Template for comments and secretariat observations

Date: 2014-10-08	Document: **ISO/IEC DIS 11889-1**	Project:

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
DE				ge	ISO/IEC International Standards are subject to periodic review no more than five years after publication. At that time, the responsible maintenance organization must determine whether the standard should be: Confirmed; Revised; Stabilized; or Withdrawn. When the maintenance responsibility is assigned to the PAS Submitter, according to JTC 1 SD 9 "Guide to the Transposition of Publicly Available Specifications into International Standards", Clause 6.2.5.2, it is the duty of the PAS Submitter to notify JTC 1 of its recommendation for approval under a systematic review ballot. In case of ISO/IEC 11889-1:2009 no systematic review ballot was conducted, nevertheless the Trusted Computing Group has initiated a fast track process of another PAS submission to replace the current edition of ISO/IEC 11889-1. For formal reasons alone, the document presented cannot be accepted as revision of ISO/IEC 11889-1.	Withdrawal of the proposed document	
DE	All	ALL	ALL	ge	The specification proposal for TPM 2.0 submitted by the Trusted Computing Group (TCG) as PAS submitter to ISO/IEC JTC 1 does not ensure conformity with the requirements of the German Federal Government as defined in the publication "Eckpunktepapier der Bundesregierung zu Trusted Computing und Secure Boot" published in August 2012 （http://www.bmi.bund.de/SharedDocs/Downloads/EN/Themen/OED_Verwaltung/Informationsgesellschaft/Eckpunktepapier_BregZuTrustedComputingSecureBoot.pdf?__blob=publicationFile), particularly with regard to the necessary controllability of the protected ICT system as well as the ICT security and privacy protection as a whole. The current ISO/IEC 11889:2009 standard does ensure conformity with the German Federal Government's requirements. The	Withdrawal of the proposed document.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					framework specification as proposed by TCG would replace the current specification in a way that future products would not necessarily meet the German Federal Government's requirements or, if certified according to ISO/IEC 11889:2009, might not be perceived as or actually count as “state of the art” anymore. Therefore, TCG's proposal is not in line with official requirements of the Federal Republic of Germany		
DE	All	ALL	ALL	ge	The new document differs greatly from the current edition of ISO/IEC 11889-1 and is much more complex. Using the fast track process for such an update does not allow for a proper consultation process where concerns of National Bodies can be adequately addressed Contrary to TCG's assertions i.a. in the Explanatory Report of the proposed specification, the PAS criteria as defined in the ISO/IEC JTC 1 Standing Document N 9 were not respected. Hence, TCG's PAS submitter status needs to be questioned. The proposed specification was not developed in a co-operative and transparent way as well within the TCG as with SC 27. Critical comments were not considered appropriately. TCG has not maintained the respective current standard sufficiently, particularly regarding the update of cryptographic algorithms. The actual PAS transposition process in combination with the Maintenance Agreement between TCG and JTC 1 is inadequate for the further development and maintenance of ISO/IEC 11889.	Withdrawal of the proposed document. TCG's PAS submitter status must be raised to question. In a possible re-application as PAS submitter ,TCG has to ensure that it will meet PAS criteria in the future considering its violations in the past. Improvement of both the Maintenance Agreement and the technical content of the specifications, especially regarding the cryptographic techniques and mechanisms provided.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
DE	All	ALL	ALL	ge	SC 27 has to be involved in the further development and maintenance of ISO/IEC 11889 in a co-operative, constructive, and transparent manner.	Withdrawal of the proposed document. TCG's PAS submitter status must be raised to question. In a possible re-application as PAS submitter ,TCG has to ensure that it will meet PAS criteria in the future considering its violations in the past. Improvement of both the Maintenance Agreement and the technical content of the specifications, especially regarding the cryptographic techniques and mechanisms provided.	
