TCG ACPI Specification

Specification Version 1.00 – FINAL
Revision 1.00
Aug 08, 2005

Contact: admin@trustedcomputinggroup.org

TCG CONFIDENTIAL

TCG

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.

No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Except that a license is hereby granted by TCG to copy and reproduce this specification for internal use only.

Contact the Trusted Computing Group at http://www.trustedcomputinggroup.org/ for information on specification licensing through membership agreements.

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

The only official, normative version of a TCG Specification or related document is the English-language text adopted by TCG under its Bylaws and published on the TCG website, www.trustedcomputing.org. TCG does not guarantee the accuracy or completeness of any other version. Other language versions of Specifications and related documents are provided for convenience and are intended to be technically identical to the official English version, but they may contain translation and other errors.

Translations may be provided by volunteers through the Trusted Computing Group's translation program (see www.trustedcomputinggroup.org/specifications.

Other legal notices and terms governing the publication of materials on the TCG website are found at www.trustedcomputinggroup.org/about/legal. TCG incorporates by reference the same notices and terms with respect to TCG-authorized translations of Specifications and related documents, whether published on the TCG website or at another online location.

Change History

Revision	Description
1.00	Initial Final release

Contents

Tables

1. Introduction

Start of informative comment

This specification defines the framework of necessary ACPI tables and basic methods to be used on a TCG compliant platform. The table and ACPI namespace objects provide enough information to the operating system to enable access to the TCG compliant hardware in a platform.

End of informative comment

The intention of this specification is to provide a framework for all platform types that employ ACPI. These platform types can draw from this specification as necessary, and may further specify ACPI functionality that is required for a particular platform type.

2. ACPI Table

The correct platform type specific table MUST be provided by a TCG compliant platform. All TCG platforms supporting ACPI utilize the same header section, which is marked with grey shading in the client and server ACPI table formats, shown in Tables 1 and 2.

Start of informative comment

ACPI tables are defined to be laid out in little-endian byte format per the ACPI specification.

End of informative comment

2.1 Client ACPI Table

2.1.1 Client Common Header Values

These are the specific values to be used in the client platform version of the ACPI table.

Field	Value	Description
Length	32h	Size of the table
Revision	02h	Revision for PC Client Platform Class
Platform Class	00h	PC Client Platform Class

Table 1: TCG Hardware Interface Description Table Format for Clients

Field	Byte Length	Byte Offset	Description
Header			
Signature	4h	00h	'TCPA'. Signature for the TCG Hardware Interface Table.
Length	4h	04h	See section 2.1.1. The length of this table starting from the Signature field up to and including the LASA field. It does not include the size of the area storing events or other data that is referenced or pointed to by any of these fields.
Revision	1h	08h	See section 2.1.1. Revision of this table including the data and structures reference by it. E.g., If the event structures with the area reference by LASA change, this revision MUST be incremented. *Note:* The purview of this revision is within platform class as indicated by the Platform Class field. This means that each platform class increments this field autonomously. Software referencing this table SHOULD interpret the Platform Class field prior to interpreting this Revision field.
Checksum	1h	09h	Entire table must sum to zero.
OEMID	6h	0Ah	OEM ID. Per ACPI specification. An OEM-supplied string that identifies the OEM.
OEM Table ID	8h	10h	For the TPM Interface Table, the table ID is the manufacturer model ID (assigned by the OEM identified by "OEM ID").
OEM Revision	4h	18h	OEM revision of TPM Interface Table for the given OEM Table ID. Per ACPI, this is "An OEM-supplied revision number. Larger numbers are assumed to be newer revisions."
Creator ID	4h	1Ch	Vendor ID of utility that created the table. For the tables containing Definition Blocks, this is the ID for the ASL Compiler.

Field	Byte Length	Byte Offset	Description
Creator Revision	4h	20h	Revision of utility that created the table. For the tables containing Definition Blocks, this is the revision for the ASL Compiler.
Platform Class	2h	24h	See section 2.1.1.
Log Area Minimum Length (LAML)	4h	26h	Identifies the minimum length (in bytes) of the system's pre-boot TCG event log area. *Note*: For PC Client Implementation Specification up to and including 1.2 the minimum log size is 64KB.
Log Area Start Address (LASA)	8h	2Ah	Contains the 64-bit physical address of the start of the system's pre-boot TCG event log area, in QWORD format. *Note*: The log area ranges from address LASA to LASA+(LAML-1).

2.2 Server ACPI Table

2.2.1 Server Common Header Values

These are the specific values to be used in the server platform version of the ACPI table.

