TCG Responses to the German Federal Government Position Paper Points

General
This document is the Trusted Computing Group’s (TCG’s) response to the “Federal Government’s Comments on the TCG and NGSCB in the Field of Trusted Computing” position paper dated 29 December 2003 (subsequently referred to as FGP). The TCG hopes that this document answers many of the questions raised in the FGP or at least serves as a basis for continued discussion and resolution of any concerns.

TCG wishes to once again thank the Federal Ministries of the Interior and of Economics and Labor (and the Federal Agency for Information Security) for the considered review and position paper on TCG and TCG specifications.

TCG Point-by-Point Response
The sections that follow contain specific responses to the points of the FGP. Section numbers noted below are references to the original sections of the FGP. As is often the case in written communications, it was not always possible for TCG to be certain we had the correct interpretation of the underlying concern.

Some of the responses in the points of the FGP tend to make similar comments. While we did not intend to make the answers overly repetitive, it was felt best to have the most complete answer as a standalone response to each point to facilitate discussions that might jump from point-to-point.

In several points of the FGP, TCG believes we have met the intent of the concern. In these areas, TCG would like to: 1) understand if this point is just a shared view of the goal of the effort; or 2) understand specific instances where such intent is not met. TCG, within the scope of its bylaws and organization responsibility, is committed to resolve any concerns in area #2.

Section 1 – Transparency and disclosure of interface and specifications
- Section 1.1, “Standard and ‘approved’ algorithms”
  - TCG believe we have met these requirements. Over time, TCG expects algorithms to advance to meet changing market conditions.
  - TCG is open to discussion of specific areas of concern.
- Section 1.2, “Key lengths, etc. must conform to German Government requirements”
  - TCG specifications provide for a trustworthy and marketable level of security. If there are unique requirement for specific markets, TPM and OEM vendors can differentiate and compete to meet those market needs, and are responsible for complying with any relevant laws in force in each jurisdiction.
  - Specifically regarding the use of the SHA-1 algorithm: The TCG and BSI agree that there is no current weakness in the SHA-1 algorithm employed in TCG specifications. The reason that SHA is only used with an output length of 160-bits is that allowing flexibility would have greatly complicated the data structures and in many cases made interoperability impossible. It is not feasible or necessary to change this now because it would break backward compatibility and require too great a change to the specification. TCG understands the concern and when it
becomes clear that an upgrade of SHA-1 becomes necessary, the TCG would plan to upgrade as appropriate.

- Section 1.3, “no undocumented TPM functions / Backdoors”
  - TPM’s are evaluated by 3rd party Common Criteria evaluation labs. TPM vendors are responsible to provide for this evaluation.
  - TCG would like to better understand recommended approaches that would help alleviate this concern.
- Section 1.4, “TCG should document application scenarios around TPMs”
  - TCG has use scenarios documented and can provide this information.

Section 2 – Certification of the security system

- Section 2.1, “Must Certify to EAL 4”
  - The TCG is in the process of creating the protection profile for the TPM 1.2 version. The TPM protection profile (work-in-progress) will be modified to reflect the EAL4-Medium cc certification requirement.
- Section 2.2, “No integration of TPM functionality, TPM remains a discrete component”
  - We believe that higher levels of integration will continue to occur on the platform as we have seen in the past. With each integration opportunity, tradeoffs need to be assessed. Integration will need to be weighed against the security model, as well as against other considerations such as manufacturability, cost, etc. In the case of the TPM, we do see integration into other subsystems occurring and it will be up to the vendors to provide assurance that they continue to meet the TPM specification and provide appropriate security assurance.
  - It is also important to note that integration does not affect the user/owner functional controls provided for in the TPM specification. The user still must choose to ‘opt in’ regardless of physical integration point.
  - For markets that demand a discrete TPM, vendors have the opportunity to differentiate and satisfy market specific requirements.

Section 3 – System security, data backup and migration

- Section 3.1, “Transfer of data and keys from old or defective platform”
  - TCG provides both migration and optional maintenance capabilities.
  - With migration, keys can be specified as migratable or non-migratable. When data is encrypted, either a migratable or non-migratable key is chosen to indicate whether the data can be moved.
  - With maintenance, the TPM manufacturer can assist the Owner in securely moving migratable and normally non-migratable data from one TPM to another from the same manufacturer.
  - TCG does not specify how data used by applications may be bound, transferred or recovered from a platform. It is the anticipated that application developers will provide appropriate security, portability, controllability and ease of use features to the users of the software. The TPM migration and maintenance capabilities can be used to support such features. The Best Practices Design, Implementation, and Usage Principles will also offer specific guidance to OSVs and ISVs.
- Section 3.2, 3.3, “ability of user to migrate copyrighted and non-copyrighted data to other systems”
  - The TCG specifications certainly provide for this kind of use. Applications (in the case of copyrighted data, DRM systems) and the policy they implement must allow for this kind of data migration, whether or not they use a TPM as the basis for aspects of their implementation. TCG’s Best Practices Design,
Implementation, and Usage Principles document will provide ISVs guidance here as well.

