# Stellungnahme der Bundesregierung zu den Sicherheitsinitiativen TCG und NGSCB im Bereich Trusted Computing

## Vorbemerkung

Die Informationstechnik ist bedeutsam für alle Bereiche der Wirtschaft, Verwaltung und des Privatlebens. Eine funktionierende und sichere Informationstechnik ist ein Grundpfeiler für moderne Geschäftsprozesse und Kommunikationsverbindungen. Verlässliches E-Government und erfolgreicher E-Commerce sind nur mit sicheren IT-Komponenten realisierbar.
Zunehmend wird damit die Informationstechnik zum kritischen Faktor, deren Ausfall oder Kompromittierung schwerwiegende Konsequenzen für die Nutzer der IT haben kann. Dass die Bedrohungen von IT-Systemen nicht geringer geworden sind, zeigen aktuelle Meldungen in Bezug auf das Auftreten neuer Viren, Schwachstellen, DoS-Attacken und weiterer Bedrohungen. IT-Systeme werden auch in kritischen Infrastrukturbereichen genutzt, die für das Funktionieren der Gesellschaft unverzichtbar sind. Dem Schutz dieser Komponenten muss eine hohe Priorität beigemessen werden.

## Grundsätzliches

Die Bundesregierung begrüßt grundsätzlich jede Maßnahme, die dem Schutz der Informationstechnik dient. Die Maßnahmen müssen dabei allerdings derart gestaltet sein, dass alle Bestandteile gesetzeskonform sind. Dabei sind insbesondere die Aspekte des Datenschutzes zu berücksichtigen.
Darüber hinaus können nur Maßnahmen unterstützt werden, die dazu geeignet sind, das Vertrauen in die Informationstechnik zu erhöhen. Voraussetzung hierzu sind eine transparente Informationspolitik in Bezug auf die Schutzkonzepte und Schutzmaßnahmen, sowie die Einbeziehung unterschiedlicher Interessengruppen bei der Planung, Entwicklung und Vermarktung von Schutzmechanismen. Darüber hinaus dürfen Schutzmaßnahmen im IT-Bereich nicht dazu missbraucht werden, Marktzugangsschranken zu schaffen.

## Zu den Sicherheitsinitiativen TCG und NGSCB

Die Bundesregierung begrüßt grundsätzlich die Absicht der in der TCG versammelten Hersteller sowie der Firma Microsoft, mit TCG und NGSCB die Sicherheit von PC-Plattformen zu erhöhen.

Zum Sicherheitskonzept der TCG:

**Sicherheitstechnische Anforderungen:**

## 1. Transparenz und Offenlegung von Schnittstellen und Spezifikationen

1.1. Die für Verschlüsselungs- und Signaturfunktionen genutzten Algorithmen müssen standardisiert und national und international als sicher erachtet sein.

1.2. Die verwendeten Schlüssellängen und sonstigen Parameter müssen mindestens denen entsprechen, die vom Bundesamt für Sicherheit in der Informationstechnik in bezug auf sichere Verschlüsselung und sichere Signatur vorgegeben wurden.

1.3. Das Sicherheitsmodul (TPM) darf keine undokumentierten Funktionen enthalten; insbesondere keine Funktionen, die als potentielle Schwachstelle genutzt werden können oder einen sonstigen Zugriff auf geschützte Daten durch Dritte ermöglichen.

1.4. Die TCG sollte die Anwendungsszenarien verständlich und anschaulich dokumentieren, auf deren Grundlage die Spezifikation für das TPM erarbeitet wurde. Nur so können perspektivisch die Auswirkungen des TPM im praktischen Einsatz anschaulich verständlich gemacht werden und die betroffenen Endanwendungen identifiziert werden.

## 2. Zertifizierung des Sicherheitssystems

2.1. Das Sicherheitsmodul (TPM) muss mindestens nach CC EAL4 medium zertifiziert werden. Die Zertifizierung muss auch den physikalischen und logischen Schutz vor Angriffen auf das Sicherheitsmodul (TPM) umfassen.

