

Eckpunktepapier „Trusted Computing“ der Bundesregierung

04 September 2007

1. **Begriffsbestimmung**

Die Bundesregierung versteht unter „Trusted Computing“ die Architekturen, Implementierungen, Systeme und Infrastrukturen, die auf den Standards der Trusted Computing Group (TCG) basieren oder diese nutzen. Zur Vermeidung von Missverständnissen wird eine darüber hinausgehende, allgemeinere Verwendung des Begriffs „Trusted Computing“ stets besonders gekennzeichnet.

2. **Erhöhung der IT-Sicherheit**

Die Bundesregierung begrüßt und unterstützt eine Erhöhung des Niveaus der IT-Sicherheit durch die Einführung von „Trusted Computing“-Lösungen auf IT-Plattformen von Unternehmen, öffentlicher Verwaltung und Privatanwendern auf Grundlage der Standards der TCG. Dieser Prozess wird durch die Bundesregierung gefördert und aktiv mitgestaltet.

3. **Verfügbarkeit der Standards**

Alle geltenden Standards zu „Trusted Computing“ müssen unabhängig von einer Mitgliedschaft in der TCG für jedermann jederzeit kostenfrei und vollständig verfügbar sein. Ebenso müssen ggf. vorhandene erläuternde, konkretisierende oder abgrenzende Sekundärdokumente der TCG jedem Interessierten frei zur Verfügung stehen.

4. **Offene Standards**

Unabhängig von einer Mitgliedschaft in der TCG müssen alle Standards zu „Trusted Computing“ von jedermann vollständig zur Umsetzung in Architekturen, Implementierungen, Systemen und Infrastrukturen verwendet werden können. Für die Anwendungen der Standards dürfen keine Lizenzgebühren (z. B. aus Patentansprüchen) erhoben werden.

5. **Freiheit der Forschung**

Standards zu „Trusted Computing“ sind so zu gestalten, dass die akademische Forschung zu „Trusted Computing“-basierten Lösungen und deren Zusammenspiel mit Alternativen nicht behindert wird. Die Bundesregierung fördert die unabhängige akademische Forschung zur Technologie des „Trusted Computing“ und deren Folgen.

6. **Interoperabilität**

Bei der Realisierung sicherer Plattformen muss der interoperable Einsatz von „Trusted Computing“-Lösungen mit alternativen Ansätzen jederzeit im Vordergrund stehen. Für den Einsatz in der Bundesverwaltung muss gewährleistet sein, dass „Trusted Computing“-Produkte sowohl mit anderen „Trusted Computing“-basierten als auch mit alternativen Lösungen interoperabel sind.

7. **Transparenz**

Sämtliche Standards, Lösungen und deren Erarbeitung im Bereich „Trusted Computing“ sind transparent im Hinblick auf ihren tatsächlichen Zweck, ihre funktionalen Eigenschaften und verwendete kryptographische Techniken zu erstellen.

8. **Zertifizierung**

Jede „Trusted Computing“-Lösung auf Basis der Standards der TCG soll transparent, nachvollziehbar und für unterschiedliche Sicherheitsniveaus zertifizierbar sein. Das Trusted Platform Module (TPM) als grundlegende Komponente muss mindestens eine Zertifizierung nach Common Criteria EAL4+ („resistant against moderate attack potential“) aufweisen. Zertifizierungsansätze sollen dabei weder zum Ausschluss von Unternehmen, der akademischen Forschung oder Lösungen unter freien Lizenzen führen.

9. **Nationale IT-Industrie**

Die Bundesregierung sieht durch die „Trusted Computing“-Technologie sowohl nationale Sicherheitsinteressen als auch die Wettbewerbsfähigkeit der deutschen IT-Sicherheitsindustrie betroffen. Die Bundesregierung fordert daher faire, transparente Wettbewerbsbedingungen für alle IT-Sicherheitsunternehmen und ruft deutsche Unternehmen nachdrücklich auf, Produkte auf Basis der Standards der TCG anzubieten, sofern die Voraussetzungen von Punkt 4 gegeben sind.

10. **Entscheidungsfreiheit**

IT-Verantwortliche, IT-Administratoren und IT-Anwender müssen in der Lage sein, aufgrund der vorausgesetzten technischen und inhaltlichen Transparenz von „Trusted Computing“-Lösungen eigenverantwortliche Entscheidungen zur Produktauswahl, Inbetriebnahme, Konfiguration, Anwendung und Stilllegung zu treffen. Eine Deaktivierung darf keine negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktion der „Trusted Computing“-Technologie nutzen.

