

Das Risiko Trusted Computing für die deutsche Versicherungswirt- schaft

Positionspapier der deutschen Versicherungswirtschaft

Band 13
der Schriftenreihe
des Betriebswirtschaftlichen Institutes des GDV

Herausgeber:
Ausschuss Betriebswirtschaft und Informationstechnologie
Gesamtverband der Deutschen Versicherungswirtschaft e.V.
Friedrichstraße 191, 10117 Berlin
Telefon (030) 2020 54 53
Telefax (030) 2020 66 06
www.gdv.de

Inhaltsverzeichnis

1	Summary – Risiko Trusted Computing	7
2	Forderungen der Versicherungswirtschaft	9
3	Technologien des Trusted Computing	10
3.1	Ansätze zur Schaffung sicherer Systeme	11
3.1.1	Der TPM-Chip (Trusted Platform Module)	12
3.1.2	Die Next Generation Secure Computing Base (NGSCB)	13
3.1.3	LaGrande von Intel	14
4	Warum Trusted Computing?	15
4.1	Auswirkungen im Versicherungsunternehmen	16
4.1.1	Kosten	16
4.1.2	Sicherheitsgewinn	17
4.1.3	Sicherheitsrisiken	19
4.1.4	Kontrollgewinn	20
4.1.5	Kontrollverlust	20
4.1.6	Geschäftsprozesse	22
4.2	Szenarien	22
4.2.1	Keine Nutzung von Trusted Computing	23
4.2.2	Nutzung von Trusted Computing	23
4.3	Zusammenfassung	24
5	Anhang	25
5.1	Schlüssel, Signaturen und Zertifikate	25
5.1.1	Digitale Signatur	26
5.1.2	Hashwert (Fingerabdruck)	27
5.1.3	Zertifikat	27
5.2	Glossar	28
5.3	Autoren	30

Inhaltsverzeichnis

1 Summary – Risiko Trusted Computing

Die Trusted Computing Group (TCG), eine Initiative der maßgeblichen Hard- und Softwarehersteller¹, verspricht, mit dem Einsatz der von ihr vorgeschlagenen Standards, die Absicherung von IT-Geräten und der in ihnen gespeicherten digitalen Daten. Kern des TCG-Standards ist ein Hardwarechip (vergleichbar einer „eingelöteten“ Smartcard), der in die Hardware von PCs, Servern, PDAs und Smartphones integriert ist, und der den Kern einer umfassenden Absicherung von Geräten und Inhalten darstellt.

Heute existierende Verfahren leisten bereits das, was Trusted Computing in Zukunft verspricht. Daher besteht aus Sicherheitsgesichtspunkten keine unmittelbare Notwendigkeit, Technologien der TCG einzusetzen. TCG-konforme Technologie alleine bietet weder Schutz vor Computerviren noch macht sie den Einsatz von Firewalls überflüssig. Als Basis zukünftiger Erweiterungen durch Hardware, Anwendungen und Betriebssysteme bietet der TCG-Standard eher Vorteile für die Anbieter, die so bestimmte Interessen durchsetzen könnten. Der Anwender bezahlt dafür mit dem Risiko erweiterter Kontrollmöglichkeiten seiner Geräte, Daten und Inhalte durch Dritte. Die gesamte Absicherungsphilosophie basiert dabei auf dem Vertrauen der Anwender in die „positiven“ Absichten und „sicheren“ Verfahrensweisen der Anbieter.

Die mit dem Einsatz der Technologien des Trusted oder auch des Trustworthy Computings² entstehenden Risikopotentiale (Kontrollverlust, Plattformabhängigkeiten, finanzielle Aufwände, ...) liegen insbesondere in den heute noch nicht endgültig abschätzbaren Möglichkeiten der Kombination verschiedener Kontrollmechanismen im Bereich der Anwendungen, notwendiger Hardwareerweiterungen und Betriebssysteme. Vor allem die Integration des TCG-Standards in die Betriebssysteme und die damit einhergehenden Hardwareerweiterungen sollten sehr kritisch beobachtet werden, da diese Entwicklung nur unzureichend und unvollständig transparent gemacht wird. Es kann vermutet werden, dass hier individuelle Interessen der Hersteller verdeckt transportiert und umgesetzt werden sollen.

Die grundsätzliche Sicherheitsphilosophie des Trusted Computings beruht auf Vertrauen: Vertrauen in die Verfahren und korrekten Implementierungen der Hardwarelieferanten; Vertrauen in die Leistungen und Motive der Softwareanbieter. Dieses Vertrauen ist nach derzeitiger Informationslage aufgrund des hohen Missbrauchspotentials in keinem Fall gerechtfertigt. Solange es keine rechtlichen Rahmenbedingungen oder adäquaten Kontrollmechanismen gibt, ist ein Missbrauch der hier geschaffenen Infrastrukturkomponenten im Hinblick auf die Durchsetzung

¹ Promoters: AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, Sun Microsystems Inc. (laut Internetseiten der TCG, Stand 2/2004)

² „Trusted Computing“ bezieht sich auf die Hardware, der Begriff „Trustworthy Computing“ bezieht sich auf Anwendungen, Betriebssystem und Hardware als integriertes Sicherheitspaket

wirtschaftlicher wie auch politischer Interessen Dritter nicht auszuschließen oder gar wahrscheinlich. Dabei liegen die Gefahren weniger im einzelnen Standard. Die TCG steht – trotz der individuellen Interessen ihrer Mitglieder – in der öffentlichen Beobachtung und muss ihre Standards publizieren. Damit sind sie einer gewissen Kontrolle unterworfen. Die beschriebenen Verfahren ermöglichen darüber hinaus – zumindest für den Hardwarechip – eine Trennung der Verantwortung. Die TCG legt zwar die Standards und Zertifizierungsmechanismen des Hardware-Chips fest, die Produktion wird aber von unabhängigen Firmen übernommen. Diese rudimentären Kontrollmöglichkeiten gelten aber nicht für die auf den TCG-Mechanismen aufsetzenden Erweiterungen und deren Integration in weitere Technologien. Erst die Betrachtung des Zusammenspiels einzelner, für sich genommen relativ unkritischer Entwicklungen, erlaubt die endgültige Bewertung der Missbrauchsmöglichkeiten und damit eine realistische Abschätzung des Gesamtrisikos.

**Trusted Computing setzt
Vertrauen der Anwender in
die Motive und Technolo-
gien der Anbieter von Hard-
und Software voraus.**

Die sich hier abzeichnenden Risiken sind für die Versicherungswirtschaft inakzeptabel, da sie nicht zuletzt infolge gesetzlicher Vorschriften als verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes die vollständige Kontrolle über ihre Daten, Inhalte und Geräte behalten muss.

Der Einsatz von TCG in VU ist aufgrund fehlender gesetzlicher Rahmenbedingungen, fehlender Kontrollmöglichkeiten und des hohen Missbrauchspotentials somit grundsätzlich abzulehnen.

Als Alternative zur TCG-Sicherheitstechnologie, die an die Hardware gebunden ist, kann die personengebundene Smartcard eingesetzt werden³. Diese Entwicklung wird insbesondere im Rahmen des Signaturlösungs bündnisses „Bund-online-2005“ forciert. Sie ist im Gegensatz zur reinen Hardwarebindung durch das Signaturgesetz rechtlich abgesichert und entspricht darüber hinaus den Ansätzen der europäischen Institutionen.

³ „Sicherheit für den Anwender bedeutet, dass er selbstbestimmt über alle seine Daten verfügen kann. Ein vertrauenswürdiger Umgang mit seinen Daten setzt vollständige Transparenz für ihn selbst bei strikter Geheimhaltung gegenüber Dritten voraus. Welche Daten wie und an wen weitergegeben werden, entscheidet allein der Anwender. An diesen Grundsätzen müssen sich kommende Sicherheitslösungen ausrichten.“ Quelle: Internet unter www.bsi.de, Sichere Plattformen und die Trusted Computing Group, Februar 2004, Bundesamt für Sicherheit in der Informationstechnologie

2 Forderungen der Versicherungswirtschaft

Vor dem Hintergrund dieser Risikopotentiale muss aus wirtschaftlichen Erwägungen und aufgrund gesetzlicher Rahmenbedingungen (KonTraG, BDSG, StGB, ...) für Versicherungen und ihre assoziierten Unternehmen gefordert werden:

1. Die vorhandenen Anwendungen müssen auch in Zukunft ohne Beeinträchtigung weiter ausgeführt werden können (**Investitionsschutz**). Insbesondere muss mindestens die bisher erreichte Interaktion von Hard- und Software und die freie Wahl der Plattform auch zukünftig uneingeschränkt gewährleistet sein (**Interoperabilität**). Insbesondere die Freiheit zur Nutzung von Open Source-Produkten darf nicht eingeschränkt werden.

