Annex to the
TCG Generic Server Specification
Version 1.0 Revision 0.8 (23 March 2005)

Mandatory and optional TPM Commands for Servers
Version 1.0 Revision 1.1 (10 April 2007)

Contact: *admin@trustedcomputinggroup.org*

TCG

TCG PUBLISHED

Disclaimers, Notices, and License Terms:

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.

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

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

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

Change History

Release	Description
Version 1.0 Revision 1.0	Initial final release
Version 1.0 Revision 1.1	Rectified accidentally unchanged status of the SetOrdinalAuditStatus command from optional to mandatory in order to align with the changed status of the GetAuditDigest and GetAuditDigestSigned commands. See also *TPM Main Specification Version 1.2 Level 2, Part 3 "Commands", Chapter 8 "Auditing"*.

To be conformant to this specification, the TPM **must** adhere to table 1 below.

Table 1:   **Ordinal Table of TPM Commands for Servers**

Function (by Ordinal Identifier)	M = Mandatory O = Optional X = Deleted in TPM 1.2
TPM_ORD_ActivateIdentity	M
TPM_ORD_AuthorizeMigrationKey	M
TPM_ORD_CertifyKey	M
TPM_ORD_CertifyKey2	M
TPM_ORD_CertifySelfTest	X
TPM_ORD_ChangeAuth	M
TPM_ORD_ChangeAuthAsymFinish	O
TPM_ORD_ChangeAuthAsymStart	O
TPM_ORD_ChangeAuthOwner	M
TPM_ORD_CMK_ApproveMA	M
TPM_ORD_CMK_ConvertMigration	M
TPM_ORD_CMK_CreateBlob	M
TPM_ORD_CMK_CreateKey	M
TPM_ORD_CMK_CreateTicket	M
TPM_ORD_CMK_SetRestrictions	M
TPM_ORD_ContinueSelfTest	M
TPM_ORD_ConvertMigrationBlob	M
TPM_ORD_CreateCounter	M
TPM_ORD_CreateEndorsementKeyPair	M
TPM_ORD_CreateMaintenanceArchive	O[1]
TPM_ORD_CreateMigrationBlob	M
TPM_ORD_CreateRevocableEK	O
TPM_ORD_CreateWrapKey	M
TPM_ORD_DAA_JOIN	**O[2]**
TPM_ORD_DAA_SIGN	**O[2]**
TPM_ORD_Delegate_CreateKeyDelegation	M
TPM_ORD_Delegate_CreateOwnerDelegation	M
TPM_ORD_Delegate_LoadOwnerDelegation	M
TPM_ORD_Delegate_Manage	M

Function (by Ordinal Identifier)	M = Mandatory O = Optional X = Deleted in TPM 1.2
TPM_ORD_Delegate_ReadTable	M
TPM_ORD_Delegate_UpdateVerification	M
TPM_ORD_Delegate_VerifyDelegation	M
TPM_ORD_DirRead	O³
TPM_ORD_DirWriteAuth	O³
TPM_ORD_DisableForceClear	M
TPM_ORD_DisableOwnerClear	M
TPM_ORD_DisablePubekRead	Oᴬ
TPM_ORD_DSAP	M
TPM_ORD_EstablishTransport	M
TPM_ORD_EvictKey	O
TPM_ORD_ExecuteTransport	M
TPM_ORD_Extend	M
TPM_ORD_FieldUpgrade	O
TPM_ORD_FlushSpecific	M
TPM_ORD_ForceClear	M
TPM_ORD_GetAuditDigest	**M**
TPM_ORD_GetAuditDigestSigned	**M**
TPM_ORD_GetAuditEvent	X
TPM_ORD_GetAuditEventSigned	X
TPM_ORD_GetCapability	M
TPM_ORD_GetCapabilityOwner	M
TPM_ORD_GetCapabilitySigned	X
TPM_ORD_GetOrdinalAuditStatus	X
TPM_ORD_GetPubKey	M
TPM_ORD_GetRandom	M
TPM_ORD_GetTestResult	M
TPM_ORD_GetTick	M
TPM_ORD_IncrementCounter	M
TPM_ORD_Init	M
TPM_ORD_KeyControlOwner	M
TPM_ORD_KillMaintenanceFeature	O¹
TPM_ORD_LoadAuthContext	O
TPM_ORD_LoadContext	M