- Section 3.4, “no single point of failure”
  The use of secure systems certainly puts a greater onus on the users and administrators of these systems to properly backup their system so that failures are recoverable. The TCG specifications provide mechanisms by which keys can be backed up and restored to recover from failures. Therefore we believe that TCG implementations will accommodate your quite valid concerns.

- Section 3.5, “EK generated on-chip or through certified process”
  - TCG agrees and believes we have the same expectation in the specification.

**Section 4 –System check by the user**

- Section 4.1, “Switch for opt-in control”
  - The TCG specifications require provable “physical presence” for the opt-in control of TPM. This “physical presence” provides strong owner control, ensuring that the TPM can not be turned on without the owner’s knowledge. There are multiple ways to implement “physical presence”. The BIOS method (a logical switch) is one approach, and a physical switch is another. The implementation of “physical presence” is an OEM option and opportunity to differentiate.
  - In systems where the TPM is indeed disabled, TCG expects software that does not require the security facilities of the TPM to function properly. TCG’s Best Practices Design, Implementation, and Usage Principles document will provide guidance here as well.

- Section 4.2, “Security module default disabled”
  - TCG agrees and already supports the “opt-in” approach. TCG’s Best Practices Design, Implementation, and Usage Principles document will provide guidance here as well.

- Section 4.3, “Full User control of keys”
  - There are a variety of keys provided for in the TCG/TPM specifications. The owner controls the ability to create, use and invalidate any key. The TPM specification provides the ability for the owner to delegate this control to the user. Use of a key created by a user (as delegated by the owner) is under the control of the user.
  - The Endorsement Key (EK), generally installed during the TPM manufacturing or system configuration process, is the basis for establishing TPM authenticity and hence the foundation for trust in the platform. The Endorsement Key (EK) is a special case and, though the TPM V1.2 specification allows deletion of the EK, it is expected that TPM owners will use the EK as provided.
  - Please clarify any specific concerns.

- Section 4.4, “User control of access to keys and protection against unauthorized access”
  - Agree, and believe TPM specification provides for such control.

- Section 4.5, “Requirement for Smartcard”
  - Smart cards and TPMs are complementary technologies with smart cards generally providing user authentication and TPMs providing platform authentication. In some uses, a TPM alone can be sufficient. In other uses, the combination of TPM and Smart Card would provide superior protection. Providing the right “mix” of security technologies is an opportunity for OEM differentiation, and market forces will determine the right mix to address user needs.

- Section 4.6, “No external certification of software enforced by TPM”
  - Agree, and TPM specs and TCG information clearly indicate there is no such requirement, nor intent, to establish any 3rd party certification of SW for
“goodness”. The user chooses what SW to run. Furthermore, TSS provides an OS neutral interface for access to TPM functions. TCG’s Best Practices Design, Implementation, and Usage Principles document will provide guidance here as well.

Section 5 – Data protection

- Section 5.1, “assured ability for user to exercise data protection control”
  - TCG believes it has provided the fundamental controls in the TPM and platform to accomplish this. Requires cooperation of the OS and SW. TCG’s Best Practices Design, Implementation, and Usage Principles document will provide guidance here as well.
- Section 5.2, “per-transaction approval”
  - TCG believes it has provided specifications that allow the fundamental user and fine grained owner controls in the TPM and platform to accomplish this. The TCG specifications provide for a range of software implementations allowing the OS and applications to provide the proper balance within the dimensions of control, privacy and ease-of-use. TCG’s Best Practices Design, Implementation, and Usage Principles document will provide guidance here as well.
- Section 5.3, “use of security must be possible without connection to internet”
  - TCG agrees. TCG Best Practices Design, Implementation, and Usage Principles will advise SW vendors in this way.
- Section 5.4, “prevent indirect linking of AIK’s”
  - TCG agrees with the concern. TCG Best Practices Design, Implementation, and Usage Principles will offer guidance here.
- Section 5.5, “User option to select alternate CA’s”
  - TCG provides the mechanisms for user selection of multiple of Privacy CA’s (Trusted Third Parties - a role that is a little different than a traditional CA) to be used. It is still a business decision for a company to enter the Privacy CA market.
- Section 5.6, “CA’s must operate under government supervision, …”
  - TCG will offer Best Practices Design, Implementation, and Usage Principles for Privacy CA vendors. Any necessity of Government supervision of CA/Privacy CA is a concern and decision of each individual government and is outside the scope of TCG. It is expected that Privacy CAs will necessarily adhere to local government regulations.
- Section 5.7, “preference for Direct Proof approach”
  - Direct Proof and Privacy CA approaches offer different means to validate the authenticity of a TPM-enabled platform. The needs of different use models and market forces will determine which approach is used to best solve user needs.
  - TCG Best Practices Design, Implementation, and Usage Principles will also provide guidance on where and how each approach might best be used.