Nach allen bisherigen Informationen ist mit dem Einsatz von TCG-Komponenten in Verbindung mit entsprechenden Anwendungen und Betriebssystemen die Gefahr der Einflussnahme oder des Zugriffs unberechtigter Dritter auf Geräte, Daten und Infrastruktur der Versicherer gegeben. Deshalb gilt:

2. Außerhalb der gesetzlichen Vorschriften darf keine unternehmensfremde Institution und kein unternehmensfremder Rechner im Rahmen einer Sicherheitsinfrastruktur Einfluss auf die Geräte und elektronisch gespeicherten Inhalte eines Versicherungsunternehmens nehmen können.
3. Daten und elektronische Inhalte dürfen das Firmennetz nur nach Autorisierung durch verantwortliche Stellen und im Rahmen der gesetzlichen Vorschriften verlassen.
4. Neue Technologien müssen auch auf den Plattformen uneingeschränkt möglich bleiben, die nicht die Technologie der TCG einsetzen. Insbesondere müssen Eigenentwicklungen und geschäftskritische Anwendungen auch ohne vorhandene TCG-Architektur voll einsatzfähig bleiben.

Weiterhin wird gefordert, dass

5. der betriebswirtschaftliche Nutzen des Einsatzes von TCG-Komponenten in der Versicherungswirtschaft durch die Anbieter grundsätzlich dargelegt werden muss.

Die bisherigen Freiheitsgrade müssen uneingeschränkt erhalten bleiben. Dies ist nur gewährleistet, wenn alle obigen Forderungen erfüllt sind. Sollte eine dieser Forderungen nicht nachweisbar erfüllt sein, ist der Einsatz von Technologien des Trustworthy Computing nicht zu empfehlen. Bei bereits heute erhältlicher TCG-konformer Hardware sollten die enthaltenen TCG-Komponenten zumindest bis zur Erfüllung dieser Forderungen deaktiviert bleiben.

3 Technologien des Trusted Computing

Die aktuelle Sicherheitsdiskussion in der Informationstechnologie (IT) wird von zwei wesentlichen Zielrichtungen geprägt:

- Die einzelnen Geräte müssen vor Attacken und vor schadenstiftender Software geschützt werden (IT-Sicherheit).
- Die auf den Geräten verwendbaren Inhalte müssen vor mißbräuchlicher Nutzung geschützt werden (DRM, Digitales Rechte Management).

Um dies sicherstellen zu können, muss feststellbar sein, inwieweit die Trägerplattform, ihr Betriebssystem und die ablaufenden Anwendungen vertrauenswürdig (trusted) sind. Dabei heißt vertrauenswürdig, dass die Trägerplattform den im Rahmen der Sicherheitsanforderungen definierten Vorgaben nachweislich genügt. Es müssen also alle Veränderungen des Geräts gegen einen definierten Sollzustand erkannt und als Basis einer Sicherheitsbewertung genutzt werden können.

Trusted Computing möchte die Kontrollierbarkeit von Hardware sicherstellen

Zur Schaffung eines definierten Sicherheitsumfelds haben maßgebliche Hardware- und Softwarehersteller⁴ eine Initiative zur Definition eines vertrauenswürdigen Umfelds für Hardwareplattformen (Server, PCs, PDAs und Smartphones) initiiert und entsprechende Vorschläge verabschiedet. Diese sogenannte Trusted Computing Group oder kurz **TCG** ist die Nachfolgeorganisation der TCPA (Trusted Computing Platform Alliance), die sich schon mit dem gleichen Thema beschäftigt hat⁵. Zentrales Element dieser Initiative ist ein Chip, der sogenannte **TPM**⁶, der auf jedem Gerät verbaut werden muss und mit dessen Hilfe Veränderungen dieser Plattform festgestellt werden können. Über geschützte, nicht veränderbare und nicht transportierbare Schlüssel wird das Gerät eindeutig identifizierbar und somit eine sichere Authentifizierung ermöglicht. Ein geschützter Speicherbereich erlaubt die Ablage von Kennungen und Hashwerten des Systemzustands. Der TPM ist somit mit einer „eingelöteten“ **Smartcard** zu vergleichen.

Trustworthy Computing möchte Herstellern und Anbietern vertrauenswürdige Systeme bereitstellen

⁴ Promoters: AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, Sun Microsystems Inc. (laut Internetseiten der TCG, Stand 2/2004)

⁵ „Die „Trusted Computing Group“ (TCG) ging am 8. April 2003 als eine Neugründung aus der TCPA hervor, da sich die Entscheidungsfindung in der TCPA als ineffektiv erwiesen hatte. Bereits erarbeitete Standards der TCPA wurden dabei von der TCG übernommen. Zudem erhofften sich die beteiligten Firmen einen Imagewechsel durch die neue Organisation, da die TCPA durch eine wenig transparente Öffentlichkeitsarbeit bereits in Misskredit geraten war.“ Quelle: Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de vom Februar 2004

⁶ TPM = Trusted Platform Module

Auf dieser absicherbaren – aber noch nicht de facto sicheren – Umgebung setzen die Anbieter von Betriebssystemen auf, in dem sie zum einen eine sichere Ablaufumgebung für zu schützende Programme bereitstellen, zum anderen sichere Schutzmechanismen für die Dateien ermöglichen, die von den zu schützenden Programmen bearbeitet oder erzeugt werden. Beispiel hierfür ist Microsoft mit seiner Initiative NGSCB⁷ (Next Generation Secure Computing Base). Die oben erwähnten Schutzmechanismen sind in Teilen schon heute sowohl auf der Hardwareseite als auch auf der Betriebssystemseite im Einsatz.

Mit dieser Entwicklung gehen neben den positiven Aspekten einer sicheren betrieblichen Umgebung in erheblichem Ausmaß Missbrauchsmöglichkeiten – insbesondere durch die enge Verzahnung von Hardware und Betriebssystem – einher.

3.1 Ansätze zur Schaffung sicherer Systeme

Die Abbildung 1 fasst die bisherigen Entwicklungen hin zu einer vertrauenswürdigen Plattform zusammen.

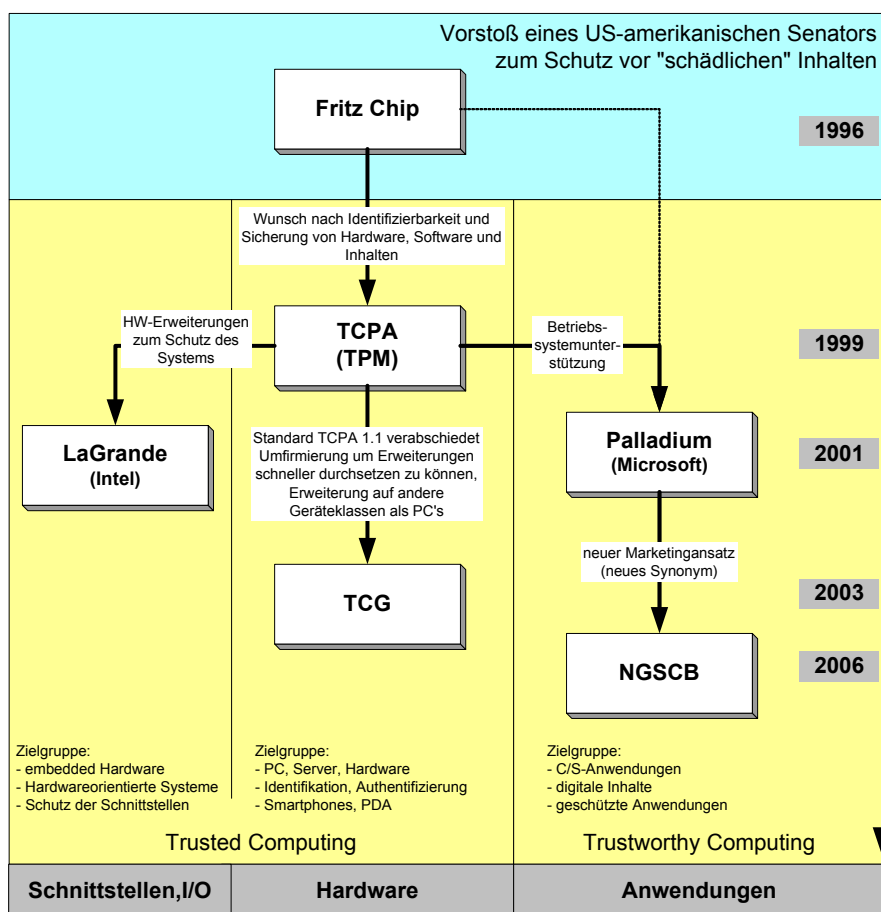


Abbildung 1: Entwicklung zum "Trusted Computing"

