start of Informative comment

These flags maintain state information for the TPM. The values are not affected by any TPM_Startup command.

The TPM_SetCapability command indicating TPM_PF_READPUBEK can set readPubek either TRUE or FALSE. It has more capability than the deprecated TPM_DisablePubekRead, which can only set readPubek to FALSE.

If the optional TSC_PhysicalPresence command is not implemented, physicalPresenceHWEnable should be set by the TPM vendor.

If the TSC_PhysicalPresence command is implemented, physicalPresenceHWEnable and/or physicalPresenceCMDEnable should be set and physicalPresenceLifetimeLock should be set before the TPM platform is delivered to the user.

The FIPS indicator can be set by the manufacturer to indicate restrictions on TPM operation. It cannot be changed using a command.

The rationale for setting allowMaintenace to FALSE if a TPM_FieldUpgrade implements the maintenance commands is that the current owner might not realize that maintenance commands have appeared. Further, the TPM may have certified to a remote entity that maintenance is disabled, the TPM_FieldUpgrade should not change that security property.

Certain platform manufacturers might require a specific readSRKPub default value.

The flag history includes:

Rev 62 specLevel 1 errataRev 0: 15 BOOLs

Rev 85 specLevel 2 errataRev 0: 19 BOOLs

Added: nvLocked, readSRKPub, tpmEstablished, maintenanceDone

Rev 94 specLevel 2 errataRev 1: 19 BOOLs

Rev 103 specLevel 2 errataRev 2: 20 BOOLs

Added: disableFullDALogicInfo

End of informative comment

```
typedef struct tdTPM_PERMANENT_FLAGS{
  TPM_STRUCTURE_TAG tag;
  BOOL disable;
  BOOL ownership;
  BOOL deactivated;
  BOOL readPubek;
  BOOL disableOwnerClear;
  BOOL allowMaintenance;
  BOOL physicalPresenceLifetimeLock;
  BOOL physicalPresenceHWEnable;
  BOOL physicalPresenceCMDEnable;
  BOOL CEKPUsed;
  BOOL TPMpost;
  BOOL TPMpostLock;
```

```
    BOOL FIPS;
    BOOL operator;
    BOOL enableRevokeEK;
    BOOL nvLocked;
    BOOL readSRKPub;
    BOOL tpmEstablished;
    BOOL maintenanceDone;
    BOOL disableFullDALogicInfo;
} TPM_PERMANENT_FLAGS;
```

Parameters

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_PERMANENT_FLAGS	
BOOL	disable	The state of the disable flag. The default state is TRUE	TPM_PF_DISABLE
BOOL	ownership	The ability to install an owner. The default state is TRUE.	TPM_PF_OWNERSHIP
BOOL	deactivated	The state of the inactive flag. The default state is TRUE.	TPM_PF_DEACTIVATED
BOOL	readPubek	The ability to read the PUBEK without owner AuthData. The default state is TRUE.	TPM_PF_READPUBEK
BOOL	disableOwnerClear	Whether the owner authorized clear commands are active. The default state is FALSE.	TPM_PF_DISABLEOWNERCLEAR
BOOL	allowMaintenance	Whether the TPM Owner may create a maintenance archive. The default state is TRUE if maintenance is implemented, vendor specific if maintenance is not implemented.	TPM_PF_ALLOWMAINTENANCE
BOOL	physicalPresenceLifetimeLock	This bit can only be set to TRUE; it cannot be set to FALSE except during the manufacturing process. FALSE: The state of either physicalPresenceHWEnable or physicalPresenceCMDEnable MAY be changed. (DEFAULT) TRUE: The state of either physicalPresenceHWEnable or physicalPresenceCMDEnable MUST NOT be changed for the life of the TPM.	TPM_PF_PHYSICALPRESENCELIFETIMELOCK
BOOL	physicalPresenceHWEnable	FALSE: Disable the hardware signal indicating physical presence. (DEFAULT) TRUE: Enables the hardware signal indicating physical presence.	TPM_PF_PHYSICALPRESENCEHWENABLE
BOOL	physicalPresenceCMDEnable	FALSE: Disable the command indicating physical presence. (DEFAULT) TRUE: Enables the command indicating physical presence.	TPM_PF_PHYSICALPRESENCECMDENABLE
BOOL	CEKPUsed	TRUE: The PRIVEK and PUBEK were created using TPM_CreateEndorsementKeyPair. FALSE: The PRIVEK and PUBEK were created using a manufacturer's process. NOTE: This flag has no default value as the key pair MUST be created by one or the other mechanism.	TPM_PF_CEKPUSED
BOOL	TPMpost	The meaning of this bit clarified in rev87. While actual use does not match the name, for backwards compatibility there is no change to the name. TRUE: After TPM_Startup, if there is a call to	TPM_PF_TPMPOST

Type	Name	Description	Flag Name
		TPM_ContinueSelfTest the TPM MUST execute the actions of TPM_SelfTestFull FALSE: After TPM_Startup, if there is a call to TPM_ContinueSelfTest the TPM MUST execute the actions of TPM_ContinueSelfTest If the TPM supports the implicit invocation of TPM_ContinueSelftTest upon the use of an untested resource, the TPM MUST use the TPMPost flag to execute the actions of either TPM_ContinueSelfTest or TPM_SelfTestFull The TPM manufacturer sets this bit during TPM manufacturing and the bit is unchangeable after shipping the TPM The default state is FALSE	
BOOL	TPMpostLock	With the clarification of TPMPost TPMpostLock is now unnecessary. This flag is now deprecated	TPM_PF_TPMPOSTLOCK
BOOL	FIPS	TRUE: This TPM operates in FIPS mode FALSE: This TPM does NOT operate in FIPS mode	TPM_PF_FIPS
BOOL	operator	TRUE: The operator AuthData value is valid FALSE: the operator AuthData value is not set (DEFAULT)	TPM_PF_OPERATOR
BOOL	enableRevokeEK	TRUE: The TPM_RevokeTrust command is active FALSE: the TPM RevokeTrust command is disabled	TPM_PF_ENABLEREVOKEEK
BOOL	nvLocked	TRUE: All NV area authorization checks are active FALSE: No NV area checks are performed, except for maxNVWrites. FALSE is the default value	TPM_PF_NV_LOCKED
BOOL	readSRKPub	TRUE: GetPubKey will return the SRK pub key FALSE: GetPubKey will not return the SRK pub key Default SHOULD be FALSE. See the informative.	TPM_PF_READSRKPUB
BOOL	tpmEstablished	TRUE: TPM_HASH_START has been executed at some time FALSE: TPM_HASH_START has not been executed at any time Default is FALSE. Reset to FALSE using TSC_ResetEstablishmentBit	TPM_PF_TPMESTABLISHED
BOOL	maintenanceDone	TRUE: A maintenance archive has been created for the current SRK	TPM_PF_MAINTENANCEDONE
BOOL	disableFullDALogicInfo	TRUE: The full dictionary attack TPM_GetCapability info is deactivated. The returned structure is TPM_DA_INFO_LIMITED. FALSE: The full dictionary attack TPM_GetCapability info is activated. The returned structure is TPM_DA_INFO. Default is FALSE.	TPM_PF_DISABLEFULLDALOGICINFO

902**Description**

903These values are permanent in the TPM and MUST not change upon execution of 904TPM_Startup(any) command.

905**Actions**

9061. If disable is TRUE the following commands will execute with their normal protections

907 a. The Avail Disabled column in the ordinal table indicates which commands can and
908 cannot execute

909 b. If the command is not available the TPM MUST return TPM_DISABLED upon any
910 attempt to execute the ordinal

911 c. TSC_PhysicalPresence can execute when the TPM is disabled

912 d. A disabled TPM never prevents the extend capabilities from operating. This is
913 necessary in order to ensure that the records of sequences of integrity metrics in a
914 TPM are always up-to-date. It is irrelevant whether an inactive TPM prevents the
915 extend capabilities from operating, because PCR values cannot be used until the
916 platform is rebooted, at which point existing PCR values are discarded

9172. If ownership has the value of FALSE, then any attempt to install an owner fails with the
918 error value TPM_INSTALL_DISABLED.

9193. If deactivated is TRUE

920 a. This flag does not directly cause capabilities to return the error code
921 TPM_DEACTIVATED.

922 b. TPM_Startup uses this flag to set the state of TPM_STCLEAR_FLAGS -> deactivated
923 when the TPM is booted in the state stType==TPM_ST_CLEAR. Only
924 TPM_STCLEAR_FLAGS -> deactivated determines whether capabilities will return the
925 error code TPM_DEACTIVATED.

926 c. A change in TPM_PERMANENT_FLAGS -> deactivated therefore has no effect on
927 whether capabilities will return the error code TPM_DEACTIVATED until the next
928 execution of TPM_Startup(ST_CLEAR)

9294. If readPubek is TRUE then the TPM_ReadPubek will return the PUBEK, if FALSE the
930 command will return TPM_DISABLED_CMD.

9315. If disableOwnerClear is TRUE then TPM_OwnerClear will return
932 TPM_CLEAR_DISABLED, if false the commands will execute.

9336. The physicalPresenceHWEnable and physicalPresenceCMDEnable flags MUST mask
934 their respective signals before further processing. The hardware signal, if enabled by the
935 physicalPresenceHWEnable flag, MUST be logically ORed with the PhysicalPresence flag,
936 if enabled, to obtain the final physical presence value used to allow or disallow local
937 commands.

9387. If a TPM_FieldUpgrade adds previously unimplemented maintenance commands and the
939 SRK remains valid, allowMaintanance MUST be set to FALSE.

940 7.1.1 Flag Restrictions

Flag SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_PF_DISABLE	Y	Owner authorization or physical presence	TPM_OwnerSetDisable TPM_PhysicalEnable TPM_PhysicalDisable
+2 TPM_PF_OWNERSHIP	Y	No authorization. No ownerinstalled. Physical presence asserted Not available when TPM deactivated or disabled	TPM_SetOwnerInstall
+3 TPM_PF_DEACTIVATED	Y	No authorization, physical presence assertion Not available when TPM disabled	TPM_PhysicalSetDeactivated
+4 TPM_PF_READPUBEK	Y	Owner authorization. Not available when TPM deactivated or disabled	
+5 TPM_PF_DISABLEOWNERCLEAR	Y	Owner authorization. Can only set to TRUE. After being set only ForceClear resets back to FALSE. Not available when TPM deactivated or disabled	TPM_DisableOwnerClear
+6 TPM_PF_ALLOWMAINTENANCE	Y	Owner authorization. Can only set to FALSE, TRUE invalid value. After being set only changing TPM owner resets back to TRUE Not available when TPM deactivated or disabled	TPM_KillMaintenanceFeature
+7 TPM_PF_PHYSICALPRESENCELIFETIMELOCK	N		
+8 TPM_PF_PHYSICALPRESENCEHWENABLE	N		
+9 TPM_PF_PHYSICALPRESENCECMDENABLE	N		
+10 TPM_PF_CEKPUSED	N		
+11 TPM_PF_TPMPOST	N		
+12 TPM_PF_TPMPOSTLOCK	N		
+13 TPM_PF_FIPS	N		
+14 TPM_PF_OPERATOR	N		
+15 TPM_PF_ENABLEREVOKEEK	N		
+16 TPM_PF_NV_LOCKED	N		
+17 TPM_PF_READSRKPUB	Y	Owner Authorization Not available when TPM deactivated or disabled	TPM_SetCapability
+18 TPM_PF_TPMESTABLISHED	Y	Locality 3 or locality 4. Can only set to FALSE.	TSC_ResetEstablishmentBit
+19 TPM_PF_MAINTENANCEDONE	N		
+20 TPM_PF_DISABLEFULLDALOGICINFO	Y	Owner Authorization	TPM_SetCapability

7.2 TPM_STCLEAR_FLAGS

Start of Informative comment

These flags maintain state that is reset on each TPM_Startup(ST_CLEAR) command. The values are not affected by TPM_Startup(ST_STATE) commands.

End of informative comment

```
#define TPM_MAX_FAMILY 8

typedef struct tdTPM_STCLEAR_FLAGS{
   TPM_STRUCTURE_TAG tag;
   BOOL deactivated;
   BOOL disableForceClear;
   BOOL physicalPresence;
   BOOL physicalPresenceLock;
   BOOL bGlobalLock;
} TPM_STCLEAR_FLAGS;
```

Parameters

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_STCLEAR_FLAGS	
BOOL	deactivated	Prevents the operation of most capabilities. There is no default state. It is initialized by TPM_Startup to the same value as TPM_PERMANENT_FLAGS -> deactivated or a set value depending on the type of TPM_Startup. TPM_SetTempDeactivated sets it to TRUE.	TPM_SF_DEACTIVATED
BOOL	disableForceClear	Prevents the operation of TPM_ForceClear when TRUE. The default state is FALSE. TPM_DisableForceClear sets it to TRUE.	TPM_SF_DISABLEFORCECLEAR
BOOL	physicalPresence	Command assertion of physical presence. The default state is FALSE. This flag is affected by the TSC_PhysicalPresence command but not by the hardware signal.	TPM_SF_PHYSICALPRESENCE
BOOL	physicalPresenceLock	Indicates whether changes to the TPM_STCLEAR_FLAGS -> physicalPresence flag are permitted. TPM_Startup(ST_CLEAR) sets PhysicalPresenceLock to its default state of FALSE (allow changes to the physicalPresence flag). When TRUE, the physicalPresence flag is FALSE. TSC_PhysicalPresence can change the state of physicalPresenceLock.	TPM_SF_PHYSICALPRESENCELOCK
BOOL	bGlobalLock	Set to FALSE on each TPM_Startup(ST_CLEAR). Set to TRUE when a write to NV_Index =0 is successful	TPM_SF_BGLOBALLOCK

Description

1. These values MUST reset upon execution of TPM_Startup(ST_CLEAR).
2. These values MUST NOT reset upon execution of TPM_Startup(ST_STATE).
3. Upon execution of TPM_Startup(ST_DEACTIVATED), all values must be reset except the 'deactivated' flag.

Actions

1. If deactivated is TRUE the following commands SHALL execute with their normal protections
   a. The Avail Deactivated column in the ordinal table indicates which commands can and cannot execute
   b. If the command is not available the TPM MUST return TPM_DEACTIVATED upon any attempt to execute the ordinal
   c. TSC_PhysicalPresence can execute when deactivated
   d. TPM_Extend and TPM_SHA1CompleteExtend MAY execute with their normal protections
2. If disableForceClear is TRUE then the TPM_ForceClear command returns TPM_CLEAR_DISABLED, if FALSE then the command will execute.
3. If physicalPresence is TRUE, the Owner physical presence is proven.
4. If physicalPresenceLock is TRUE, the physicalPresence flag is FALSE. If physicalPresenceLock is FALSE, TSC_PhysicalPresence can set or clear the physicalPresence flag.

978**7.2.1 Flag Restrictions**

Flag SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_SF_DEACTIVATED	N		
+2 TPM_SF_DISABLEFORCECLEAR	Y	Not available when TPM deactivated or disabled. Can only set to TRUE.	TPM_DisableForceClear
+3 TPM_SF_PHYSICALPRESENCE	N		
+4 TPM_SF_PHYSICALPRESENCELOCK	N		
+5 TPM_SF_BGLOBALLOCK	N		

979 7.3 TPM_STANY_FLAGS

980 **Start of Informative comment**

981 These flags reset on any TPM_Startup command.

982 postInitialise indicates only that TPM_Startup has run, not that it was successful.

983 TOSPresent indicates the presence of a Trusted Operating System (TOS) that was
984 established using the TPM_HASH_START command in the TPM Interface.

985 **End of informative comment**

```
986 typedef struct tdTPM_STANY_FLAGS{
987    TPM_STRUCTURE_TAG tag;
988    BOOL postInitialise;
989    TPM_MODIFIER_INDICATOR localityModifier;
990    BOOL transportExclusive;
991    BOOL TOSPresent;
992 } TPM_STANY_FLAGS;
```

993 Parameters

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_STANY_FLAGS	
BOOL	postInitialise	Prevents the operation of most capabilities. There is no default state. It is initialized by TPM_Init to TRUE. TPM_Startup sets it to FALSE.	TPM_AF_POSTINITIALISE
TPM_MODIFIER_INDICATOR	localityModifier	This SHALL indicate for each command the presence of a locality modifier for the command. It MUST be always ensured that the value during usage reflects the currently active locality.	TPM_AF_LOCALITYMODIFIER
BOOL	transportExclusive	Defaults to FALSE. TRUE when there is an exclusive transport session active. Execution of ANY command other than TPM_ExecuteTransport targeting the exclusive transport session MUST invalidate the exclusive transport session.	TPM_AF_TRANSPORTEXCLUSIVE
BOOL	TOSPresent	Defaults to FALSE Set to TRUE on TPM_HASH_START set to FALSE using setCapability	TPM_AF_TOSPRESENT

994 Description

995 This structure MUST reset on TPM_Startup(any)

996 Actions

9971. If postInitialise is TRUE, TPM_Startup SHALL execute as normal

998 a. All other commands SHALL return TPM_INVALID_POSTINIT

9992. localityModifier is set upon receipt of each command to the TPM. The localityModifier
1000 MUST be cleared when the command execution response is read

10013. If transportExclusive is TRUE

1002 a. If a command invalidates the exclusive transport session, the command MUST still
1003 execute.

1004 b. If TPM_EstablishTransport specifies an exclusive transport session, the existing
1005 session is invalidated, a new session is created, and transportExclusive remains
1006 TRUE.

1007 7.3.1 Flag Restrictions

Flag SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_AF_POSTINITIALISE	N		
+2 TPM_AF_LOCALITYMODIFIER	N		
+3 TPM_AF_TRANSPORTEXCLUSIVE	N		
+4 TPM_AF_TOSPRESENT	Y	Locality 3 or 4, can only set to FALSE Not available when TPM deactivated or disabled	TPM_SetCapability

1008 7.4 TPM_PERMANENT_DATA

1009**Start of Informative comment**

1010This is an informative structure and not normative. It is purely for convenience of writing 1011the spec.

1012This structure contains the data fields that are permanently held in the TPM and not 1013affected by TPM_Startup(any).

1014Many of these fields contain highly confidential and privacy sensitive material. The TPM 1015must maintain the protections around these fields.

1016**End of informative comment**

1017 Definition

```
1018#define TPM_MIN_COUNTERS 4 // the minimum number of counters is 4
1019#define TPM_DELEGATE_KEY TPM_KEY
1020#define TPM_NUM_PCR 16
1021#define TPM_MAX_NV_WRITE_NOOWNER 64
1022
1023typedef struct tdTPM_PERMANENT_DATA{
1024   TPM_STRUCTURE_TAG       tag;
1025   BYTE                    revMajor;
1026   BYTE                    revMinor;
1027   TPM_SECRET              tpmProof;
1028   TPM_NONCE               ekReset;
1029   TPM_SECRET              ownerAuth;
1030   TPM_SECRET              operatorAuth;
1031   TPM_DIRVALUE            authDIR[1];
1032   TPM_PUBKEY              manuMaintPub;
1033   TPM_KEY                 endorsementKey;
1034   TPM_KEY                 srk;
1035   TPM_KEY                 contextKey;
1036   TPM_KEY                 delegateKey;
1037   TPM_COUNTER_VALUE       auditMonotonicCounter;
1038   TPM_COUNTER_VALUE       monotonicCounter[TPM_MIN_COUNTERS];
1039   TPM_PCR_ATTRIBUTES      pcrAttrib[TPM_NUM_PCR];
1040   BYTE[]                  ordinalAuditStatus[];
1041   BYTE[]                  rngState;
1042   TPM_FAMILY_TABLE        familyTable;
1043   TPM_DELEGATE_TABLE      delegateTable;
1044   UINT32                  lastFamilyID;
1045   UINT32                  noOwnerNVWrite;
1046   TPM_CMK_DELEGATE        restrictDelegate;
1047   TPM_DAA_TPM_SEED        tpmDAASeed;
1048   TPM_NONCE               daaProof;
1049   TPM_KEY                 daaBlobKey;
1050}TPM_PERMANENT_DATA;
```

Parameters

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_PERMANENT_DATA	
BYTE	revMajor	This is the TPM major revision indicator. This SHALL be set by the TPME, only. The default value is manufacturer-specific.	TPM_PD_REVMAJOR
BYTE	revMinor	This is the TPM minor revision indicator. This SHALL be set by the TPME, only. The default value is manufacturer-specific.	TPM_PD_REVMINOR
TPM_SECRET	tpmProof	This is a random number that each TPM maintains to validate blobs in the SEAL and other processes. The default value is manufacturer-specific.	TPM_PD_TPMPROOF
TPM_SECRET	ownerAuth	This is the TPM-Owner's AuthData data. The default value is manufacturer-specific.	TPM_PD_OWNERAUTH
TPM_SECRET	operatorAuth	The value that allows the execution of the TPM_SetTempDeactivated command	TPM_PD_OPERATORAUTH
TPM_PUBKEY	manuMaintPub	This is the manufacturer's public key to use in the maintenance operations. The default value is manufacturer-specific.	TPM_PD_MANUMAINTPUB
TPM_KEY	endorsementKey	This is the TPM's endorsement key pair.	TPM_PD_ENDORSEMENTKEY
TPM_KEY	srk	This is the TPM's StorageRootKey.	TPM_PD_SRK
TPM_KEY	delegateKey	This key encrypts delegate rows that are stored outside the TPM. The key MAY be symmetric or asymmetric. The key size for the algorithm SHOULD be equivalent to 128-bit AES key. The TPM MAY set this value once or allow for changes to this value. This key MUST NOT be the EK or SRK To save space this key MAY be the same key that performs context blob encryption. If an asymmetric algorithm is in use for this key the public portion of the key MUST never be revealed by the TPM. This value MUST be reset when the TPM Owner changes. The value MUST be invalidated with the actions of TPM_OwnerClear. The value MUST be set on TPM_TakeOwnership. The contextKey and delegateKey MAY be the same value.	TPM_PD_DELEGATEKEY
TPM_KEY	contextKey	This is the key in use to perform context saves. The key may be symmetric or asymmetric. The key size is predicated by the algorithm in use. This value MUST be reset when the TPM Owner changes. This key MUST NOT be a copy of the EK or SRK. The contextKey and delegateKey MAY be the same value.	TPM_PD_CONTEXTKEY
TPM_COUNTER_VALUE	auditMonotonicCounter	This SHALL be the audit monotonic counter for the TPM. This value starts at 0 and increments according to the rules of auditing. The label SHALL be fixed at 4 bytes of 0x00.	TPM_PD_AUDITMONOTONICCOUNTER
TPM_COUNTER_VALUE	monotonicCounter	This SHALL be the monotonic counters for the TPM. The individual counters start and increment according to the rules of monotonic counters.	TPM_PD_MONOTONICCOUNTER
TPM_PCR_ATTRIBUTES	pcrAttrib	The attributes for all of the PCR registers supported by the TPM.	TPM_PD_PCRATTRIB
BYTE[]	ordinalAuditStatus	Table indicating which ordinals are being audited.	TPM_PD_ORDINALAUDITSTATUS
TPM_DIRVALUE	authDIR	The array of TPM Owner authorized DIR. Points to the same location as the NV index value.	TPM_PD_AUTHDIR
BYTE[]	rngState	State information describing the random number generator.	TPM_PD_RNGSTATE
TPM_FAMILY_TABLE	familyTable	The family table in use for delegations	TPM_PD_FAMILYTABLE
TPM_DELEGATE_TABLE	delegateTable	The delegate table	TPM_DELEGATETABLE
TPM_NONCE	ekReset	Nonce held by TPM to validate TPM_RevokeTrust. This value is set as the next 20 bytes from the TPM RNG when the EK is set	TPM_PD_EKRESET

7.4.1 Structure Member Restrictions

Structure Member SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_PD_REVMAJOR	N		
+2 TPM_PD_REVMINOR	N		
+3 TPM_PD_TPMPROOF	N		
+4 TPM_PD_OWNERAUTH	N		
+5 TPM_PD_OPERATORAUTH	N		
+6 TPM_PD_MANUMAINTPUB	N		
+7 TPM_PD_ENDORSEMENTKEY	N		
+8 TPM_PD_SRK	N		
+9 TPM_PD_DELEGATEKEY	N		
+10 TPM_PD_CONTEXTKEY	N		
+11 TPM_PD_AUDITMONOTONICCOUNTER	N		
+12 TPM_PD_MONOTONICCOUNTER	N		
+13 TPM_PD_PCRATTRIB	N		
+14 TPM_PD_ORDINALAUDITSTATUS	N		
+15 TPM_PD_AUTHDIR	N		
+16 TPM_PD_RNGSTATE	N		
+17 TPM_PD_FAMILYTABLE	N		
+18 TPM_DELEGATETABLE	N		
+19 TPM_PD_EKRESET	N		
+20 unused	N		
+21 TPM_PD_LASTFAMILYID	N		
+22 TPM_PD_NOOWNERNVWRITE	N		
+23 TPM_PD_RESTRICTDELEGATE	Y	Owner authorization. Not available when TPM deactivated or disabled.	TPM_CMK_SetRestrictions
+24 TPM_PD_TPMDAASEED	N		
+25 TPM_PD_DAAPROOF	Y	Owner authorization.	

