

Vorwort

Die Informationstechnik (IT) hat in den letzten zwei Jahrzehnten alle wichtigen Lebensbereiche durchdrungen. In Privatleben, Wirtschaft, Verwaltung und selbst bei kritischen Infrastrukturen ist die funktionierende und sichere IT der Grundpfeiler moderner Geschäftsprozesse und Kommunikationsverbindungen. Sichere Verfahren des E-Government und des E-Commerce sind ebenso nur mit Hilfe sicherer IT realisierbar.

Damit wird die Informationstechnik zunehmend selbst zu einer kritischen Infrastruktur, deren Ausfall oder missbräuchliche Nutzung ernste Folgen für die gesamte Gesellschaft begründen kann. Dies geht einher mit einer qualitativ und quantitativ steigenden Zahl von IT-Sicherheitsvorfällen, wie der Bericht zur Lage der IT-Sicherheit in Deutschland 2007 des Bundesamtes für Sicherheit in der Informationstechnik zeigt. Der Trend zur Kommerzialisierung und Professionalisierung der Internetkriminalität scheint bei einem zum Teil nur geringen Schutzniveau vieler IT-Systeme ungebrochen.



Dr. Markus Dürig,
Bundesministerium des Innern

Konventionelle Ansätze zur Verbesserung der IT-Sicherheit versuchen oft, potenziell unsichere Systemkerne mit einer Vielzahl von Schutzschichten nach außen hin sicherer zu machen. Die Trusted Computing-Technologie etabliert die Sicherheitsfunktionalität dagegen direkt in den Systemkern. Das Bundesministerium des Innern hält diesen Ansatz für vielversprechend und begrüßt grundsätzlich jede Maßnahme, die dem Ziel eines besseren Schutzes der Informationstechnik dient. Allerdings müssen die Maßnahmen derart gestaltet sein, dass alle Bestandteile gesetzeskonform sind. Insbesondere die Aspekte des Datenschutzes müssen berücksichtigt werden. Denn es können nur Maßnahmen unterstützt werden, die dazu geeignet sind, das Vertrauen der Nutzer in die Informationstechnik zu erhöhen. Voraussetzungen sind eine transparente Informationspolitik in Bezug auf die Schutzkonzepte und Schutzmaßnahmen, sowie die Einbeziehung aller Interessengruppen bei der Planung, Entwicklung und Vermarktung von Schutzmechanismen. Schutzmaßnahmen im IT-Bereich dürfen keinesfalls dazu missbraucht werden, Marktzugangsschranken zu schaffen.

Der Grundidee „vertrauenswürdiger Informationstechnik“ folgend, sieht das Bundesministerium des Innern mit großem Interesse auf die Standardisierungen innerhalb der Trusted Computing Group (TCG), insbesondere der Spezifikationen zum Trusted Platform Module (TPM). Bereits im Jahre 2004 suchte die Bundesregierung das Gespräch mit der TCG, indem in Form eines Anforderungskataloges zu den

damaligen Entwicklungen Stellung genommen wurde. Die seinerzeitigen Forderungen gelten in ihrem Grundsatz bis heute fort und lassen sich wie folgt zusammenfassen:

- Offenheit, Transparenz und freie Verfügbarkeit der Standards
- Entscheidungsfreiheit für einen Einsatz TPM-basierter Systeme
- Nachvollziehbare und transparente Zertifizierung
- Gewährleistung der Interoperabilität mit alternativen Lösungen
- Volle Kontrolle über Inbetriebnahme, Konfiguration, Anwendung und Stilllegung von TC-Lösungen
- Einhaltung der Bestimmungen des Datenschutzes.

Werden Trusted Computing-Lösungen, diesen Anforderungen gerecht, so können Sie einen wesentlichen Beitrag zur Erhöhung der IT-Grundsicherheit eines jeden Nutzers darstellen. Dabei ist es unwesentlich, ob sie auf den Spezifikationen der TCG basieren oder alternativen Ansätzen folgen. Gleichzeitig ergeben sich neue Chancen und Möglichkeiten, die Sicherheitsmechanismen auch anderen IT-Anwendungen zur Verfügung zu stellen und ein höheres Vertrauen in E-Government und E-Commerce zu begründen.

Inhaltsverzeichnis

Einleitung	1
Trusted Computing – eine Einführung	3
Norbert Pohlmann ¹ · Helmut Reimer ²	
Grundlagen	13
Die Trusted Computing Group	15
Thomas Rosteck	
Trusted Computing Grundlagen	21
Hans Brandl	
TPM Virtualization: Building a General Framework	43
Vincent Scarlata · Carlos Rozas · Monty Wiseman · David Grawrock · Claire Vishik	
Trusted Computing und die Umsetzung in heutigen Betriebssystemen	57
Sebastian Rohr	
Sicherheitsbausteine für Anwendungen	71
Mehr Vertrauenswürdigkeit für Anwendungen durch eine Sicherheitsplattform	73
Markus Linnemann · Niklas Heibel · Norbert Pohlmann	
Die Sicherheitsplattform Turaya	86
Ammar Alkassar · Christian Stüble	
Trusted Network Connect – Vertrauenswürdige Netzwerkverbindungen	97
Marian Jungbauer · Norbert Pohlmann	
Interaktionen TPM und Smart Card	110
Florian Gawlas · Gisela Meister · Axel Heider · Sebastian Wallner	

Anwendungsszenarien	123
Enterprise Security – Informationsschutz im Unternehmen	125
Michael Hartmann · Gunter Bitz	
Unternehmensweites TPM Key Management	140
Bernhard Weiss	
Trusted Computing im Hochsicherheitsbereich	156
Peter Kraaibeek · Hans Marcus Krüger · Kai Martius	
Trusted Computing für automobiler IT-Systeme	170
Andrey Bogdanov ¹ · Thomas Eisenbarth ² · Christof Paar ² · Marko Wolf ¹	
Trusted Computing in mobiler Anwendung: Von Zugangskontrolle zu Identitäten	187
Andreas U. Schmidt · Nicolai Kuntze	
Datenschutz- und rechtliche Aspekte	207
Auswirkungen von Trusted Computing auf die Privatsphäre	209
Markus Hansen · Marit Hansen	
Rechtliche Chancen und Risiken des „Trusted Computing“	221
Andreas Neumann	
Biographien der Autoren	236
Glossar	242
Stichwortverzeichnis	249