Die einzelnen Bereiche werden in den folgenden Abschnitten detailliert erläutert.

⁷ vormals auch unter dem Begriff Palladium bekannt.

3.1.1 Der TPM-Chip (Trusted Platform Module)⁸

Kern der sicheren Umgebung der TCG ist der sogenannte TPM-Chip (Trusted Platform Module). Dieser Chip wird nach dem amerikanischen Senator Fritz Holling auch „Fritz-Chip“ genannt. Dieser Chip soll die folgenden wesentlichen Aufgaben erfüllen:

- Bereitstellung eines abgesicherten Bereichs für Schlüssel, Zertifikate und andere Daten.
- Generierung und Verwaltung von geheimen Schlüsseln durch kryptografische Verfahren.

Der TPM-Chip wird als integraler Bestandteil in die Hardware der jeweiligen Geräte eingebaut und kann nicht mehr entfernt werden. Spätestens mit der in Zukunft geplanten Integration in die CPU ist diese Verbindung unauflösbar. Der Chip selber enthält nicht übertragbare Schlüssel (Non Migratable Keys). Damit ist die Hardwareplattform über den Chip eindeutig identifizierbar. Derartige Schlüssel können nach der Beschickung des TPM-Chips nicht mehr gesichert oder in einen anderen Chip überführt werden⁹. Als Folge kann z. B. eine Festplatte, die mit einem nicht migrierbaren Schlüssel des TPM-Chips verschlüsselt worden ist, im Falle eines Defekts unter keinem Umstand mehr auf einem anderen Gerät gelesen werden. Der TPM-Chip enthält mindestens zwei nicht übertragbare Schlüssel. Diese sind der

- Endorsement Key (EK), der die Basis für eine unverwechselbare Kennung des TPM-Chips liefert, und der
- Storage Root Key (SRK), der als Ausgangspunkt für die im TPM gespeicherten Daten und Schlüssel dient.

Die Ablage der Daten erfolgt in einem vom Hauptspeicher getrennten, separaten Speicherbereich des TPM. Die Daten werden durch kryptographische Verfahren zusätzlich abgesichert. Durch die Speichermöglichkeit zusätzlicher Daten können definierte Systemzustände sichergestellt werden. Damit ist prinzipiell die Bindung von Anwendungen und von digitalen Inhalten an ein bestimmtes Gerät bzw. einen bestimmten Gerätezustand durch Anbieter und Lieferanten möglich.

⁸ Nach dem Artikel „Trusted Computing im Überblick“, heise Security, www.heise.de/security/artikel/print/43179 vom 20.1.2004

⁹ mit der Spezifikation 1.2 der TCG ist die Möglichkeit gegeben, den Endorsement Key zu löschen bzw. zu ersetzen. Ob dies der Eigentümer selbst tun kann oder dies durch externe Firmen erfolgt, ist noch unklar.

3.1.2 Die Next Generation Secure Computing Base (NGSCB)

Auf der Betriebssystemseite (Trustworthy Computing) wird der hardwaregebundene Schutz durch die nächsten Generationen der Betriebssysteme z. B. von Windows genutzt. In Windows wird dazu eine umfassend abgesicherte Laufzeitumgebung für Programme integriert. Diese Laufzeitumgebung wird als NGSCB (Next Generation Secure Computing Base) oder vormals Palladium bezeichnet. Kern dieser abgesicherten Laufzeitumgebung ist der sogenannte „Nexus“, der die Anwendungen in speziell per Hardware abgesicherten Speicherbereichen ausführt. Die Programme müssen speziell für diese Laufzeitumgebung entwickelt werden. Zur endgültigen Absicherung werden neben dem TPM-Chip ab Version 1.2 spezielle Hardwareerweiterungen benötigt, die in der Spezifikation LaGrande von Intel beschrieben werden:

- Chipsatz mit entsprechenden Sicherheitserweiterungen,
- Prozessor, der sich in einen abgesicherten Zustand versetzen lässt,
- Gesicherte Eingabegeräte (Tastatur, Maus, ...),
- Gesicherte Ausgabegeräte (Grafikkarte, ...).

Aufgabe dieser Hardwareerweiterungen ist im Wesentlichen die Absicherung der I/O-Kanäle.

Nach jetzigem Kenntnisstand wird neben der sicheren Laufumgebung auch eine Laufzeitumgebung enthalten sein, in der die „bisherigen“ Programme laufen können. Der parallele Ablauf geschützter und ungeschützter Programme sowie ein Datenaustausch zwischen den beiden Bereichen, muss aus Sicherheitserwägungen wohl eher ausgeschlossen werden.

Es sei an dieser Stelle darauf hingewiesen, dass zumindest die Chipkartenleser der Klasse 3 (mit externer Tastatur) in Verbindung mit elektronischen Signaturkarten ein hinreichendes auch gesetzlich abgesichertes Verfahren für eine qualifizierte elektronische Unterschrift gewährleisten, welches keine darüber hinausgehenden Hardwareerweiterungen benötigt.

3.1.3 LaGrande von Intel

LaGrande (LT) ist Teil der „Safer Computing Initiative“ des Prozessorherstellers Intel zur Steigerung der Sicherheit bei der Eingabe, Verarbeitung und Speicherung von Informationen mittels Intel-PC-Systemen. Motivation ist das Missverhältnis zwischen bestehenden Sicherheitsoptionen im Server- und Netzwerkkumfeld auf der einen Seite und der auf der anderen Seite unzureichenden Möglichkeiten, Client-PC-Systeme¹⁰ im Hinblick auf die finanziellen Werte der von ihnen erzeugten und gespeicherten Informationen angemessen zu schützen. Client-PC-Systeme bieten zunehmend ein attraktives Angriffsziel für Hacker und ein ausreichender Schutz kann in Zukunft auf Basis reiner Software-Schutzmaßnahmen nicht mehr gewährleistet werden.

Hinter dem Arbeitstitel LaGrande-Technologie (LT) verbirgt sich die Entwicklung von Hardwarekomponenten, die um Sicherheitsfunktionen erweitert werden. Im Zusammenspiel mit LT-unterstützenden Betriebssystemen und Applikationen helfen diese Erweiterungen – insbesondere durch Absicherung der I/O-Kanäle – die Vertraulichkeit und Integrität der Datenverarbeitung zu wahren. Darüber hinaus haben die Erweiterungen die Aufrechterhaltung der Management-Funktionen, der Performance, der Flexibilität und Rückwärtskompatibilität von Intel-Rechnersystemen zum Ziel.

Folgende erweiterte Schlüsselkomponenten bilden dabei eine LT-spezifische Hardwareplattform:

- Prozessor,
- Chipsätze (Speicher, Ein-/Ausgabe-Subsystem),
- Tastatur und Maus,
- Grafik-Subsystem,
- Trusted Platform Module (TPM) Version 1.2.