Section 6 – Fair license policy

- Sections 6.1-6.4, 7.1 – Concern about ability of the technology to be used by a variety of HW and OS platforms.
  - It is TCGs goal to have this technology widely deployed and used. TCG is under a RAND IP licensing policy, very common for the computer industry. Members have IP rights per the TCG bylaws.
  - TCG specs are vendor neutral (CPU and OS neutral). They can be implemented and used on a variety of HW and OS platforms. TCG hopes to see wide implementation of the specifications and will do what it can to further that goal.
• Section 6.2, “TSS should be offered under (effectively) open source license”
  - Implementations of TCG specifications are generally developed by individual companies and as such TCG is not the owner or supplier of these implementations. TCG has not implemented TSS nor does TCG own TSS source code. Vendors that implement TSS must determine their own licensing policy.

• Section 6.3, “TCG Members should commit to offering their IP under RAND terms”
  - To reach “Final” TCG specification status, member companies with IP in the TCG specification must commit to RAND IP licensing to other TCG members. TCG “Adopter” membership provides for a low fee membership allowing participation in the TCG RAND licensing scheme.
  - The TCG plans to create a new fee tier for the Adopter level membership, aimed at making Adopter level membership more attractive for small and medium enterprise (SME) companies. This new fee tier will be available at a cost of $1000 annually, for companies with 100 employees or less. The fee for companies of greater than 100 employees will be $7500 annually.
  - We would like to re-emphasize that all TCG member companies are legally committed to the RAND licensing provisions of the organization. We would like to continue our discussions clarifying TCG RAND licensing policies.

• Section 6.4, “Potential creation of ‘patent pool’, allowing ‘one-stop’ licensing”
  - The creation and management of a ‘patent pool’ is currently outside the scope of TCG. TCG IP provisions are consistent with common practices of similar industry standards groups.

Section 7 – Non-discriminating information policy
• Section 7.1, “Free membership to TCG”
  - The Liaison and Advisory Council programs provide additional ($0 membership cost) means for participation in TCG activities for qualified individuals and organizations.
  - TCG believes its membership policies are consistent with similar organizations. If there are specific instances of discrimination in violation of TCG bylaws, the TCG BOD will remedy them.

• Section 7.2, “Balanced representation of interests…in TCG”
  - TCG is a transparent, non-discriminating organization whose membership is open to companies that adhere to the bylaws and pay the associated yearly membership fee.
  - TCG membership spans the globe, with members from many countries and representing many different market segments.

Section 8 – Security technology may not create market access barriers
• Section 8.1, 8.2 – “No reinforcement or creation of market access barriers”
  - TCG is a transparent, non-discriminating organization that is open to companies that adhere to the bylaws and pay the associated yearly membership fee. It is TCGs goal to have this technology widely deployed and used.
  - TCG members of a given membership level are treated equally and have access to the specifications and ability to contribute to the development of TCG specifications as defined by the TCG bylaws. TCG specifications are vendor neutral (CPU and OS neutral) and it is therefore expected that a large number of companies from different parts of the world will offer TCG compliant products.
  - TCG Best Practices Design, Implementation, and Usage Principles will offer clear guidelines for interoperability.
• Section 8.3, “arbitration council for disputes”
  - The TCG BOD, in adherence to and within the scope of the TCG Bylaws, is prepared to address any concerns raised from inside or from outside the TCG organization.

Section 9 – Technological openness

• Section 9.1, “comparable cost and effort for inclusion of TPMs in different systems”
  - This is a goal of TCG and TCG specs are vendor neutral (CPU and OS neutral). If there are specific situations where this is not true, TCG will work to address them.
  - As another point, there is active work inside TCG on the investigation and specification of TPM devices that will be suitable for use in other computing platforms such as handheld devices and servers.

• Section 9.2, “interoperability with non-TCG based systems”
  - TCG Best Practices Design, Implementation, and Usage Principles and the efforts of the Infrastructure Work Group are currently addressing these interoperability issues.

• Section 9.3, “specifications should not give unfair advantage to individual member companies…”
  - TCG bylaws provide for open and equal access to the TCG work product for all Contributor and Promoter members. Any company that is interested in early access to TCG specifications is invited to join TCG as a Contributor and thus gain access to and influence the ongoing specification development work.
  - In order to provide timely information access, TCG workgroups will post their work-in-progress, on specifications that are under development, on a quarterly basis, available to all members, including Adopter members. Additionally, adopter members see early versions of the specification as part of the mandatory IP review process called out in the TCG bylaws.
  - Approved TCG Specifications are made available to the public.
  - TCG is committed to developing open, vendor-neutral specifications that serve the common interests of our membership, and is not structured nor governed in a way as to provide any individual company with advantage over other companies.

Sections 10 & 11 – Microsoft’s NGSCB security concept

• Sections 10 and 11
  - It is inappropriate for TCG to comment on specific plans/positions of individual companies. Please discuss any concerns with the specific company.