Description

1. `TPM_PD_DAAPROOF` This capability has no value. When specified by TPM_SetCapability, a new daaProof, tpmDAASeed, and daaBlobKey are generated.

1058 7.5 TPM_STCLEAR_DATA

1059 **Start of Informative comment**

1060 This is an informative structure and not normative. It is purely for convenience of writing
1061 the spec.

1062 Most of the data in this structure resets on TPM_Startup(ST_CLEAR). A TPM may
1063 implement rules that provide longer-term persistence for the data. The TPM reflects how it
1064 handles the data in various TPM_GetCapability fields including startup effects.

1065 **End of informative comment**

1066 Definition

```
1067 typedef struct tdTPM_STCLEAR_DATA{
1068    TPM_STRUCTURE_TAG  tag;
1069    TPM_NONCE          contextNonceKey;
1070    TPM_COUNT_ID       countID;
1071    UINT32             ownerReference;
1072    BOOL               disableResetLock;
1073     TPM_PCRVALUE      PCR[TPM_NUM_PCR];
1074    UINT32             deferredPhysicalPresence;
1075
1076 }TPM_STCLEAR_DATA;
```

1077 Parameters

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_STCLEAR_DATA	
TPM_NONCE	contextNonceKey	This is the nonce in use to properly identify saved key context blobs This SHALL be set to all zeros on each TPM_Startup (ST_Clear).	TPM_SD_CONTEXTNONCEKEY
TPM_COUNT_ID	countID	This is the handle for the current monotonic counter. This SHALL be set to zero on each TPM_Startup(ST_Clear).	TPM_SD_COUNTID
UINT32	ownerReference	Points to where to obtain the owner secret in OIAP and OSAP commands. This allows a TSS to manage 1.1 applications on a 1.2 TPM where delegation is in operation. Default value is TPM_KH_OWNER.	TPM_SD_OWNERREFERENCE
BOOL	disableResetLock	Disables TPM_ResetLockValue upon authorization failure. The value remains TRUE for the timeout period. Default is FALSE. The value is in the STCLEAR_DATA structure as the implementation of this flag is TPM vendor specific.	TPM_SD_DISABLERESETLOCK
TPM_PCRVALUE	PCR	Platform configuration registers	TPM_SD_PCR
UINT32	deferredPhysicalPresence	The value can save the assertion of physicalPresence. Individual bits indicate to its ordinal that physicalPresence was previously asserted when the software state is such that it can no longer be asserted. Set to zero on each TPM_Startup(ST_Clear).	TPM_SD_DEFERREDPHYSICALPRESENCE

7.5.1 Structure Member Restrictions

Structure Member SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_SD_CONTEXTNONCEKEY	N		
+2 TPM_SD_COUNTID	N		
+3 TPM_SD_OWNERREFERENCE	N		
+4 TPM_SD_DISABLERESETLOCK	N		
+5 TPM_SD_PCR	N		
+6 TPM_SD_DEFERREDPHYSICALPRESENCE	Y	Can only set to TRUE if PhysicalPresence is asserted. Can set to FALSE at any time.	TPM_SetCapability

7.5.2 Deferred Physical Presence Bit Map

Start of Informative comment

These bits of deferredPhysicalPresence are used in the Actions of the listed ordinals.

Bits are set and cleared using TPM_SetCapability. When physicalPresence is asserted, individual bits can be set or cleared. When physicalPresence is not asserted, individual bits can only be cleared, not set, but bits already set can remain set. Attempting to set a bit when physical presence is not asserted is an error.

End of informative comment

Description

1. If physical presence is not asserted
   a. If TPM_SetCapability -> setValue has a bit set that is not already set in TPM_STCLEAR_DATA -> deferredPhysicalPresence, return TPM_BAD_PRESENCE.
2. Set TPM_STCLEAR_DATA -> deferredPhysicalPresence to TPM_SetCapability -> setValue.

Bit Position	Name	Ordinals Affected
31-1	Unused	Unused
0	unownedFieldUpgrade	TPM_FieldUpgrade

7.6 TPM_STANY_DATA

Start of Informative comment

This is an informative structure and not normative. It is purely for convenience of writing the spec.

Most of the data in this structure resets on TPM_Startup(ST_STATE). A TPM may implement rules that provide longer-term persistence for the data. The TPM reflects how it handles the data in various TPM_GetCapability fields including startup effects.

End of informative comment

Definition

```
#define TPM_MIN_SESSIONS 3
#define TPM_MIN_SESSION_LIST 16

typedef struct tdTPM_SESSION_DATA{
… // vendor specific
} TPM_SESSION_DATA;

typedef struct tdTPM_STANY_DATA{
   TPM_STRUCTURE_TAG  tag;
   TPM_NONCE          contextNonceSession;
   TPM_DIGEST         auditDigest ;
   TPM_CURRENT_TICKS  currentTicks;
   UINT32             contextCount;
   UINT32             contextList[TPM_MIN_SESSION_LIST];
   TPM_SESSION_DATA   sessions[TPM_MIN_SESSIONS];
}TPM_STANY_DATA;
```

Parameters of STANY_DATA

Type	Name	Description	Flag Name
TPM_STRUCTURE_TAG	tag	TPM_TAG_STANY_DATA	
TPM_NONCE	contextNonceSession	This is the nonce in use to properly identify saved session context blobs. This MUST be set to all zeros on each TPM_Startup (ST_Clear). The nonce MAY be set to all zeros on TPM_Startup(any).	TPM_AD_CONTEXTNONCESESSION
TPM_DIGEST	auditDigest	This is the extended value that is the audit log. This SHALL be set to all zeros at the start of each audit session.	TPM_AD_AUDITDIGEST
TPM_CURRENT_TICKS	currentTicks	This is the current tick counter. This is reset to 0 according to the rules when the TPM can tick. See See Part 1 'Design Section for Time Stamping' for details.	TPM_AD_CURRENTTICKS
UINT32	contextCount	This is the counter to avoid session context blob replay attacks. This MUST be set to 0 on each TPM_Startup (ST_Clear). The value MAY be set to 0 on TPM_Startup (any).	TPM_AD_CONTEXTCOUNT
UINT32	contextList	This is the list of outstanding session blobs.	TPM_AD_CONTEXTLIST

Type	Name	Description	Flag Name
		All elements of this array MUST be set to 0 on each TPM_Startup (ST_Clear). The values MAY be set to 0 on TPM_Startup (any). TPM_MIN_SESSION_LIST MUST be 16 or greater.	
TPM_SESSION_DATA	sessions	List of current sessions. Sessions can be OSAP, OIAP, DSAP and Transport	TPM_AD_SESSIONS

1119**Descriptions**

11201. The group of contextNonceSession, contextCount, contextList MUST reset at the same 1121 time.

11222. The contextList MUST keep track of UINT32 values. There is NO requirement that the 1123 actual memory be 32 bits

11243. contextList MUST support a minimum of 16 entries, it MAY support more.

11254. The TPM MAY restrict the absolute difference between contextList entries

1126 a. For instance if the TPM enforced distance was 10

1127 i. Entries 8 and 15 would be valid

1128 ii. Entries 8 and 28 would be invalid

1129 b. The minimum distance that the TPM MUST support is 2^16, the TPM MAY support 1130 larger distances

1131**7.6.1 Structure Member Restrictions**

Structure Member SubCap number 0x00000000 +	Set	Set restrictions	Actions from
+1 TPM_AD_CONTEXTNONCESESSION	N		
+2 TPM_AD_AUDITDIGEST	N		
+3 TPM_AD_CURRENTTICKS	N		
+4 TPM_AD_CONTEXTCOUNT	N		
+5 TPM_AD_CONTEXTLIST	N		
+6 TPM_AD_SESSIONS	N		

1132 8. PCR Structures

1133 **Start of informative comment**

1134 The PCR structures expose the information in PCR register, allow for selection of PCR
1135 register or registers in the SEAL operation and define what information is held in the PCR
1136 register.

1137 These structures are in use during the wrapping of keys and sealing of blobs.

1138 **End of informative comment**

8.1 TPM_PCR_SELECTION

Start of informative comment

This structure provides a standard method of specifying a list of PCR registers.

Design points

1. The user needs to be able to specify the null set of PCR. The mask in pcrSelect indicates if a PCR is active or not. Having the mask be a null value that specifies no selected PCR is valid. This is useful when an entity does not require checking of digestAtRelease but requires checking of localityAtRelease.

2. The TPM must support a sizeOfSelect that indicates the minimum number of PCR on the platform. For a 1.2 PC TPM with 24 PCR this value would be 3.

3. The TPM may support additional PCR over the platform minimum. When supporting additional PCR the TPM must support a sizeOfSelect that can indicate the use of an individual PCR.

4. The TPM may support sizeOfSelect that reflects PCR use other than the maximum. For instance, a PC TPM that supported 48 PCR would require support for a sizeOfSelect of 6 and a sizeOfSelect of 3 (for the 24 required PCR). The TPM could support sizes of 4 and 5.

5. It is desirable for the TPM to support fixed size structures. Nothing in these rules prevents a TPM from only supporting a known set of sizeOfSelect structures.

Odd bit ordering

To the new reader the ordering of the PCR may seem strange. It is. However, the original TPM vendors all interpreted the 1.0 specification to indicate the ordering as it is. The scheme works and is understandable, so to avoid any backwards compatibility no change to the ordering occurs in 1.2. The TPM vendor's interpretation of the 1.0 specification is the start to the comment that there are no ambiguities in the specification just context sensitive interpretations.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_SELECTION {
  UINT16 sizeOfSelect;
  [size_is(sizeOfSelect)] BYTE* pcrSelect;
  } TPM_PCR_SELECTION;
```

Parameters

Type	Name	Description
UINT16	sizeOfSelect	The size in bytes of the pcrSelect structure
BYTE*	pcrSelect	This SHALL be a bit map that indicates if a PCR is active or not

Description

1. PCR selection occurs modulo 8. The minimum granularity for a PCR selection is 8. The specification of registers MUST occur in banks of 8.

2. pcrSelect is a contiguous bit map that shows which PCR are selected. Each byte represents 8 PCR. For each byte, the individual bits represent a corresponding PCR. Refer to the figures below for the mapping of an individual bit to a PCR within a byte. All pcrSelect bytes follow the same mapping.
   a. For example, byte 0 indicates PCR 0-7, byte 1 8-15 and so on.
   b. For example, if the TPM supported 48 PCR, to select PCR 0 and 47, the sizeOfSelect would be 6 and only two bits would be set to a 1. The remaining bits of pcrSelect would be 0.

```
Byte 0
+-+-+-+-+-+-+-+-+
|7|6|5|4|3|2|1|0|
+-+-+-+-+-+-+-+-+

      Byte 1
+-+-+-+-+-+-+-+-+
|F|E|D|C|B|A|9|8|
+-+-+-+-+-+-+-+-+

      Byte 2
+--+--+--+--+--+--+--+--+
|17|16|15|14|13|12|11|10|
+--+--+--+--+--+--+--+--+
```

3. When an individual bit is 1, the indicated PCR is selected. If 0, the PCR is not selected.
   a. For example, to select PCR 0, pcrSelect would be 00000001
   b. For example, to select PCR 7, pcrSelect would by 10000000
   c. For example, to select PCR 7 and 0, pcrSelect would be 10000001
4. If TPM_PCR_SELECTION.pcrSelect is all 0's
   a. For digestAtCreation, the TPM MUST set TPM_COMPOSITE_HASH to be all 0's.
   b. The TPM MUST not check digestAtRelease.
5. Else
   a. The process creates a TPM_PCR_COMPOSITE structure from the TPM_PCR_SELECTION structure and the PCR values to be hashed. If constructed by the TPM, the values MUST come from the current PCR registers indicated by the PCR indices in the TPM_PCR_SELECTION structure.
6. The TPM MUST support sizeOfSelect values as specified in the platform specific specification
7. The TPM MAY return an error if the sizeOfSelect is a value greater than one that represents the number of PCR on the TPM
8. The TPM MUST return an error if sizeOfSelect is 0

8.2 TPM_PCR_COMPOSITE

Start of informative comment

The composite structure provides the index and value of the PCR register to be used when creating the value that SEALS an entity to the composite.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_COMPOSITE {
  TPM_PCR_SELECTION select;
  UINT32 valueSize;
  [size_is(valueSize)] TPM_PCRVALUE pcrValue[];
} TPM_PCR_COMPOSITE;
```

Parameters

Type	Name	Description
TPM_PCR_SELECTION	select	This SHALL be the indication of which PCR values are active
UINT32	valueSize	This SHALL be the size of the pcrValue field (not the number of PCR's)
TPM_PCRVALUE	pcrValue[]	This SHALL be an array of TPM_PCRVALUE structures. The values come in the order specified by the select parameter and are concatenated into a single blob

8.3 TPM_PCR_INFO

Start of informative comment

The TPM_PCR_INFO structure contains the information related to the wrapping of a key or the sealing of data, to a set of PCRs.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_INFO{
  TPM_PCR_SELECTION pcrSelection;
  TPM_COMPOSITE_HASH digestAtRelease;
  TPM_COMPOSITE_HASH digestAtCreation;
} TPM_PCR_INFO;
```

Parameters

Type	Name	Description
TPM_PCR_SELECTION	pcrSelection	This SHALL be the selection of PCRs to which the data or key is bound.
TPM_COMPOSITE_HASH	digestAtRelease	This SHALL be the digest of the PCR indices and PCR values to verify when revealing Sealed Data or using a key that was wrapped to PCRs.
TPM_COMPOSITE_HASH	digestAtCreation	This SHALL be the composite digest value of the PCR values, at the time when the sealing is performed.

8.4 TPM_PCR_INFO_LONG

Start of informative comment

The TPM_PCR_INFO structure contains the information related to the wrapping of a key or the sealing of data, to a set of PCRs.

The LONG version includes information necessary to properly define the configuration that creates the blob using the PCR selection.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_INFO_LONG{
  TPM_STRUCTURE_TAG tag;
  TPM_LOCALITY_SELECTION localityAtCreation;
  TPM_LOCALITY_SELECTION localityAtRelease;
  TPM_PCR_SELECTION creationPCRSelection;
  TPM_PCR_SELECTION releasePCRSelection;
  TPM_COMPOSITE_HASH digestAtCreation;
  TPM_COMPOSITE_HASH digestAtRelease;
} TPM_PCR_INFO_LONG;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_PCR_INFO_LONG
TPM_LOCALITY_SELECTION	localityAtCreation	This SHALL be the locality modifier when the blob is created
TPM_LOCALITY_SELECTION	localityAtRelease	This SHALL be the locality modifier required to reveal Sealed Data or use a key that was wrapped to PCRs This value MUST not be zero (0).
TPM_PCR_SELECTION	creationPCRSelection	This SHALL be the selection of PCRs active when the blob is created
TPM_PCR_SELECTION	releasePCRSelection	This SHALL be the selection of PCRs to which the data or key is bound.
TPM_COMPOSITE_HASH	digestAtCreation	This SHALL be the composite digest value of the PCR values, when the blob is created
TPM_COMPOSITE_HASH	digestAtRelease	This SHALL be the digest of the PCR indices and PCR values to verify when revealing Sealed Data or using a key that was wrapped to PCRs.

8.5 TPM_PCR_INFO_SHORT

Start of informative comment

This structure is for defining a digest at release when the only information that is necessary is the release configuration.

This structure does not have a tag to keep the structure short. Software and the TPM need to evaluate the structures where the INFO_SHORT structure resides to avoid miss identifying the INFO_SHORT structure.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_INFO_SHORT{
  TPM_PCR_SELECTION pcrSelection;
  TPM_LOCALITY_SELECTION localityAtRelease;
  TPM_COMPOSITE_HASH digestAtRelease;
} TPM_PCR_INFO_SHORT;
```

Parameters

Type	Name	Description
TPM_PCR_SELECTION	pcrSelection	This SHALL be the selection of PCRs that specifies the digestAtRelease
TPM_LOCALITY_SELECTION	localityAtRelease	This SHALL be the locality modifier required to release the information. This value must not be zero (0).
TPM_COMPOSITE_HASH	digestAtRelease	This SHALL be the digest of the PCR indices and PCR values to verify when revealing auth data

8.6 TPM_LOCALITY_SELECTION

Start of informative comment

When used with localityAtCreation only one bit is set and it corresponds to the locality of the command creating the structure.

When used with localityAtRelease the bits indicate which localities CAN perform the release.

TPM_LOC_TWO would indicate that only locality 2 can perform the release

TPM_LOC_ONE || TPM_LOC_TWO would indicate that localities 1 or 2 could perform the release

TPM_LOC_FOUR || TPM_LOC_THREE would indicate that localities 3 or 4 could perform the release.

The TPM MAY treat a localityAtCreation value of 0 as an error. For interoperability, an externally generated localityAtCreation SHOULD contain a legal value.

End of informative comment

Definition

```
#define TPM_LOCALITY_SELECTION BYTE
```

Bit	Name	Description
7:5	Reserved	Must be 0
4	TPM_LOC_FOUR	Locality 4
3	TPM_LOC_THREE	Locality 3
2	TPM_LOC_TWO	Locality 2
1	TPM_LOC_ONE	Locality 1
0	TPM_LOC_ZERO	Locality 0. This is the same as the legacy interface.

1. The TPM MUST treat a localityAtRelease value of 0 as an error. The default value is 0x1F, which indicates that localities 0-4 have been selected.

8.7 PCR Attributes

Start of informative comment

Each PCR has attributes associated with it. These attributes allow each PCR to have different behavior. This specification defines the generic meaning of the attributes. For a specific platform, the actual setting of the attribute is a platform specific issue.

The attributes are values that are set during the manufacturing process of the TPM and platform and are not field settable or changeable values.

To accommodate debugging, PCR[16] for all platforms will have a certain set of attributes. The setting of these attributes is to allow for easy debugging. This means that values in PCR[16] provide no security information. It is anticipated that PCR[16] would be used by a developer during the development cycle. Developers are responsible for ensuring that a conflict between two programs does not invalidate the settings they are interested in.

The attributes are pcrReset, pcrResetLocal, pcrExtendLocal. Attributes can be set in any combination that is appropriate for the platform.

The pcrReset attribute allows the PCR to be reset at times other than TPM_Startup.

The pcrResetLocal attribute allows the PCR to be reset at times other than TPM_Startup. The reset is legal when the mapping of the command locality to PCR flags results in accept. See 8.8.1 for details.

The pcrExtendLocal attribute modifies the PCR such that the PCR can only be extended when the mapping of the command locality to PCR flags results in accept. See 8.8.1 for details.

End of informative comment

1. The PCR attributes MUST be set during manufacturing.
2. For a specific PCR register, the PCR attributes MUST match the requirements of the TCG platform specific specification that describes the platform.

8.8 TPM_PCR_ATTRIBUTES

Informative comment :

These attributes are available on a per PCR basis.

The TPM is not required to maintain this structure internally to the TPM.

When a challenger evaluates a PCR, an understanding of this structure is vital to the proper understanding of the platform configuration. As this structure is static for all platforms of the same type, the structure does not need to be reported with each quote.

This normative describes the default response to initialization or a reset. The actual response is platform specific. The platform specification has the final say on the PCR value after initialization or a reset.

End of informative comment

Definition

```
typedef struct tdTPM_PCR_ATTRIBUTES{
   BOOL pcrReset;
   TPM_LOCALITY_SELECTION pcrExtendLocal;
   TPM_LOCALITY_SELECTION pcrResetLocal;
} TPM_PCR_ATTRIBUTES;
```

Types of Persistent Data

Type	Name	Description
BOOL	pcrReset	A value of TRUE SHALL indicate that the PCR register can be reset using the TPM_PCR_Reset command. If pcrReset is: FALSE- Default value of the PCR MUST be 0x00..00 Reset on TPM_Startup(ST_Clear) only Saved by TPM_SaveState Can not be reset by TPM_PCR_Reset TRUE – Default value of the PCR MUST be 0xFF..FF. Reset on TPM_Startup(any) MUST not be part of any state stored by TPM_SaveState Can be reset by TPM_PCR_Reset When reset as part of HASH_START the starting value MUST be 0x00..00
TPM_LOCALITY_SELECTION	pcrResetLocal	An indication of which localities can reset the PCR
TPM_LOCALITY_SELECTION	pcrExtendLocal	An indication of which localities can perform extends on the PCR.

8.8.1 Comparing command locality to PCR flags

Start of informative comment

This is an informative section to show the details of how to check locality against the locality modifier received with a command. The operation works for any of reset, extend or use but for example this will use read.

Map L1 to TPM_STANY_FLAGS -> localityModifier

Map P1 to TPM_PERMANENT_DATA -> pcrAttrib->[selectedPCR].pcrExtendLocal

If, for the value L1, the corresponding bit is set in the bit map P1

return accept

else return reject

End of informative comment

8.9 Debug PCR register

Start of informative comment

There is a need to define a PCR that allows for debugging. The attributes of the debug register are such that it is easy to reset, but the register provides no measurement value that can not be spoofed. Production applications should not use the debug PCR for any SEAL or other operations. The anticipation is that the debug PCR is set and used by application developers during the application development cycle. Developers are responsible for ensuring that a conflict between two programs does not invalidate the settings they are interested in.

The specific register that is the debug PCR MUST be set by the platform specific specification.

End of informative comment

The attributes for the debug PCR SHALL be the following:

```
pcrReset = TRUE;
pcrResetLocal = 0x1f;
pcrExtendLocal = 0x1f;
pcrUseLocal = 0x1f;
```

These settings are to create a PCR register that developers can use to reset at any time during their development cycle.

The debug PCR does NOT need to be saved during TPM_SaveState

13658.10 Mapping PCR Structures

1366**Start of informative comment**

1367When moving information from one PCR structure type to another, i.e. TPM_PCR_INFO to
1368TPM_PCR_INFO_SHORT, the mapping between fields could be ambiguous. This section
1369describes how the various fields map and what the TPM must do when adding or losing
1370information.

1371**End of informative comment**

13721. Set IN to TPM_PCR_INFO
13732. Set IL to TPM_PCR_INFO_LONG
13743. Set IS to TPM_PCR_INFO_SHORT
13754. To set IS from IN
1376 a. Set IS -> pcrSelection to IN -> pcrSelection
1377 b. Set IS -> digestAtRelease to IN -> digestAtRelease
1378 c. Set IS -> localityAtRelease to 0x1F to indicate all localities are valid
1379 d. Ignore IN -> digestAtCreation
13805. To set IS from IL
1381 a. Set IS -> pcrSelection to IL -> releasePCRSelection
1382 b. Set IS -> localityAtRelease to IL -> localityAtRelease
1383 c. Set IS -> digestAtRelease to IL -> digestAtRelease
1384 d. Ignore all other IL values
13856. To set IL from IN
1386 a. Set IL -> localityAtCreation to 0x1F
1387 b. Set IL -> localityAtRelease to 0x1F
1388 c. Set IL -> creationPCRSelection to IN -> pcrSelection
1389 d. Set IL -> releasePCRSelection to IN -> pcrSelection
1390 e. Set IL -> digestAtCreation to IN -> digestAtCreation
1391 f. Set IL -> digestAtRelease to IN -> digestAtRelease
13927. To set IL from IS
1393 a. Set IL -> localityAtCreation to 0x1F
1394 b. Set IL -> localityAtRelease to IS localityAtRelease
1395 c. Set IL -> creationPCRSelection to all zeros
1396 d. Set IL -> releasePCRSelection to IS -> pcrSelection
1397 e. Set IL -> digestAtCreation to all zeros
1398 f. Set IL -> digestAtRelease to IS -> digestAtRelease

13998. To set IN from IS

1400 a. Set IN -> pcrSelection to IS -> pcrSelection

1401 b. Set IN -> digestAtRelease to IS -> digestAtRelease

1402 c. Set IN -> digestAtCreation to all zeros

14039. To set IN from IL

1404 a. Set IN -> pcrSelection to IL -> releasePCRSelection

1405 b. Set IN -> digestAtRelease to IL -> digestAtRelease

1406 c. If IL -> creationPCRSelection and IL -> localityAtCreation both match IL ->
1407 releasePCRSelection and IL –> localityAtRelease

1408 i. Set IN -> digestAtCreation to IL -> digestAtCreation

1409 d. Else

1410 i. Set IN -> digestAtCreation to all zeros

9. Storage Structures

9.1 TPM_STORED_DATA

Start of informative comment

The definition of this structure is necessary to ensure the enforcement of security properties.