DE				ge	DIN NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ within NA 043-01-27 AA „ITSicherheitsverfahren“ recommends that its technical comments from 2012 should be discussed again to clarify, whether they have been considered appropriately in more recent documents of the TCG. According to ISO/IEC JTC 1 Standing Document N 9 “Guide to the Transposition of Publicly Available Specifications Into International Standards”: When the maintenance responsibility is assigned to the PAS Submitter, there are no provisions for minor updates/corrections/amendments as used by JTC 1 Subcommittees to maintain their documents, but the PAS Submitter must respond to maintenance issues raised by implementers and National Bodies.	Withdrawal of the proposed Document. Improvement to both the Maintenance Agreement and the technical content of the specifications, including but not limited to the improvement to cryptographic techniques and mechanisms provided. Actively maintain ISO/IEC 11889:2009 all parts. Reapplication for PAS submitter status. Improvement of the new proposal with a more appropriate inclusion of the technical comments received.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
					Decisions to approve modification requests and create updates are made using the PAS Submitter's procedures, and the decision to submit the revision to JTC 1 is made according to the process described in SD 9.		
DE	all			ge	According to ISO/IEC JTC 1 Standing Document N 9 "Guide to the Transposition of Publicly Available Specifications Into International Standards": When the maintenance responsibility is assigned to the PAS Submitter, a recommendation to Stabilize is not used with PAS submissions, as the PAS Submitter must actively maintain their document.	Actively maintain ISO/IEC 11889:2009 all parts and improved revision with a more appropriate inclusion of the technical comments received during the 11889 project. Establishment of a new project for a new TPM 2.x PAS proposal.	
DE	All	ALL	ALL	ge	The specification as proposed by TCG has to be complemented by a normative annex and appropriate normative reference to the existing ISO/IEC 11889:2009 document parts.	Withdrawal of the proposed document. Establishment of an appropriate normative annex and sufficient normative reference to the existing ISO/IEC 11889:2009 document parts. Stabilizing ISO/IEC 11889:2009 all parts and establishment of a new project for proposal.	
DE				ge	In any case the disappointment about "Trusted Computing", specifically the "Trusted Platform Module (TPM)" losing essential features with regard to the trustworthiness of this technology for device-owners, will neither foster TCG-specified technologies nor trustworthy Information and Communication Technology in general. Furthermore, the TPM 2.0 draft specification reduces potential, being present in IS 11889, to contribute to trust in ICT infrastructures, as well as precludes developing such potential even	Withdrawal of the proposed Document. Establishment of an appropriate normative annex and sufficient normative reference to the existing ISO/IEC 11889:2009 document parts. Actively maintain ISO/IEC 11889:2009 all parts and establishment of a new project for a new TPM 2.0 PAS proposal.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					further. It is useful to note that the “Key Requirements on “Trusted Computing” and “Secure Boot” by the German Federal Government, August 2012” became even more explicit in supporting “Complete control by device owners”, “Freedom of choice”, deactivation at time of delivery (opt-in principle), and privacy by design.		
DE	All	ALL	ALL	ge	For the certification of products which comply with the requirements of the German Federal Government a respective Common Criteria EAL4+ Protection Profile must be published as ISO/IEC standard.	Withdrawal of the proposed document. Initiation of the development of a Protection Profile according to ISO/IEC 15408.	