LT erlaubt die Realisierung verschiedenster Modelle für eine gesicherte Rechner-Betriebsumgebung. Ein Beispiel dafür ist die Unterteilung in eine Standard- und eine geschützte Betriebspartition. Die Standardpartition entspricht dabei einer heute bestehenden Rechnerumgebung, innerhalb der die heute genutzten Applikationen unverändert laufen. Inwieweit geschützte und ungeschützte Programme parallel ablaufen oder gar Daten austauschen können, muss aus Sicherheitserwägungen wohl eher ausgeschlossen werden.

Die gesicherte Betriebsumgebung bedient sich dabei der Funktionen des TPM.

¹⁰ z. B. Arbeitsplatzrechner – netzwerkgebundene oder netzwerkunabhängige Notebookrechner

4 Warum Trusted Computing?

Die Initiativen zum „Trusted Computing“ sind keine Vorstöße einzelner Firmen. Ihnen liegt vielmehr ein in den Grundsätzen nachvollziehbarer Wunsch nach Durchsetzung gesellschaftspolitischer wie auch wirtschaftlicher Interessen zugrunde.

Exekutive und Legislative müssen die folgenden Ziele durchsetzen und unterstützen:

- Schutz kritischer Infrastrukturen,
- Verhinderung strafbewehrter Inhalte,
- Entdeckung strafbarer Handlungen.

Firmen und Institutionen haben sowohl als Anbieter wie auch als Nutzer von IT ein elementares Interesse

- an der Einhaltung von Lizenzbedingungen,
- an der Durchsetzung ihrer Rechte an digitalen Inhalten,
- an der Vermeidung schadenstiftender Software,
- an abgesicherten elektronischen Geschäfts- und Kommunikationsprozessen,
- an Möglichkeiten einer gesicherten Fernwartung,
- an der Kontrolle von mobilen Codes wie z. B. ActiveX, Javascript,
- ...

Diese Ziele glauben die Anbieter von Hard- und Software durch eine vertrauenswürdige IT-Umgebung (trusted¹¹) durchsetzen zu können. Dazu wird eine Umgebung von IT-Geräten mit folgenden Möglichkeiten bereitgestellt:

- erkennen, ob ein zugesicherter Zustand der Plattform noch vorhanden ist
- sichere Speicherung plattformabhängiger, geheimzuhaltender Daten

Diese Umgebung wird durch zunehmende Integration in die Gerätehardware auf Dauer nur mit unverhältnismäßig hohem Aufwand zu umgehen sein. Durch die Integration der hardwareseitigen Absicherungen in Verbindung mit Anwendungen und Betriebssystemen kann eine umfassende, kaum beeinflussbare Absicherung realisiert werden. Wie diese Umgebung aussieht, wird im Kapitel „Technologien des Trusted Computing“ auf Seite 10 detailliert beschrieben. Eine benutzerorientierte Absicherung ist nur indirekt vorgesehen.

Durch Ausnutzung dieser hardwaremäßigen Gegebenheiten können digitale Inhalte unveränderbar an ein Gerät und sogar an einen bestimmten Gerätezustand gebunden werden. Sollte dieses Gerät nicht mehr verfügbar sein, ist kein Zugriff auf die an dieses Gerät gebundenen Inhalte mehr möglich.

¹¹ trusted = vertrauenswürdig, gesichert, aber auch Trust = Kartell

Letztendlich basieren die vorgeschlagenen Verfahren auf Vertrauen, welches der Nutzer den Anbietern und Lieferanten von Hard- und Software gegenüber aufbringen muss. Dieses Vertrauen wird allerdings nur durch die Zusicherungen und Prozesse der Anbieter und nicht durch einforder- und durchsetzbare Qualitätseigenschaften, z. B. im Rahmen gesetzlicher Vorschriften, sichergestellt.

4.1 Auswirkungen im Versicherungsunternehmen

In den folgenden Abschnitten werden wesentliche Aspekte der möglichen Auswirkungen auf ein Versicherungsunternehmen betrachtet. Auch wenn letztendlich gesicherte, abschließende Bewertungen noch nicht umfassend möglich sind, lassen doch die potentiellen Risiken einen Einsatz in der Versicherungswirtschaft als kritisch erscheinen, insbesondere, da auch der erzielte Sicherheitsgewinn durchaus kritisch hinterfragt werden kann¹².

Mit den vorgeschlagenen Mechanismen des „Trusted Computing“ können die Sicherheitsziele in einem VU in folgenden Aspekten unterstützt werden:

- Kontrolle der eigenen Geräte,
- Kontrolle der eingesetzten Software,
- Kontrolle von Inhalten,
- Absicherung der Netze und Geräte,

Weitere Anwendungsgebiete finden sich in den Bereichen,

- Lizenzmanagement für die eingesetzte Software,
- Digital Rights Management für Dokumente, Daten, ...,
- Gesichertes Inventory- und Assetmanagement,
- System- und Changemanagement.

Für viele dieser Aufgabengebiete existieren heute schon hinreichend sichere Lösungen im betrieblichen Umfeld eines Versicherungsunternehmens.

4.1.1 Kosten

Trusted Computing setzt die Beschaffung TCG-konformer Plattformen mit TPM-Chip voraus. Von IBM und HP gibt es bereits erste PCs mit TPM und Schnittstellensupport.

¹² „Zudem werden in den Dokumenten der TCG fast durchgängig technische Details intensiv behandelt, während die übergeordnete Motivation der Beteiligten meist im Dunkeln bleibt. Sowohl die TCG als auch die Hersteller schildern ihre Ziele nur nebulös. Eine genaue Strategie, die konkrete Anwendungsszenarien beschreibt, sind sie bisher schuldig geblieben.“ Quelle: Internet, www.bsi.de „Sichere Plattformen und die Trusted Computing Group, Februar 2004, Bundesamt für Sicherheit in der Informationstechnologie

Die Initiativen von Microsoft (NGSCB) und Intel (LaGrande) setzen darüber hinaus spezielle Prozessoren, Chips und Ein- und Ausgabegeräte voraus, die vermutlich in zwei bis drei Jahren auf den Markt kommen werden.

Es ist davon auszugehen, dass durch Anschaffung der reinen Basistechnologie keine nennenswerten Zusatzkosten entstehen. Es war von vornherein Ziel der TCPA, eine kostengünstige Lösung zu schaffen. Die führenden Hersteller werden den TPM-Chip vermutlich im Laufe der nächsten Jahre in alle Geräte integrieren. Im gleichen Maße wird Software mit Schnittstellen zum TPM zur Verfügung gestellt werden.

Der Nexus ist als integraler Bestandteil der nächsten Betriebssystem-Generation von Microsoft geplant. Setzt sich NGSCB durch, wird infolge der weiten Verbreitung von Windows auch NGSCB-konforme Hardware und Software ausreichend und zu marktüblichen Preisen zur Verfügung stehen.

Durch den Einsatz von Trusted Computing wird sich unseres Erachtens kein gravierendes Einsparungspotential ergeben, da nach wie vor Sicherheitstechnologien wie Antivirensoftware, (Personal) Firewalls oder Kryptosoftware parallel eingesetzt werden müssen.

Trusted Computing ist ein sehr komplexes Thema. Je nach geplantem Anwendungsszenario sind für die Einführung entsprechend hohe Aufwände einzuplanen (Besitznahme und Aktivierung des Chips, Schlüsselmanagement, Backup, Migration, Useradministration, PKI-Support, Einbindung von Dienstleistern etc.).

Entsprechende Kosten ergeben sich durch den zusätzlichen Verwaltungsaufwand im laufenden Betrieb, hier insbesondere durch die Verwaltung der individuellen Schlüssel und Zertifikate, aber auch infolge der gestiegenen Komplexität der gesamten IT-Infrastruktur.

4.1.2 Sicherheitsgewinn

Durch Trusted Computing soll insbesondere in der PC-Welt ein deutlich höheres Sicherheitsniveau erreicht werden. Eine solche Initiative ist in Anbetracht der Verwundbarkeit heutiger Systeme prinzipiell zu begrüßen.

Es ist allerdings kritisch zu hinterfragen, welchen effektiven Sicherheitsgewinn ein Versicherungsunternehmen durch Trusted Computing erreichen kann und welche neuen Sicherheitsrisiken im Gegenzug entstehen können.