This structure is in use by the TPM_Seal and TPM_Unseal commands to identify the PCR index and values that must be present to properly unseal the data.

This structure only provides 1.1 data store and uses TPM_PCR_INFO

End of informative comment

Definition

```
typedef struct tdTPM_STORED_DATA {
   TPM_STRUCT_VER ver;
   UINT32 sealInfoSize;
   [size_is(sealInfoSize)] BYTE* sealInfo;
   UINT32 encDataSize;
   [size_is(encDataSize)] BYTE* encData;
} TPM_STORED_DATA;
```

Parameters

Type	Name	Description
TPM_STRUCT_VER	ver	This MUST be 1.1.0.0
UINT32	sealInfoSize	Size of the sealInfo parameter
BYTE*	sealInfo	This SHALL be a structure of type TPM_PCR_INFO or a 0 length array if the data is not bound to PCRs.
UINT32	encDataSize	This SHALL be the size of the encData parameter
BYTE*	encData	This shall be an encrypted TPM_SEALED_DATA structure containing the confidential part of the data.

Descriptions

1. This structure is created during the TPM_Seal process. The confidential data is encrypted using a non-migratable key. When the TPM_Unseal decrypts this structure the TPM_Unseal uses the public information in the structure to validate the current configuration and release the decrypted data
2. When sealInfoSize is not 0 sealInfo MUST be TPM_PCR_INFO

TCG Published

9.2 TPM_STORED_DATA12

Start of informative comment

The definition of this structure is necessary to ensure the enforcement of security properties.

This structure is in use by the TPM_Seal and TPM_Unseal commands to identify the PCR index and values that must be present to properly unseal the data.

End of informative comment

Definition

```
typedef struct tdTPM_STORED_DATA12 {
   TPM_STRUCTURE_TAG tag;
   TPM_ENTITY_TYPE et;
   UINT32 sealInfoSize;
   [size_is(sealInfoSize)] BYTE* sealInfo;
   UINT32 encDataSize;
   [size_is(encDataSize)] BYTE* encData;
} TPM_STORED_DATA12;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_STORED_DATA12
TPM_ENTITY_TYPE	et	The type of blob
UINT32	sealInfoSize	Size of the sealInfo parameter
BYTE*	sealInfo	This SHALL be a structure of type TPM_PCR_INFO_LONG
UINT32	encDataSize	This SHALL be the size of the encData parameter
BYTE*	encData	This shall be an encrypted TPM_SEALED_DATA structure containing the confidential part of the data.

Descriptions

1. This structure is created during the TPM_Seal process. The confidential data is encrypted using a non-migratable key. When the TPM_Unseal decrypts this structure the TPM_Unseal uses the public information in the structure to validate the current configuration and release the decrypted data.

2. If sealInfoSize is not 0 then sealInfo MUST be TPM_PCR_INFO_LONG

9.3 TPM_SEALED_DATA

Start of informative comment

This structure contains confidential information related to sealed data, including the data itself.

End of informative comment

Definition

```
typedef struct tdTPM_SEALED_DATA {
   TPM_PAYLOAD_TYPE payload;
   TPM_SECRET authData;
   TPM_SECRET tpmProof;
   TPM_DIGEST storedDigest;
   UINT32 dataSize;
   [size_is(dataSize)] BYTE* data;
} TPM_SEALED_DATA;
```

Parameters

Type	Name	Description
TPM_PAYLOAD_TYPE	payload	This SHALL indicate the payload type of TPM_PT_SEAL
TPM_SECRET	authData	This SHALL be the AuthData data for this value
TPM_SECRET	tpmProof	This SHALL be a copy of TPM_PERMANENT_DATA -> tpmProof
TPM_DIGEST	storedDigest	This SHALL be a digest of the TPM_STORED_DATA structure, excluding the fields TPM_STORED_DATA -> encDataSize and TPM_STORED_DATA -> encData.
UINT32	dataSize	This SHALL be the size of the data parameter
BYTE*	data	This SHALL be the data to be sealed

Description

1. To tie the TPM_STORED_DATA structure to the TPM_SEALED_DATA structure this structure contains a digest of the containing TPM_STORED_DATA structure.
2. The digest calculation does not include the encDataSize and encData parameters.

9.4 TPM_SYMMETRIC_KEY

Start of informative comment

This structure describes a symmetric key, used during the process "Collating a Request for a Trusted Platform Module Identity".

End of informative comment

Definition

```
typedef struct tdTPM_SYMMETRIC_KEY {
   TPM_ALGORITHM_ID algId;
   TPM_ENC_SCHEME encScheme;
   UINT16 size;
   [size_is(size)] BYTE* data;
} TPM_SYMMETRIC_KEY;
```

Parameters

Type	Name	Description
TPM_ALGORITHM_ID	algId	This SHALL be the algorithm identifier of the symmetric key.
TPM_ENC_SCHEME	encScheme	This SHALL fully identify the manner in which the key will be used for encryption operations.
UINT16	size	This SHALL be the size of the data parameter in bytes
BYTE*	data	This SHALL be the symmetric key data

9.5 TPM_BOUND_DATA

Start of informative comment

This structure is defined because it is used by a TPM_UnBind command in a consistency check.

The intent of TCG is to promote "best practice" heuristics for the use of keys: a signing key shouldn't be used for storage, and so on. These heuristics are used because of the potential threats that arise when the same key is used in different ways. The heuristics minimize the number of ways in which a given key can be used.

One such heuristic is that a key of type TPM_KEY_BIND, and no other type of key, should always be used to create the blob that is unwrapped by TPM_UnBind. Binding is not a TPM function, so the only choice is to perform a check for the correct payload type when a blob is unwrapped by a key of type TPM_KEY_BIND. This requires the blob to have internal structure.

Even though payloadData has variable size, TPM_BOUND_DATA deliberately does not include the size of payloadData. This is to maximize the size of payloadData that can be encrypted when TPM_BOUND_DATA is encrypted in a single block. When using TPM_UnBind to obtain payloadData, the size of payloadData is deduced as a natural result of the (RSA) decryption process.

End of informative comment

Definition

```
typedef struct tdTPM_BOUND_DATA {
   TPM_STRUCT_VER ver;
   TPM_PAYLOAD_TYPE payload;
   BYTE[] payloadData;
   } TPM_BOUND_DATA;
```

Parameters

Type	Name	Description
TPM_STRUCT_VER	ver	This MUST be 1.1.0.0
TPM_PAYLOAD_TYPE	payload	This SHALL be the value TPM_PT_BIND
BYTE[]	payloadData	The bound data

Descriptions

1. This structure MUST be used for creating data when (wrapping with a key of type TPM_KEY_BIND) or (wrapping using the encryption algorithm TPM_ES_RSAESOAEP_SHA1_MGF1). If it is not, the TPM_UnBind command will fail.

10. TPM_KEY complex

Start of informative comment

The TPA_KEY complex is where all of the information regarding keys is kept. These structures combine to fully define and protect the information regarding an asymmetric key.

One overriding design goal is for a 2048 bit RSA key to be able to properly protect another 2048 bit RSA key. This stems from the fact that the SRK is a 2048 bit key and all identities are 2048 bit keys. A goal is to have these keys only require one decryption when loading an identity into the TPM. The structures as defined meet this goal.

Every TPM_KEY is allowed only one encryption scheme or one signature scheme (or one of each in the case of legacy keys) throughout its lifetime. Note however that more than one scheme could be used with externally generated keys, by introducing the same key in multiple blobs.

End of informative comment:

1533 10.1 TPM_KEY_PARMS

1534**Start of informative comment**

1535This provides a standard mechanism to define the parameters used to generate a key pair, 1536and to store the parts of a key shared between the public and private key parts.

1537**End of informative comment**

1538 Definition

```
1539typedef struct tdTPM_KEY_PARMS {
1540   TPM_ALGORITHM_ID algorithmID;
1541   TPM_ENC_SCHEME encScheme;
1542   TPM_SIG_SCHEME sigScheme;
1543   UINT32 parmSize;
1544   [size_is(parmSize)] BYTE* parms;
1545} TPM_KEY_PARMS;
```

1546 Parameters

Type	Name	Description
TPM_ALGORITHM_ID	algorithmID	This SHALL be the key algorithm in use
TPM_ENC_SCHEME	encScheme	This SHALL be the encryption scheme that the key uses to encrypt information
TPM_SIG_SCHEME	sigScheme	This SHALL be the signature scheme that the key uses to perform digital signatures
UINT32	parmSize	This SHALL be the size of the parms field in bytes
BYTE*	parms	This SHALL be the parameter information dependant upon the key algorithm.

1547 Descriptions

1548The contents of the ‘parms’ field will vary depending upon algorithmId:

Algorithm Id	PARMS Contents
TPM_ALG_RSA	A structure of type TPM_RSA_KEY_PARMS
TPM_ALG_SHA	No content
TPM_ALG_HMAC	No content
TPM_ALG_AESxxx	A structure of type TPM_SYMMETRIC_KEY_PARMS
TPM_ALG_MGF1	No content

10.1.1 TPM_RSA_KEY_PARMS

Start of informative comment

This structure describes the parameters of an RSA key.

End of informative comment

Definition

```
typedef struct tdTPM_RSA_KEY_PARMS {
   UINT32 keyLength;
   UINT32 numPrimes;
   UINT32 exponentSize;
   [size_is(exponentSize)]BYTE* exponent;
} TPM_RSA_KEY_PARMS;
```

Parameters

Type	Name	Description
UINT32	keyLength	This specifies the size of the RSA key in bits
UINT32	numPrimes	This specifies the number of prime factors used by this RSA key.
UINT32	exponentSize	This SHALL be the size of the exponent. If the key is using the default exponent then the exponentSize MUST be 0.
BYTE*	exponent	The public exponent of this key

10.1.2 TPM_SYMMETRIC_KEY_PARMS

Start of informative comment

This structure describes the parameters for symmetric algorithms

End of informative comment

Definition

```
typedef struct tdTPM_SYMMETRIC_KEY_PARMS {
   UINT32 keyLength;
   UINT32 blockSize;
   UINT32 ivSize;
   [size_is(ivSize)] BYTE* IV;
} TPM_SYMMETRIC_KEY_PARMS;
```

Parameters

Type	Name	Description
UINT32	keyLength	This SHALL indicate the length of the key in bits
UINT32	blockSize	This SHALL indicate the block size of the algorithm
UINT32	ivSize	This SHALL indicate the size of the IV
BYTE*	IV	The initialization vector

10.2 TPM_KEY

Start of informative comment

The TPM_KEY structure provides a mechanism to transport the entire asymmetric key pair. The private portion of the key is always encrypted.

The reason for using a size and pointer for the PCR info structure is save space when the key is not bound to a PCR. The only time the information for the PCR is kept with the key is when the key needs PCR info.

The 1.2 version has a change in the PCRInfo area. For 1.2 the structure uses the TPM_PCR_INFO_LONG structure to properly define the PCR registers in use.

End of informative comment:

Definition

```
typedef struct tdTPM_KEY{
   TPM_STRUCT_VER ver;
   TPM_KEY_USAGE keyUsage;
   TPM_KEY_FLAGS keyFlags;
   TPM_AUTH_DATA_USAGE authDataUsage;
   TPM_KEY_PARMS algorithmParms;
   UINT32 PCRInfoSize;
   [size_is(PCRInfoSize)] BYTE* PCRInfo;
   TPM_STORE_PUBKEY   pubKey;
   UINT32 encDataSize;
   [size_is(encDataSize)] BYTE* encData;
} TPM_KEY;
```

Parameters

Type	Name	Description
TPM_STRUCT_VER	ver	This MUST be 1.1.0.0
TPM_KEY_USAGE	keyUsage	This SHALL be the TPM key usage that determines the operations permitted with this key
TPM_KEY_FLAGS	keyFlags	This SHALL be the indication of migration, redirection etc.
TPM_AUTH_DATA_USAGE	authDataUsage	This SHALL Indicate the conditions where it is required that authorization be presented.
TPM_KEY_PARMS	algorithmParms	This SHALL be the information regarding the algorithm for this key
UINT32	PCRInfoSize	This SHALL be the length of the pcrInfo parameter. If the key is not bound to a PCR this value SHOULD be 0.
BYTE*	PCRInfo	This SHALL be a structure of type TPM_PCR_INFO, or an empty array if the key is not bound to PCRs.
TPM_STORE_PUBKEY	pubKey	This SHALL be the public portion of the key
UINT32	encDataSize	This SHALL be the size of the encData parameter.
BYTE*	encData	This SHALL be an encrypted TPM_STORE_ASYMKEY structure or TPM_MIGRATE_ASYMKEY structure

Version handling

1. A TPM MUST be able to read and create TPM_KEY structures
2. A TPM MUST not allow a TPM_KEY structure to contain a TPM_PCR_INFO_LONG structure

1601 10.3 TPM_KEY12

1602**Start of informative comment**

1603This provides the same functionality as TPM_KEY but uses the new PCR_INFO_LONG
1604structures and the new structure tagging. In all other aspects this is the same structure.

1605**End of informative comment:**

1606 Definition

```
1607typedef struct tdTPM_KEY12{
1608   TPM_STRUCTURE_TAG tag;
1609   UINT16 fill;
1610   TPM_KEY_USAGE keyUsage;
1611   TPM_KEY_FLAGS keyFlags;
1612   TPM_AUTH_DATA_USAGE authDataUsage;
1613   TPM_KEY_PARMS algorithmParms;
1614   UINT32 PCRInfoSize;
1615   [size_is(PCRInfoSize)] BYTE* PCRInfo;
1616   TPM_STORE_PUBKEY   pubKey;
1617   UINT32 encDataSize;
1618   [size_is(encDataSize)] BYTE* encData;
1619} TPM_KEY12;
```

1620 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_KEY12
UINT16	fill	MUST be 0x0000
TPM_KEY_USAGE	keyUsage	This SHALL be the TPM key usage that determines the operations permitted with this key
TPM_KEY_FLAGS	keyFlags	This SHALL be the indication of migration, redirection etc.
TPM_AUTH_DATA_USAGE	authDataUsage	This SHALL Indicate the conditions where it is required that authorization be presented.
TPM_KEY_PARMS	algorithmParms	This SHALL be the information regarding the algorithm for this key
UINT32	PCRInfoSize	This SHALL be the length of the pcrInfo parameter. If the key is not bound to a PCR this value SHOULD be 0.
BYTE*	PCRInfo	This SHALL be a structure of type TPM_PCR_INFO_LONG,
TPM_STORE_PUBKEY	pubKey	This SHALL be the public portion of the key
UINT32	encDataSize	This SHALL be the size of the encData parameter.
BYTE*	encData	This SHALL be an encrypted TPM_STORE_ASYMKEY structure TPM_MIGRATE_ASYMKEY structure

1621 Version handling

16221. The TPM MUST be able to read and create TPM_KEY12 structures

16232. The TPM MUST not allow a TPM_KEY12 structure to contain a TPM_PCR_INFO structure

1624 10.4 TPM_STORE_PUBKEY

1625**Start of informative comment**

1626This structure can be used in conjunction with a corresponding TPM_KEY_PARMS to
1627construct a public key which can be unambiguously used.

1628**End of informative comment**

```
1629typedef struct tdTPM_STORE_PUBKEY {
1630   UINT32 keyLength;
1631   [size_is(keyLength)] BYTE* key;
1632} TPM_STORE_PUBKEY;
```

1633 Parameters

Type	Name	Description
UINT32	keyLength	This SHALL be the length of the key field.
BYTE*	key	This SHALL be a structure interpreted according to the algorithm Id in the corresponding TPM_KEY_PARMS structure.

1634 Descriptions

1635The contents of the 'key' field will vary depending upon the corresponding key algorithm:

Algorithm Id	'Key' Contents
TPM_ALG_RSA	The RSA public modulus

1636 10.5 TPM_PUBKEY

1637**Start of informative comment**

1638The TPM_PUBKEY structure contains the public portion of an asymmetric key pair. It
1639contains all the information necessary for its unambiguous usage. It is possible to construct
1640this structure from a TPM_KEY, using the algorithmParms and pubKey fields.

1641**End of informative comment**

1642 Definition

```
1643typedef struct tdTPM_PUBKEY{
1644   TPM_KEY_PARMS algorithmParms;
1645   TPM_STORE_PUBKEY pubKey;
1646} TPM_PUBKEY;
```

1647 Parameters

Type	Name	Description
TPM_KEY_PARMS	algorithmParms	This SHALL be the information regarding this key
TPM_STORE_PUBKEY	pubKey	This SHALL be the public key information

1648 Descriptions

1649The pubKey member of this structure shall contain the public key for a specific algorithm.

1650 10.6 TPM_STORE_ASYMKEY

1651**Start of informative comment**

1652The TPM_STORE_ASYMKEY structure provides the area to identify the confidential 1653information related to a key. This will include the private key factors for an asymmetric key.

1654The structure is designed so that encryption of a TPM_STORE_ASYMKEY structure 1655containing a 2048 bit RSA key can be done in one operation if the encrypting key is 2048 1656bits.

1657Using typical RSA notation the structure would include P, and when loading the key include 1658the unencrypted P*Q which would be used to recover the Q value.

1659To accommodate the future use of multiple prime RSA keys the specification of additional 1660prime factors is an optional capability.

1661This structure provides the basis of defining the protection of the private key.

1662Changes in this structure MUST be reflected in the TPM_MIGRATE_ASYMKEY structure 1663(section 10.8).

1664**End of informative comment**

1665 Definition

```
1666typedef struct tdTPM_STORE_ASYMKEY {   // pos     len         total
1667   TPM_PAYLOAD_TYPE payload;            //   0       1           1
1668   TPM_SECRET usageAuth;                //   1      20          21
1669   TPM_SECRET migrationAuth;            //  21      20          41
1670   TPM_DIGEST    pubDataDigest;         //  41      20          61
1671   TPM_STORE_PRIVKEY privKey;           //  61     132-151  193-214
1672} TPM_STORE_ASYMKEY;
```

1673 Parameters

Type	Name	Description
TPM_PAYLOAD_TYPE	payload	This SHALL set to TPM_PT_ASYM to indicate an asymmetric key. If used in TPM_CMK_ConvertMigration the value SHALL be TPM_PT_MIGRATE_EXTERNAL If used in TPM_CMK_CreateKey the value SHALL be TPM_PT_MIGRATE_RESTRICTED
TPM_SECRET	usageAuth	This SHALL be the AuthData data necessary to authorize the use of this value
TPM_SECRET	migrationAuth	This SHALL be the migration AuthData data for a migratable key, or the TPM secret value tpmProof for a non-migratable key created by the TPM. If the TPM sets this parameter to the value tpmProof, then the TPM_KEY.keyFlags.migratable of the corresponding TPM_KEY structure MUST be set to 0. If this parameter is set to the migration AuthData data for the key in parameter PrivKey, then the TPM_KEY.keyFlags.migratable of the corresponding TPM_KEY structure SHOULD be set to 1.
TPM_DIGEST	pubDataDigest	This SHALL be the digest of the corresponding TPM_KEY structure, excluding the fields TPM_KEY.encSize and TPM_KEY.encData. When TPM_KEY -> pcrInfoSize is 0 then the digest calculation has no input from the pcrInfo field. The pcrInfoSize field MUST always be part of the digest calculation.
TPM_STORE_PRIVKEY	privKey	This SHALL be the private key data. The privKey can be a variable length which allows for differences in the key format. The maximum size of the area would be 151 bytes.

1674 10.7 TPM_STORE_PRIVKEY

1675**Start of informative comment**

1676This structure can be used in conjunction with a corresponding TPM_PUBKEY to construct
1677a private key which can be unambiguously used.

1678**End of informative comment**

```
1679typedef struct tdTPM_STORE_PRIVKEY {
1680   UINT32 keyLength;
1681   [size_is(keyLength)] BYTE* key;
1682} TPM_STORE_PRIVKEY;
```

1683 Parameters

Type	Name	Description
UINT32	keyLength	This SHALL be the length of the key field.
BYTE*	key	This SHALL be a structure interpreted according to the algorithm Id in the corresponding TPM_KEY structure.

1684 Descriptions

1685All migratable keys MUST be RSA keys with two (2) prime factors.

1686For non-migratable keys, the size, format and contents of privKey.key MAY be vendor
1687specific and MAY not be the same as that used for migratable keys. The level of
1688cryptographic protection MUST be at least as strong as a migratable key.

Algorithm Id	key Contents
TPM_ALG_RSA	When the numPrimes defined in the corresponding TPM_RSA_KEY_PARMS field is 2, this shall be one of the prime factors of the key. Upon loading of the key the TPM calculates the other prime factor by dividing the modulus, TPM_RSA_PUBKEY, by this value. The TPM MAY support RSA keys with more than two prime factors. Definition of the storage structure for these keys is left to the TPM Manufacturer.

10.8 TPM_MIGRATE_ASYMKEY

Start of informative comment

The TPM_MIGRATE_ASYMKEY structure provides the area to identify the private key factors of a asymmetric key while the key is migrating between TPM's.

This structure provides the basis of defining the protection of the private key.

End of informative comment

Definition

```
typedef struct tdTPM_MIGRATE_ASYMKEY {          // pos   len      total
  TPM_PAYLOAD_TYPE payload;                     //   0     1          1
  TPM_SECRET usageAuth;                         //   1    20         21
  TPM_DIGEST   pubDataDigest;                   //  21    20         41
  UINT32 partPrivKeyLen;                        //  41     4         45
  [size_is(partPrivKeyLen)] BYTE* partPrivKey;  //  45   112-127  157-172
} TPM_MIGRATE_ASYMKEY;
```

Parameters

Type	Name	Description
TPM_PAYLOAD_TYPE	payload	This SHALL set to TPM_PT_MIGRATE or TPM_PT_CMK_MIGRATE to indicate an migrating asymmetric key or TPM_PT_MAINT to indicate a maintenance key.
TPM_SECRET	usageAuth	This SHALL be a copy of the usageAuth from the TPM_STORE_ASYMKEY structure.
TPM_DIGEST	pubDataDigest	This SHALL be a copy of the pubDataDigest from the TPM_STORE_ASYMKEY structure.
UINT32	partPrivKeyLen	This SHALL be the size of the partPrivKey field
BYTE*	partPrivKey	This SHALL be the k2 area as described in TPM_CreateMigrationBlob

10.9 TPM_KEY_CONTROL

Start of informative comment

Attributes that can control various aspects of key usage and manipulation

End of informative comment

Bit	Name	Description
31:1	Reserved	Must be 0
0	TPM_KEY_CONTROL_OWNER_EVICT	Owner controls when the key is evicted from the TPM. When set the TPM MUST preserve key the key across all TPM_Init invocations.

Descriptions

There is no mimimum number of owner evict keys. That is, the minimum number is 0.

1710 11. Signed Structures

1711 11.1 TPM_CERTIFY_INFO Structure

1712 **Start of informative comment**

1713 When the TPM certifies a key, it must provide a signature with a TPM identity key on
1714 information that describes that key. This structure provides the mechanism to do so.

1715 Key usage and keyFlags must have their upper byte set to zero to avoid collisions with the
1716 other signature headers.

1717 **End of informative comment**

1718 Definition

```
1719 typedef struct tdTPM_CERTIFY_INFO{
1720   TPM_STRUCT_VER version;
1721   TPM_KEY_USAGE keyUsage;
1722   TPM_KEY_FLAGS keyFlags;
1723   TPM_AUTH_DATA_USAGE authDataUsage;
1724   TPM_KEY_PARMS algorithmParms;
1725   TPM_DIGEST pubkeyDigest;
1726   TPM_NONCE data;
1727   BOOL parentPCRStatus;
1728   UINT32 PCRInfoSize;
1729   [size_is(pcrInfoSize)] BYTE* PCRInfo;
1730 } TPM_CERTIFY_INFO;
```

1731 Parameters

Type	Name	Description
TPM_STRUCT_VER	version	This MUST be 1.1.0.0
TPM_KEY_USAGE	keyUsage	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified. The upper byte MUST be zero.
TPM_KEY_FLAGS	keyFlags	This SHALL be set to the same value as the corresponding parameter in the TPM_KEY structure that describes the public key that is being certified. The upper byte MUST be zero.
TPM_AUTH_DATA_USAGE	authDataUsage	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified
TPM_KEY_PARMS	algorithmParms	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified
TPM_DIGEST	pubKeyDigest	This SHALL be a digest of the value TPM_KEY -> pubKey -> key in a TPM_KEY representation of the key to be certified
TPM_NONCE	data	This SHALL be externally provided data.
BOOL	parentPCRStatus	This SHALL indicate if any parent key was wrapped to a PCR
UINT32	PCRInfoSize	This SHALL be the size of the pcrInfo parameter. A value of zero indicates that the key is not wrapped to a PCR
BYTE*	PCRInfo	This SHALL be the TPM_PCR_INFO structure.

1732 11.2 TPM_CERTIFY_INFO2 Structure

1733**Start of informative comment**

1734When the TPM certifies a key, it must provide a signature with a TPM identity key on
1735information that describes that key. This structure provides the mechanism to do so.

1736Key usage and keyFlags must have their upper byte set to zero to avoid collisions with the
1737other signature headers.

1738**End of informative comment**

1739 Definition