DE				ge	The TPM as currently specified in IS 11889 has a number of properties and assurances, which are essential for its wide acceptance and application. These properties and assurances were guaranteed by the original (as of 2009) TCG-specifications (i.e. TPM v1.2rev103, and accompanying platform-specifications as TIS v1.20, PPI v1.10, UEFI v1.20, BIOS v1.20 etc.) and general TCG-documents (e.g. the TCG-Principles v2.0), reasonably detailed and specific with regard to features and non-features of the TPM and TCG’s “Trusted Computing” in general. Moreover, the aforementioned specifications and documents are in line with the German Federal Government’s “Key Requirements on „Trusted Computing“ ”(2007) and “Position Paper on Trusted Computing” (2004), which emphasise on overarching political and technical design principles. In contrast, the drafts of the TPM 2.0 specification (called “Trusted Platform Module Library”) encompass a much broader approach, which	Withdrawal of the proposed Document.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
					mean many more TPM variants can be conformant to the specification. Unfortunately, this broadness also implies, that the TPM 2.0 draft specification in itself does not anymore guarantee the essential properties and assurances that IS 11889 is guaranteeing. Unfortunately, this broadness also implies, that the essential properties and assurances are not guaranteed anymore by every TPM variant, which conforms to the TPM 2.0 draft specification This is a major issue, as German legal and possibly constitutional requirements are affected. There are e.g. doubts, whether the current specification is compliant with the “right to confidentiality and integrity of IT systems” as formulated by the German Supreme Court in 2008. Especially there is concern regarding the integrity of the platform, given the fact that the platform hierarchy is not under full control of the owner. Specifically, it may be difficult, if not impossible to develop IT-Systems compliant with the aforementioned right, when the current specification is implemented as an integral part of the system. German interests may be affected by platforms, e.g. of German government systems, being under alien control.		
DE				ge	There is a radical departure from the former TPM design goals. The main reason for this change given by the TCG is the ease for corporate IToperations to remotely manage their TPMequipped devices. This is implausible, as these IT-operations do own these devices.	Withdrawal of the proposed document	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
					While the TPM 2.0 design is a perfect fit for ITdevices under alien control, usually called appliances, the fear of PCs, Servers, Laptops and Netbooks being rid of their most essential property as general purpose computers seems to be well-founded.		
DE	All			ge	Standardising the current TPM 2.0 specification in ISO/IEC JTC 1 is at least premature and may not be advisable anyway given the broad nature of this specification and its lack of security guarantees.	An option for resolving the issues in the context of general purpose computers is to define platformspecific profiles of the TCG-specifications, of which at least one comprises equivalent or stronger guarantees with regard to aforementioned properties and assurances, as the TCG-specifications and -documents did for the TPM 1.2 before 2011. This could also be a way to include the aspects which are relevant for the a.m. four requirements, but are currently specified in other TCG documents than IS 11889. The profile should include a detailed assuring explanation why and how the controllability for the owner is assured on the several levels of abstraction as described in the draft specification. This assurance document should then be the basis for certifications. ISO/IEC JTC 1/SC 27/WG 3 would be an excellent forum to	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
						specify the requirements for these profiles and their properties.	
DE	Page 20	7 Compliance	See citation in comment	te	"Unless the ISO/IEC 11889-3 general description of a command indicates that the command is mandatory, a compliant TPM need not implement the command. However, if implemented, the command is required to have the behavior defined in ISO/IEC 11889- 3. A platform-specific specification will indicate the commands from ISO/IEC 11889 that are required to be implemented in order to be compliant with that platform-specific specification." COMMENT: The text illustrates the non-binding character of the proposed standard. It is not defined what has to be implemented precisely. That means that commands required for plattform control may also not be implemented.	Withdrawal of the proposed document.	
DE	Page 20	7 Compliance	See citation in comment	te	"Even though the code in the reference implementation has undergone extensive testing, it is likely that some errors exist and one or more of those errors could lead to a TPM failure or exploit. Regardless of any other statement about normative behavior, one should not assume that a TPM exploit or failure is an intended behavior. It is not necessary to reproduce such a behavior in order to be compliant with ISO/IEC 11889." COMMENT: The specification refers to the reference implementation, which is not part of the ISO standardization. Therefore, it should not be mentioned in the document.	Withdrawal of the proposed document.	
DE	Page 50	11.4.11.2 Algorithm Support	See citation in comment	te	"If a TPM supports RSA, it should support a key size of 2048 bits or larger. Support for smaller key sizes is allowed but discouraged. Support for	Withdrawal of the proposed document.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
					smaller keys is allowed so that legacy keys may continue to be supported. Use of key sizes less than 1024 bits is strongly discouraged." COMMENT: No minimum key length is required. Also unsecure key lengths are still possible.		