2.2. Das Sicherheitsmodul (TPM) muss prüfbar sein und seine Funktionalität muss von unabhängigen Institutionen bestätigt werden können. Die Erarbeitung entsprechender Protection-Profiles wird als unerlässlich angesehen, um einen international gleichmäßigen Sicherheitsstandard zu etablieren. Um die Funktion des Sicherheitsmoduls (TPM) eindeutig zuordnen zu können und eine eindeutige Prüffähigkeit zu gewährleisten, müssen die Sicherheitsfunktionen an einer zentralen Stelle in einem separaten Baustein (TPM) gebündelt werden. Eine Vermischung des Sicherheitsmoduls mit anderen Funktionseinheiten (z.B. CPU, Chipsatz, etc.) führt zu Intransparenz

und dazu, dass eine sicherheitstechnische Überprüfung nicht mehr einfach durchführbar ist.

## 3. Systemsicherheit, Datensicherung und Migration

3.1. Die in dem vorhandenen Sicherheitsmodul gespeicherten Informationen müssen sich auf eine neue Hardwareplattform insoweit übertragen lassen, dass vom Anwender erworbene Software weiterhin auf der neuen Hardwareplattform lauffähig ist. Alle kryptographischen Schlüssel des TPM, die für die Nutzung von Software, Daten und Onlinedienstleistungen benötigt werden, müssen von einer Hardware-Plattform auf eine andere migrierbar sein. Der Fall eines defekten TPM muss ebenfalls berücksichtigt werden und eine Migrationsmöglichkeit für Daten bzw. Schlüssel implementiert werden.

3.2. Werden auf dem Sicherheitsmodul (TPM) aufbauende DRM-Lösungen entwickelt, ist bei der Entwicklung das Recht des Nutzers auf Privatkopie zu berücksichtigen und entsprechend technisch zu implementieren.

3.3. Daten die nicht urheberrechtlich geschützt sind und unter Einbeziehung des Sicherheitsmoduls (TPM) verarbeitet werden, müssen sich auch auf Systeme zur weiteren Nutzung übertragen lassen, die über kein Sicherheitsmodul verfügen.

3.4. Im Konzept des Sicherheitsmoduls (TPM) müssen für alle wesentlichen Komponenten Redundanzen vorgesehen werden, so dass „Single Point of Failures“ vermieden werden.

3.5. Insofern Schlüssel verwendet werden, die aus Sicherheitsgründen zwingend in dem Sicherheitsmodul (TPM) verbleiben müssen und nicht auslesbar sind (z.B. Endorsement-Key), müssen diese auf dem TPM selbst erzeugt werden können oder durch einen Prozess erzeugt werden, der eine gleichwertige Sicherheit garantiert. Die sichere Erzeugung dieser Schlüssel muss durch eine unabhängige Instanz bestätigt werden.

## 4. Systemkontrolle durch den Anwender

4.1. Abschaltbarkeit der Sicherheitsmodule.
Der Anwender muss entscheiden können ob er die neuen Funktionen zur Verbesserung der Sicherheit nutzen möchte. Daher müssen in die Hardware integrierte Sicherheitsmodule (TPM) vollständig deaktivierbar sein. Hierbei sollte, alternativ zu einer Softwarelösung, auch eine Hardwarelösung (z.B.

Schalter oder Sockel für TPM) implementiert werden. Die Deaktivierung darf keine negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktionen der neuen Sicherheitsarchitektur (TCG) nutzen.

4.2. Sicherheitsmodul deaktiviert als Standardeinstellung.
Zusätzlich integrierte Sicherheitsmodule müssen standardmäßig in deaktiviertem Zustand ausgeliefert werden. Der Eigentümer oder Anwender muss vorhandene Sicherheitsmodule selbständig aktivieren.