```
1740typedef struct tdTPM_CERTIFY_INFO2{
1741   TPM_STRUCTURE_TAG tag;
1742   BYTE fill;
1743   TPM_PAYLOAD_TYPE payloadType;
1744   TPM_KEY_USAGE keyUsage;
1745   TPM_KEY_FLAGS keyFlags;
1746   TPM_AUTH_DATA_USAGE authDataUsage;
1747   TPM_KEY_PARMS algorithmParms;
1748   TPM_DIGEST pubkeyDigest;
1749   TPM_NONCE data;
1750   BOOL parentPCRStatus;
1751   UINT32 PCRInfoSize;
1752   [size_is(pcrInfoSize)] BYTE* PCRInfo;
1753   UINT32 migrationAuthoritySize ;
1754   [size_is(migrationAuthoritySize)] BYTE* migrationAuthority;
1755} TPM_CERTIFY_INFO2;
```

1756 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_CERTIFY_INFO2
BYTE	fill	MUST be 0x00
TPM_PAYLOAD_TYPE	payloadType	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified
TPM_KEY_USAGE	keyUsage	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified. The upper byte MUST be zero.
TPM_KEY_FLAGS	keyFlags	This SHALL be set to the same value as the corresponding parameter in the TPM_KEY structure that describes the public key that is being certified. The upper byte MUST be zero.
TPM_AUTH_DATA_USAGE	authDataUsage	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified
TPM_KEY_PARMS	algorithmParms	This SHALL be the same value that would be set in a TPM_KEY representation of the key to be certified
TPM_DIGEST	pubKeyDigest	This SHALL be a digest of the value TPM_KEY -> pubKey -> key in a TPM_KEY representation of the key to be certified
TPM_NONCE	data	This SHALL be externally provided data.
BOOL	parentPCRStatus	This SHALL indicate if any parent key was wrapped to a PCR
UINT32	PCRInfoSize	This SHALL be the size of the pcrInfo parameter.

Type	Name	Description
BYTE*	PCRInfo	This SHALL be the TPM_PCR_INFO_SHORT structure.
UINT32	migrationAuthoritySize	This SHALL be the size of migrationAuthority
BYTE*	migrationAuthority	If the key to be certified has [payload == TPM_PT_MIGRATE_RESTRICTED or payload ==TPM_PT_MIGRATE_EXTERNAL], migrationAuthority is the digest of the TPM_MSA_COMPOSITE and has TYPE == TPM_DIGEST. Otherwise it is NULL.

1757 11.3 TPM_QUOTE_INFO Structure

1758**Start of informative comment**

1759This structure provides the mechanism for the TPM to quote the current values of a list of
1760PCRs.

1761**End of informative comment**

1762 Definition

```
1763typedef struct tdTPM_QUOTE_INFO{
1764   TPM_STRUCT_VER version;
1765   BYTE fixed[4];
1766   TPM_COMPOSITE_HASH digestValue;
1767   TPM_NONCE externalData;
1768} TPM_QUOTE_INFO;
```

1769 Parameters

Type	Name	Description
TPM_STRUCT_VER	version	This MUST be 1.1.0.0
BYTE[4]	fixed	This SHALL always be the string 'QUOT'
TPM_COMPOSITE_HASH	digestValue	This SHALL be the result of the composite hash algorithm using the current values of the requested PCR indices.
TPM_NONCE	externalData	160 bits of externally supplied data

11.4 TPM_QUOTE_INFO2 Structure

Start of informative comment

This structure provides the mechanism for the TPM to quote the current values of a list of PCRs.

End of informative comment

Definition

```
typedef struct tdTPM_QUOTE_INFO2{
   TPM_STRUCTURE_TAG tag;
   BYTE fixed[4];
   TPM_NONCE externalData;
   TPM_PCR_INFO_SHORT infoShort;
} TPM_QUOTE_INFO2;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_QUOTE_INFO2
BYTE[4]	fixed	This SHALL always be the string 'QUT2'
TPM_NONCE	externalData	160 bits of externally supplied data
TPM_PCR_INFO_SHORT	infoShort	the quoted PCR registers

12. Identity Structures

12.1 TPM_EK_BLOB

Start of informative comment

This structure provides a wrapper to each type of structure that will be in use when the endorsement key is in use.

End of informative comment

Definition

```
typedef struct tdTPM_EK_BLOB{
   TPM_STRUCTURE_TAG  tag;
   TPM_EK_TYPE ekType;
   UINT32 blobSize;
   [size_is(blobSize)] BYTE* blob;
} TPM_EK_BLOB;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_EK_BLOB
TPM_EK_TYPE	ekType	This SHALL be set to reflect the type of blob in use
UINT32	blobSize	The size of the blob field
BYTE*	blob	The blob of information depending on the type

12.2 TPM_EK_BLOB_ACTIVATE

Start of informative comment

This structure contains the symmetric key to encrypt the identity credential.

This structure always is contained in a TPM_EK_BLOB.

End of informative comment

Definition

```
typedef struct tdTPM_EK_BLOB_ACTIVATE{
   TPM_STRUCTURE_TAG  tag;
   TPM_SYMMETRIC_KEY sessionKey;
   TPM_DIGEST idDigest;
   TPM_PCR_INFO_SHORT pcrInfo;
} TPM_EK_BLOB_ACTIVATE;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_EK_BLOB_ACTIVATE
TPM_SYMMETRIC_KEY	sessionKey	This SHALL be the session key used by the CA to encrypt the TPM_IDENTITY_CREDENTIAL
TPM_DIGEST	idDigest	This SHALL be the digest of the TPM_PUBKEY that is being certified by the CA
TPM_PCR_INFO_SHORT	pcrInfo	This SHALL indicate the PCR's and localities

12.3 TPM_EK_BLOB_AUTH

Start of informative comment

This structure contains the symmetric key to encrypt the identity credential.

This structure always is contained in a TPM_EK_BLOB.

End of informative comment

Definition

```
typedef struct tdTPM_EK_BLOB_AUTH{
   TPM_STRUCTURE_TAG  tag;
   TPM_SECRET authValue;
} TPM_EK_BLOB_AUTH;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_EK_BLOB_AUTH
TPM_SECRET	authValue	This SHALL be the AuthData value

1822 12.4 TPM_CHOSENID_HASH

1823This definition specifies the operation necessary to create a TPM_CHOSENID_HASH 1824structure.

1825 Parameters

Type	Name	Description
BYTE [ ]	identityLabel	The label chosen for a new TPM identity
TPM_PUBKEY	privacyCA	The public key of a TTP chosen to attest to a new TPM identity

1826 Action

18271. TPM_CHOSENID_HASH = SHA(identityLabel || privacyCA)

12.5 TPM_IDENTITY_CONTENTS

Start of informative comment

TPM_MakeIdentity uses this structure and the signature of this structure goes to a privacy CA during the certification process. There is no reason to update the version as this structure did not change for version 1.2.

End of informative comment

Definition

```
typedef struct tdTPM_IDENTITY_CONTENTS {
  TPM_STRUCT_VER          ver;
  UINT32                  ordinal;
  TPM_CHOSENID_HASH       labelPrivCADigest;
  TPM_PUBKEY              identityPubKey;
} TPM_IDENTITY_CONTENTS;
```

Parameters

Type	Name	Description
TPM_STRUCT_VER	ver	This MUST be 1.1.0.0. This is the version information for this structure and not the underlying key.
UINT32	ordinal	This SHALL be the ordinal of the TPM_MakeIdentity command.
TPM_CHOSENID_HASH	labelPrivCADigest	This SHALL be the result of hashing the chosen identityLabel and privacyCA for the new TPM identity
TPM_PUBKEY	identityPubKey	This SHALL be the public key structure of the identity key

1842 12.6 TPM_IDENTITY_REQ

1843 **Start of informative comment**

1844 This structure is sent by the TSS to the Privacy CA to create the identity credential.

1845 This structure is informative only.

1846 **End of informative comment**

1847 Parameters

Type	Name	Description
UINT32	asymSize	This SHALL be the size of the asymmetric encrypted area created by TSS_CollateIdentityRequest
UINT32	symSize	This SHALL be the size of the symmetric encrypted area created by TSS_CollateIdentityRequest
TPM_KEY_PARMS	asymAlgorithm	This SHALL be the parameters for the asymmetric algorithm used to create the asymBlob
TPM_KEY_PARMS	symAlgorithm	This SHALL be the parameters for the symmetric algorithm used to create the symBlob
BYTE*	asymBlob	This SHALL be the asymmetric encrypted area from TSS_CollateIdentityRequest
BYTE*	symBlob	This SHALL be the symmetric encrypted area from TSS_CollateIdentityRequest

12.7 TPM_IDENTITY_PROOF

Start of informative comment

Structure in use during the AIK credential process.

End of informative comment

Type	Name	Description
TPM_STRUCT_VER	ver	This MUST be 1.1.0.0
UINT32	labelSize	This SHALL be the size of the label area
UINT32	identityBindingSize	This SHALL be the size of the identitybinding area
UINT32	endorsementSize	This SHALL be the size of the endorsement credential
UINT32	platformSize	This SHALL be the size of the platform credential
UINT32	conformanceSize	This SHALL be the size of the conformance credential
TPM_PUBKEY	identityKey	This SHALL be the public key of the new identity
BYTE*	labelArea	This SHALL be the text label for the new identity
BYTE*	identityBinding	This SHALL be the signature value of TPM_IDENTITY_CONTENTS structure from the TPM_MakeIdentity command
BYTE*	endorsementCredential	This SHALL be the TPM endorsement credential
BYTE*	platformCredential	This SHALL be the TPM platform credential
BYTE*	conformanceCredential	This SHALL be the TPM conformance credential

12.8 TPM_ASYM_CA_CONTENTS

Start of informative comment

This structure contains the symmetric key to encrypt the identity credential.

End of informative comment

Definition

```
typedef struct tdTPM_ASYM_CA_CONTENTS{
  TPM_SYMMETRIC_KEY sessionKey;
  TPM_DIGEST idDigest;
} TPM_ASYM_CA_CONTENTS;
```

Parameters

Type	Name	Description
TPM_SYMMETRIC_KEY	sessionKey	This SHALL be the session key used by the CA to encrypt the TPM_IDENTITY_CREDENTIAL
TPM_DIGEST	idDigest	This SHALL be the digest of the TPM_PUBKEY of the key that is being certified by the CA

12.9 TPM_SYM_CA_ATTESTATION

Start of informative comment

This structure returned by the Privacy CA with the encrypted identity credential.

End of informative comment

Type	Name	Description
UINT32	credSize	This SHALL be the size of the credential parameter
TPM_KEY_PARMS	algorithm	This SHALL be the indicator and parameters for the symmetric algorithm
BYTE*	credential	This is the result of encrypting TPM_IDENTITY_CREDENTIAL using the session_key and the algorithm indicated “algorithm”

1866 13. Transport structures

1867 13.1 TPM _TRANSPORT_PUBLIC

1868 **Start of informative comment**

1869 The public information relative to a transport session

1870 **End of informative comment**

1871 Definition

```
1872 typedef struct tdTPM_TRANSPORT_PUBLIC{
1873   TPM_STRUCTURE_TAG  tag;
1874   TPM_TRANSPORT_ATTRIBUTES transAttributes;
1875   TPM_ALGORITHM_ID algId;
1876   TPM_ENC_SCHEME encScheme;
1877 } TPM_TRANSPORT_PUBLIC;
```

1878 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_TRANSPORT_PUBLIC
TPM_TRANSPORT_ATTRIBUTES	transAttributes	The attributes of this session
TPM_ALGORITHM_ID	algId	This SHALL be the algorithm identifier of the symmetric key.
TPM_ENC_SCHEME	encScheme	This SHALL fully identify the manner in which the key will be used for encryption operations.

1879 13.1.1 TPM_TRANSPORT_ATTRIBUTES Definitions

Name	Value	Description
TPM_TRANSPORT_ENCRYPT	0x00000001	The session will provide encryption using the internal encryption algorithm
TPM_TRANSPORT_LOG	0x00000002	The session will provide a log of all operations that occur in the session
TPM_TRANSPORT_EXCLUSIVE	0X00000004	The transport session is exclusive and any command executed outside the transport session causes the invalidation of the session

13.2 TPM_TRANSPORT_INTERNAL

Start of informative comment

The internal information regarding transport session

End of informative comment

Definition

```
typedef struct tdTPM_TRANSPORT_INTERNAL{
  TPM_STRUCTURE_TAG  tag;
  TPM_AUTHDATA authData;
  TPM_TRANSPORT_PUBLIC transPublic;
  TPM_TRANSHANDLE transHandle;
  TPM_NONCE transNonceEven;
  TPM_DIGEST transDigest;
} TPM_TRANSPORT_INTERNAL;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_TRANSPORT_INTERNAL
TPM_AUTHDATA	authData	The shared secret for this session
TPM_TRANSPORT_PUBLIC	transPublic	The public information of this session
TPM_TRANSHANDLE	transHandle	The handle for this session
TPM_NONCE	transNonceEven	The even nonce for the rolling protocol
TPM_DIGEST	transDigest	The log of transport events

13.3 TPM_TRANSPORT_LOG_IN structure

Start of informative comment

The logging of transport commands occurs in two steps, before execution with the input parameters and after execution with the output parameters.

This structure is in use for input log calculations.

End of informative comment

Definition

```
typedef struct tdTPM_TRANSPORT_LOG_IN{
   TPM_STRUCTURE_TAG  tag;
   TPM_DIGEST parameters;
   TPM_DIGEST pubKeyHash;
} TPM_TRANSPORT_LOG_IN;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_TRANSPORT_LOG_IN
TPM_DIGEST	parameters	The actual parameters contained in the digest are subject to the rules of the command using this structure. To find the exact calculation refer to the actions in the command using this structure.
TPM_DIGEST	pubKeyHash	The hash of any keys in the transport command

13.4 TPM_TRANSPORT_LOG_OUT structure

Start of informative comment

The logging of transport commands occurs in two steps, before execution with the input parameters and after execution with the output parameters.

This structure is in use for output log calculations.

This structure is in use for the INPUT logging during releaseTransport.

End of informative comment

Definition

```
typedef struct tdTPM_TRANSPORT_LOG_OUT{
   TPM_STRUCTURE_TAG tag;
   TPM_CURRENT_TICKS currentTicks;
   TPM_DIGEST parameters;
   TPM_MODIFIER_INDICATOR locality;
} TPM_TRANSPORT_LOG_OUT;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_TRANSPORT_LOG_OUT
TPM_CURRENT_TICKS	currentTicks	The current tick count. This SHALL be the value of the current TPM tick counter.
TPM_DIGEST	parameters	The actual parameters contained in the digest are subject to the rules of the command using this structure. To find the exact calculation refer to the actions in the command using this structure.
TPM_MODIFIER_INDICATOR	locality	The locality that called TPM_ExecuteTransport

13.5 TPM_TRANSPORT_AUTH structure

Start of informative comment

This structure provides the validation for the encrypted AuthData value.

End of informative comment

Definition

```
typedef struct tdTPM_TRANSPORT_AUTH {
   TPM_STRUCTURE_TAG  tag;
   TPM_AUTHDATA authData;
} TPM_TRANSPORT_AUTH;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_TRANSPORT_AUTH
TPM_AUTHDATA	authData	The AuthData value

14. Audit Structures

14.1 TPM_AUDIT_EVENT_IN structure

Start of informative comment

This structure provides the auditing of the command upon receipt of the command. It provides the information regarding the input parameters.

End of informative comment

Definition

```
typedef struct tdTPM_AUDIT_EVENT_IN {
  TPM_STRUCTURE_TAG  tag;
  TPM_DIGEST inputParms;
  TPM_COUNTER_VALUE auditCount;
} TPM_AUDIT_EVENT_IN;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_AUDIT_EVENT_IN
TPM_DIGEST	inputParms	Digest value according to the HMAC digest rules of the "above the line" parameters (i.e. the first HMAC digest calculation). When there are no HMAC rules, the input digest includes all parameters including and after the ordinal.
TPM_COUNTER_VALUE	auditCount	The current value of the audit monotonic counter

14.2 TPM_AUDIT_EVENT_OUT structure

Start of informative comment

This structure reports the results of the command execution. It includes the return code and the output parameters.

End of informative comment

Definition

```
typedef struct tdTPM_AUDIT_EVENT_OUT {
  TPM_STRUCTURE_TAG  tag;
  TPM_DIGEST outputParms;
  TPM_COUNTER_VALUE auditCount;
} TPM_AUDIT_EVENT_OUT;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_AUDIT_EVENT_OUT
TPM_DIGEST	outputParms	Digest value according to the HMAC digest rules of the "above the line" parameters (i.e. the first HMAC digest calculation). When there are no HMAC rules, the output digest includes the return code, the ordinal, and all parameters after the return code.
TPM_COUNTER_VALUE	auditCount	The current value of the audit monotonic counter

15. Tick Structures

15.1 TPM_CURRENT_TICKS

Start of informative comment

This structure holds the current number of time ticks in the TPM. The value is the number of time ticks from the start of the current session. Session start is a variable function that is platform dependent. Some platforms may have batteries or other power sources and keep the TPM clock session across TPM initialization sessions.

The <tickRate> element of the TPM_CURRENT_TICKS structure provides the number of microseconds per tick. The platform manufacturer must satisfy input clock requirements set by the TPM vendor to ensure the accuracy of the tickRate.

No external entity may ever set the current number of time ticks held in TPM_CURRENT_TICKS. This value is always reset to 0 when a new clock session starts and increments under control of the TPM.

Maintaining the relationship between the number of ticks counted by the TPM and some real world clock is a task for external software.

End of informative comment

Definition

```
typedef struct tdTPM_CURRENT_TICKS {
   TPM_STRUCTURE_TAG  tag;
   UINT64 currentTicks;
   UINT16  tickRate;
   TPM_NONCE     tickNonce;
}TPM_CURRENT_TICKS;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_CURRENT_TICKS
UINT64	currentTicks	The number of ticks since the start of this tick session
UINT16	tickRate	The number of microseconds per tick. The maximum resolution of the TPM tick counter is thus 1 microsecond. The minimum resolution SHOULD be 1 millisecond.
TPM_NONCE	tickNonce	The nonce created by the TPM when resetting the currentTicks to 0. This indicates the beginning of a time session. This value MUST be valid before the first use of TPM_CURRENT_TICKS. The value can be set at TPM_Startup or just prior to first use.

16. Return Codes

Start of informative comment

The TPM has five types of return code. One indicates successful operation and four indicate failure. TPM_SUCCESS (00000000) indicates successful execution. The failure reports are: TPM defined fatal errors (00000001 to 000003FF), vendor defined fatal errors (00000400 to 000007FF), TPM defined non-fatal errors (00000800 to 00000BFF), and vendor defined non-fatal errors (00000C00 to 00000FFF).

The range of vendor defined non-fatal errors was determined by the TSS-WG, which defined XXXX YCCC with XXXX as OS specific and Y defining the TSS SW stack layer (0: TPM layer)

All failure cases return only a non-authenticated fixed set of information. This is because the failure may have been due to authentication or other factors, and there is no possibility of producing an authenticated response.

Fatal errors also terminate any authorization sessions. This is a result of returning only the error code, as there is no way to return the nonces necessary to maintain an authorization session. Non-fatal errors do not terminate authorization sessions.

Sessions are not terminated when the fatal error is due to an incorrect command size. In these cases, there is no way for the TPM to know that a four byte sequence is a session handle.

Examples (not a complete set) include:

- A command that should be auth-0 sees any tag and extra bytes at the end of the command.

- A command that can be auth-1 sees an auth-1 tag and extra bytes at the end of the command. No session is terminated, even though there are enough bytes to assemble the first session handle.

- A command that can be auth-2 sees an auth-2 tag and extra bytes at the end of the command. No session is terminated, even though there are enough bytes to assemble both session handles.

- A command that can be auth-2 sees an auth-2 tag but too few bytes to assemble the second session. No session is terminated, even though there are enough bytes to assemble the first session handle.

- A command that can be auth-1 sees an auth-0 tag and enough bytes to assemble a set of below-the-line parameters. No session is terminated, because the tag did not indicate a session handle.

- A TPM_EstablishTransport with an auth-1 tag parsed the command correctly. It fails because the key handle is TPM_KH_TRANSPORT, which requires auth-0. The session **is** terminated, because the command parsed correctly and failed later during processing.

End of informative comment

Description

1. When a command fails for ANY reason, the TPM MUST return only the following three items:

2022 a. tag (2 bytes, fixed at TPM_TAG_RSP_COMMAND)

2023 b. paramSize (4 bytes, fixed at 10)

2024 c. returnCode (4 bytes, never TPM_SUCCESS)

20252. When a command succeeds, the TPM MUST return TPM_SUCCESS. When a command 2026 fails, the TPM MUST return a legal error code.

2027 a. If a TPM returns an error code after executing a command, it SHOULD be the error 2028 code specified by the command or another legal error code that is appropriate to the 2029 error condition.

2030 b. A legal error code is an error code documented either by a TCG specification or by 2031 vendor documentation.

20323. A fatal failure SHALL cause termination of the associated authorization or transport 2033 session. A non-fatal failure SHALL NOT cause termination of the associated 2034 authorization or transport session.

2035 a. If the incoming command size is not equal to the proper size (of the command plus 2036 authorization data), an error MUST be returned but sessions MUST NOT be 2037 terminated.

2038 b. If the incoming command tag is inconsistent with the tag values allowed for the 2039 command, an error MUST be returned but sessions MUST NOT be terminated.

20404. A fatal failure of a wrapped command SHALL not cause any disruption of a transport 2041 session that wrapped the failing command. The exception to this is when the failure 2042 causes the TPM itself to go into failure mode (selftest failure, etc.)

2043The return code MUST use the following base. The return code MAY be TCG defined or 2044vendor defined.

2045Mask Parameters

Name	Value	Description
TPM_BASE	0x0	The start of TPM return codes
TPM_SUCCESS	TPM_BASE	Successful completion of the operation
TPM_VENDOR_ERROR	TPM_Vendor_Specific32	Mask to indicate that the error code is vendor specific for vendor specific commands.
TPM_NON_FATAL	0x00000800	Mask to indicate that the error code is a non-fatal failure.