Field	Value	Description
Length	64h	Size of the table
Revision	02h	Revision for Server Platform Class
Platform Class	01h	Server Platform Class

Table 2: TCG Hardware Interface Description Table Format for Servers

Field	Byte Length	Byte Offset	Description
Header			
Signature	4h	00h	'TCPA'. Signature for the TCG Hardware Interface Table.
Length	4h	04h	See Section 2.2.1. The length of this table starting from the Signature field up to and including the PCI Function Number field. It does not include the size of the area storing events or other data that is referenced or pointed to by any of these fields.
Revision	1h	08h	See Section 2.2.1. Revision of this table including the data and structures reference by it. E.g., If the event structures with the area reference by LASA change, this revision MUST be incremented. *Note:* The purview of this revision is within platform class as indicated by the Platform Class field. This means that each platform class increments this field autonomously. Software referencing this table SHOULD interpret the Platform Class field prior to interpreting this Revision field.
Checksum	1h	09h	Entire table must sum to zero.
OEMID	6h	0Ah	OEM ID. Per ACPI specification. An OEM-supplied string that identifies the OEM.
OEM Table ID	8h	10h	For the TPM Interface Table, the table ID is the manufacturer model ID (assigned by the OEM identified by "OEM ID").
OEM Revision	4h	18h	OEM revision of TPM Interface Table for the given OEM Table ID. Per ACPI, this is "An OEM-supplied revision number. Larger numbers are assumed to be newer revisions."

Field	Byte Length	Byte Offset	Description
Creator ID	4h	1Ch	Vendor ID of utility that created the table. For the tables containing Definition Blocks, this is the ID for the ASL Compiler.
Creator Revision	4h	20h	Revision of utility that created the table. For the tables containing Definition Blocks, this is the revision for the ASL Compiler.
Platform Class	2h	24h	See Section 2.2.1.
Reserved	2h	26h	This field is reserved and set to 0. This creates natural alignment for the fields that follow.
Log Area Minimum Length (LAML)	8h	28h	Identifies the minimum length (in bytes) of the system's pre-boot TCG event log area.
Log Area Start Address (LASA)	8h	30h	Contains the 64-bit physical address of the start of the system's pre-boot TCG event log area, in QWORD format. *Note*: The log area ranges from address LASA to LASA+(LAML-1).
Specification Revision	2h	38h	Identifies the TCG specification revision, in BCD format, to which the interface was designed. The first byte holds the most significant digits, while second byte holds the least significant digits of the revision, e.g. a value of 0x0110 indicates the interface is compatible with TCG specification v1.1.
Device Flags	1h	3Ah	Bit [7:3]: Reserved BIT[2]: TPM configuration address valid 0 = TPM configuration address is invalid 1 = TPM configuration address is valid BIT[1]: TPM Bus is PNP 0 = FALSE (the TPM address and interrupt must not be changed) 1 = TRUE (the TPM address and interrupt may be changed by PNP OS code) Bit [0]: PCI Device Flag. For PCI TCG devices, this bit is set. 0 = non-PCI device, the PCI Segment Group, Bus, Device and Function Number fields combined corresponds to the ACPI _UID value of the device whose _HID or _CID contains a TPM plug and play ID. 1 = PCI Device
Interrupt Flags	1h	3Bh	Bit [7:4]: Reserved Bit[3]: I/O APIC/SAPIC interrupt (Global System Interrupt) 0 = not supported 1 = supported Bit[2]: SCI triggered through GPE 0 = not supported 1 = supported Bit[1]: Interrupt Polarity, 0 = Active-High: This interrupt is sampled when the signal is high, or true. 1 = Active-Low: This interrupt is sampledwhen the signal is low, or false. Bit[0]: Interrupt Mode, 0 = Level-Triggered: This interrupt is triggered in response to the signal being in either a high or low state. 1 = Edge-Triggered: This interrupt is triggered in response to a change in signalstate, either high to low or low to high. PCI devices are always level triggered and active low, so these two bits are set to 10b for PCI devices.
GPE	1h	3Ch	The bit assignment of the SCI interrupt within the GPEx_STS register of a GPE described if the FADT that the interface triggers. *Note:* This field is valid only if Bit[2] of the Interrupt Flags field is set.)
Reserved	3h	3Dh	00h.

Field	Byte Length	Byte Offset	Description
Global System Interrupt	4h	40h	The I/O APIC or I/O SAPIC Global System Interrupt used by the interface. *Note:* This field is valid only if Bit[3] of the Interrupt Flags field is set.
Base Address	Ch	44h	The base address of the hardware register set described using the Generic Address Structure (GAS, See the [ACPI 3.0] for the definition). The Address_Space_ID field in the GAS can only be of the value of 0 (System Memory) and 1 (System IO). All other values are not permitted. This address must be the Host Side address in the case of MMIO, and it must be the Host Side IO port address in the case of IO Port.
Reserved	4h	50h	Set to 0. This is to naturally align the data fields that follow.
Configuration Address	Ch	54h	The configuration address of the TPM hardware device described using the Generic Address Structure (GAS, See the [ACPI 3.0] for the definition). The Address_Space_ID field in the GAS can only be of the value of 0 (System Memory) and 1 (System IO). All other values are not permitted. This is only valid if Bit[2] of the Device Flags field is set. This address must be the Host Side address in the case of MMIO, and it must be the Host Side IO port address in the case of IO Port.
PCI Segment Group Number	1h	60h	PCI Segment Group Number, if the TPM device is a PCI device
PCI Bus Number	1h	61h	PCI Bus Number, if the TPM device is a PCI device
PCI Device Number	1h	62h	Bit 4:0 – PCI Device Number: The PCI device number if the TPM device is a PCI device. Bit 7:5 – Reserved
PCI Function Number	1h	63h	Bit 2:0 – PCI Function Number: The PCI function number if the TPM device is a PCI device. Bit 7:3 – Reserved