4.3. Der Nutzer muss die volle Kontrolle über seine Schlüssel haben und diese ggf. löschen und neu erzeugen können. Ausgenommen vom Zugriff durch den Nutzer sind lediglich Schlüssel, die zur Sicherstellung der Integrität und Authentizität des TPM dienen (z.B. Endorsement-Key). Diese Schlüssel, sofern Sie nicht zur eindeutigen Identifizierung des Sicherheitsmoduls dienen (z.B. Endorsement-Key), müssen jedoch durch den Nutzer bzw. Besitzer reinitialisierbar sein. Eine Löschung aller auf dem TPM gespeicherten Informationen sollte, unter Aufgabe der Funktionalität des TPM, möglich sein (z.B. bei Verschrottung des PC).

4.4. Der Nutzer muss den Zugriff auf seine Schlüssel kontrollieren können und seine Schlüssel gegen fremden Zugriff verlässlich sichern können.

4.5. Insofern das Sicherheitsmodul (TPM) fest mit der restlichen Hardware des IT-Systems (z.B. PC) verbunden ist, sollte sich die Funktionalität des Sicherheitsmoduls darauf beschränken, die Sicherheit und Integrität der Plattform zu gewährleisten. Die Nutzung von personalisierten Programmen, Daten und Onlinedienstleistungen sollte wenn nötig nicht an das Sicherheitsmodul (TPM) gebunden werden, sondern an eine personalisierte Smart-Card. Damit ließe sich der anwenderbezogene Zugriff auf Daten flexibler gestalten und Migrationsprobleme würden deutlich reduziert. Hier wird für das TPM die Auslagerung der Funktionen zur Identitätsfeststellung (z.B. die AIKs) und der zugehörigen kryptographischen Schlüssel in eine mobile Smart-Card gefordert.

4.6. Das Sicherheitsmodul (TPM) darf die Nutzung von Software nicht dadurch behindern, dass für die Nutzung der Software die Zertifizierung durch eine externe Zentralstelle benötigt wird, die außerhalb des Verantwortungsbereichs des Eigentümers bzw. Nutzers liegt.

## 5. Datenschutz

5.1. Alle datenschutzrechtlichen Vorgaben müssen unter allen Betriebsbedingungen des Sicherheitsmoduls eingehalten werden. Insbesondere müssen datenschutzrechtliche Funktionen so transparent gestaltet werden, dass der Endnutzer jederzeit von seinem Recht der informationellen Selbstbestimmung Gebrauch machen kann und diese Funktionen deaktivieren kann.

5.2. Datenschutzrechtlich relevante Funktionen dürfen sich nicht automatisch von außen aktivieren lassen, ohne das der Endanwender im Einzelfall zustimmt.

5.3. Die Nutzung der Sicherheitsfunktionen des Sicherheitsmoduls (TPM) muss auch ohne Onlineverbindung (Internet) möglich sein.

5.4. Bei der Nutzung von anonymen Identitäten (AIK), die vom Sicherheitsmodul (TPM) zur Verfügung gestellt werden, muss eine Schwächung der Anonymität, durch indirekte Verknüpfungen von Daten aus dem TPM verhindert werden (z.B. durch die Verknüpfung der AIKs über das TPM-Endorsement-Crendential in einer CA). Dazu sind entsprechende technische oder organisatorische Mechanismen vorzusehen, die dies sicherstellen.

5.5. Sofern die Nutzung einer CA vorgesehen ist, muss der Anwender eine Wahlmöglichkeit bzgl. der verwendeten CA haben.

5.6. Zur Gewährleistung eines Maximums an Objektivität und zum Schutz der Anwender insbesondere in datenschutzrechtlicher Hinsicht müssen die genutzten CAs unter staatlicher Aufsicht arbeiten.

5.7. Unter datenschutzrechtlichen Aspekten ist eine pseudonyme Attestierung („Zero-Knowledge-Verfahren“ für Beglaubigungsprozesse) der Identität (auch anonyme Identität) ohne externe CA anzustreben.