2046**TPM-defined fatal error codes**

Name	Value	Description
TPM_AUTHFAIL	TPM_BASE + 1	Authentication failed
TPM_BADINDEX	TPM_BASE + 2	The index to a PCR, DIR or other register is incorrect
TPM_BAD_PARAMETER	TPM_BASE + 3	One or more parameter is bad
TPM_AUDITFAILURE	TPM_BASE + 4	An operation completed successfully but the auditing of that operation failed.
TPM_CLEAR_DISABLED	TPM_BASE + 5	The clear disable flag is set and all clear operations now require physical access
TPM_DEACTIVATED	TPM_BASE + 6	The TPM is deactivated
TPM_DISABLED	TPM_BASE + 7	The TPM is disabled
TPM_DISABLED_CMD	TPM_BASE + 8	The target command has been disabled
TPM_FAIL	TPM_BASE + 9	The operation failed
TPM_BAD_ORDINAL	TPM_BASE + 10	The ordinal was unknown or inconsistent
TPM_INSTALL_DISABLED	TPM_BASE + 11	The ability to install an owner is disabled
TPM_INVALID_KEYHANDLE	TPM_BASE + 12	The key handle can not be interpreted
TPM_KEYNOTFOUND	TPM_BASE + 13	The key handle points to an invalid key
TPM_INAPPROPRIATE_ENC	TPM_BASE + 14	Unacceptable encryption scheme
TPM_MIGRATEFAIL	TPM_BASE + 15	Migration authorization failed
TPM_INVALID_PCR_INFO	TPM_BASE + 16	PCR information could not be interpreted
TPM_NOSPACE	TPM_BASE + 17	No room to load key.
TPM_NOSRK	TPM_BASE + 18	There is no SRK set. This is an appropriate response when an unowned TPM receives a command that requires a TPM owner.
TPM_NOTSEALED_BLOB	TPM_BASE + 19	An encrypted blob is invalid or was not created by this TPM
TPM_OWNER_SET	TPM_BASE + 20	There is already an Owner
TPM_RESOURCES	TPM_BASE + 21	The TPM has insufficient internal resources to perform the requested action.
TPM_SHORTRANDOM	TPM_BASE + 22	A random string was too short
TPM_SIZE	TPM_BASE + 23	The TPM does not have the space to perform the operation.
TPM_WRONGPCRVAL	TPM_BASE + 24	The named PCR value does not match the current PCR value.
TPM_BAD_PARAM_SIZE	TPM_BASE + 25	The paramSize argument to the command has the incorrect value
TPM_SHA_THREAD	TPM_BASE + 26	There is no existing SHA-1 thread.
TPM_SHA_ERROR	TPM_BASE + 27	The calculation is unable to proceed because the existing SHA-1 thread has already encountered an error.
TPM_FAILEDSELFTEST	TPM_BASE + 28	Self-test has failed and the TPM has shutdown.
TPM_AUTH2FAIL	TPM_BASE + 29	The authorization for the second key in a 2 key function failed authorization
TPM_BADTAG	TPM_BASE + 30	The tag value sent to for a command is invalid
TPM_IOERROR	TPM_BASE + 31	An IO error occurred transmitting information to the TPM
TPM_ENCRYPT_ERROR	TPM_BASE + 32	The encryption process had a problem.
TPM_DECRYPT_ERROR	TPM_BASE + 33	The decryption process did not complete.
TPM_INVALID_AUTHHANDLE	TPM_BASE + 34	An invalid handle was used.
TPM_NO_ENDORSEMENT	TPM_BASE + 35	The TPM does not have a EK installed
TPM_INVALID_KEYUSAGE	TPM_BASE + 36	The usage of a key is not allowed
TPM_WRONG_ENTITYTYPE	TPM_BASE + 37	The submitted entity type is not allowed
TPM_INVALID_POSTINIT	TPM_BASE + 38	The command was received in the wrong sequence relative to TPM_Init and a subsequent TPM_Startup
TPM_INAPPROPRIATE_SIG	TPM_BASE + 39	Signed data cannot include additional DER information

2047**TPM-defined non-fatal errors**

Name	Value	Description
TPM_RETRY	TPM_BASE + TPM_NON_FATAL	The TPM is too busy to respond to the command immediately, but the command could be resubmitted at a later time The TPM MAY return TPM_RETRY for any command at any time.
TPM_NEEDS_SELFTEST	TPM_BASE + TPM_NON_FATAL + 1	TPM_ContinueSelfTest has not been run.
TPM_DOING_SELFTEST	TPM_BASE + TPM_NON_FATAL + 2	The TPM is currently executing the actions of TPM_ContinueSelfTest because the ordinal required resources that have not been tested.
TPM_DEFEND_LOCK_RUNNING	TPM_BASE + TPM_NON_FATAL + 3	The TPM is defending against dictionary attacks and is in some time-out period.

2048 17. Ordinals

2049**Start of informative comment**

2050The command ordinals provide the index value for each command. The following list
2051contains the index value and other information relative to the ordinal.

2052TPM commands are divided into three classes: Protected/Unprotected, Non-
2053Connection/Connection related, and TPM/Vendor. The P and C bits are reserved but their
2054functions were never used, although some ordinals have the C bit set.

2055**End of informative comment**

2056Ordinals are 32 bit values of type TPM_COMMAND_CODE. The upper byte contains values
2057that serve as flag indicators, the next byte contains values indicating what committee
2058designated the ordinal, and the final two bytes contain the Command Ordinal Index.

```
2059          3                   2                   1
2060        1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
2061       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
2062       |P|C|V| Reserved|    Purview    |   Command Ordinal Index       |
2063       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2064Where:

2065P is Protected/Unprotected command. When 0 the command is a Protected command, when
20661 the command is an Unprotected command.

2067C is Non-Connection/Connection related command. When 0 this command passes through
2068to either the protected (TPM) or unprotected (TSS) components.

2069V is TPM/Vendor command. When 0 the command is TPM defined, when 1 the command is
2070vendor defined.

2071All reserved area bits are set to 0.

2072The following masks are created to allow for the quick definition of the commands

Value	Event Name	Comments
0x00000000	TPM_PROTECTED_COMMAND	TPM protected command, specified in main specification
0x80000000	TPM_UNPROTECTED_COMMAND	TSS command, specified in the TSS specification
0x40000000	TPM_CONNECTION_COMMAND	TSC command, protected connection commands are specified in the main
0x20000000	TPM_VENDOR_COMMAND	Command that is vendor specific for a given TPM or TSS.

2073The following Purviews have been defined:

Value	Event Name	Comments
0x00	TPM_MAIN	Command is from the main specification
0x01	TPM_PC	Command is specific to the PC
0x02	TPM_PDA	Command is specific to a PDA
0x03	TPM_CELL_PHONE	Command is specific to a cell phone
0x04	TPM_SERVER	Command is specific to servers
0x05	TPM_PERIPHERAL	Command is specific to peripherals
0x06	TPM_TSS	Command is specific to TSS

2074

2075Combinations for the main specification would be

Value	Event Name
TPM_PROTECTED_COMMAND | TPM_MAIN	TPM_PROTECTED_ORDINAL
TPM_UNPROTECTED_COMMAND | TPM_MAIN	TPM_UNPROTECTED_ORDINAL
TPM_CONNECTION_COMMAND | TPM_MAIN	TPM_CONNECTION_ORDINAL

2076

2077If a command is tagged from the audit column, the default state is that use of that 2078command SHALL be audited. Otherwise, the default state is that use of that command 2079SHALL NOT be audited.

Column	Column Values	Comments and valid column entries
AUTH2	x	Does the command support two authorization entities, normally two keys
AUTH1	x	Does the commands support an single authorization session
RQU	x	Does the command execute without any authorization
Optional	O	Is the command optional
No Owner	x	Is the command executable when no owner is present
PCR Use Enforced	x	Does the command enforce PCR restrictions when executed
Physical presence	P	P = The command sometimes considers the physical presence indication during execution. See the ordinal actions for details.
Audit	X, N	Is the default for auditing enabled N = Never the ordinal is never audited X = Auditing is enabled by default
Duration	S, M, L	What is the expected duration of the command, S = Short implies no asymmetric cryptography M = Medium implies an asymmetric operation L = Long implies asymmetric key generation
1.2 Changes	N, D, X, C	N = New for 1.2 X = Deleted in 1.2 D = Deprecated in 1.2 C = Changed in 1.2
FIPS changes	x	Ordinal has change to satisfy FIPS 140 requirements
Avail Deactivated	X, A	X = Ordinal will execute when deactivated A = Ordinal sometimes executes when deactivated. See ordinal actions for details.

Avail Disabled	X, A	X = Ordinal will execute when disabled A = Ordinal sometimes executes when disabled. See ordinal actions for details. The TPM MUST return TPM_DISABLED for all commands other than those marked as available

2080

2081The following table is normative, and is the overriding authority in case of discrepancies in 2082other parts of this specification.

2083

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TPM_ORD_ActivateIdentity	122	0x0000007A	X	X						X	X	M				
TPM_ORD_AuthorizeMigrationKey	43	0x0000002B		X							X	S				
TPM_ORD_CertifyKey	50	0x00000032	X	X	X					X		M				
TPM_ORD_CertifyKey2	51	0x00000033	X	X	X					X		M	N			
TPM_ORD_CertifySelfTest	82	0x00000052		X	X					X		M	X			
TPM_ORD_ChangeAuth	12	0x0000000C	X							X		M				
TPM_ORD_ChangeAuthAsymFinish	15	0x0000000F		X	X					X		M	D			
TPM_ORD_ChangeAuthAsymStart	14	0x0000000E		X	X					X		L	D			
TPM_ORD_ChangeAuthOwner	16	0x00000010		X						X	X	S				
TPM_ORD_CMK_ApproveMA	29	0x0000001D		X		O						S	N			
TPM_ORD_CMK_ConvertMigration	36	0x00000024		X		O				X		M	N			
TPM_ORD_CMK_CreateBlob	27	0x0000001B		X		O				X		M	N			
TPM_ORD_CMK_CreateKey	19	0x00000013		X		O				X		L	N	X		
TPM_ORD_CMK_CreateTicket	18	0x00000012		X		O						M	N			
TPM_ORD_CMK_SetRestrictions	28	0x0000001C		X		O						S	N			
TPM_ORD_ContinueSelfTest	83	0x00000053			X			X				L		X	X	X
TPM_ORD_ConvertMigrationBlob	42	0x0000002A		X	X					X	X	M				
TPM_ORD_CreateCounter	220	0x000000DC		X								S	N			
TPM_ORD_CreateEndorsementKeyPair	120	0x00000078			X			X				L				
TPM_ORD_CreateMaintenanceArchive	44	0x0000002C		X		O					X	S				
TPM_ORD_CreateMigrationBlob	40	0x00000028	X	X						X	X	M				
TPM_ORD_CreateRevocableEK	127	0x0000007F			X	O		X				L	N			
TPM_ORD_CreateWrapKey	31	0x0000001F		X						X	X	L		X		
TPM_ORD_DAA_Join	41	0x00000029		X		O						L	N			

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TPM_ORD_DAA_Sign	49	0x00000031		X		O						L	N			
TPM_ORD_Delegate_CreateKeyDelegation	212	0x000000D4		X								M	N			
TPM_ORD_Delegate_CreateOwnerDelegation	213	0x000000D5		X								M	N			
TPM_ORD_Delegate_LoadOwnerDelegation	216	0x000000D8		X	X			X				M	N			
TPM_ORD_Delegate_Manage	210	0x000000D2		X	X			X				M	N			
TPM_ORD_Delegate_ReadTable	219	0x000000DB			X			X				S	N			
TPM_ORD_Delegate_UpdateVerification	209	0x000000D1		X								S	N			
TPM_ORD_Delegate_VerifyDelegation	214	0x000000D6			X							M	N			
TPM_ORD_DirRead	26	0x0000001A			X							S	D			
TPM_ORD_DirWriteAuth	25	0x00000019		X								S	D			
TPM_ORD_DisableForceClear	94	0x0000005E			X			X			X	S				
TPM_ORD_DisableOwnerClear	92	0x0000005C		X							X	S				
TPM_ORD_DisablePubekRead	126	0x0000007E		X							X	S				
TPM_ORD_DSAP	17	0x00000011			X							S	N		X	X
TPM_ORD_EstablishTransport	230	0x000000E6		X	X					X		M	N			
TPM_ORD_EvictKey	34	0x00000022			X							S	D			
TPM_ORD_ExecuteTransport	231	0x000000E7		X								? L	N			
TPM_ORD_Extend	20	0x00000014			X			X				S			X	X
TPM_ORD_FieldUpgrade	170	0x000000AA	X	X	X	O		X	P			?			X	X
TPM_ORD_FlushSpecific	186	0x000000BA			X			X				S	N		X	X
TPM_ORD_ForceClear	93	0x0000005D			X			X	P		X	S				
TPM_ORD_GetAuditDigest	133	0x00000085			X	O		X			N	S	N			
TPM_ORD_GetAuditDigestSigned	134	0x00000086		X	X	O					N	M	N			
TPM_ORD_GetAuditEvent	130	0x00000082			X	O					N	S	X			
TPM_ORD_GetAuditEventSigned	131	0x00000083		X	X	O					N	M	X			
TPM_ORD_GetCapability	101	0x00000065			X			X				S	C		X	X
TPM_ORD_GetCapabilityOwner	102	0x00000066		X								S	D			
TPM_ORD_GetCapabilitySigned	100	0x00000064		X	X					X		M	X			
TPM_ORD_GetOrdinalAuditStatus	140	0x0000008C			X						N	S	X			

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TPM_ORD_GetPubKey	33	0x00000021		X	X					X		S	C			
TPM_ORD_GetRandom	70	0x00000046			X			X				S				
TPM_ORD_GetTestResult	84	0x00000054			X			X				S			X	X
TPM_ORD_GetTicks	241	0x000000F1			X			X				S	N			
TPM_ORD_IncrementCounter	221	0x000000DD		X								S	N			
TPM_ORD_Init	151	0x00000097			X			X				M			X	X
TPM_ORD_KeyControlOwner	35	0x00000023		X								S	N			
TPM_ORD_KillMaintenanceFeature	46	0x0000002E		X		O					X	S				
TPM_ORD_LoadAuthContext	183	0x000000B7			X	O		X				M	D			
TPM_ORD_LoadContext	185	0x000000B9			X							M	N			
TPM_ORD_LoadKey	32	0x00000020		X	X					X		M	D	X		
TPM_ORD_LoadKey2	65	0x00000041		X	X					X		M	N	X		
TPM_ORD_LoadKeyContext	181	0x000000B5			X	O		X				S	D			
TPM_ORD_LoadMaintenanceArchive	45	0x0000002D		X		O					X	S				
TPM_ORD_LoadManuMaintPub	47	0x0000002F			X	O		X			X	S				
TPM_ORD_MakeIdentity	121	0x00000079	X	X						X	X	L		X		
TPM_ORD_MigrateKey	37	0x00000025		X	X					X		M	N			
TPM_ORD_NV_DefineSpace	204	0x000000CC		X	X			X	P			S	N		A	A
TPM_ORD_NV_ReadValue	207	0x000000CF		X	X			X	P	X		S	N		A	A
TPM_ORD_NV_ReadValueAuth	208	0x000000D0		X					P	X		S	N			
TPM_ORD_NV_WriteValue	205	0x000000CD		X	X			X	P	X		S	N		A	A
TPM_ORD_NV_WriteValueAuth	206	0x000000CE		X					P	X		S	N			
TPM_ORD_OIAP	10	0x0000000A			X			X				S			X	X
TPM_ORD_OSAP	11	0x0000000B			X							S			X	X
TPM_ORD_OwnerClear	91	0x0000005B		X							X	S				
TPM_ORD_OwnerReadInternalPub	129	0x00000081		X								S	C			
TPM_ORD_OwnerReadPubek	125	0x0000007D		X							X	S	D			
TPM_ORD_OwnerSetDisable	110	0x0000006E		X							X	S			X	X
TPM_ORD_PCR_Reset	200	0x000000C8			X			X				S	N		X	X
TPM_ORD_PcrRead	21	0x00000015			X			X				S				
TPM_ORD_PhysicalDisable	112	0x00000070			X			X	P		X	S			X	
TPM_ORD_PhysicalEnable	111	0x0000006F			X			X	P		X	S			X	X

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TPM_ORD_PhysicalSetDeactivated	114	0x00000072			X			X	P		X	S			X	
TPM_ORD_Quote	22	0x00000016		X	X					X		M				
TPM_ORD_Quote2	62	0x0000003E		X	X	O				X		M	N			
TPM_ORD_ReadCounter	222	0x000000DE			X			X				S	N			
TPM_ORD_ReadManuMaintPub	48	0x00000030			X	O		X			X	S				
TPM_ORD_ReadPubek	124	0x0000007C			X			X			X	S				
TPM_ORD_ReleaseCounter	223	0x000000DF		X				X				S	N			
TPM_ORD_ReleaseCounterOwner	224	0x000000E0		X								S	N			
TPM_ORD_ReleaseTransportSigned	232	0x000000E8	X	X						X		M	N			
TPM_ORD_Reset	90	0x0000005A			X			X				S	C		X	X
TPM_ORD_ResetLockValue	64	0x00000040		X								S	N			
TPM_ORD_RevokeTrust	128	0x00000080			X	O		X	P			S	N			
TPM_ORD_SaveAuthContext	182	0x000000B6			X	O		X				M	D			
TPM_ORD_SaveContext	184	0x000000B8			X							M	N			
TPM_ORD_SaveKeyContext	180	0x000000B4			X	O		X				M	D			
TPM_ORD_SaveState	152	0x00000098			X			X				M			X	X
TPM_ORD_Seal	23	0x00000017		X						X		M				
TPM_ORD_Sealx	61	0x0000003D		X		O				X		M	N			
TPM_ORD_SelfTestFull	80	0x00000050			X			X				L			X	X
TPM_ORD_SetCapability	63	0x0000003F		X	X			X	P			S	N		X	X
TPM_ORD_SetOperatorAuth	116	0x00000074			X			X	P			S	N			
TPM_ORD_SetOrdinalAuditStatus	141	0x0000008D		X		O					X	S				
TPM_ORD_SetOwnerInstall	113	0x00000071			X			X	P		X	S				
TPM_ORD_SetOwnerPointer	117	0x00000075			X							S	N			
TPM_ORD_SetRedirection	154	0x0000009A		X	X	O			P		X	S				
TPM_ORD_SetTempDeactivated	115	0x00000073		X	X			X	P		X	S				X
TPM_ORD_SHA1Complete	162	0x000000A2			X			X				S			X	X
TPM_ORD_SHA1CompleteExtend	163	0x000000A3			X			X				S			X	X
TPM_ORD_SHA1Start	160	0x000000A0			X			X				S			X	X
TPM_ORD_SHA1Update	161	0x000000A1			X			X				S			X	X
TPM_ORD_Sign	60	0x0000003C		X	X					X		M				
TPM_ORD_Startup	153	0x00000099			X			X				S			X	X

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TPM_ORD_StirRandom	71	0x00000047			X			X				S				
TPM_ORD_TakeOwnership	13	0x0000000D		X				X			X	L			X	
TPM_ORD_Terminate_Handle	150	0x00000096			X			X				S	D		X	X
TPM_ORD_TickStampBlob	242	0x000000F2		X	X					X		M	N			
TPM_ORD_UnBind	30	0x0000001E		X	X					X		M				
TPM_ORD_Unseal	24	0x00000018	X	X						X		M	C			
UNUSED	38	0x00000026														
UNUSED	39	0x00000027														
UNUSED	66	0x00000042														
UNUSED	67	0x00000043														
UNUSED	68	0x00000044														
UNUSED	69	0x00000045														
UNUSED	72	0x00000048														
UNUSED	73	0x00000049														
UNUSED	74	0x0000004A														
UNUSED	75	0x0000004B														
UNUSED	76	0x0000004C														
UNUSED	77	0x0000004D														
UNUSED	78	0x0000004E														
UNUSED	79	0x0000004F														
UNUSED	81	0x00000051														
UNUSED	85	0x00000055														
UNUSED	86	0x00000056														
UNUSED	87	0x00000057														
UNUSED	88	0x00000058														
UNUSED	89	0x00000059														
UNUSED	95	0x0000005F														
UNUSED	96	0x00000060														
UNUSED	97	0x00000061														
UNUSED	98	0x00000062														
UNUSED	99	0x00000063														
UNUSED	103	0x00000067														

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
UNUSED	104	0x00000068														
UNUSED	105	0x00000069														
UNUSED	106	0x0000006A														
UNUSED	107	0x0000006B														
UNUSED	108	0x0000006C														
UNUSED	109	0x0000006D														
UNUSED	118	0x00000076														
UNUSED	119	0x00000077														
UNUSED	132	0x00000084														
UNUSED	135	0x00000087														
UNUSED	136	0x00000088														
UNUSED	137	0x00000089														
UNUSED	138	0x0000008A														
UNUSED	139	0x0000008B														
UNUSED	142	0x0000008E														
UNUSED	143	0x0000008F														
UNUSED	144	0x00000090														
UNUSED	145	0x00000091														
UNUSED	146	0x00000092														
UNUSED	147	0x00000093														
UNUSED	148	0x00000094														
UNUSED	149	0x00000095														
UNUSED	155	0x0000009B														
UNUSED	156	0x0000009C														
UNUSED	157	0x0000009D														
UNUSED	158	0x0000009E														
UNUSED	159	0x0000009F														
UNUSED	164	0x000000A4														
UNUSED	165	0x000000A5														
UNUSED	166	0x000000A6														
UNUSED	167	0x000000A7														
UNUSED	168	0x000000A8														

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
UNUSED	169	0x000000A9														
UNUSED	171	0x000000AB														
UNUSED	172	0x000000AC														
UNUSED	173	0x000000AD														
UNUSED	174	0x000000AE														
UNUSED	175	0x000000AF														
UNUSED	176	0x000000B0														
UNUSED	177	0x000000B1														
UNUSED	178	0x000000B2														
UNUSED	179	0x000000B3														
UNUSED	187	0x000000BB														
UNUSED	188	0x000000BC														
UNUSED	189	0x000000BD														
UNUSED	190	0x000000BE														
UNUSED	191	0x000000BF														
UNUSED	192	0x000000C0														
UNUSED	193	0x000000C1														
UNUSED	194	0x000000C2														
UNUSED	195	0x000000C3														
UNUSED	196	0x000000C4														
UNUSED	197	0x000000C5														
UNUSED	198	0x000000C6														
UNUSED	199	0x000000C7														
UNUSED	202	0x000000CA														
UNUSED	203	0x000000CB														
UNUSED	211	0x000000D3														
UNUSED	215	0x000000D7														
Unused	217	0x000000D9			x							S				
UNUSED	218	0x000000DA														
UNUSED	225	0x000000E1														
UNUSED	233	0x000000E9														
UNUSED	234	0x000000EA														

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	Physical Presence	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
UNUSED	235	0x000000EB														
UNUSED	236	0x000000EC														
UNUSED	237	0x000000ED														
UNUSED	238	0x000000EE														
UNUSED	239	0x000000EF														
UNUSED	240	0x000000F0														
UNUSED	201	0x00000C9														

2084 17.1 TSC Ordinals

2085 **Start of informative comment**

2086 The TSC ordinals are optional in the main specification. They are mandatory in the PC
2087 Client specification.

2088 **End of informative comment**

2089 The connection commands manage the TPM's connection to the TBB.

	TPM_PROTECTED_ORDINAL +	Complete ordinal	AUTH2	AUTH1	RQU	Optional		No Owner	PCR Use enforced	Audit	Duration	Changes 1.2	FIPS Changes	Avail Deactivated	Avail Disabled
TSC_ORD_PhysicalPresence	10	0x4000000A			X	O		X			S	C		X	X
TSC_ORD_ResetEstablishmentBit	11	0x4000000B			X	O		X			S	N		X	X

18. Context structures

18.1 TPM_CONTEXT_BLOB

Start of informative comment

This is the header for the wrapped context. The blob contains all information necessary to reload the context back into the TPM.

The additional data is used by the TPM manufacturer to save information that will assist in the reloading of the context. This area must not contain any shielded data. For instance, the field could contain some size information that allows the TPM more efficient loads of the context. The additional area could not contain one of the primes for a RSA key.

To ensure integrity of the blob when using symmetric encryption the TPM vendor could use some valid cipher chaining mechanism. To ensure the integrity without depending on correct implementation, the TPM_CONTEXT_BLOB structure uses a HMAC of the entire structure using tpmProof as the secret value.

Since both additionalData and sensitiveData are informative, any or all of additionalData could be moved to sensitiveData.

End of informative comment

Definition

```
typedef struct tdTPM_CONTEXT_BLOB {
   TPM_STRUCTURE_TAG tag;
   TPM_RESOURCE_TYPE resourceType;
   TPM_HANDLE handle;
   BYTE[16] label;
   UINT32 contextCount;
   TPM_DIGEST integrityDigest;
   UINT32 additionalSize;
   [size_is(additionalSize)] BYTE* additionalData;
   UINT32 sensitiveSize;
   [size_is(sensitiveSize)] BYTE* sensitiveData;
}TPM_CONTEXT_BLOB;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_CONTEXTBLOB
TPM_RESOURCE_TYPE	resourceType	The resource type
TPM_HANDLE	handle	Previous handle of the resource
BYTE[16]	label	Label for identification of the blob. Free format area.
UINT32	contextCount	MUST be TPM_STANY_DATA -> contextCount when creating the structure. This value is ignored for context blobs that reference a key.
TPM_DIGEST	integrityDigest	The integrity of the entire blob including the sensitive area. This is a HMAC calculation with the entire structure (including sensitiveData) being the hash and tpmProof is the secret

Type	Name	Description
UINT32	additionalSize	The size of additionalData
BYTE*	additionalData	Additional information set by the TPM that helps define and reload the context. The information held in this area MUST NOT expose any information held in shielded locations. This should include any IV for symmetric encryption
UINT32	sensitiveSize	The size of sensitiveData
BYTE*	sensitiveData	The normal information for the resource that can be exported

18.2 TPM_CONTEXT_SENSITIVE

Start of informative comment

The internal areas that the TPM needs to encrypt and store off the TPM.