11. **Gewährleistung der IT-Sicherheit**

„Trusted Computing“ bietet aus Sicht der Bundesregierung einen wesentlichen Schritt zur Erreichung der IT-Sicherheitsziele, wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Jede eingesetzte „Trusted Computing“-Lösung ist auf die Einhaltung dieser geforderten Sicherheitsziele zu prüfen. Insbesondere darf die Verfügbarkeit nicht zwangsweise externer Kontrolle unterliegen und die Vertraulichkeit nicht durch unzureichende Verfügungsgewalt über eigene Schlüssel kompromittiert werden.

Im Interesse der für die Beurteilung der IT-Sicherheit erforderlichen Transparenz ist es in jedem Fall wichtig, dass keine undokumentierten Funktionen enthalten sind, sowie eine Beeinflussung der TPM-Funktionalität durch andere Hardware-Komponenten oder -funktionalitäten ausgeschlossen ist. Insbesondere für den Einsatz in sicherheitskritischen Netzen (z. B. in der öffentlichen Verwaltung) können ausschließlich zertifizierte TPM zum Einsatz kommen. Diese Voraussetzung sieht die Bundesregierung derzeit lediglich bei diskreten TPM gegeben.

12. **Verfügbarkeit von Kritischen Infrastrukturen**

Der Einsatz von „Trusted Computing“-Lösungen bei Betreibern Kritischer Infrastrukturen muss so erfolgen, dass sich daraus keine zusätzlichen Risiken für Kritische Prozesse ergeben – dies gilt insbesondere für das Sicherheitsziel Verfügbarkeit. Eine schnelle Infrastrukturwiederherstellung selbst im Rahmen von Krisen- und Katastrophenbewältigung muss unbehindert und flexibel erfolgen können.

13. Schutz digitaler Werke

Die Bundesregierung sieht eine wesentliche Funktionalität von „Trusted Computing“ in einem nachhaltigen Schutz der mittels Informationstechnik (IT) gespeicherten, verarbeiteten und übertragenen digitalen Werke für jedermann. Dieser Schutz ist unter einer ausgewogenen, fairen Berücksichtigung der Interessen von Rechteinhabern und Besitzern (d. h. Nutzern) von Daten und den Geräten, auf denen diese verarbeitet werden, zu realisieren.

14. Datenschutz

Der Schutz personenbezogener Daten ist eine wichtige Voraussetzung für die Steigerung der Sicherheit im IT-Bereich. Daher sind die Bestimmungen des Datenschutzes bei „Trusted Computing“-Anwendungen zu berücksichtigen und haben aufgrund ihrer Ableitung aus grundgesetzlich verbrieften Rechten immer Vorrang vor wirtschaftlichen Interessen.

15. Standardisierung

Für einen breiten Einsatz der „Trusted Computing“-Technologie ist es essentiell, diese zu standardisieren. Dies ist hauptsächlich eine Aufgabe der beteiligten Unternehmen. Darüber hinaus gestaltet die Bundesregierung den Standardisierungsprozess aktiv mit und achtet darauf, dass der Zugang zur Erstellung der Standards für deutsche Unternehmen, Forschungseinrichtungen und Interessengruppen fair, offen, angemessen und diskriminierungsfrei gestaltet wird. Die Beteiligung deutscher Organisationen wird aktiv unterstützt.

16. Internationale Zusammenarbeit

Nationale Alleingänge sind im Zeitalter der Globalisierung, insbesondere in Bezug auf die Informations- und Kommunikationstechnologie, wenig Erfolg versprechend. Aus diesem Grund fordert die Bundesregierung deutsche Unternehmen und Organisationen nachdrücklich zum Engagement in den Projekten zu „Trusted Computing“, insbesondere aber in der TCG auf. Darüber hinaus arbeitet die Bundesregierung international aktiv mit staatlichen und nicht-staatlichen Organisationen zu Fragen des „Trusted Computing“ zusammen, insbesondere um die in diesem Eckpunktepapier festgelegten Anforderungen an das „Trusted Computing“-Konzept zu realisieren. Die Bundesregierung bringt darüber hinaus die besonderen IT-Sicherheits-Anforderungen des öffentlichen Sektors aktiv in die TCG und andere Projekte und Initiativen zur „Trusted Computing“-Technologie ein.