DE	Page 229	Annex B (normative/informative) RSA, B.1 Introduction	See citation in comment	te	"A TPM that supports RSA should support a public modulus size of at least 2,048 bits. Support for other key sizes is permitted." COMMENT: No minimum key length is required. Also unsecure key lengths are still possible.	Withdrawal of the proposed document.	
DE	Page 67	13.3 Platform Controls	See citation in comment	te	"The platform manufacturer decides if it is possible to disable use of the TPM by the platform. The method for disabling use of the TPM by the platform is platform-manufacturer specific." COMMENT: Disabling a TPM is not part of the standard.	Withdrawal of the proposed document.	
DE	Page 70	13.8.1 Taking Ownership	See citation in comment	te	"Taking ownership of a TPM is the process of inserting authorization values for the ownerAuth, endorsementAuth, and lockoutAuth. A TPM that has been cleared (TPM2_Clear()) has its ownerAuth, endorsementAuth, and lockoutAuth values set to EmptyAuth and its ownerPolicy, endorsementPolicy, and lockoutPolicy values set to Empty Buffers. The OS is expected to change these values and manage them on behalf of the platform Owner." COMMENT: The definition of platform control is	Withdrawal of the proposed document.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	**Line number** (e.g. 17)	**Clause/ Subclause** (e.g. 3.1)	**Paragraph/ Figure/ Table/** (e.g. Table 1)	**Type of comment**[2]	**Comments**	**Proposed change**	**Observations of the secretariat**
					abstract. The entity having the auth value has control over the corresponding hierarchy. It is not defined who controls these values. There is only a hint but no requirement, that the OS should do this. We do not agree with this.		
DE	All			te	On by default (no Opt-In) A TPM 2.0 is on and immediately usable for technical components (e.g. firmware or operating systems), when an IT-device is delivered to its purchaser.	Opt-In The TPM must be completely off, when an ITdevice is delivered to its purchaser and can only be switched on by an explicit, conscious and informed decision met by its respective owner.	
DE	All			te	Lack of Choice A TPM 2.0 cannot be switched off completely: Hence, there is no way to fully opt-out of the TPM's use. The use of many critical functions (e.g. cryptographic key-, signature- and certificate-creation, -storage, -use and -deletion) cannot be prevented by the device-owner.	Freedom of Choice It is the device-owner's freedom, whether and which TPM functions to use, or not. In consequence this is also valid for securitysubsystems utilising a TPM.	
DE	All			te	Lack of Controllability Several key- and control-hierarchies exist in a TPM 2.0, some of which are not at all under owner-control, while others are under partial control of the device-owner, but still can be overruled (e.g. deleted) anytime by means of technical components (e.g. firmware or operating systems).	Controllability The TPM is solely controlled by the device-owner, unless he consciously decides otherwise (i.e. delegates his power of control).	
DE	All			te	No Privacy-friendliness DAA has become just an optional feature in	Privacy-friendliness Direct Anonymous Attestation (DAA) is	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Observations of the secretariat
					the TPM 2.0 draft specifications. Thus the guarantee that a TPM branded device supports DAA, will cease to exist e.g. for purchasers / owners, software providers, and system architects.	essential for the privacy-friendliness of TPMs and is therefore a mandatory feature of every TPM.	
DE	All			te	Since the SHA1 hash function is broken since many years all leading national standardisation organisations have requested to stop the use of SHA1. Unfortunately, the Trusted Computing organisation has only partly followed this advice. The actual proposal still allows to use SHA1. Since a migration to a more secure hash function is an additional task it is not unlikely that some implementations will continue using insecure cryptographic algorithms since it is not prohibited in the proposed document.	Withdrawal of the proposed Document. Actively maintain ISO/IEC 11889:2009 all parts and establishment of a new project for a new TPM 2.x PAS proposal. A technical specification shall not make use of the SHA1 hash function. Improvement of the new proposal with a more appropriate technical specification.	

[1] **MB** = Member body / **NC** = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by ******)

[2] **Type of comment:** **ge** = general **te** = technical **ed** = editorial