This is an informative structure and the TPM can implement in any manner they wish.

End of informative comment

Definition

```
typedef struct tdTPM_CONTEXT_SENSITIVE {
   TPM_STRUCTURE_TAG tag;
   TPM_NONCE contextNonce;
   UINT32 internalSize;
   [size_is(internalSize)] BYTE* internalData;
}TPM_CONTEXT_SENSITIVE;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_CONTEXT_SENSITIVE
TPM_NONCE	contextNonce	On context blobs other than keys this MUST be TPM_STANY_DATA -> contextNonceSession For keys the value is TPM_STCLEAR_DATA -> contextNonceKey
UINT32	internalSize	The size of the internalData area
BYTE*	internalData	The internal data area

2133 19. NV storage structures

2134 19.1 TPM_NV_INDEX

2135 **Start of informative comment**

2136 The index provides the handle to identify the area of storage. The reserved bits allow for a
2137 segregation of the index name space to avoid name collisions.

2138 The TPM may check the 'resvd' bits for zero. Thus, applications should set the bits to zero.

2139 The TCG defines the space where the high order bits (T, P, U) are 0. The other spaces are
2140 controlled by the indicated entity.

2141 T is the TPM manufacturer reserved bit. 0 indicates a TCG defined value. 1 indicates a TPM
2142 manufacturer specific value.

2143 P is the platform manufacturer reserved bit. 0 indicates a TCG defined value. 1 indicates
2144 that the index is controlled by the platform manufacturer.

2145 U is for the platform user. 0 indicates a TCG defined value. 1 indicates that the index is
2146 controlled by the platform user.

2147 **End of informative comment**

2148 The TPM_NV_INDEX is a 32-bit value.

```
2149          3                   2                   1
2150       1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
2151      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
2152      |T|P|U|D| resvd |   Purview     |          Index                |
2153      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2154 **Where:**

21551. The TPM MAY return an error if the resvd bits are not set to 0.

21562. The TPM MUST accept all values for T, P, and U

21573. D indicates defined. 1 indicates that the index is permanently defined and that any
2158 TPM_NV_DefineSpace operation will fail after nvLocked is set TRUE.

2159 a. TCG reserved areas MAY have D set to 0 or 1

21604. Purview is the value used to indicate the platform specific area. This value is the same
2161 purview as uses for command ordinals.

2162 a. The TPM MUST accept purview 0, TPM_MAIN.

2163 b. The TPM MUST reject purview values that the TPM cannot support. This means that
2164 an index value for a PDA MUST be rejected by a TPM designed to work only on the
2165 PC Client.

19.1.1 Required TPM_NV_INDEX values

Start of informative comment

The required index values must be found on each TPM regardless of platform. These areas are always present and do not require a TPM_NV_DefineSpace command to allocate.

A platform specific specification may add additional required index values for the platform.

End of informative comment

1. The TPM MUST reserve the space as indicated for the required index values

Required Index values

Value	Index Name	Default Size	Attributes
0xFFFFFFFF	TPM_NV_INDEX_LOCK	This value turns on the NV authorization protections. Once executed all NV areas us the protections as defined. This value never resets. Attempting to execute TPM_NV_DefineSpace on this value with non-zero size MAY result in a TPM_BADINDEX response.	None
0x00000000	TPM_NV_INDEX0	This value allows for the setting of the bGlobalLock flag, which is only reset on TPM_Startup(ST_Clear) Attempting to execute TPM_NV_WriteValue with a size other than zero MAY result in the TPM_BADINDEX error code.	None
0x10000001	TPM_NV_INDEX_DIR	Size MUST be 20. This index points to the deprecated DIR command area from 1.1. The TPM MUST map this reserved space to be the area operated on by the 1.1 DIR commands. As the DIR commands are deprecated any additional DIR functionally MUST use the NV commands and not the DIR command. Attempts to execute TPM_NV_DefineSpace with this index MUST result in TPM_BADINDEX	TPM_NV_PER_OWNERWRITE TPM_NV_PER_WRITEALL

2174 19.1.2 Reserved Index values

2175**Start of informative comment**

2176The reserved values are defined to avoid index collisions. These values are not in each and
2177every TPM.

2178**End of informative comment**

21791. The reserved index values are to avoid index value collisions.

21802. These index values require a TPM_NV_DefineSpace to have the area for the index
2181 allocated

21823. A platform specific specification MAY indicate that reserved values are required.

21834. The reserved index values MAY have their D bit set by the TPM vendor to permanently
2184 reserve the index in the TPM

Value	Event Name	Default Size
0x0000Fxxx	TPM_NV_INDEX_TPM	Reserved for TPM use
0x0000F000	TPM_NV_INDEX_EKCert	The Endorsement credential
0x0000F001	TPM_NV_INDEX_TPM_CC	The TPM Conformance credential
0x0000F002	TPM_NV_INDEX_PlatformCert	The platform credential
0x0000F003	TPM_NV_INDEX_Platform_CC	The Platform conformance credential
0x0000F004	TPM_NV_INDEX_TRIAL	To try TPM_NV_DefineSpace without actually allocating NV space
0x0001xxxx	TPM_NV_INDEX_PC	Reserved for PC Client use
0x000116xx	TPM_NV_INDEX_GPIO_xx	Reserved for GPIO pins
0x0002xxxx	TPM_NV_INDEX_PDA	Reserved for PDA use
0x0003xxxx	TPM_NV_INDEX_MOBILE	Reserved for mobile use
0x0004xxxx	TPM_NV_INDEX_SERVER	Reserved for Server use
0x0005xxxx	TPM_NV_INDEX_PERIPHERAL	Reserved for peripheral use
0x0006xxxx	TPM_NV_INDEX_TSS	Reserved for TSS use
0x00xxxxxx	TPM_NV_INDEX_GROUP_RESV	Reserved for TCG WG's

19.2 TPM_NV_ATTRIBUTES

Start of informative comment

This structure allows the TPM to keep track of the data and permissions to manipulate the area.

A write once per lifetime of the TPM attribute, while attractive, is simply too dangerous (attacker allocates all of the NV area and uses it). The locked attribute adds close to that functionality. This allows the area to be "locked" and only changed when unlocked. The lock bit would be set for all indexes sometime during the initialization of a platform. The use model would be that the platform BIOS would lock the TPM and only allow changes in the BIOS setup routine.

There are no locality bits to allow for a locality to define space. The rationale behind this is that the define space includes the permissions so that would mean any locality could define space. The use model for localities would assume that the platform owner was opting into the use of localities and would define the space necessary to operate when the opt-in was authorized.

The attributes TPM_NV_PER_AUTHREAD and TPM_NV_PER_OWNERREAD cannot both be set to TRUE. Similarly, the attributes TPM_NV_PER_AUTHWRITE and TPM_NV_PER_OWNERWRITE cannot both be set to TRUE.

End of informative comment

Definition

```
typedef struct tdTPM_NV_ATTRIBUTES{
  TPM_STRUCTURE_TAG tag;
  UINT32 attributes;
} TPM_NV_ATTRIBUTES;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	TPM_TAG_NV_ATTRIBUTES
UINT32	attributes	The attribute area

Attributes values

Bit	Name	Description
31	TPM_NV_PER_READ_STCLEAR	The value can be read until locked by a read with a data size of 0. It can only be unlocked by TPM_Startup(ST_Clear) or a successful write. Lock held for each area in bReadSTClear.
30:19	Reserved	
18	TPM_NV_PER_AUTHREAD	The value requires authorization to read
17	TPM_NV_PER_OWNERREAD	The value requires TPM Owner authorization to read.
16	TPM_NV_PER_PPREAD	The value requires physical presence to read
15	TPM_NV_PER_GLOBALLOCK	The value is writable until a write to index 0 is successful. The lock of this attribute is reset by TPM_Startup(ST_CLEAR). Lock held by SF -> bGlobalLock

Bit	Name	Description
14	TPM_NV_PER_WRITE_STCLEAR	The value is writable until a write to the specified index with a datasize of 0 is successful. The lock of this attribute is reset by TPM_Startup(ST_CLEAR). Lock held for each area in bWriteSTClear.
13	TPM_NV_PER_WRITEDEFINE	Lock set by writing to the index with a datasize of 0. Lock held for each area in bWriteDefine. This is a persistent lock.
12	TPM_NV_PER_WRITEALL	The value must be written in a single operation
11:3	Reserved for write additions	
2	TPM_NV_PER_AUTHWRITE	The value requires authorization to write
1	TPM_NV_PER_OWNERWRITE	The value requires TPM Owner authorization to write
0	TPM_NV_PER_PPWRITE	The value requires physical presence to write

2211 19.3 TPM_NV_DATA_PUBLIC

2212**Start of informative comment**

2213This structure represents the public description and controls on the NV area.

2214bReadSTClear and bWriteSTClear are volatile, in that they are set FALSE at 2215TPM_Startup(ST_Clear). bWriteDefine is persistent, in that it remains TRUE through 2216startup.

2217A pcrSelect of 0 indicates that the digestAsRelease is not checked. In this case, the TPM is 2218not required to consume NVRAM space to store the digest, although it may do so. When 2219TPM_GetCapability (TPM_CAP_NV_INDEX) returns the structure, a TPM that does not store 2220the digest can return zero. A TPM that does store the digest may return either the digest or 2221zero. Software should not be written to depend on either implementation.

2222**End of informative comment**

2223Definition

```
2224typedef struct tdTPM_NV_DATA_PUBLIC {
2225   TPM_STRUCTURE_TAG tag;
2226   TPM_NV_INDEX nvIndex;
2227   TPM_PCR_INFO_SHORT pcrInfoRead;
2228   TPM_PCR_INFO_SHORT pcrInfoWrite;
2229   TPM_NV_ATTRIBUTES permission;
2230   BOOL bReadSTClear;
2231   BOOL bWriteSTClear;
2232   BOOL bWriteDefine;
2233   UINT32 dataSize;
2234} TPM_NV_DATA_PUBLIC;
```

2235Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_NV_DATA_PUBLIC
TPM_NV_INDEX	nvIndex	The index of the data area
TPM_PCR_INFO_SHORT	pcrInfoRead	The PCR selection that allows reading of the area
TPM_PCR_INFO_SHORT	pcrInfoWrite	The PCR selection that allows writing of the area
TPM_NV_ATTRIBUTES	permission	The permissions for manipulating the area
BOOL	bReadSTClear	Set to FALSE on each TPM_Startup(ST_Clear) and set to TRUE after a ReadValuexxx with datasize of 0
BOOL	bWriteSTClear	Set to FALSE on each TPM_Startup(ST_CLEAR) and set to TRUE after a WriteValuexxx with a datasize of 0.
BOOL	bWriteDefine	Set to FALSE after TPM_NV_DefineSpace and set to TRUE after a successful WriteValuexxx with a datasize of 0
UINT32	dataSize	The size of the data area in bytes

2236Actions

22371. On read of this structure (through TPM_GetCapability) if pcrInfoRead -> pcrSelect is 0 2238 then pcrInfoRead -> digestAtRelease MAY be 0x00…00

22392. On read of this structure (through TPM_GetCapability) if pcrInfoWrite -> pcrSelect is 0
2240 then pcrInfoWrite -> digestAtRelease MAY be 0x00…00

19.4 TPM_NV_DATA_SENSITIVE

Start of informative comment

This is an internal structure that the TPM uses to keep the actual NV data and the controls regarding the area.

This entire section is informative

End of informative comment

Definition

```
typedef struct tdTPM_NV_DATA_SENSITIVE {
   TPM_STRUCTURE_TAG tag;
   TPM_NV_DATA_PUBLIC pubInfo;
   TPM_AUTHDATA authValue;
   [size_is(dataSize)] BYTE* data;
} TPM_NV_DATA_SENSITIVE;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_NV_DATA_SENSITIVE
TPM_NV_DATA_PUBLIC	pubInfo	The public information regarding this area
TPM_AUTHDATA	authValue	The AuthData value to manipulate the value
BYTE*	data	The data area. This MUST not contain any sensitive information as the TPM does not provide any confidentiality on the data.

2255 19.5 Max NV Size

2256The value TPM_MAX_NV_SIZE is a value where the minimum value is set by the platform
2257specific specification. The TPM vendor can design a TPM with a size that is larger than the
2258minimum.

2259 19.6 TPM_NV_DATA_AREA

2260**Start of informative comment**

2261TPM_NV_DATA_AREA is an indication of the internal structure the TPM uses to track NV
2262areas. The structure definition is TPM vendor specific and never leaves the TPM. The
2263structure would contain both the TPM_NV_DATA_PUBLIC and TPM_NV_DATA_SENSITIVE
2264areas.

2265**End of informative comment**

20. Delegate Structures

20.1 Structures and encryption

Start of informative comment

The TPM is responsible for encrypting various delegation elements when stored off the TPM. When the structures are TPM internal structures and not in use by any other process (i.e. TPM_DELEGATE_SENSITIVE) the structure is merely an informative comment as to the information necessary to make delegation work. The TPM may put additional, or possibly, less information into the structure and still obtain the same result.

Where the structures are in use across TPM's or in use by outside processes (i.e. TPM_DELEGATE_PUBLIC) the structure is normative and the must use the structure without modification.

End of informative comment

1. The TPM MUST provide encryption of sensitive areas held outside of the TPM. The encryption MUST be comparable to AES 128-bit key.

20.2 Delegate Definitions

Informative comment

The delegations are in a 64-bit field. Each bit describes a capability that the TPM Owner or an authorized key user can delegate to a trusted process by setting that bit. Each delegation bit setting is independent of any other delegation bit setting in a row.

If a TPM command is not listed in the following table, then the TPM Owner or the key user cannot delegate that capability to a trusted process. For the TPM commands that are listed in the following table, if the bit associated with a TPM command is set to zero in the row of the table that identifies a trusted process, then that process has not been delegated to use that TPM command.

The minimum granularity for delegation is at the ordinal level. It is not possible to delegate an option of an ordinal. This implies that if the options present a difficulty and there is a need to separate the delegations then there needs to be a split into two separate ordinals.

End of informative comment

```
#define TPM_DEL_OWNER_BITS 0x00000001
#define TPM_DEL_KEY_BITS  0x00000002

typedef struct tdTPM_DELEGATIONS{
   TPM_STRUCTURE_TAG tag;
   UINT32 delegateType;
   UINT32 per1;
   UINT32 per2;
} TPM_DELEGATIONS;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_DELEGATIONS
UINT32	delegateType	Owner or key
UNIT32	per1	The first block of permissions
UINT32	per2	The second block of permissions

2304 20.2.1 Owner Permission Settings

2305**Informative comment**

2306This section is going to remove any ambiguity as to the order of bits in the permission array

2307**End of informative comment**

2308 Per1 bits

Bit Number	Ordinal	Bit Name
31	TPM_ORD_KeyControlOwner	TPM_DELEGATE_KeyControlOwner
30	TPM_ORD_SetOrdinalAuditStatus	TPM_DELEGATE_SetOrdinalAuditStatus
29	TPM_ORD_DirWriteAuth	TPM_DELEGATE_DirWriteAuth
28	TPM_ORD_CMK_ApproveMA	TPM_DELEGATE_CMK_ApproveMA
27	TPM_ORD_NV_WriteValue	TPM_DELEGATE_NV_WriteValue
26	TPM_ORD_CMK_CreateTicket	TPM_DELEGATE_CMK_CreateTicket
25	TPM_ORD_NV_ReadValue	TPM_DELEGATE_NV_ReadValue
24	TPM_ORD_Delegate_LoadOwnerDelegation	TPM_DELEGATE_Delegate_LoadOwnerDelegation
23	TPM_ORD_DAA_Join	TPM_DELEGATE_DAA_Join
22	TPM_ORD_AuthorizeMigrationKey	TPM_DELEGATE_AuthorizeMigrationKey
21	TPM_ORD_CreateMaintenanceArchive	TPM_DELEGATE_CreateMaintenanceArchive
20	TPM_ORD_LoadMaintenanceArchive	TPM_DELEGATE_LoadMaintenanceArchive
19	TPM_ORD_KillMaintenanceFeature	TPM_DELEGATE_KillMaintenanceFeature
18	TPM_ORD_OwnerReadInternalPub	TPM_DELEGATE_OwnerReadInternalPub
17	TPM_ORD_ResetLockValue	TPM_DELEGATE_ResetLockValue
16	TPM_ORD_OwnerClear	TPM_DELEGATE_OwnerClear
15	TPM_ORD_DisableOwnerClear	TPM_DELEGATE_DisableOwnerClear
14	TPM_ORD_NV_DefineSpace	TPM_DELEGATE_NV_DefineSpace
13	TPM_ORD_OwnerSetDisable	TPM_DELEGATE_OwnerSetDisable
12	TPM_ORD_SetCapability	TPM_DELEGATE_SetCapability
11	TPM_ORD_MakeIdentity	TPM_DELEGATE_MakeIdentity
10	TPM_ORD_ActivateIdentity	TPM_DELEGATE_ActivateIdentity
9	TPM_ORD_OwnerReadPubek	TPM_DELEGATE_OwnerReadPubek
8	TPM_ORD_DisablePubekRead	TPM_DELEGATE_DisablePubekRead
7	TPM_ORD_SetRedirection	TPM_DELEGATE_SetRedirection
6	TPM_ORD_FieldUpgrade	TPM_DELEGATE_FieldUpgrade
5	TPM_ORD_Delegate_UpdateVerification	TPM_DELEGATE_Delegate_UpdateVerification
4	TPM_ORD_CreateCounter	TPM_DELEGATE_CreateCounter
3	TPM_ORD_ReleaseCounterOwner	TPM_DELEGATE_ReleaseCounterOwner
2	TPM_ORD_Delegate_Manage	TPM_DELEGATE_Delegate_Manage
1	TPM_ORD_Delegate_CreateOwnerDelegation	TPM_DELEGATE_Delegate_CreateOwnerDelegation
0	TPM_ORD_DAA_Sign	TPM_DELEGATE_DAA_Sign

2309**Per2 bits**

Bit Number	Ordinal	Bit Name
31:0	Reserved	Reserved MUST be 0

2310 20.2.2 Owner commands not delegated

2311**Start of informative comment**

2312Not all TPM Owner authorized commands can be delegated. The following table lists those 2313commands the reason why the command is not delegated.

2314**End of informative comment**

Command	Rationale
TPM_ChangeAuthOwner	Delegating change owner allows the delegatee to control the TPM Owner. This implies that the delegate has more control than the owner. The owner can create the same situation by merely having the process that the owner wishes to control the TPM to perform ChangeOwner with the current owners permission.
TPM_TakeOwnership	If you don't have an owner how can the current owner delegate the command.
TPM_CMK_SetRestrictions	This command allows the owner to restrict what processes can be delegated the ability to create and manipulate CMK keys
TPM_GetCapabilityOwner	This command is deprecated. Its only purpose is to find out/verify the owner password correctness, Therefore it makes no sense to delegate it.

20.2.3 Key Permission settings

Informative comment

This section is going to remove any ambiguity as to the order of bits in the permission array

End of informative comment

Per1 bits

Bit Number	Ordinal	Bit Name
31:29	Reserved	Reserved MUST be 0
28	TPM_ORD_CMK_ConvertMigration	TPM_KEY_DELEGATE_CMK_ConvertMigration
27	TPM_ORD_TickStampBlob	TPM_KEY_DELEGATE_TickStampBlob
26	TPM_ORD_ChangeAuthAsymStart	TPM_KEY_DELEGATE_ChangeAuthAsymStart
25	TPM_ORD_ChangeAuthAsymFinish	TPM_KEY_DELEGATE_ChangeAuthAsymFinish
24	TPM_ORD_CMK_CreateKey	TPM_KEY_DELEGATE_CMK_CreateKey
23	TPM_ORD_MigrateKey	TPM_KEY_DELEGATE_MigrateKey
22	TPM_ORD_LoadKey2	TPM_KEY_DELEGATE_LoadKey2
21	TPM_ORD_EstablishTransport	TPM_KEY_DELEGATE_EstablishTransport
20	TPM_ORD_ReleaseTransportSigned	TPM_KEY_DELEGATE_ReleaseTransportSigned
19	TPM_ORD_Quote2	TPM_KEY_DELEGATE_Quote2
18	TPM_ORD_Sealx	TPM_KEY_DELEGATE_Sealx
17	TPM_ORD_MakeIdentity	TPM_KEY_DELEGATE_MakeIdentity
16	TPM_ORD_ActivateIdentity	TPM_KEY_DELEGATE_ActivateIdentity
15	TPM_ORD_GetAuditDigestSigned	TPM_KEY_DELEGATE_GetAuditDigestSigned
14	TPM_ORD_Sign	TPM_KEY_DELEGATE_Sign
13	TPM_ORD_CertifyKey2	TPM_KEY_DELEGATE_CertifyKey2
12	TPM_ORD_CertifyKey	TPM_KEY_DELEGATE_CertifyKey
11	TPM_ORD_CreateWrapKey	TPM_KEY_DELEGATE_CreateWrapKey
10	TPM_ORD_CMK_CreateBlob	TPM_KEY_DELEGATE_CMK_CreateBlob
9	TPM_ORD_CreateMigrationBlob	TPM_KEY_DELEGATE_CreateMigrationBlob
8	TPM_ORD_ConvertMigrationBlob	TPM_KEY_DELEGATE_ConvertMigrationBlob
7	TPM_ORD_Delegate_CreateKeyDelegation	TPM_KEY_DELEGATE_Delegate_CreateKeyDelegation
6	TPM_ORD_ChangeAuth	TPM_KEY_DELEGATE_ChangeAuth
5	TPM_ORD_GetPubKey	TPM_KEY_DELEGATE_GetPubKey
4	TPM_ORD_UnBind	TPM_KEY_DELEGATE_UnBind
3	TPM_ORD_Quote	TPM_KEY_DELEGATE_Quote
2	TPM_ORD_Unseal	TPM_KEY_DELEGATE_Unseal
1	TPM_ORD_Seal	TPM_KEY_DELEGATE_Seal
0	TPM_ORD_LoadKey	TPM_KEY_DELEGATE_LoadKey

TCG Published

Per2 bits

Bit Number	Ordinal	Bit Name
31:0	Reserved	Reserved MUST be 0

20.2.4 Key commands not delegated

Start of informative comment

Not all TPM key commands can be delegated. The following table lists those commands the reason why the command is not delegated.

End of informative comment

Command	Rationale
None	
TPM_CertifySelfTest	This command has a security hole and is deleted

2326 20.3 TPM_FAMILY_FLAGS

2327 **Start of informative comment**

2328 These flags indicate the operational state of the delegation and family table. These flags are
2329 additions to TPM_PERMANENT_FLAGS and are not standalone values.

2330 **End of informative comment**

2331 TPM_FAMILY_FLAGS bit settings

Bit Number	Bit Name	Comments
31:2	Reserved MUST be 0	
1	TPM_DELEGATE_ADMIN_LOCK	TRUE: Some TPM_Delegate_XXX commands are locked and return TPM_DELEGATE_LOCK FALSE: TPM_Delegate_XXX commands are available Default is FALSE
0	TPM_FAMFLAG_ENABLED	When TRUE the table is enabled. The default value is FALSE.

20.4 TPM_FAMILY_LABEL

Start of informative comment

Used in the family table to hold a one-byte numeric value (sequence number) that software can map to a string of bytes that can be displayed or used by applications.

This is not sensitive data.

End of informative comment

```
typedef struct tdTPM_FAMILY_LABEL{
   BYTE label;
} TPM_FAMILY_LABEL;
```

Parameters

Type	Name	Description
BYTE	label	A sequence number that software can map to a string of bytes that can be displayed or used by the applications. This MUST not contain sensitive information.

20.5 TPM_FAMILY_TABLE_ENTRY

Start of informative comment

The family table entry is an individual row in the family table. There are no sensitive values in a family table entry.

Each family table entry contains values to facilitate table management: the familyID sequence number value that associates a family table row with one or more delegate table rows, a verification sequence number value that identifies when rows in the delegate table were last verified, and a BYTE family label value that software can map to an ASCII text description of the entity using the family table entry

End of informative comment