Function (by Ordinal Identifier)	M = Mandatory O = Optional X = Deleted in TPM 1.2
TPM_ORD_LoadKey	O
TPM_ORD_LoadKey2	M
TPM_ORD_LoadKeyContext	O
TPM_ORD_LoadMaintenanceArchive	O[1]
TPM_ORD_LoadManuMaintPub	O[1]
TPM_ORD_MakeIdentity	M
TPM_ORD_MigrateKey	M
TPM_ORD_NV_DefineSpace	M
TPM_ORD_NV_ReadValue	M
TPM_ORD_NV_ReadValueAuth	M
TPM_ORD_NV_WriteValue	M
TPM_ORD_NV_WriteValueAuth	M
TPM_ORD_OIAP	M
TPM_ORD_OSAP	M
TPM_ORD_OwnerClear	M
TPM_ORD_OwnerReadInternalPub	M
TPM_ORD_OwnerReadPubek	O[B]
TPM_ORD_OwnerSetDisable	M
TPM_ORD_PCR_Reset	M
TPM_ORD_PcrRead	M
TPM_ORD_PhysicalDisable	M
TPM_ORD_PhysicalEnable	M
TPM_ORD_PhysicalSetDeactivated	M
TPM_ORD_Quote	M
TPM_ORD_Quote2	M
TPM_ORD_ReadCounter	M
TPM_ORD_ReadManuMaintPub	O[1]
TPM_ORD_ReadPubek	M[c]
TPM_ORD_ReleaseCounter	M
TPM_ORD_ReleaseCounterOwner	M
TPM_ORD_ReleaseTransportSigned	M
TPM_ORD_Reset	O
TPM_ORD_ResetLockValue	M
TPM_ORD_RevokeTrust	O

Function (by Ordinal Identifier)	M = Mandatory O = Optional X = Deleted in TPM 1.2
TPM_ORD_SaveAuthContext	O
TPM_ORD_SaveContext	M
TPM_ORD_SaveKeyContext	O
TPM_ORD_SaveState	M
TPM_ORD_Seal	M
TPM_ORD_Sealx	O
TPM_ORD_SelfTestFull	M
TPM_ORD_SetCapability	M
TPM_ORD_SetOperatorAuth	M
TPM_ORD_SetOrdinalAuditStatus	**M**
TPM_ORD_SetOwnerInstall	M
TPM_ORD_SetOwnerPointer	M
TPM_ORD_SetRedirection	O
TPM_ORD_SetTempDeactivated	O
TPM_ORD_SHA1Complete	M
TPM_ORD_SHA1CompleteExtend	M
TPM_ORD_SHA1Start	M
TPM_ORD_SHA1Update	M
TPM_ORD_Sign	M
TPM_ORD_Startup	M
TPM_ORD_StirRandom	M
TPM_ORD_TakeOwnership	M
TPM_ORD_Terminate_Handle	O
TPM_ORD_TickStampBlob	M
TPM_ORD_UnBind	M
TPM_ORD_Unseal	M

Table Notes:

- [1], [2], [3]: For each of these flags, if any of these optional commands are implemented, all those commands being flagged with the same label/value **must** become mandatory.

- [A]: The DisablePubekRead command may become mandatory on the PC-Client as part of an errata. At that time the Server Workgroup will consider to follow the PC-Client Workgroup.

- **B**: The OwnerReadPubek command needs to remain optional due to the general reviewing guideline (see paragraph "informative comments" below).

- **C**: The ReadPubek command needs to remain mandatory because there has to be a way to read the EK when there is no owner.

- **M**, **O**, **X**: Set in **bold face** denotes changes relative to the leveraged *TCG PC Client Specific TPM Interface Specification*.

Start of informative comments
- As the general reviewing guideline currently is to be able to have any PC-Client TPM being used as a Server TPM, any "M" in the PC-Client TPM Interface Specification can be turned into an "O", but turning an "O" into an "M" should be considered with care. The introduction of new TPM Commands should be avoided.
- Since for example the LPC-Bus is not necessarily present in servers, the leveraged *TCG PC Client Specific TPM Interface Specification* as a whole cannot be referenced bindingly in the *TCG Generic Server Specification* or this annex.

End of informative comments