In Anbetracht vieler ungeklärter Details kann zur Zeit noch keine fundierte Aussage getroffen werden. Auf der Basis einer manipulationssicheren Hardware können grundsätzlich bessere Sicherheitslösungen implementiert werden. Entscheidend für den Erfolg oder das Risikopotential von Trusted Computing wird aber die Integration der TPM-Funktionalität in die darüber liegenden Betriebssysteme und Anwendungen sein. Das Vertrauen in eine solche Plattform ist also nur dann berechtigt, wenn die darauf basierenden zentralen Softwarekomponenten ebenfalls

höchsten Ansprüchen genügen. Es bleibt also abzuwarten, wie dies mit dem Wunsch nach Flexibilität, Features, Offenheit, Abwärtskompatibilität und den daraus entstehenden Kompromissen vereinbar ist. In jedem Fall bilden die vielen offenen Fragen heute noch keine gute Basis für ein vertrauenswürdiges System.

Die TCG informiert auf ihrer Homepage über Hintergründe und Vorteile der Technologie¹³. Überträgt man die dort zitierten Szenarien auf ein typisches Versicherungsunternehmen, relativieren sich viele der von der TCG adressierten Benefits.

Dies soll an einigen Beispielen verdeutlicht werden:

- Die TCG fokussiert eindeutig externe Bedrohungen. Es wird der exponentielle Anstieg erkannter Sicherheitslücken und bekannter Sicherheitsvorfälle zitiert. Entsprechend ist die Integrität vernetzter Systeme (in erster Linie PC, aber zunehmend auch PDAs, Handies u. Ä.) und die Sicherheit der dort gespeicherten Daten durch Hacker, Viren, Würmer oder Trojaner sowie physikalischen Diebstahl gefährdet. Im Corporate Network eines Versicherungsunternehmens werden diese Bedrohungen aber heute nicht mehr am Client abgewehrt. Zentrale Sicherheitslösungen wie Firewalls, Virenschleusen, Mail- und Webfilter wehren heute beinahe 100 % der Angriffe ab. Die dann noch auftretenden Schadenfälle sind häufig auf fehlendes Sicherheitsbewusstsein, nicht jedoch auf unzureichende technische Unterstützung zurückzuführen.
- Der TPM stellt kryptographische Funktionen und einen sicheren Speicher zur Verfügung. Im TPM gespeicherte private Signaturschlüssel verlassen den Chip nie. Passwörter können direkt im TPM gespeichert werden. Lokal gespeicherte (sensible) Daten können über einen im TPM gespeicherten Schlüssel sicher geschützt und über Schlüsselhierarchien auch an die lokale Hardware gebunden werden. Hierzu existieren bereits erste Produkte am Markt. Im Netzwerk eines VU sind sensible Daten jedoch in der Regel auf Servern gespeichert. Die Bindung dieser Daten an den Client bringt also keinen Mehrwert, sondern eher Probleme. In den meisten Unternehmen sind User-ID und Passwort immer noch die übliche Authentifizierungsmethode! Diese Passwörter werden aber sowieso nicht am Client, sondern nur zentral gespeichert. Laptops (des Außendienstes) wiederum werden meist standardmäßig mit aktivierter Verschlüsselung versehen. In der Kombination mit pre-boot-authentication kann bereits ein sehr hohes Sicherheitsniveau erreicht, mit Smartcards und ggf. Biometrie können gar höchste Ansprüche erfüllt werden. Insbesondere können die Smartcard und die auf ihr gespeicherten Credentials getrennt vom PC aufbewahrt werden.
- Jeder TPM hat einen eindeutigen privaten Schlüssel (Endorsement Key EK) aus dem sich wiederum pseudo-anonyme Schlüssel (Attestation Identity Key AIK) bilden lassen. Es kann z. B. einen AIK für eine Windows- und

¹³ TCG_Backgrounder, <https://www.trustedcomputinggroup.org/home>

einen für eine Linux-Partition geben. Mit Hilfe dieser AIKs kann gegenüber Dritten die Vertrauenswürdigkeit der Plattform nachgewiesen bzw. von diesen geprüft werden. Lösungen sind aufgrund vieler offener Fragen und fehlendem PKI-Support noch nicht in Sicht. Versicherungsunternehmen verfolgen allerdings eher den Sicherheitsansatz, keine direkten Zugriffe von außen in das interne Netz zu gestatten. Dies wird heute mit viel Aufwand durch (Reverse-) Proxies, demilitarisierte Zonen, dedizierte Webserver etc. umgesetzt. Ferner wird der Zugriff auf den lokalen Client, z. B. durch Sperrung von ActiveX, bewusst unterbunden. Nach außen wollen wir also allenfalls die Vertrauenswürdigkeit von Stellvertretern, nicht aber jedes einzelnen Clients bekunden.

Zusammenfassend lässt sich sagen, dass für die von der TCG adressierten Handlungsfelder in der Regel bereits alternative Sicherheitsverfahren existieren. Mit Trusted Computing können in diesem Kontext zwar Restrisiken minimiert werden. Diesem Nutzen sind aber der dazu notwendige Aufwand und die Risiken gegenüberzustellen, die aus dem Einsatz der Technologie resultieren können.

4.1.3 Sicherheitsrisiken

Neben den von den Herstellern versprochenen Vorteilen birgt Trusted Computing auch neue Sicherheitsrisiken:

- Trusted Computing ist komplex. Fehlbedienung und organisatorische Defizite sind somit reale Bedrohungen.
- Besonders heikel ist in diesem Zusammenhang die Möglichkeit, Inhalte und Software an Hardware bzw. sogar an definierte Systemzustände zu binden. Dies setzt durchdachte Backup- und Notfallszenarien voraus, um bei Defekt des TPM, der Festplatte oder der CPU keinen Verlust von Daten bzw. der Systemverfügbarkeit zu erleiden.
- Es sind neue Möglichkeiten für DoS-Attacks¹⁴ denkbar. So kann eine bewusste Manipulation der Systemintegrität dazu führen, dass Software und Daten nicht mehr oder nur mit hohem Aufwand wieder genutzt werden können.
- Die Technologie kann auch von Angreifern genutzt werden, um z. B. versteckte Kanäle oder strafbare Inhalte noch effizienter abzusichern.
- Gibt es Schwachstellen in den Vertrauensbeziehungen können diese verheerende Auswirkungen haben. Besonders heikel ist der Endorsement Key, auf dem die gesamte Vertrauenshierarchie aufbaut. Dieser kann nach der aktuellen TCG-Spezifikation 1.2 im Unternehmen zwar durch den Owner neu gesetzt werden. Wie aber soll man sich verhalten, wenn Rechner heute z. B. durch Dienstleister bereitgestellt werden?
- Die TCG kennt keine Black- und Whitelists und keine zentralen Kontrollserver.

Viele Kritiker fürchten aber, dass mit Trusted Computing die Grundlage für solche Ansätze geschaffen wird. Beispiele aus der Praxis des DRM (z. B. Windows Media Player) zeigen, dass solche Befürchtungen nicht unbegründet sind. Durch Manipulation solcher Listen oder durch vorsätzliche Störungen zentraler Kontrollserver können Angreifer den Betrieb eines VU massiv beeinträchtigen.

4.1.4 Kontrollgewinn

Als Vorteil von Trusted Computing wird häufig aufgeführt, dass sich die IT-Infrastruktur besser kontrollieren lässt, da die Integrität der Systeme einfacher überwacht und Manipulationen wirkungsvoll verhindert werden können.

Der TPM selbst ist passiv und trifft aktiv keine Entscheidung. Um den zitierten Kontrollgewinn zu erreichen, müssen also erst entsprechende Schnittstellen, Überwachungs- bzw. Managementtools, ausreichend TCG- bzw. NGSCB-konforme Anwendungen und ein stimmiges Gesamtkonzept zur Verfügung stehen.

Für exponierte Clients (Fernwartung, Remote Access, Konsolen) können solche Lösungen dann einen echten Mehrwert darstellen. Dabei handelt es sich in der Regel aber um eine überschaubare Anzahl von Endgeräten.

Im internen Netzwerk – und somit für die Mehrheit der PCs – sind Kontrolldefizite dagegen häufig eher auf organisatorische Unzulänglichkeiten (zu viele lokale Administratoren, keine verbindlichen Bestell- und Beschaffungsprozesse, unzureichendes Change-, Release- und Lizenzmanagement) zurückzuführen. Technisch sind z. B. die Entfernung einer lokalen Administrationsberechtigung oder eine Softwaresignatur in der Regel vollkommen ausreichend.