3. ACPI Device

Start of informative comment

Devices are not required to be exposed in ACPI namespace if the device exists on a bus that is enumerable by the Operating System, or on a bus which is plug-n-play capable.

A TCG platform class-specific ACPI Table may provide a mechanism that can be used before the ability to execute ACPI control methods in the OS is available. The Server ACPI Table in section 2.2 of this specification is one example of such a table. This table is not, however, intrinsically supported in the OSPM as a way of discovering and reporting system resources. Therefore, it is recommended that non-PCI TCG Hardware on the platform be described in the ACPI name space. This makes it possible for the OSPM to enumerate the TCG Hardware as a device. In addition, the ACPI name space description is more flexible and friendly in hot-plug scenarios.

Note that to be ACPI compatible, the fixed resources for TCG Hardware must still be accounted for in accordance with the ACPI specification. If the device is not formally described in the ACPI Name Space, its resources must be described as fixed system resources or the resources appended to some other fixed resource system device in order to ensure that the OSPM does not attempt to allocate those resources to some other device.

To formally describe the TCG Hardware System Interface in ACPI Name Space, a TCG hardware device is created using the named device object. Table 2 is a non-exhaustive list of ACPI control methods that may be used in a TCG hardware device object, along with a recommended support level for each method.

End of informative comment

A TCG platform MAY provide an ACPI device object representing the TPM in the ACPI namespace, if the bus where the TPM is located is not PNP capable or the bus is not exposed to the OS for PNP operations.

Table 3: TCG Hardware Device Object Control Methods

Object	Description	Support Level
_ADR	Named object that evaluates to the interface's address on its parent bus. _ADR is a standard device configuration control method defined in the ACPI Specification.	Required only for devices on a bus that has standard enumeration mechanism.
_HID	Named object that provides the interface's Plug and Play identifier. This value may be TPM vendor specific. _HID is a standard device configuration control method defined in the ACPI Specification.	Required only for devices that do not have standard enumeration mechanism.
_STR	Named object that evaluates to a Unicode string that may be used by an OS to provide information to an end user describing the device. __STR is a standard device configuration control method defined in the ACPI Specification.	Optional
_UID	Named object that specifies a device's unique persistent ID, or a control method that generates it. _UID is a standard device configuration control method defined in the ACPI Specification.	Optional
_CRS	Named object that returns the TPM interface's current resource settings. Security hardware Interfaces are considered static resources; hence only return their defined resources. The address region definition is interface type/subtype dependent. _CRS is a standard device configuration control method defined in the ACPI Specification.	Required
_STA	Object that returns the status of the device: enabled, disabled or removed, as defined in the ACPI Specification. If this method is not present, the device is assumed to be enabled.	Recommended

_DSM	Device Specific Method Function 0 – standard query function Function 1 – TCG Hardware Information Arguments: Arg0 (Buffer): UUID - {CF8E16A5-C1E8-4e25-B712-4F54A96702C8} Arg1 (Integer): Revision ID = 1 Arg2 (Integer): Function Index = 1 Arg3 (Package): Arguments = empty package Returns: ACPI Buffer type; the definition of the return a package of 2 items and the description is as follows. Package item 1: Type: Integer Purpose: status of operation Description: 0: Failure 1: Success Package item 2: Type: Package Purpose: TCG Revision implemented in security hardware Description: A package of 2 integers: Integer 1: (BCD format) – most significant digits of TCG version Integer 2: (BCD format) – least significant digits of TCG version For example: a value of 0x0110 indicates the interface is compatible with TCG specification v1.1.	Optional
_GPE	Named object that evaluates to either an integer or a package. If _GPE evaluates to an integer, the value is the bit assignment of the SCI interrupt within the GPEx_STS register of a GPE block described in the FADT that the Security hardware device will trigger. If _GPE evaluates to a package, then that package contains two elements. The first is an object reference to the GPE Block device that contains the GPE register that will be triggered by the interface. The second element is numeric (integer) that specifies the bit assignment of the SCI interrupt within the GPEx_STS register of the GPE Block device referenced by the first element in the package. *Note:* This object is only provided if the interface supports a GPE.	Required if interrupt through GPE is supported