Key requirements on „Trusted Computing“
by the German Federal Government, 04 September 2007

1. Definition of terms
   The German Federal Government defines Trusted Computing as architectures, implementations, systems and infrastructures which are based on or are utilising the specifications of the Trusted Computing Group (TCG). A more general, broader meaning of the term Trusted Computing will be explicitly stated in order to avoid misinterpretations.

2. Enhancing IT security
   The German Federal Government appreciates and supports an increased level of IT security provided by the deployment of Trusted Computing solutions on IT platforms of enterprises, public administrations and citizens on the basis of TCG’s specifications. The German Federal Government promotes and actively participates in this process.

3. Availability of the specifications
   All effective specifications on Trusted Computing must be available free of charge and completely for everyone at any time, irrespective of a TCG membership. Likewise possible secondary documents by the TCG that contain explanatory, substantiating or confining information must be freely available for any interested party.

4. Open standards
   Regardless of a TCG membership, everybody must be entitled to apply all specifications in their completeness in architectures, implementations, systems and infrastructures. No royalties shall be imposed for applications of the specifications (e.g. due to patent claims).

5. Freedom of research
   Specifications concerning Trusted Computing shall be designed in a manner not hampering academic research on Trusted Computing-based solutions and their interaction with alternative approaches. The German Federal Government promotes independent academic research on Trusted Computing technologies and their implications.

6. Interoperability
   While implementing secure platforms, the use of Trusted Computing solutions which are interoperable with alternative approaches must be to the fore. For the deployment in the German Federal Administration the interoperability of Trusted Computing solutions with either other Trusted Computing-based solutions or alternative approaches has to be guaranteed.

7. Transparency
   All specifications, solutions and their development in the field of Trusted Computing have to be created transparently regarding their actual purpose, their functional characteristics and the applied cryptographic mechanisms.
8. **Certification**  
Each Trusted Computing solution based on the specifications of the TCG shall be transparent, comprehensible and certifiable for various security levels. The Trusted Platform Module (TPM) as a fundamental component must feature a Common Criteria certification at least of level EAL4+ ("resistant against moderate attack potential"). All certification approaches shall not preclude enterprises, academic research or solutions under free licences.

9. **National IT industry**  
The German Federal Government regards Trusted Computing technology as affecting national security interests as well as the competitiveness of the German IT security industry. Therefore, the Federal Government calls for fair and transparent competition conditions for all IT security businesses and insistently invites German companies to offer products based on the specifications of the TCG, provided that the prerequisites of requirement 4 are given.

10. **Freedom of choice**  
IT managers, IT administrators, and IT users must be enabled to responsibly decide about product selection, deployment, configuration, operation and decommissioning of Trusted Computing solutions due to the required technical and functional transparency. A deactivation must not result in any negative effect on the functionality of hardware and software which is not using the features of Trusted Computing technology.

11. **Guarantee of IT security**  
From the perspective of the German Federal Government, Trusted Computing is an important step towards achieving IT security objectives such as confidentiality, integrity, availability and authenticity. Every Trusted Computing solution in use has to be tested for compliance with these security objectives. Notably the availability must not be subject to coercive external control and the confidentiality must not be compromised by inadequate sway over one’s own keys.  
In the interest of the transparency necessary for examination of IT security, it is essential, that neither undocumented functionality is incorporated nor the TPM functionality can be tampered with by other hardware functionality or components. Particularly the deployment in security critical networks (e.g. in public administration) exclusively demands certified TPMs. Currently the German Federal Government only considers discrete TPMs to match this prerequisite.

12. **Availability of critical infrastructures**  
The use of Trusted Computing solutions by critical infrastructure providers has to be conducted such that no additional risks for critical processes arise – particularly concerning the security objective availability. The ability for an unhindered and flexible immediate recovery of infrastructures is a must, even in case of crisis or disaster management.

13. **Protection of digital works**  
The German Federal Government considers sustainable protection of digital works stored, processed and transmitted by means of IT as a substantial feature of Trusted Computing for everyone. This protection has to be achieved under a balanced and fair consideration of the interests of proprietors and holders (i.e. users) of data and devices on which such data is processed.
14. **Data protection**
   The protection of personal data is an important prerequisite for increasing IT security. Thus Trusted Computing applications have to comply with the data protection regulations which are always prioritised over economical interests due to being derived from constitutionally guaranteed rights.

15. **Standardisation**
   For a broad usage of Trusted Computing technology, its standardisation is essential. This is mainly a task of the corporations involved. Moreover, the German Federal Government actively takes part in devising the standardisation process and pays attention that the terms for participating in the creation of the specifications are fair, open, reasonable and non-discriminatory for German enterprises, research institutes and interest groups. The participation of German organisations is actively promoted.

16. **International cooperation**
   National solo-attempts are not very promising in the age of globalisation, notably in the context of information and communication technologies. For this reason, the German Federal Government insistently calls on German enterprises and organisations to engage in Trusted Computing projects, particularly participating in the TCG. Furthermore, the German Federal Government actively cooperates with governmental and non-governmental organisations at international level on issues of Trusted Computing, particularly aiming at implementing the key requirements for Trusted Computing as stated in this paper. Beyond that, the German Federal Government places the special IT security requirements of the public sector in the TCG as well as in other projects and initiatives concerning Trusted Computing technology.