4.1.5 Kontrollverlust

Der Gewinn an Kontrolle über die eingesetzte Technologie und die genutzten Inhalte durch die Firmen wird durch eine standardisierte Technologieplattform sichergestellt. Es besteht die Gefahr, dass diese Technologie auch Dritten Kontrollmöglichkeiten über Bestandteile der Firmeninfrastruktur erlaubt. Die hiermit einhergehende Möglichkeit eines **Kontrollverlustes** der Firmen außerhalb gesetzlicher Bestimmungen kann sich sowohl auf die internen Ressourcen der Firmen wie auch auf deren Inhalte beziehen, die von außerhalb bezogen bzw. geliefert werden. Beispielhaft seien hier Programme, Dokumente und sonstige Unterlagen in elektronischer Form genannt. Die hier mögliche **Fremdbestimmung** darf keine Realität werden. Es liegen jedoch auch einige Risiken in den eingesetzten Technologien, die im Folgenden betrachtet werden sollen.

- Die Schlüssel- und Signaturvergabe der in der Hardware enthaltenen Schlüssel

¹⁴ Denial of Service-Attacken

ist nicht abgesichert. Dies betrifft insbesondere den grundlegenden „Endorsement Key“. In der Version 1.2 der Standardisierung des TPM ist allerdings eine Löschung des Endorsement Keys durch den „Owner“ vorgesehen. Ob dies allerdings durch das Versicherungsunternehmen selber oder durch eine externe, zertifizierte Firma zu geschehen hat, ist derzeit noch nicht festgelegt.

- Die Verwendung nicht zertifizierter Hard- und Software kann insbesondere im Zusammenspiel mit einem vertrauenswürdigen Betriebssystem zu erheblichen Problemen führen. So ist denkbar, dass derartige Software nicht mit zertifizierter Software zusammen ausgeführt werden kann. Dies ist allerdings keine definierte Eigenschaft von TCG. Die Steuerung erfolgt hier ausschließlich über das Betriebssystem, welches sich der Mechanismen des TPM bedient.
- Die Firmenrechner können auch durch jemanden außerhalb der Firma authentifiziert bzw. identifiziert werden. Damit wäre es theoretisch möglich, diese Rechner von außen zu beeinflussen oder abzuschalten. Insbesondere muss sichergestellt werden, dass maximal die Firma, in deren Netz der Rechner eingesetzt wird, aber nicht der Rechner selbst, identifiziert und damit angesprochen werden kann.
- Der Wechsel auf eine andere Plattform und andere Software wird auf Dauer erschwert und damit so verteuert, dass quasi ein Monopol durchgesetzt werden kann.

Diese Risiken können sich in konkreten Auswirkungen auf Standardsoftware, Anwendungen, Open Source Strategien oder Daten und Inhalte äußern:

- **Standardsoftware:**
Echter Wettbewerb wird häufig durch enge (nicht transparente) Verzahnung von Betriebssystemen, Middleware und Standardsoftware erschwert. Mittels Trusted Computing können solche Monopolstellungen mit Hilfe von Sicherheitstechnologie weiter zementiert werden. Kritiker sprechen vom sogenannten „lock-in“. Auch kann das Einspielen von Patches und Updates – ohne Berücksichtigung der betrieblichen Notwendigkeiten des VU – erzwungen werden. Führt man bewusst eine durchgehende Herstellerstrategie stellt dies vermutlich ein geringeres Problem dar. Gerade in einem sehr heterogenen Umfeld kann es aber nachteilige Auswirkungen auf die Interoperabilität geben. Durch die mögliche Bindung von Daten und Anwendungen an Hardware werden Plattformwechsel zusätzlich erschwert.
- **Anwendungen:**
Weder TCG noch NGSCB fordern die Zertifizierung eigener Anwendungen. Die Konzepte versprechen Abwärtskompatibilität. So sollen bestehende Windows-Anwendungen auch künftig im unsicheren Bereich lauffähig sein. Hat die Anzahl von Rechnern mit Trusted Computing aber erst mal eine kritische Masse überschritten, kann man sich externen Einflüssen durch die Hersteller oder durch externe Geschäftspartner nur noch schwer entziehen. Ob sich in der

Folge Auswirkungen auf Anwendungsarchitekturen und größere Umstellungsaufwände ergeben, ist zur Zeit reine Spekulation, kann aber auch nicht ausgeschlossen werden.

- **Open Source:**
Ähnlich wie bei Eigenentwicklungen ist noch nicht absehbar, wie Trusted Computing und der Open Source Gedanke miteinander harmonieren. Kritiker fürchten, dass für (bestimmte) Softwarekomponenten der Zwang zur (kostenpflichtigen) Zertifizierung entsteht und diese die schnelle Änderung und Nutzung von Open Source Lösungen behindert.
- **Daten / Inhalte (IRM) und DRM:**
Trusted Computing ermöglicht die Bindung von Daten und Inhalten an Hardware. Bei Hardwaredefekten und unzureichenden Backupkonzepten kann dies zu Datenverlusten führen. Ebenso kann künftig über Daten, Inhalte und Software der Zwang entstehen, Trusted Computing zu aktivieren.

4.1.6 Geschäftsprozesse

Wir erwarten nicht, dass Trusted Computing Ansätze zur Etablierung grundsätzlich neuer Geschäftsprozesse bietet:

- Im Corporate Network der Versicherungsunternehmen werden heute schon alle Geschäftsprozesse realisiert, die sinnvoll und beherrschbar sind.
- Bei Kunden- und Vermittlerportalen werden in der Regel bewußt geringe Anforderungen an die Ausstattung (und somit Integrität) des Clients gestellt. Es besteht nicht der Wunsch, die zugrunde liegende Hardware zu identifizieren. Im Vordergrund steht die Authentifizierung der Person. Ferner fehlt für eine Plattform-Authentifizierung die rechtliche Basis. Die Bestrebungen gehen hier eindeutig in Richtung Smartcard-Technologie (Bündnis für Signatur).
- Der Datenaustausch mit anderen Unternehmen (Banken, Behörden, Assisteuren etc.) scheitert heute nicht an einem fehlenden TPM-Chip. Da es sich dabei um klassische Maschine-zu-Maschine Kommunikationen handelt, können sich im B-2-B-Sektor durch zweifelsfreie Authentifizierung der Gegenseite noch am ehesten Mehrwerte ergeben.

4.2 Szenarien

Die in Abschnitt 4.1 beschriebenen Auswirkungen und Hintergrundtendenzen werden abschließend in zwei Extremszenarien beleuchtet.

4.2.1 Keine Nutzung von Trusted Computing

Verzichtet ein VU bewusst auf Trusted Computing im Sinne der TCG, geht es mittelfristig kein Risiko ein:

- Nach allen Bekundungen der Hersteller kann sowohl der TPM als auch der Nexus optional aktiviert werden, und bestehende Applikationen sind dennoch lauffähig.
- Wie in Abschnitt 4.1.2 aufgeführt, können die von der TCG adressierten Sicherheitsrisiken im Umfeld eines VU heute durch bestehende Sicherheitstechnologien beherrscht werden. Dafür entstehen dem VU keine neuen Sicherheitsrisiken.

Langfristig drohen folgende Risiken:

- Ist Trusted Computing im Markt auf genügend vielen Systemen installiert, kann durch Herstellerabhängigkeit ein Zwang zur Nach- und Umrüstung der IT-Infrastruktur entstehen. Der Umstieg wird eventuell durch Lockangebote (z. B. bessere Preiskonditionen bei aktiviertem TPM oder neuen Features) schmackhaft gemacht, ist aber vermutlich mit einem hohen Einführungsaufwand verbunden und bringt unseres Erachtens keinen betriebswirtschaftlichen Nutzen für das VU.
- Sofern Geschäftspartner auf Trusted Computing setzen (und z. B. Inhalte an Anwendungen binden), muss die Technologie punktuell eingeführt werden.

