Key Requirements on “Trusted Computing” and “Secure Boot”

by the German Federal Government, August 2012

1. Definition of terms

The Federal Government defines ”Trusted Computing“ as architectures, implementations, systems and infrastructures which are based on or utilise the specifications of the Trusted Computing Group (TCG). This includes ”Secure Boot“ and additional functions in the Unified Extensible Firmware Interface (UEFI) specification of the Unified EFI forum which builds on the TCG specifications or closely related technologies.
To avoid misunderstanding, any more general use of the term ”Trusted Computing“ will always be explicitly stated.

2. Enhancing IT security

The Federal Government supports raising the level of IT security on IT platforms of enterprises, public administrations and private users by introducing Trusted Computing solutions based on TCG specifications that meet the criteria listed in these key requirements.

3. Complete control by device owners

Device owners must be in complete control (i. e., having controllability and observability) of all the Trusted Computing security systems of their devices. As part of exercising control over their devices, device owners must be able to decide how much of this control to delegate to their users or administrators. Delegating this control to third parties (to the device manufacturer or to hardware or software components of the device) requires conscious and informed consent by the device owner (i. e., also the device owner’s full awareness of possible limits of availability due to measures taken by the third party to whom control options were delegated).

4. Freedom of choice

When devices are delivered, Trusted Computing security systems must be deactivated (opt-in principle). Based on the necessary transparency with regard to technical features and content of Trusted Computing solutions, device owners must be able to make responsible decisions when it comes to product selection, deployment, configuration, operation and decommissioning. Deactivation must also be possible later (opt-out feature) and must not have any negative impact on the functioning of hardware and software that does not use Trusted Computing technology.

5. Public administration, national and public security interests

Because Trusted Computing security systems are widely used in the private-law mass market, public administration can and should be able to benefit from the availability of cost-effective solutions as well. However, the operation and availability of devices in public administration and in the field of national and public security require the owner's sole control over the Trusted Computing security systems on the devices used by the owner. Due to public and national security interests, under no circumstances may the owner be forced to give up control, even partial control, over a Trusted Computing security system to other third parties outside the public administration's sphere of influence.

6. Personal use
The Federal Government explicitly calls on makers of trusted computing devices and components (both hardware and software) to offer devices and components also to private users which allow owners complete control over the Trusted Computing security system at all times.

7. Availability of the specifications
All effective specifications on Trusted Computing must be available in full and free of charge to everyone, members of TCG and non-members alike, at all times. Any secondary TCG documents which explain, specify or delimit must also be freely available to all interested parties.

8. Open standards
Everyone, whether member of TCG or not, must be in a position to fully use all Trusted Computing specifications for application in architectures, implementations, systems and infrastructures. No licensing fees (e. g. based on patent rights) may be charged for using the specifications.

9. Freedom of Research
Trusted Computing specifications should be designed not to create barriers to academic research on Trusted Computing based solutions and their interaction with alternative approaches. Ways to restore defined previous settings should be provided. The Federal Government supports independent academic research on the technology of Trusted Computing and its implications.

10. Interoperability
When creating secure platforms, the interoperable use of Trusted Computing solutions with alternative approaches must be a priority at all times and should be implemented wherever it does not interfere with the specific purpose of the device. In addition, same types of Trusted Computing applications should be interoperable. For use in the Federal Administration, Trusted Computing products must be interoperable both with other solutions based on Trusted Computing and with alternative solutions.

11. Transparency
All specifications, solutions and their development in the field of Trusted Computing have to be created transparently with regard to their actual purpose, their functional features and the cryptographic mechanisms. The required transparency means that only completely documented functions without any hidden processes will be carried out. Transparency refers not only to documentation, but also to explaining the technologies used and their effects to owners and users in terminology they can understand.

12. Certification
Every Trusted Computing solution based on TCG specifications should be transparent, understandable and certifiable for various security levels. As a basic component, the Trusted Platform Module (TPM) must feature at least a Common Criteria certification of level EAL4+ (“resistant against moderate attack potential“). Certification may not lead to the exclusion of businesses, academic research or solutions under free licences if these solutions can be examined in the necessary depth.

13. National IT industry
In the Federal Government's view, Trusted Computing technology affects both national security interests and the competitiveness of the German IT security industry. The Federal Government therefore calls for fair, transparent and non-discriminatory competition between all IT security companies and calls on German industry to offer products based on the TCG specifications that meet the criteria given in these key requirements.

14. Ensuring IT security
The Federal Government believes that Trusted Computing can significantly contribute to achieve the IT security objectives of confidentiality, integrity, availability and authenticity. Every Trusted Computing solution is to be checked for compliance with the required security objectives. In particular, availability must not be subject to external control, and confidentiality must not be compromised by insufficient authority over own keys. In the interest of the transparency needed to evaluate IT security, it is in any case important that there are no undocumented functions, and that other hardware components or functions cannot influence the functioning of TPMs. For use in security-critical networks in particular (e. g. in public administration), only certified TPMs may be used. In the Federal Government's view, this criterion is currently met only by discrete TPMs.

15. Availability of critical infrastructures
Trusted Computing solutions for critical infrastructure providers must be used in a way that does not result in any additional risks to critical processes, especially with regard to the security objective of availability. It must be possible to restore infrastructure rapidly without impediment and flexibly, even in case of crisis or disaster management.

16. Protection of digital content
In line with these key requirements, the Federal Government regards the long-term protection of stored, processed and transmitted digital content for all as a substantial feature of Trusted Computing. Trusted Computing based mechanisms should not restrict or alter the general legal and social conditions for using such digital content.

17. Data protection
The protection of personal data is an important prerequisite for increasing IT security. For this reason, when developing and utilizing Trusted Computing applications, the regulations of data protection must be respected (privacy by design) and may take priority over economic interests in the context of a constitutional-law weighing of interests.

18. Standardisation
Standardisation is crucial to the widespread use of Trusted Computing technology and is primarily the responsibility of the companies involved. The Federal Government is also involved in designing the standardisation process and is watching to make sure that businesses, research institutions and interest groups in Germany have fair, open, reasonable and non-discriminatory access to the drafting of specifications. The participation of German organisations is being supported.

19. International cooperation

In this age of globalization, especially with regard to information and communications technology, ”going it alone“ at national level has little chance of success. For this reason, the Federal Government calls on businesses and organizations in Germany to become involved in Trusted Computing projects and in the TCG in particular. In addition, the Federal Government is actively working at international level with governments and non-governmental organizations on issues of Trusted Computing, in particular to see that the key requirements for the Trusted Computing strategy defined in this paper are met. The Federal Government also serves as an advocate in the TCG and other Trusted Computing projects and initiatives for the public sector's special IT security requirements.