```
typedef struct tdTPM_FAMILY_TABLE_ENTRY{
  TPM_STRUCTURE_TAG tag;
  TPM_FAMILY_LABEL familyLabel;
  TPM_FAMILY_ID familyID;
  TPM_FAMILY_VERIFICATION verificationCount;
  TPM_FAMILY_FLAGS flags;
} TPM_FAMILY_TABLE_ENTRY;
```

Description

The default value of all fields in a family row at TPM manufacture SHALL be null.

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_FAMILY_TABLE_ENTRY
TPM_FAMILY_LABEL	familyLabel	A sequence number that software can map to a string of bytes that can be displayed or used by the applications. This MUST not contain sensitive information.
TPM_FAMILY_ID	familyID	The family ID in use to tie values together. This is not a sensitive value.
TPM_FAMILY_VERIFICATION	verificationCount	The value inserted into delegation rows to indicate that they are the current generation of rows. Used to identify when a row in the delegate table was last verified. This is not a sensitive value.
TPM_FAMILY_FLAGS	flags	See section on TPM_FAMILY_FLAGS.

20.6 TPM_FAMILY_TABLE

Start of informative comment

The family table is stored in a TPM shielded location. There are no confidential values in the family table. The family table contains a minimum of 8 rows.

End of informative comment

```
#define TPM_NUM_FAMILY_TABLE_ENTRY_MIN 8

typedef struct tdTPM_FAMILY_TABLE{
   TPM_FAMILY_TABLE_ENTRY famTableRow[TPM_NUM_FAMILY_TABLE_ENTRY_MIN];
} TPM_FAMILY_TABLE;
```

Parameters

Type	Name	Description
TPM_FAMILY_TABLE_ENTRY	famTableRow	The array of family table entries

2373 20.7 TPM_DELEGATE_LABEL

2374**Start of informative comment**

2375Used in the delegate table to hold a byte that can be displayed or used by applications. This
2376is not sensitive data.

2377**End of informative comment**

```
2378typedef struct tdTPM_DELEGATE_LABEL{
2379   BYTE label;
2380} TPM_DELEGATE_LABEL;
```

2381**Parameters**

Type	Name	Description
BYTE	label	A byte that can be displayed or used by the applications. This MUST not contain sensitive information.

20.8 TPM_DELEGATE_PUBLIC

Start of informative comment

The information of a delegate row that is public and does not have any sensitive information.

TPM_PCR_INFO_SHORT is appropriate here as the command to create this is done using owner authorization, hence the owner authorized the command and the delegation. There is no need to validate what configuration was controlling the platform during the blob creation.

End of informative comment

```
typedef struct tdTPM_DELEGATE_PUBLIC{
   TPM_STRUCTURE_TAG tag;
   TPM_DELEGATE_LABEL rowLabel;
   TPM_PCR_INFO_SHORT pcrInfo;
   TPM_DELEGATIONS permissions;
   TPM_FAMILY_ID familyID;
   TPM_FAMILY_VERIFICATION verificationCount
} TPM_DELEGATE_PUBLIC;
```

Description

The default value of all fields of a delegate row at TPM manufacture SHALL be null. The table MUST NOT contain any sensitive information.

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_DELEGATE_PUBLIC
TPM_DELEGATE_LABEL	rowlabel	This SHALL be the label for the row. It MUST not contain any sensitive information.
TPM_PCR_INFO_SHORT	pcrInfo	This SHALL be the designation of the process that can use the permission. This is a not sensitive value. PCR_SELECTION may be NULL. If selected the pcrInfo MUST be checked on each use of the delegation. Use of the delegation is where the delegation is passed as an authorization handle.
TPM_DELEGATIONS	permissions	This SHALL be the permissions that are allowed to the indicated process. This is not a sensitive value.
TPM_FAMILY_ID	familyID	This SHALL be the family ID that identifies which family the row belongs to. This is not a sensitive value.
TPM_FAMILY_VERIFICATION	verificationCount	A copy of verificationCount from the associated family table. This is not a sensitive value.

2403 20.9 TPM_DELEGATE_TABLE_ROW

2404**Start of informative comment**

2405A row of the delegate table.

2406**End of informative comment**

```
2407typedef struct tdTPM_DELEGATE_TABLE_ROW{
2408   TPM_STRUCTURE_TAG tag;
2409   TPM_DELEGATE_PUBLIC pub;
2410   TPM_SECRET authValue;
2411} TPM_DELEGATE_TABLE_ROW;
```

2412 Description

2413The default value of all fields of a delegate row at TPM manufacture SHALL be empty

2414 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This SHALL be TPM_TAG_DELEGATE_TABLE_ROW
TPM_DELEGATE_PUBLIC	pub	This SHALL be the public information for a table row.
TPM_SECRET	authValue	This SHALL be the AuthData value that can use the permissions. This is a sensitive value.

20.10 TPM_DELEGATE_TABLE

Start of informative comment

This is the delegate table. The table contains a minimum of 2 rows.

This will be an entry in the TPM_PERMANENT_DATA structure.

End of informative comment

```
#define TPM_NUM_DELEGATE_TABLE_ENTRY_MIN 2

typedef struct tdTPM_DELEGATE_TABLE{
   TPM_DELEGATE_TABLE_ROW delRow[TPM_NUM_DELEGATE_TABLE_ENTRY_MIN];
} TPM_DELEGATE_TABLE;
```

Parameters

Type	Name	Description
TPM_DELEGATE_TABLE_ROW	delRow	The array of delegations

2426 20.11 TPM_DELEGATE_SENSITIVE

2427 **Start of informative comment**

2428 The TPM_DELEGATE_SENSITIVE structure is the area of a delegate blob that contains
2429 sensitive information.

2430 This structure is normative for loading unencrypted blobs before there is an owner. It is
2431 informative for TPM_CreateOwnerDelegation and TPM_LoadOwnerDelegation after there is
2432 an owner and encrypted blobs are used, since the structure is under complete control of the
2433 TPM.

2434 **End of informative comment**

```
2435 typedef struct tdTPM_DELEGATE_SENSITIVE {
2436   TPM_STRUCTURE_TAG tag;
2437   TPM_SECRET authValue;
2438 } TPM_DELEGATE_SENSITIVE;
```

2439 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This MUST be TPM_TAG_DELEGATE_SENSITIVE
TPM_SECRET	authValue	AuthData value

20.12 TPM_DELEGATE_OWNER_BLOB

Start of informative comment

This data structure contains all the information necessary to externally store a set of owner delegation rights that can subsequently be loaded or used by this TPM.

The encryption mechanism for the sensitive area is a TPM choice. The TPM may use asymmetric encryption and the SRK for the key. The TPM may use symmetric encryption and a secret key known only to the TPM.

End of informative comment

```
typedef struct tdTPM_DELEGATE_OWNER_BLOB{
  TPM_STRUCTURE_TAG tag;
  TPM_DELEGATE_PUBLIC pub;
  TPM_DIGEST integrityDigest;
  UINT32 additionalSize;
  [size_is(additionalSize)] BYTE* additionalArea;
  UINT32 sensitiveSize;
  [size_is(sensitiveSize)] BYTE* sensitiveArea;
} TPM_DELEGATE_OWNER_BLOB;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This MUST be TPM_TAG_DELEGATE_OWNER_BLOB
TPM_DELEGATE_PUBLIC	pub	The public information for this blob
TPM_DIGEST	integrityDigest	The HMAC to guarantee the integrity of the entire structure
UINT32	additionalSize	The size of additionalArea
BYTE*	additionalArea	An area that the TPM can add to the blob which MUST NOT contain any sensitive information. This would include any IV material for symmetric encryption
UINT32	sensitiveSize	The size of the sensitive area
BYTE*	sensitiveArea	The area that contains the encrypted TPM_DELEGATE_SENSITIVE

2458 20.13 TPM_DELEGATE_KEY_BLOB

2459 **Start of informative comment**

2460 A structure identical to TPM_DELEGATE_OWNER_BLOB but which stores delegation
2461 information for user keys. As compared to TPM_DELEGATE_OWNER_BLOB, it adds a hash
2462 of the corresponding public key value to the public information.

2463 **End of informative comment**

```
2464 typedef struct tdTPM_DELEGATE_KEY_BLOB{
2465   TPM_STRUCTURE_TAG tag;
2466   TPM_DELEGATE_PUBLIC pub;
2467   TPM_DIGEST integrityDigest;
2468   TPM_DIGEST pubKeyDigest;
2469   UINT32 additionalSize;
2470   [size_is(additionalSize)] BYTE* additionalArea;
2471   UINT32 sensitiveSize;
2472   [size_is(sensitiveSize)] BYTE* sensitiveArea;
2473 } TPM_DELEGATE_KEY_BLOB;
```

2474 **Parameters**

Type	Name	Description
TPM_STRUCTURE_TAG	tag	This MUST be TPM_TAG_DELG_KEY_BLOB
TPM_DELEGATE_PUBLIC	pub	The public information for this blob
TPM_DIGEST	integrityDigest	The HMAC to guarantee the integrity of the entire structure
TPM_DIGEST	pubKeyDigest	The digest, that uniquely identifies the key for which this usage delegation applies. This is a hash of the TPM_STORE_PUBKEY structure.
UINT32	additionalSize	The size of the integrity area
BYTE*	additionalArea	An area that the TPM can add to the blob which MUST NOT contain any sensitive information. This would include any IV material for symmetric encryption
UINT32	sensitiveSize	The size of the sensitive area
BYTE*	sensitiveArea	The area that contains the encrypted TPM_DELEGATE_SENSITIVE

2475 20.14 TPM_FAMILY_OPERATION Values

2476**Start of informative comment**

2477These are the opFlag values used by TPM_Delegate_Manage.

2478**End of informative comment**

Value	Capability Name	Comments
0x00000001	TPM_FAMILY_CREATE	Create a new family
0x00000002	TPM_FAMILY_ENABLE	Set or reset the enable flag for this family.
0x00000003	TPM_FAMILY_ADMIN	Prevent administration of this family.
0x00000004	TPM_FAMILY_INVALIDATE	Invalidate a specific family row.

2479 21. Capability areas

2480 21.1 TPM_CAPABILITY_AREA for TPM_GetCapability

2481 **Start of informative comment**

2482 The TPM needs to provide to outside entities various pieces of information regarding the
2483 design and current state of the TPM. The process works by first supplying an area to look at
2484 and then optionally a refinement to further indicate the type of information requested. The
2485 documents use the terms capability and subCap to indicate the area and subarea in
2486 question.

2487 Some capabilities have a single purpose and the subCap is either ignored or supplies a
2488 handle or other generic piece of information.

2489 The following table contains both the values for the capabilities but also the sub
2490 capabilities. When providing the value for a subCap it appears in the capability name slot.

2491 **End of informative comment**

2492 1. For the capability TPM_CAP_AUTH_ENCRYPT, the response to the sub cap
2493 TPM_ALGORITHM_ID is as follows:

2494 a. TPM_ALG_AES128 returns TRUE if OSAP supports TPM_ET_AES128_CTR.

2495 b. TPM_ALG_XOR returns TRUE if OSAP supports TPM_ET_XOR.

2496 c. The above are the only ADIP encryption entity types supported.

2497 2. For the capability TPM_CAP_NV_LIST, the list includes both indices that are owner
2498 defined and those that were defined before there was a user.

2499 a. The list MAY include TPM_NV_INDEX_DIR, although it is not allocated through
2500 TPM_NV_DefineSpace. If included, the response to TPM_CAP_NV_INDEX MUST
2501 be this TPM_NV_DATA_PUBLIC:

2502 tag = TPM_TAG_NV_DATA_PUBLIC

2503 nvIndex = TPM_NV_INDEX_DIR

2504 pcrInfoRead and pcrInfoWrite MUST both be

2505 TPM_PCR_INFO_SHORT -> pcrSelection -> sizeOfSelect = indicating the

2506 number of PCRs supported

2507 TPM_PCR_INFO_SHORT -> pcrSelection -> pcrSelect = all zeros

2508 TPM_PCR_INFO_SHORT -> localityAtRelease = 0x1f

2509 TPM_PCR_INFO_SHORT -> digestAtRelease = null (all zeros)

2510 permission = TPM_NV_PER_OWNERWRITE || TPM_NV_PER_WRITEALL

2511 bReadSTClear = FALSE

2512 bWriteSTClear = FALSE

2513 bWriteDefine = FALSE

2514 dataSize = 20

2515 b. The list MUST NOT include TPM_NV_INDEX_LOCK, or TPM_NV_INDEX0, as they
2516 do not allocate NV storage.

25173. Unspecified capArea or subCap values are handled according to this general rule

2518 a. If the value is unknown to the TPM_GetCapability command, such that no
2519 meaningful response can be returned, return an error.

2520 i. Examples are a capArea value not in the below table, a subCap value for
2521 TPM_CAP_FLAG not in the below table, or a subCap TPM_KEY_PARMS
2522 structure that cannot be parsed.

2523 ii. Examples include a capArea or subCap of invalid length.

2524 b. If the value is known to the TPM_GetCapability command, but the subCap value
2525 is an enumeration requesting a boolean response, return TPM_SUCCESS and
2526 FALSE.

2527 i. Examples include TPM_CAP_ORD and an unused ordinal, TPM_CAP_ALG
2528 and an unused algorithm ID, or TPM_CAP_SYM_MODE and an unused
2529 mode.

2530TPM_CAPABILITY_AREA Values for TPM_GetCapability

Value	Capability Name	Sub cap	Comments
0x00000001	TPM_CAP_ORD	A command ordinal	Boolean value. TRUE indicates that the TPM supports the ordinal. FALSE indicates that the TPM does not support the ordinal. Unimplemented optional ordinals and unused (unassigned) ordinals return FALSE.
0x00000002	TPM_CAP_ALG	TPM_ALG_XX: A value from TPM_ALGORITHM_ID	Boolean value. TRUE means that the TPM supports the asymmetric algorithm for TPM_Sign, TPM_Seal, TPM_UnSeal and TPM_UnBind and related commands. FALSE indicates that the asymmetric algorithm is not supported for these types of commands. The TPM MAY return TRUE or FALSE for other than asymmetric algoroithms that it supports. Unassigned and unsupported algorithm IDs return FALSE.
0x00000003	TPM_CAP_PID	TPM_PID_xx: A value of TPM_PROTOCOL_ID:	Boolean value. TRUE indicates that the TPM supports the protocol, FALSE indicates that the TPM does not support the protocol. Unassigned protocol IDs return FALSE.
0x00000004	TPM_CAP_FLAG		Either of the next two subcaps
	0x00000108	TPM_CAP_FLAG_PERMANENT	Return the TPM_PERMANENT_FLAGS structure. Each flag in the structure returns as a byte.
	0x00000109	TPM_CAP_FLAG_VOLATILE	Return the TPM_STCLEAR_FLAGS structure. Each flag in the structure returns as a byte.
0x00000005	TPM_CAP_PROPERTY		See following table for the subcaps
0x00000006	TPM_CAP_VERSION	Ignored	TPM_STRUCT_VER structure. The major and minor version MUST indicate 1.1. The firmware revision MUST indicate 0.0. The use of this value is deprecated, new software SHOULD use TPM_CAP_VERSION_VAL to obtain version and revision information regarding the TPM.
0x00000007	TPM_CAP_KEY_HANDLE	Ignored	A TPM_KEY_HANDLE_LIST structure that enumerates all key handles loaded on the TPM. The list only contains the number of handles that an external manager can operate with and does not include the EK or SRK. This is command is available for backwards compatibility. It is the same as

Value	Capability Name	Sub cap	Comments
			TPM_CAP_HANDLE with a resource type of keys.
0x00000008	TPM_CAP_CHECK_LOADED	A TPM_KEY_PARMS structure	A Boolean value. TRUE indicates that the TPM supports and has enough memory available to load a key of the type specified by the TPM_KEY_PARMS structure. FALSE indicates that the TPM does not support the key type or does not have enough memory. The Sub cap MUST be a valid TPM_KEY_PARMS structure. The TPM MAY validate the entire TPM_KEY_PARMS structure.
0x00000009	TPM_CAP_SYM_MODE	TPM_SYM_MODE	A Boolean value. TRUE indicates that the TPM supports the TPM_SYM_MODE, FALSE indicates the TPM does not support the mode. Unassigned modes return FALSE.
0x0000000A	Unused		
0x0000000B	Unused		
0x0000000C	TPM_CAP_KEY_STATUS	handle	Boolean value of ownerEvict. The handle MUST point to a valid key handle. Return TPM_INVALID_KEYHANDLE for an unvalid handle.
0x0000000D	TPM_CAP_NV_LIST	ignored	A list of TPM_NV_INDEX values that are currently allocated NV storage through TPM_NV_DefineSpace.
0x0000000E	Unused		
0x0000000F	Unused		
0x00000010	TPM_CAP_MFR	manufacturer specific	Manufacturer specific. The manufacturer may provide any additional information regarding the TPM and the TPM state but MUST not expose any sensitive information.
0x00000011	TPM_CAP_NV_INDEX	TPM_NV_INDEX	A TPM_NV_DATA_PUBLIC structure that indicates the values for the TPM_NV_INDEX. Returns TPM_BADINDEX if the index is not in the TPM_CAP_NV_LIST list.
0x00000012	TPM_CAP_TRANS_ALG	TPM_ALG_XXX	Boolean value. TRUE means that the TPM supports the algorithm for TPM_EstablishTransport, TPM_ExecuteTransport and TPM_ReleaseTransportSigned. FALSE indicates that for these three commands the algorithm is not supported. Unassigned algorithm IDs return FALSE.
0x00000013			
0x00000014	TPM_CAP_HANDLE	TPM_RESOURCE_TYPE	A TPM_KEY_HANDLE_LIST structure that enumerates all handles currently loaded in the TPM for the given resource type. When describing keys the handle list only contains the number of handles that an external manager can operate with and does not include the EK or SRK. Legal resources are TPM_RT_KEY, TPM_RT_AUTH, TPM_RT_TRANS,, TPM_RT_COUNTER, TPM_RT_DAA_TPM TPM_RT_CONTEXT is valid and returns not a list of handles but a list of the context count values. Return TPM_BAD_MODE for an illegal resource type.
0x00000015	TPM_CAP_TRANS_ES	TPM_ES_XXX	Boolean value. TRUE means the TPM supports the encryption scheme in a transport session for at least one algorithm. Unassigned schemes return FALSE.
0x00000016			
0x00000017	TPM_CAP_AUTH_ENCRYPT	TPM_ALGORITHM_ID	Boolean value. TRUE indicates that the TPM supports the encryption algorithm in OSAP encryption of AuthData values. Unassigned algorithm IDs return FALSE.
0x00000018	TPM_CAP_SELECT_SIZE	TPM_SELECT_SIZE	Boolean value. TRUE indicates that the TPM supports reqSize in TPM_PCR_SELECTION -> sizeOfSelect for the given version. For instance a request could ask for version 1.1 size 2 and the TPM would indicate TRUE. For 1.1 size 3 the TPM would indicate FALSE. For 1.2 size 3 the TPM would

Value	Capability Name	Sub cap	Comments
			indicate TRUE.
0x00000019	TPM_CAP_DA_LOGIC (OPTIONAL)	TPM_ENTITY_TYPE	A TPM_DA_INFO or TPM_DA_INFO_LIMITED structure that returns data according to the selected entity type (e.g., TPM_ET_KEYHANDLE, TPM_ET_OWNER, TPM_ET_SRK, TPM_ET_COUNTER, TPM_ET_OPERATOR, etc.). If the implemented dictionary attack logic does not support different secret types, the entity type can be ignored. Return TPM_WRONG_ENTITYTYPE for an illegal entity type.
0x0000001A	TPM_CAP_VERSION_VAL	Ignored	TPM_CAP_VERSION_INFO structure. The TPM fills in the structure and returns the information indicating what the TPM currently supports.

2531 21.2 CAP_PROPERTY Subcap values for TPM_GetCapability

2532**Start of informative comment**

2533The TPM_CAP_PROPERTY capability has numerous subcap values. The definition for all 2534subcap values occurs in this table.

2535TPM_CAP_PROP_MANUFACTURER returns a vendor ID unique to each manufacturer. The 2536same value is returned as the TPM_CAP_VERSION_INFO -> tpmVendorID. A company 2537abbreviation such as a null terminated stock ticker is a typical choice. However, there is no 2538requirement that the value contain printable characters. The document "TCG Vendor 2539Naming" lists the vendor ID values.

2540TPM_CAP_PROP_MAX_xxxSESS is a constant. At TPM_Startup(ST_CLEAR) 2541TPM_CAP_PROP_xxxSESS == TPM_CAP_PROP_MAX_xxxSESS. As sessions are created on 2542the TPM, TPM_CAP_PROP_xxxSESS decreases toward zero. As sessions are terminated, 2543TPM_CAP_PROP_xxxSESS increases toward TPM_CAP_PROP_MAX_xxxSESS.

2544There is a similar relationship between the constants TPM_CAP_PROP_MAX_COUNTERS 2545and TPM_CAP_PROP_MAX_CONTEXT and the varying TPM_CAP_PROP_COUNTERS and 2546TPM_CAP_PROP_CONTEXT.

2547In one typical implementation where authorization and transport sessions reside in 2548separate pools, TPM_CAP_PROP_SESSIONS will be the sum of TPM_CAP_PROP_AUTHSESS 2549and TPM_CAP_PROP_TRANSESS. In another typical implementation where authorization 2550and transport sessions share the same pool, TPM_CAP_PROP_SESSIONS, 2551TPM_CAP_PROP_AUTHSESS, and TPM_CAP_PROP_TRANSESS will all be equal.

2552**End of informative comment**

2553 TPM_CAP_PROPERTY Subcap Values for TPM_GetCapability

Value	Capability Name	Comments
0x00000101	TPM_CAP_PROP_PCR	UINT32 value. Returns the number of PCR registers supported by the TPM
0x00000102	TPM_CAP_PROP_DIR	UNIT32. Deprecated. Returns the number of DIR, which is now fixed at 1
0x00000103	TPM_CAP_PROP_MANUFACTURER	UINT32 value. Returns the vendor ID unique to each TPM manufacturer.
0x00000104	TPM_CAP_PROP_KEYS	UINT32 value. Returns the number of 2048-bit RSA keys that can be loaded. This may vary with time and circumstances.
0x00000107	TPM_CAP_PROP_MIN_COUNTER	UINT32. The minimum amount of time in 10ths of a second that must pass between invocations of incrementing the monotonic counter.
0x0000010A	TPM_CAP_PROP_AUTHSESS	UINT32. The number of available authorization sessions. This may vary with time and circumstances.
0x0000010B	TPM_CAP_PROP_TRANSESS	UINT32. The number of available transport sessions. This may vary with time and circumstances
0x0000010C	TPM_CAP_PROP_COUNTERS	UINT32. The number of available monotonic counters. This may vary with time and circumstances.
0x0000010D	TPM_CAP_PROP_MAX_AUTHSESS	UINT32. The maximum number of loaded authorization sessions the TPM supports.
0x0000010E	TPM_CAP_PROP_MAX_TRANSESS	UINT32. The maximum number of loaded transport sessions the TPM supports.
0x0000010F	TPM_CAP_PROP_MAX_COUNTERS	UINT32. The maximum number of monotonic counters under control of TPM_CreateCounter
0x00000110	TPM_CAP_PROP_MAX_KEYS	UINT32. The maximum number of 2048 RSA keys that the TPM can support. The number does not include the EK or SRK.
0x00000111	TPM_CAP_PROP_OWNER	BOOL. A value of TRUE indicates that the TPM has successfully installed an owner.
0x00000112	TPM_CAP_PROP_CONTEXT	UINT32. The number of available saved session slots. This may vary with time and circumstances.