4.2.2 Nutzung von Trusted Computing

Mit einer breiteren Nutzung von Trusted Computing ist frühestens in zwei bis drei Jahren zu rechnen. Daraus ergeben sich mittelfristig folgende Risiken:

- Die TCG-Spezifikation kann sich noch in wesentlichen Punkten ändern. Beschaffte Hardware wird somit eventuell nicht mehr unterstützt oder sie ist zwar TCG- aber nicht NGSCB-konform und kann somit unter Windows nicht genutzt werden.
- Setzen sich die Initiativen überhaupt nicht durch, war auch der hohe Aufwand für Konzeption und Einführung vergebens.

Wie in Abschnitt 4.1.5 geschildert, kann Trusted Computing die Herstellerabhängigkeit zementieren. Der Nutzen wird zum Preis neuer Sicherheitsrisiken und eines noch nicht absehbaren Kontrollverlusts erkaufte.

4.3 Zusammenfassung

Der Einsatz der durch die TCG vorgeschlagenen Technologien ist isoliert betrachtet durchaus vorteilhaft und ermöglicht einige Sicherheitsgewinne in Firmennetzen. Der Sicherheitsgewinn für Privatanwender ist nicht nachvollziehbar, insbesondere, da der ursprünglich avisierte Schutz vor Viren und Trojanern nicht Ziel und auch nicht Ergebnis der Initiative ist. Kritisch sind im Wesentlichen zwei Punkte:

- Die vorgeschlagenen Techniken des Trusted Computings basieren auf Vertrauen gegenüber den bereitstellenden Firmen, ohne dass in irgendeiner Form entsprechende gesetzliche Kontrollen und Möglichkeiten der Anwender zur Durchsetzung ihrer Schutzinteressen existieren.
- Die Technik erlaubt eine unauflösbare Bindung von digitalen Inhalten (Software, Daten, Programme, ...) an ein definiertes Gerät oder einen definierten Gerätezustand. Sobald diese Voraussetzungen nicht mehr erfüllt sind, kann der Nutzer die derart geschützten Inhalte auch nicht mehr nutzen.

Wie im vorherigen Kapitel aufgezeigt, sind viele Missbrauchsmöglichkeiten nicht der TCG anzulasten. Sie werden vielmehr erst dadurch ermöglicht, dass derartige Funktionalitäten auf der Basis der eingesetzten Technologien im Betriebssystem implementiert werden. Die im Zusammenspiel von Hardware und Betriebssystem liegenden Missbrauchspotentiale sind extrem hoch und durch den erwarteten Kontrollgewinn nicht zu rechtfertigen.

Ein Großteil des avisierten Sicherheitsgewinns lässt sich auch durch die Bindung der Inhalte an Institutionen und Personen, z. B. durch Einsatz der Smartcardtechnologie, erreichen.

5 Anhang

5.1 Schlüssel, Signaturen und Zertifikate

Mit der breiten Verfügbarkeit des Internet werden die Möglichkeiten elektronischer Kommunikation in vielen Bereichen intensiv genutzt. Mit zunehmender Nutzung auch in sensiblen Bereichen gehen erhöhte Anforderungen an die Sicherheit der übertragenen Daten einher:

1. Es muss sichergestellt werden, dass die Nachricht nur von der vorgesehenen Person oder Institution gelesen wird (**Vertraulichkeit**).
2. Es muss sichergestellt werden, dass jede Änderung der bestätigten Nachricht auf dem Weg zum Empfänger bemerkt wird (**Integrität**).
3. Es muss sichergestellt sein, dass die Nachricht auch von demjenigen abgeschickt worden ist, der als Absender angegeben ist (**Authentizität**).

Zur Absicherung der Kommunikation werden Schlüsselpaare genutzt, die aus einem öffentlichen und einem geheimen (privaten) Schlüsselteil bestehen. Das Schlüsselpaar ist unverwechselbar. Der Ablauf ist damit wie folgt (Abbildung 2):

- Der Absender signiert (unterschreibt) sein Dokument mit seinem geheimen Schlüssel und verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Dabei wird eine digitale Signatur gebildet, die einen eindeutigen Fingerabdruck des Dokuments repräsentiert.
- Der Empfänger entschlüsselt die digitale Signatur mit dem öffentlichen Schlüssel des Absenders und prüft anhand des in der Signatur enthaltenen Fingerabdrucks, ob das Dokument zwischenzeitlich verändert wurde.
- Das unveränderte Dokument wird dann mit dem geheimen Schlüssel des Empfängers entschlüsselt und kann gelesen werden.
- Die öffentlichen Schlüssel werden im Rahmen einer Identitätsüberprüfung eindeutig einer Person oder Institution zugeordnet. Dies wird durch ein sogenanntes Zertifikat gewährleistet, welches durch ein Trustcenter auf einem geeigneten Trägermedium (Chipkarte, Diskette, ...) vergeben und der Person ausgehändigt wird. Das Trägermedium wird dabei in der Regel durch einen PIN-Code gegen Benutzung Fremder abgesichert. Dies Zertifikat wird mit dem öffentlichen Schlüssel, dem Zertifikat des Ausstellers und weiteren Informationen durch das Trustcenter in einem öffentlichen Verzeichnis publiziert und gegebenenfalls gesperrt.

Damit diese Verfahren funktionieren können, sind einheitliche Verfahren zur Verschlüsselung, Bildung des Fingerabdrucks, Entschlüsselung, ... und einheitliche Verzeichnisdienste zu verwenden.

Die folgende Abbildung beschreibt den Ablauf einer gesicherten Kommunikation und die Rollen der einzelnen Beteiligten. Die Handhabung der sicheren Kommunikation muss sehr einfach gehalten werden, wenn sie in der Breite eingesetzt werden soll. Letztendlich muss entsprechende Software bereitgestellt werden, die die komplizierten Abläufe für den Anwender unsichtbar abwickelt. Der Anwender sollte nur seine „Chipkarte“ benutzen und den Empfänger aus **einem** übergreifenden Verzeichnis ermitteln müssen.

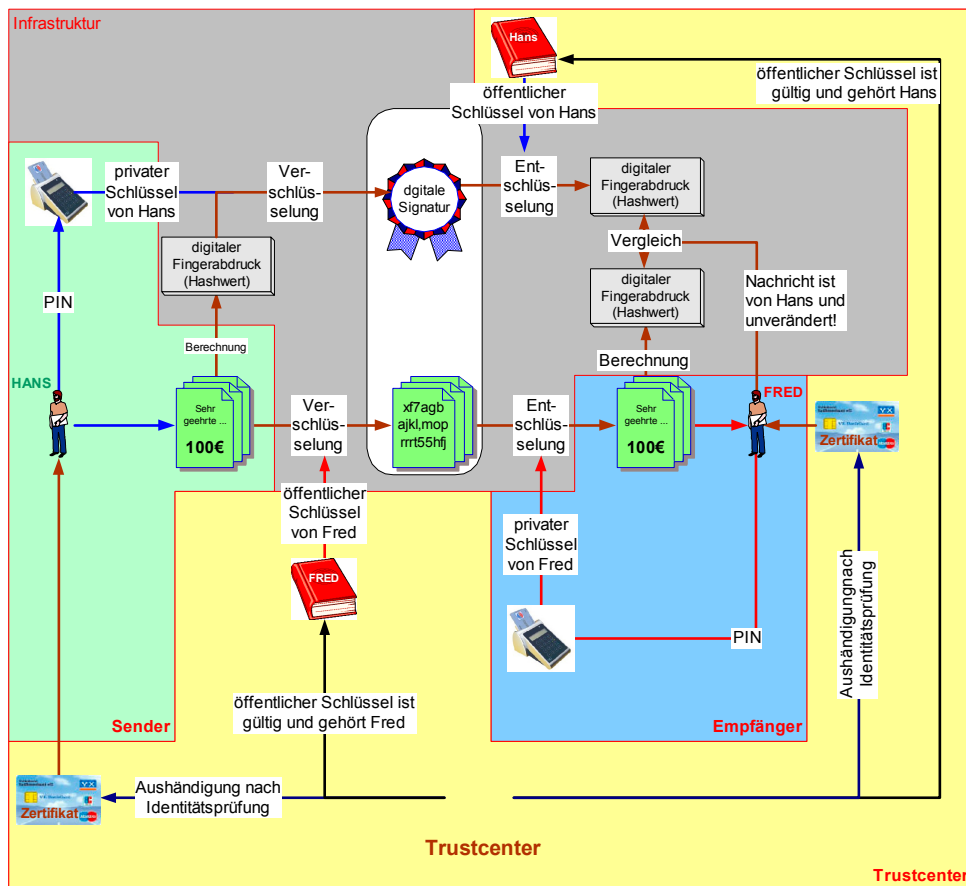


Abbildung 2: Ablauf einer gesicherten Kommunikation

Mit dem oben geschilderten Verfahren wird eine hinreichende Sicherheit in der Abwicklung der elektronischen Kommunikation erreicht. Je nach Qualität des involvierten Trustcenters (firmenintern, öffentlich ohne Akkreditierung, öffentlich mit Akkreditierung) ist die geleistete Signatur als Unterschriftenersatz auch in rechtlichem Sinne gültig oder nicht.