**Wirtschaftspolitische Anforderungen:**

## 6. Faire Lizenzpolitik

6.1. Die Patentpolitik der TCG und deren Mitgliedern darf nicht dazu genutzt werden, Wettbewerber z.B. durch unangemessene Lizenzgebühren auszugrenzen. Insbesondere für den Open-Source Bereich sollte die TCG eine Lösung finden, die nicht kommerzielle Open-Source Projekte von Lizenzgebühren frei stellt.

6.2. Die von der TCG spezifizierte Treibersoftware – der TSS – sollte unter einer Lizenz veröffentlicht werden, welche die kostenfreie Nutzung, Modifikation und Weitergabe ermöglicht, um Zeit- und Entwicklungsnachteile von Nicht-TCG-Mitgliedern auszugleichen.

6.3. Die beteiligten Firmen müssen vor Verabschiedung der Spezifikation und Standards bekannt geben, welches relevante Intellectual Property (IP) sie zu der Spezifikation haben und ob sie bereit sind, diese unter RAND zu spezifizieren.

6.4. Die TCG sollte mit ihren Mitgliedsunternehmen sowie mit den zuständigen europäischen und nationalen Wettbewerbsbehörden in einen Dialog treten, um die Möglichkeiten und Rahmenbedingungen der Schaffung eines „Technologie-Pools“ zu klären, um dadurch wettbewerbsrechtlich relevante Behinderungspotentiale bei der Nutzung von Lizenzen zu beseitigen.

## 7. Nicht diskriminierende Informationspolitik

7.1. Die TCG sollte zu offenen, transparenten und diskriminierungsfreien Bedingungen eine zusätzliche unentgeltliche Mitgliedschaft einführen, die vor allem die Möglichkeit umfasst, alle für die Entwicklung von Software (u.a. Open-Source-Software) - welche die Funktionen des Sicherheitsmoduls (TPM) nutzt - notwendigen Informationen in der erforderlichen Zeitnähe, ohne zusätzliche Kosten für nicht kommerzielle Projekte, zu erlangen. Unabhängig davon sollte Vertretern der Open-Source-Gemeinde eine angemessene Mitwirkungsmöglichkeit in der TCG geboten werden.

7.2. Eine ausgewogene Interessenvertretung sollte durch gleichrangige Vertretung innerhalb der TCG unter Berücksichtigung regionaler und branchenspezifischer Aspekte angestrebt werden.

## 8. Sicherheitstechnologie darf nicht Marktzugangsschranken schaffen

8.1. Das Handeln der TCG darf nicht dazu führen, dass im IT-Bereich marktbeherrschende Stellungen entstehen oder verstärkt werden.

8.2. Die TCG darf nicht dazu genutzt werden, Marktzutrittshemmnisse für einzelne Unternehmen oder Branchen zu schaffen.

8.3. In jedem Fall sollte die TCG gemeinsam mit Branchen- oder anderen Verbänden eine Schlichtungsstelle mit dem Ziel einrichten, Beschwerden einzelner Wirtschaftsteilnehmer über mögliche Diskriminierungen am Markt und beim Marktzutritt zu prüfen, Hilfestellung zu geben und einen Interessensausgleich aller Beteiligten herbeizuführen.

## 9. Technologische Offenheit

9.1. Das Sicherheitsmodul (TPM) muss system-offen sein, so dass die Einbindung des Sicherheitsmoduls (TPM) für verschiedene Hardwareplattformen mit ähnlichem Aufwand möglich ist. Dabei müssen unabhängig vom System alle Funktionen des Sicherheitsmoduls auf allen Hardwareplattformen gleichermaßen unterstützt werden.

9.2. TCG-gestützte Computersysteme müssen mit Nicht-TCG-gestützten Computersystemen interoperabel sein. Die Spezifikationen der TCG dürfen nicht dazu genutzt werden, bestimmte Plattformen und Systeme auszuschließen.