Value	Capability Name	Comments
0x00000113	TPM_CAP_PROP_MAX_CONTEXT	UINT32. The maximum number of saved session slots.
0x00000114	TPM_CAP_PROP_FAMILYROWS	UINT32. The maximum number of rows in the family table
0x00000115	TPM_CAP_PROP_TIS_TIMEOUT	A 4 element array of UINT32 values each denoting the timeout value in microseconds for the following in this order: TIMEOUT_A, TIMEOUT_B, TIMEOUT_C, TIMEOUT_D Where these timeouts are to be used is determined by the platform specific TPM Interface Specification.
0x00000116	TPM_CAP_PROP_STARTUP_EFFECT	The TPM_STARTUP_EFFECTS structure
0x00000117	TPM_CAP_PROP_DELEGATE_ROW	UINT32. The maximum size of the delegate table in rows.
0x00000118	open	
0x00000119	TPM_CAP_PROP_MAX_DAASESS	UINT32. The maximum number of loaded DAA sessions (join or sign) that the TPM supports.
0x0000011A	TPM_CAP_PROP_DAASESS	UINT32. The number of available DAA sessions. This may vary with time and circumstances
0x0000011B	TPM_CAP_PROP_CONTEXT_DIST	UINT32. The maximum distance between context count values. This MUST be at least 2^16-1
0x0000011C	TPM_CAP_PROP_DAA_INTERRUPT	BOOL. A value of TRUE indicates that the TPM will accept ANY command while executing a DAA Join or Sign. A value of FALSE indicates that the TPM will invalidate the DAA Join or Sign upon the receipt of any command other than the next join/sign in the session or a TPM_SaveContext
0X0000011D	TPM_CAP_PROP_SESSIONS	UNIT32. The number of available authorization and transport sessions from the pool. This may vary with time and circumstances.
0x0000011E	TPM_CAP_PROP_MAX_SESSIONS	UINT32. The maximum number of sessions the TPM supports.
0x0000011F	TPM_CAP_PROP_CMK_RESTRICTION	UINT32 TPM_Permanent_Data -> restrictDelegate
0x00000120	TPM_CAP_PROP_DURATION	A 3 element array of UINT32 values each denoting the duration value in microseconds of the duration of the three classes of commands: Small, Medium and Long in the following in this order: SMALL_DURATION, MEDIUM_DURATION, LONG_DURATION
0x00000121	open	
0x00000122	TPM_CAP_PROP_ACTIVE_COUNTER	TPM_COUNT_ID. The id of the current counter. 0xff..ff if no counter is active, either because no counter has been set active or because the active counter has been released.
0x00000123	TPM_CAP_PROP_MAX_NV_AVAILABLE	UINT32. Deprecated. The maximum number of NV space that can be allocated, MAY vary with time and circumstances. This capability was not implemented consistently, and is replaced by TPM_NV_INDEX_TRIAL.
0x00000124	TPM_CAP_PROP_INPUT_BUFFER	UINT32. The maximum size of the TPM input buffer or output buffers in bytes.
0x00000125	XX Next number	

21.3 Bit ordering for structures

Start of informative comment

When returning a structure the TPM will use the following bit ordering scheme

Sample structure

```
typedef struct tdSAMPLE {
    TPM_STRUCTURE_TAG       tag;
    UINT32                  N1;
    UINT32                  N2;
} SAMPLE;
```

End of informative comment

1. Using the sample structure in the informative comment as a template the TPM performs the following marshaling
   a. Bit 0 of the output is first bit following the open bracket. The first bit of tag is then bit 0 of the output.
   b. Bit-N of the output is the nth bit from the opening bracket
      i. The bits of N1 appear before the bits of N2 in the output
2. All structures use the endianness defined in section 2.1 of this document

21.3.1 Deprecated GetCapability Responses

Num	CapArea	subCap	Response
1	TPM_CAP_PROPERTY	TPM_CAP_PROP_DIR_AUTH	UINT32 value. Returns the number of DIR registers under control of the TPM owner supported by the TPM. As there is now only 1 DIR, this is deprecated to always return a value of 1 in version 1.2.

2572 21.4 TPM_CAPABILITY_AREA Values for TPM_SetCapability

2573 TPM_CAPABILITY_AREA Values for TPM_SetCapability

Value	Capability Name	Sub cap	Comments
0x00000001	TPM_SET_PERM_FLAGS	See TPM_PERMANENT_FLAGS structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000002	TPM_SET_PERM_DATA	See TPM_PERMANENT_DATA structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000003	TPM_SET_STCLEAR_FLAGS	See TPM_STCLEAR_FLAGS structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000004	TPM_SET_STCLEAR_DATA	See TPM_STCLEAR_DATA structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000005	TPM_SET_STANY_FLAGS	See TPM_STANY_FLAGS structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000006	TPM_SET_STANY_DATA	See TPM_STANY_DATA structure	The ability to set a value is field specific and a review of the structure will disclose the ability and requirements to set a value
0x00000007	TPM_SET_VENDOR	Vendor specific	This area allows the vendor to set specific areas in the TPM according to the normal shielded location requirements

2574

2575The setValue type for TPM_SetCapability is determined by the definition of the SubCap
2576value listed in the structure definition of each flag section. The setValueSize is set according
2577to this type.

2578 21.5 SubCap Values for TPM_SetCapability

25791. SubCap values for TPM_SetCapability are found in each flag definition section under the 2580 table “Flag Restrictions for SetCapability”. Each table has the following column 2581 definitions:

2582 a. Flag SubCap Number 0x00000000+: Incremental flag value used in the SubCap field

2583 b. Set: A “Y” in this column indicates that the flag can be set by TPM_SetCapability. An 2584 “N” in this column indicates that the flag can not be set by TPM_SetCapability.

2585 c. Set restrictions: Restrictions on how and when TPM_SetCapability can set a flag. 2586 Each flag that can be set with TPM_SetCapability may have one or more restrictions 2587 on how and when TPM_SetCapability can be used to change a value of a flag. A 2588 definition of common restrictions is listed below.

2589 d. Actions From: This column contains information on other TPM command areas that 2590 can effect a flag

25912. Common Restriction Definitions

2592 a. Owner authorization: TPM_SetCapability must use owner authorization to change the 2593 value of a flag

2594 b. Physical presence assertion: Physical presence must be asserted in order for 2595 TPM_SetCapability to change the value of a flag

2596 c. No Authorization: TPM_SetCapability must be sent as TPM_TAG_RQU_COMMAND 2597 (no authorization)

2598 d. If a capability is restricted to a fixed value, setValueSize MUST still indicate the size 2599 of setValue. setValue MUST indicate the fixed value, or the TPM will return an error 2600 code.

2601 i. For example, since TPM_PERMANENT_FLAGS -> tpmEstablished can only be set 2602 to FALSE, setValueSize MUST be 1 (for a BOOL) and setValue MUST be 0.

2603 21.6 TPM_CAP_VERSION_INFO

2604**Start of informative comment**

2605This structure is an output from a TPM_GetCapability -> TPM_CAP_VERSION_VAL request.
2606TPM returns the current version and revision of the TPM.

2607The specLevel and errataRev are defined in the document "Specification and File Naming
2608Conventions".

2609The tpmVendorID is a value unique to each vendor. It is defined in the document "TCG
2610Vendor Naming".

2611The vendor specific area allows the TPM vendor to provide support for vendor options. The
2612TPM vendor may define the area to the TPM vendor's needs.

2613**End of informative comment**

2614 Definition

```
2615typedef struct tdTPM_CAP_VERSION_INFO {
2616   TPM_STRUCTURE_TAG tag;
2617   TPM_VERSION version;
2618   UINT16 specLevel;
2619   BYTE errataRev;
2620   BYTE tpmVendorID[4];
2621   UINT16 vendorSpecificSize;
2622   [size_is(vendorSpecificSize)] BYTE* vendorSpecific;
2623} TPM_CAP_VERSION_INFO;
2624
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_CAP_VERSION_INFO
TPM_VERSION	version	The version and revision
UINT16	specLevel	A number indicating the level of ordinals supported
BYTE	errataRev	A number indicating the errata version of the specification
BYTE[4]	tpmVendorID	The vendor ID unique to each TPM manufacturer.
UINT16	vendorSpecificSize	The size of the vendor specific area
BYTE*	vendorSpecific	Vendor specific information

21.7 TPM_DA_INFO

Revision	specLevel	errataRev
62	0x0001	0x00
85	0x0002	0x00
94	0x0002	0x01
103	0x0002	0x02
116	0x0002	0x03

Start of informative comment

This structure is an output from a TPM_GetCapability -> TPM_CAP_DA_LOGIC request if TPM_PERMANENT_FLAGS -> disableFullDALogicInfo is FALSE.

It returns static information describing the TPM response to authorization failures that might indicate a dictionary attack and dynamic information regarding the current state of the dictionary attack mitigation logic.

End of informative comment

Definition

```
typedef struct tdTPM_DA_INFO {
   TPM_STRUCTURE_TAG tag;
   TPM_DA_STATE state;
   UINT16 currentCount;
   UINT16 thresholdCount;
   TPM_DA_ACTION_TYPE actionAtThreshold;
   UINT32 actionDependValue;
   UINT32 vendorDataSize;
   [size_is(vendorDataSize)]  BYTE* vendorData;
} TPM_DA_INFO;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DA_INFO
TPM_DA_STATE	state	Dynamic. The actual state of the dictionary attack mitigation logic. See 21.9.
UINT16	currentCount	Dynamic. The actual count of the authorization failure counter for the selected entity type
UINT16	thresholdCount	Static. Dictionary attack mitigation threshold count for the selected entity type
TPM_DA_ACTION_TYPE	actionAtThreshold	Static Action of the TPM when currentCount passes thresholdCount. See 21.10.
UINT32	actionDependValue	Dynamic. Action being taken when the dictionary attack mitigation logic is active. E.g., when actionAtThreshold is TPM_DA_ACTION_TIMEOUT, this is the lockout time remaining in seconds.
UINT32	vendorDataSize	Size of vendor specific data field
BYTE*	vendorData	Vendor specific data field

21.8 TPM_DA_INFO_LIMITED

Start of informative comment

This structure is an output from a TPM_GetCapability -> TPM_CAP_DA_LOGIC request if TPM_PERMANENT_FLAGS -> disableFullDALogicInfo is TRUE.

It returns static information describing the TPM response to authorization failures that might indicate a dictionary attack and dynamic information regarding the current state of the dictionary attack mitigation logic. This structure omits information that might aid an attacker.

End of informative comment

Definition

```
typedef struct tdTPM_DA_INFO_LIMITED {
   TPM_STRUCTURE_TAG tag;
   TPM_DA_STATE state;
   TPM_DA_ACTION_TYPE actionAtThreshold;
   UINT32 vendorDataSize;
   [size_is(vendorDataSize)]  BYTE* vendorData;
} TPM_DA_INFO_LIMITED;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DA_INFO_LIMITED

The descriptions of the remaining structure members are identical to those of 21.7 TPM_DA_INFO.

2667 21.9 TPM_DA_STATE

2668 **Start of informative comment**

2669 TPM_DA_STATE enumerates the possible states of the dictionary attack mitigation logic.

2670 **End of informative comment**

2671 TPM_DA_STATE Values

Value	Event Name	Comments
0x00	TPM_DA_STATE_INACTIVE	The dictionary attack mitigation logic is currently inactive
0x01	TPM_DA_STATE_ACTIVE	The dictionary attack mitigation logic is active. TPM_DA_ACTION_TYPE (21.10) is in progress.

2672

21.10 TPM_DA_ACTION_TYPE

Start of informative comment

This structure indicates the action taken when the dictionary attack mitigation logic is active, when TPM_DA_STATE is TPM_DA_STATE_ACTIVE.

End of informative comment

Definition

```
typedef struct tdTPM_DA_ACTION_TYPE {
  TPM_STRUCTURE_TAG tag;
  UINT32 actions;
} TPM_DA_ACTION_TYPE;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DA_ACTION_TYPE
UINT32	actions	The action taken when TPM_DA_STATE is TPM_DA_STATE_ACTIVE.

Action Values

Bit position	Name	Description
31-4	Reserved	No information and MUST be FALSE
3	TPM_DA_ACTION_FAILURE_MODE	The TPM is in failure mode.
2	TPM_DA_ACTION_DEACTIVATE	The TPM is in the deactivated state.
1	TPM_DA_ACTION_DISABLE	The TPM is in the disabled state.
0	TPM_DA_ACTION_TIMEOUT	The TPM will be in a locked state for TPM_DA_INFO -> actionDependValue seconds. This value is dynamic, depending on the time the lock has been active.

22. DAA Structures

All byte and bit areas are byte arrays treated as large integers

22.1 Size definitions

```
#define DAA_SIZE_r0    43 (Bytes)
#define DAA_SIZE_r1    43 (Bytes)
#define DAA_SIZE_r2   128 (Bytes)
#define DAA_SIZE_r3   168 (Bytes)
#define DAA_SIZE_r4   219 (Bytes)
#define DAA_SIZE_NT    20 (Bytes)
#define DAA_SIZE_v0   128 (Bytes)
#define DAA_SIZE_v1   192 (Bytes)
#define DAA_SIZE_NE   256 (Bytes)
#define DAA_SIZE_w    256 (Bytes)
#define DAA_SIZE_issuerModulus   256 (Bytes)
```

22.2 Constant definitions

```
#define DAA_power0    104
#define DAA_power1    1024
```

22.3 TPM_DAA_ISSUER

Start of informative comment

This structure is the abstract representation of non-secret settings controlling a DAA context. The structure is required when loading public DAA data into a TPM.

TPM_DAA_ISSUER parameters are normally held outside the TPM as plain text data, and loaded into a TPM when a DAA session is required. A TPM_DAA_ISSUER structure contains no integrity check: the TPM_DAA_ISSUER structure at time of JOIN is indirectly verified by the issuer during the JOIN process, and a digest of the verified TPM_DAA_ISSUER structure is held inside the TPM_DAA_TPM structure created by the JOIN process.

Parameters DAA_digest_X are digests of public DAA_generic_X parameters, and used to verify that the correct value of DAA_generic_X has been loaded. DAA_generic_q is stored in its native form to reduce command complexity.

End of informative comment

Definition

```
typedef struct tdTPM_DAA_ISSUER {
   TPM_STRUCTURE_TAG  tag;
   TPM_DIGEST    DAA_digest_R0;
   TPM_DIGEST    DAA_digest_R1;
   TPM_DIGEST    DAA_digest_S0;
   TPM_DIGEST    DAA_digest_S1;
   TPM_DIGEST    DAA_digest_n;
   TPM_DIGEST    DAA_digest_gamma;
   BYTE[26]      DAA_generic_q;
} TPM_DAA_ISSUER;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DAA_ISSUER
TPM_DIGEST	DAA_digest_R0	A digest of the parameter “R0”, which is not secret and may be common to many TPMs.
TPM_DIGEST	DAA_digest_R1	A digest of the parameter “R1”, which is not secret and may be common to many TPMs.
TPM_DIGEST	DAA_digest_S0	A digest of the parameter “S0”, which is not secret and may be common to many TPMs.
TPM_DIGEST	DAA_digest_S1	A digest of the parameter “S1”, which is not secret and may be common to many TPMs.
TPM_DIGEST	DAA_digest_n	A digest of the parameter “n”, which is not secret and may be common to many TPMs.
TPM_DIGEST	DAA_digest_gamma	A digest of the parameter “gamma”, which is not secret and may be common to many TPMs.
BYTE[26]	DAA_ generic _q	The parameter q, which is not secret and may be common to many TPMs. Note that q is slightly larger than a digest, but is stored in its native form to simplify the TPM_DAA_join command. Otherwise, JOIN requires 3 input parameters.

2728 22.4 TPM_DAA_TPM

2729**Start of informative comment**

2730This structure is the abstract representation of TPM specific parameters used during a DAA
2731context. TPM-specific DAA parameters may be stored outside the TPM, and hence this
2732structure is needed to save private DAA data from a TPM, or load private DAA data into a
2733TPM.

2734If a TPM_DAA_TPM structure is stored outside the TPM, it is stored in a confidential format
2735that can be interpreted only by the TPM created it. This is to ensure that secret parameters
2736are rendered confidential, and that both secret and non-secret data in TPM_DAA_TPM form
2737a self-consistent set.

2738TPM_DAA_TPM includes a digest of the public DAA parameters that were used during
2739creation of the TPM_DAA_TPM structure. This is needed to verify that a TPM_DAA_TPM is
2740being used with the public DAA parameters used to create the TPM_DAA_TPM structure.

2741Parameters DAA_digest_v0 and DAA_digest_v1 are digests of public DAA_private_v0 and
2742DAA_private_v1 parameters, and used to verify that the correct private parameters have
2743been loaded.

2744**Parameter DAA_count is stored in its native form, because it is smaller than a digest,**
2745**and is required to enforce consistency.**

2746**End of informative comment**

2747 Definition

```
2748typedef struct tdTPM_DAA_TPM {
2749   TPM_STRUCTURE_TAG tag;
2750   TPM_DIGEST    DAA_digestIssuer;
2751   TPM_DIGEST    DAA_digest_v0;
2752   TPM_DIGEST    DAA_digest_v1;
2753   TPM_DIGEST    DAA_rekey;
2754   UINT32        DAA_count;
2755} TPM_DAA_TPM;
```

2756 Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DAA_TPM
TPM_DIGEST	DAA_digestIssuer	A digest of a TPM_DAA_ISSUER structure that contains the parameters used to generate this TPM_DAA_TPM structure.
TPM_DIGEST	DAA_digest_v0	A digest of the parameter “v0”, which is secret and specific to this TPM. “v0” is generated during a JOIN phase.
TPM_DIGEST	DAA_digest_v1	A digest of the parameter “v1”, which is secret and specific to this TPM. “v1” is generated during a JOIN phase.
TPM_DIGEST	DAA_rekey	A digest related to the rekeying process, which is not secret but is specific to this TPM, and must be consistent across JOIN/SIGN sessions. “rekey” is generated during a JOIN phase.
UINT32	DAA_count	The parameter “count”, which is not secret but must be consistent across JOIN/SIGN sessions. “count” is an input to the TPM from the host system.

22.5 TPM_DAA_CONTEXT

Start of informative comment

TPM_DAA_CONTEXT structure is created and used inside a TPM, and never leaves the TPM. This entire section is informative as the TPM does not expose this structure.

TPM_DAA_CONTEXT includes a digest of the public and private DAA parameters that were used during creation of the TPM_DAA_CONTEXT structure. This is needed to verify that a TPM_DAA_CONTEXT is being used with the public and private DAA parameters used to create the TPM_DAA_CONTEXT structure.

End of informative comment

Definition

```
typedef struct tdTPM_DAA_CONTEXT {
   TPM_STRUCTURE_TAG  tag;
   TPM_DIGEST         DAA_digestContext;
   TPM_DIGEST         DAA_digest;
   TPM_DAA_CONTEXT_SEED    DAA_contextSeed;
   BYTE[256]          DAA_scratch;
   BYTE               DAA_stage;
} TPM_DAA_CONTEXT;
```

Parameters

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DAA_CONTEXT
TPM_DIGEST	DAA_digestContext	A digest of parameters used to generate this structure. The parameters vary, depending on whether the session is a JOIN session or a SIGN session.
TPM_DIGEST	DAA_digest	A running digest of certain parameters generated during DAA computation; operationally the same as a PCR (which holds a running digest of integrity metrics).
TPM_DAA_CONTEXT_SEED	DAA_contextSeed	The seed used to generate other DAA session parameters
BYTE[256]	DAA_scratch	Memory used to hold different parameters at different times of DAA computation, but only one parameter at a time. The maximum size of this field is 256 bytes
BYTE	DAA_stage	A counter, indicating the stage of DAA computation that was most recently completed. The value of the counter is zero if the TPM currently contains no DAA context. When set to zero (0) the TPM MUST clear all other fields in this structure. The TPM MUST set DAA_stage to 0 on TPM_Startup(ANY)

22.6 TPM_DAA_JOINDATA

Start of informative comment

This structure is the abstract representation of data that exists only during a specific JOIN session.

End of informative comment

Definition

```
typedef struct tdTPM_DAA_JOINDATA {
   BYTE[128]     DAA_join_u0;
   BYTE[138]     DAA_join_u1;
   TPM_DIGEST    DAA_digest_n0;
} TPM_DAA_JOINDATA;
```

Parameters

Type	Name	Description
BYTE[128]	DAA_join_u0	A TPM-specific secret “u0”, used during the JOIN phase, and discarded afterwards.
BYTE[128]	DAA_join_u1	A TPM-specific secret “u1”, used during the JOIN phase, and discarded afterwards.
TPM_DIGEST	DAA_digest_n0	A digest of the parameter “n0”, which is an RSA public key with exponent 2^16 +1

22.7 TPM_STANY_DATA Additions

Informative comment

This shows that the volatile data areas are added to the TPM_STANY_DATA structure

End of informative comment

Definition

```
typedef struct tdTPM_STANY_DATA{
   TPM_DAA_ISSUER     DAA_issuerSettings;
   TPM_DAA_TPM        DAA_tpmSpecific;
   TPM_DAA_CONTEXT    DAA_session;
   TPM_DAA_JOINDATA   DAA_joinSession;
}TPM_STANY_DATA;
```

Types of Volatile Data

Type	Name	Description
TPM_DAA_ISSUER	DAA_issuerSettings	A set of DAA issuer parameters controlling a DAA session.
TPM_DAA_TPM	DAA_tpmSpecific	A set of DAA parameters associated with a specific TPM.
TPM_DAA_CONTEXT	DAA_session	A set of DAA parameters associated with a DAA session.
TPM_DAA_JOINDATA	DAA_joinSession	A set of DAA parameters used only during the JOIN phase of a DAA session, and generated by the TPM.

22.8 TPM_DAA_BLOB

Informative comment

The structure passed during the join process

End of informative comment

Definition

```
typedef struct tdTPM_DAA_BLOB {
   TPM_STRUCTURE_TAG tag;
   TPM_RESOURCE_TYPE resourceType;
   BYTE[16] label;
   TPM_DIGEST blobIntegrity;
   UINT32 additionalSize;
   [size_is(additionalSize)] BYTE* additionalData;
   UINT32 sensitiveSize;
   [size_is(sensitiveSize)] BYTE* sensitiveData;
}TPM_DAA_BLOB;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DAA_BLOB
TPM_RESOURCE_TYPE	resourceType	The resource type: enc(DAA_tpmSpecific) or enc(v0) or enc(v1)
BYTE[16]	label	Label for identification of the blob. Free format area.
TPM_DIGEST	blobIntegrity	The integrity of the entire blob including the sensitive area. This is a HMAC calculation with the entire structure (including sensitiveData) being the hash and daaProof is the secret
UINT32	additionalSize	The size of additionalData
BYTE*	additionalData	Additional information set by the TPM that helps define and reload the context. The information held in this area MUST NOT expose any information held in shielded locations. This should include any IV for symmetric encryption
UINT32	sensitiveSize	The size of sensitiveData
BYTE*	sensitiveData	A TPM_DAA_SENSITIVE structure

22.9 TPM_DAA_SENSITIVE

Informative comment

The encrypted area for the DAA parameters

End of informative comment

Definition

```
typedef struct tdTPM_DAA_SENSITIVE {
   TPM_STRUCTURE_TAG tag;
   UINT32 internalSize;
   [size_is(internalSize)] BYTE* internalData;
}TPM_DAA_SENSITIVE;
```

Type	Name	Description
TPM_STRUCTURE_TAG	tag	MUST be TPM_TAG_DAA_SENSITIVE
UINT32	internalSize	The size of the internalData area
BYTE*	internalData	DAA_tpmSpecific or DAA_private_v0 or DAA_private_v1

2828 23. Redirection

2829 23.1 TPM_REDIR_COMMAND

2830 **Informative comment**

2831 The types of redirections

2832 **End of informative comment**

2833 Command modes

Name	Value	Description
	0x00000001	

24. Deprecated Structures

24.1 Persistent Flags

Start of Informative comment

Rewritten to be part of the PERMANENT, STANY and STCLEAR structures

End of informative comment

```
typedef struct tdTPM_PERSISTENT_FLAGS{
// deleted see version 1.1
} TPM_PERSISTENT_FLAGS;
```

24.2 Volatile Flags

Start of Informative comment

Rewritten to be part of the PERMANENT, STANY and STCLEAR structures

End of informative comment

```
typedef struct tdTPM_VOLATILE_FLAGS{
// see version 1.1
} TPM_VOLATILE_FLAGS;
```

24.3 TPM persistent data

Start of Informative comment

Rewritten to be part of the PERMANENT, STANY and STCLEAR structures

End of informative comment

Definition

```
typedef struct tdTPM_PERSISTENT_DATA{
// see version 1.1
}TPM_PERSISTENT_DATA;
```

24.4 TPM volatile data

Start of Informative comment

Rewritten to be part of the PERMANENT, STANY and STCLEAR structures

End of informative comment

Definition

```
typedef struct tdTPM_VOLATILE_DATA{
// see version 1.1
}TPM_VOLATILE_DATA;
```

24.5 TPM SV data

Start of informative comment

Rewritten to be part of the PERMANENT, STANY and STCLEAR structures

End of informative comment

Definition

```
typedef struct tdTPM_SV_DATA{
// see version 1.1
}TPM_SV_DATA;
```

24.6 TPM_SYM_MODE

Start of informative comment

This indicates the mode of a symmetric encryption. Mode is Electronic CookBook (ECB) or some other such mechanism.

End of informative comment

TPM_SYM_MODE values

Value	Name	Description
0x00000001	TPM_SYM_MODE_ECB	The electronic cookbook mode (this requires no IV)
0x00000002	TPM_SYM_MODE_CBC	Cipher block chaining mode
0X00000003	TPM_SYM_MODE_CFB	Cipher feedback mode

Description

The TPM MAY support any of the symmetric encryption modes