5.1.1 Digitale Signatur

Eine „digitale“ Signatur ist eine elektronische Unterschrift für eine in Bits und Byte gespeicherte Datei bzw. eines elektronischen „Dokuments“. Dazu wird der Inhalt des elektronischen „Dokuments“ mittels mathematischer Verfahren auf eine Bitkette fester Länge komprimiert. Dieser sogenannte Hashwert ist ein elektronischer

Fingerabdruck für das Dokument. Dieser Fingerabdruck wird dann mit dem privaten Schlüssel des Unterschreibenden verschlüsselt.

Ein Empfänger kann nun den verschlüsselten Fingerabdruck mit dem öffentlichen Schlüssel des Unterschreibenden entschlüsseln, den Fingerabdruck des Dokuments erneut ermitteln und ihn mit dem entschlüsselten Fingerabdruck vergleichen. Stimmen die beiden Fingerabdrücke überein, kann er von einer gesicherten Identität des Absenders (s. u.) und von der Unversehrtheit des Dokuments ausgehen.

Eine digitale Signatur stellt die Unversehrtheit (Integrität) des „Dokuments“ sicher. Bei **entsprechender Absicherung** des privaten Schlüssels wird über dies Verfahren auch die Authentizität des Unterschreibenden sichergestellt.

5.1.2 Hashwert (Fingerabdruck)

Der Inhalt eines elektronischen „Dokuments“ wird mittels mathematischer Verfahren auf eine Bitkette fester Länge komprimiert. Dieser sogenannte Hashwert ist ein elektronischer Fingerabdruck für das Dokument. Jede Änderung des Dokuments führt zu einer Veränderung im Fingerabdruck. Dabei ist die Wahrscheinlichkeit, dass sich ein Fingerabdruck wiederholt, so gering, dass sie vernachlässigt werden kann.

5.1.3 Zertifikat

Mit einem Zertifikat wird der öffentliche Schlüssel (oder allgemeiner ein eindeutiges elektronisches Identitätsmerkmal) eindeutig und nachvollziehbar einer Person oder Institution zugeordnet. Dazu werden der öffentliche Schlüssel und entsprechende Daten der Person oder Institution durch eine Autorisierungsinstanz mit deren privatem Schlüssel elektronisch signiert. Mit dem öffentlichen Schlüssel der Autorisierungsstelle kann dann die Unversehrtheit des Zertifikats und die Legitimität des Ausstellers geprüft werden, sofern der Prozess der Zertifikatserteilung entsprechend sicher gestaltet ist.

5.2 Glossar

AIK

→ Attestation Identity Key

Der AIK wird bei Aktivierung des TPM-Chips erzeugt. Er dient zur Repräsentierung bzw. Beglaubigung der Plattform gegenüber Dritten. Bei der Generierung wird eine Anfrage an eine Trusted Party (nicht TCG) übermittelt, die den Schlüssel verifiziert. Es sind je Plattform, je User mehrere AIK möglich. Über den AIK könnte im Rahmen einer Verarbeitung gegen eine Liste von ungültigen AIK geprüft werden. Erst nach Verifizierung ist der Zugang zum Dienst gestattet.

Attestation Identity Key

→ AIK

Core Root of Trust Measurement

→ CRTM

CRTM

→ Core Root Of Trust Measurement
Erweiterung im BIOS eines Rechners zur Nutzung des → TPM beim Boot des Systems durch Analyse des Systems und Ermittlung eines Hashwerters für den Systemzustand.

EK

→ Endorsement Key

Endorsement Key

→ EK

Eindeutige Kennung des → TPM-Chips. Dabei handelt es sich um einen nicht migrierbaren Schlüssel, der

vom Hersteller des Chips fest mit dem Chip verbunden wird. Im Rahmen der TCG-Spezifikation 1.2 ist in beschränktem Umfang ein Löschen und Neusetzen des EK vorgesehen. Der EK verlässt den Chip nicht.

Identitätsschlüssel

→ AIK

NGSCB

→ Next Generation Secure Computing Base

Windows Systemerweiterungen, die auf der Funktionalität des → TPM aufbauen. NGSCB wird mit der nächsten Windows Version (Longhorn) vermutlich 2006 ausgeliefert. Erste Bestandteile finden sich heute schon in einzelnen Versionen von Windows. NGSCB setzt im sicheren Betriebsmodus neue abgesicherte Hardware voraus (z. B. LaGrande von Intel)

Palladium

→ NGSCB

Palladium bezeichnete die Erweiterungen in Richtung Trustworthy Computings des auf XP folgenden Windows Betriebssystems. Palladium wurde abgelöst durch → NGSCB

SRK

→ Storage Root Key

Storage Root Key

→ SRK

Dies ist ein nicht migrierbarer Schlüssel, der im → TPM-Chip gene-

riert wird und der alle gespeicherten Informationen schützt. Der SRK wird einem „Besitzer“ zugewiesen und bindet das Gerät an diesen „Besitzer“. Der SRK kann neu erstellt werden. Damit sind aber die sonstigen Schlüssel nicht mehr gültig und müssen neu erstellt werden.

TCG

→ Trusted Computing Group
Nachfolgeorganisation der → TCPA, gegründet in 2003. Wesentlicher Unterschied zur TCG liegt in der Möglichkeit einer Entscheidungsfindung durch Mehrheiten anstelle einstimmiger Beschlüsse. Zur Zeit wird der Standard 1.2 verabschiedet. Kern der Aktivitäten ist der → TPM und seine Standardisierung, insbesondere auch für zukünftige Erweiterungen.

TCPA

→ Trusted Computing Platform Alliance
Gegründet im Oktober 1999 mit dem Ziel, Voraussetzungen für sichere Plattformen zu schaffen und die bisherigen Aktivitäten der Hersteller zu bündeln. Ergebnis war die Spezifikation 1.1 bzw. 1.1b des TCPA-Standards. Nachfolgeorganisation ist die → TCG.

TPM

→ Trusted Platform Module

Trusted Platform Module

→ TPM

wird auch Fritz-Chip nach dem amerikanischen Senator Fritz Holling genannt. Bei diesem Chip handelt es sich um einen integralen Bestandteil einer Hardwareplattform (zur Zeit PCs, Server, PDAs, Smartphones), der eine gesicherte Schlüssel- und Zustandsverwaltung ermöglicht. Der TPM wird durch die TCG spezifiziert und ist als passives Element Grundlage für Sicherheitserweiterungen in Anwendungen, BIOS und Betriebssystemen. Jeder TPM ist eindeutig durch den → Endorsement Key identifizierbar.

Der TPM kann am ehesten als „eingelötete“ Smartcard bezeichnet werden. In diesem Sinne bietet er eine in die Hardware integrierte Funktionalität zur geschützten Speicherung von kleinen Datenmengen und zur Generierung von Schlüsseln.

5.3 Autoren

Fred Chiacharella, Berlin

Dr. Uwe Fasting, Wuppertal

Tilo Fey, Nürnberg

Stefan Leppler, Wuppertal

Gisbert Lux, Münster

Peter Lubb, Hamburg

Andreas Moser, Stuttgart

Günther Otten, Köln

Johannes Schlattmann, Münster

Sven Schumann, Coburg

Lothar Schweizer, Stuttgart

Franz-Josef Souren, Aachen