9.3. Die TCG muss dafür Sorge tragen, dass die verabschiedeten Spezifikationen nicht einzelne Mitgliedsunternehmen einseitig bevorzugen. Insbesondere sollten die Spezifikationen unabhängig von den Voraussetzungen einer speziellen Hardware oder Software sein.

<u>Zum Sicherheitskonzept NGSCB der Firma Microsoft:</u>

<u>Bemerkung:</u>

Die Sicherheitsinitiative NGSCB (vormals Palladium) der Firma Microsoft befindet sich noch im Entwicklungsstadium. NGSCB ist eine Systemlösung, die im wesentlichen auf einem sicheren Betriebssystemkern (Nexus) beruht, der durch

entsprechende Hardwareerweiterungen unterstützt und abgesichert wird. Das TPM der TCG wird vermutlich von NGSCB mit genutzt werden.
Zu NGSCB sind bisher keine Detailinformationen bekannt. Auf Grundlage des bisher bekannten Grobkonzeptes können jedoch Grundforderungen bzgl. sicherheitstechnischer und wirtschaftspolitischer Aspekte aufgestellt werden.

## 10. Sicherheitstechnische Grundforderungen:

10.1. Werden Teile von NGSCB für DRM-Zwecke konzipiert, so muss sichergestellt werden, dass die legitimen Rechte der Nutzer gewahrt bleiben und z.B. Mechanismen vorgesehen werden, die die Anfertigung einer Privatkopie erlauben.

10.2. Die Sicherheitsfunktionen von NGSCB müssen auch ohne Onlineverbindung nutzbar sein.

10.3. Werden personenbezogene Daten in Zusammenhang mit der Nutzung von NGSCB übertragen, so muss der Nutzer die Möglichkeit haben, der Übertragung im Einzelfall zuzustimmen.

10.4. Der Anwender ist über Art und Umfang der Daten zu informieren, die bei der Nutzung von NGSCB ggf. an eine externe Stelle übermittelt werden.

10.5. Der Hersteller von NGSCB (Microsoft) muss dafür Sorge tragen, dass die Schnittstellen von NGSCB transparent gestaltet sind und die Dokumentation öffentlich verfügbar ist. Sicherheitsfunktionen können nur als sicher erachtet werden, wenn diese transparent und nachvollziehbar sind.

10.6. Die Nutzung von Software nur unter Zustimmung einer zentralen Zertifizierungsinstanz wird kritisch gesehen. Ist eine Zertifizierung notwendig, so sollte diese durch eine unabhängige Stelle und zu angemessenen Gebühren erfolgen. Nicht kommerzielle Software sollte von ggf. erhobenen Zertifizierungsgebühren frei gestellt werden.

10.7. Die in dem Zusammenhang mit der Realisierung des Sicherheitskonzeptes von Microsoft entwickelten Komponenten müssen auch für andere Software-Entwickler offen sein. Dabei müssen den unabhängigen Entwicklern bereits im Vorfeld und in der erforderlichen Zeitnähe Entwicklungsunterlagen zur Verfügung stehen, damit die Möglichkeit besteht, dass nicht nur ein einziges Betriebssystem die neuen Sicherheitstechnologien unterstützt.

## 11. Wirtschaftspolitische Grundforderungen:

11.1. In jedem Fall ist eine offene und transparente Informationspolitik die unverzichtbare Voraussetzung für die Schaffung des notwendigen Vertrauens bei den Nutzern aus Wirtschaft, Verwaltung und Politik.

11.2. Eine diskriminierende Ausgrenzung von Hardware- oder Softwareherstellern durch die Lizenzbedingungen von NGSCB darf nicht stattfinden.

11.3. Software, die nicht von den neuen Funktionen von NGSCB gebrauch macht, muss weiterhin unter dem Betriebssystem lauffähig sein, das auch NGSCB unterstützt.

11.4. Sollte NGSCB für DRM (Digital Rights Management) verwendet werden, so ist einer ggf. vorgesehenen Prüfung im Offlinemodus der Vorzug vor einer Onlineprüfung zu geben.