11816/03/DE
WP 86

Arbeitspapier über vertrauenswürdige Rechnerplattformen und insbesondere die Tätigkeit der Trusted Computing Group (TCG)

Angenommen am 23. Januar 2004

DIE GRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 jener Richtlinie,

gemäß den Verfahrensregeln jener Richtlinie und insbesondere der Artikel 12 und 14

HAT FOLGENDES ARBEITSDOKUMENT ANGENOMMEN:

Vertrauenswürdige Rechnerplattformen - Kontext und Perspektive

Das Konzept der vertrauenswürdigen Rechnerplattformen geht auf die Feststellung der Informatikindustrie zurück, wonach die gegenwärtigen PCs (*Personal Computer*) unter Sicherheitsaspekten unzureichend sind – Virenangriffe, Möglichkeit des Eindringens in Datenbestände, Daten- und Softwarepiraterie usw.

Das Konzept entsteht zu einem Zeitpunkt, da die Prognosen für die Nutzung des Internet von einer abnehmenden Bedeutung des Worldwide Web, des durch die Vielzahl schlecht abgesicherter Datenübertragungen gekennzeichneten öffentlich zugänglichen Teils des Internet, zugunsten privater Räume ausgehen, bei denen Sicherheitsaspekte eine große Rolle spielen.

Während es vor diesem Hintergrund der zu schaffenden Sicherheit bei der elektronischen Signatur und deren juristischer Weiterentwicklung um Fragen im Zusammenhang mit Transaktionen in den Netzen geht, befasst sich das Konzept der vertrauenswürdigen Plattformen mit Fragen des Eigentumsrechts an immateriellen Gütern, deren Integrität, ihrer Geheimhaltung, soweit diese notwendig ist, und der Kontrolle ihrer Nutzung unter materiellen wie datentechnischen Aspekten. Die einzelnen Komponenten dieser sehr komplexen neuen Architekturen sind bislang weder vollständig spezifiziert noch geprüft oder gar verfügbar. Bekannt ist allerdings bereits, dass diese Plattformen allenfalls der Sicherheitsstufe EAL3 der gemeinsamen Kriterien (Common Criteria, CC) entsprechen werden – im Vergleich hierzu geht man bei Bank-Chipkarten von der Sicherheitsstufe EAL4 oder EAL4+ aus.

Die in der Vergangenheit unternommenen, auf der Identifizierung von Hardwarekomponenten gestützten Versuche zur Verbesserung der Sicherheit (wie beim Intel Pentium III, bei dem ein Unique Universal Identifier (UUID) eingeführt werden sollte), mussten wegen der damit verbundenen Gefährdung des Datenschutzes zurückgefahren werden. Zudem bemühen sich die Entwickler aufgrund der gemachten Erfahrungen verstärkt um eine Zusammenführung verschiedener Anwendungen von komplexen Verschlüsselungstechniken unter stark auf den Datenschutz ausgerichteten Aspekten. Daher werden im Zusammenhang mit vertrauenswürdigen Plattformen PET-Anwendungen (Privacy-Enhancing Technologies) wie die individuelle numerische Codefunktion oder der Virtual Identity Manager in Betracht gezogen, allerdings ist man

[1] Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/privacy/law_de.htm

sich darüber im Klaren, dass ein wirtschaftliches Modell für derartige Funktionen, das spezielle Chips erfordern würde, derzeit nicht realisierbar ist.

Aus den genannten Gründen sind die Anwendungen noch nicht besonders weit entwickelt, daher wäre die Verwaltung digitaler Zugriffsrechte als Pilotanwendung zu sehen.

Es ist allerdings festzustellen, dass sich der Eigentumsbegriff in der Informationsgesellschaft im Umbruch befindet und Gegenstand ebenso heftiger wie verfrühter Diskussionen ist. Auch erscheint er bislang weder unter juristischen noch unter ökonomischen Gesichtspunkten gefestigt. Daher muss die Rolle des öffentlich zugänglichen Raums wohl (neu) überdacht werden.

Der Eigentumsbegriff wird in den Spezifikationen von TCPA und TCG deutlich formuliert bzw. es wird zwischen den Rollen von Nutzern und Verwalter deutlich unterschieden, wobei letzterer die Rechte der ersteren in Bezug auf Techniken und Praktiken festlegt und einschränkt. Dies wiederum wirft allerdings gewisse Fragen im Hinblick auf die Ausgewogenheit auf.

Auf längere Sicht könnten Digital Rights Management-Systeme (DRMS) sogar dazu genutzt werden, bis zu einem gewissen Punkt den Zugang beispielsweise zu personenbezogenen Daten individuell und vertraglich festzulegen und abzusichern.
Zwar sind diese Anwendungen noch weit von der praktischen Realisierung entfernt – bislang existieren sie nur im Labormaßstab – und müssen erst noch rechtlich abgesichert werden, doch ist davon auszugehen, dass es sich bei den Rechnerplattformen zur Verwaltung dieser Rechte um dieselben handelt wie die vertrauenswürdigen Plattformen, um die es in diesem Papier geht.

Ansatz und Methodik der Datenschutzgruppe

Die Datenschutzgruppe verfolgt mit Interesse die Entwicklungen im Bereich des Trusted Computing (IT-Sicherheit), insbesondere die Arbeiten der Trusted Computing Group (TCG), eines Ad-hoc-Industriekonsortiums, das Spezifikationen für eine neue Klasse von Hardwaresicherheitschips mit der Bezeichnung Trusted Platform Modules (TPMs) erarbeitet.

Die Datenschutzgruppe ist sich der Tatsache bewusst, dass sich das Augenmerk der TCG hauptsächlich auf die Definition einiger Plattformkomponenten richtet und nicht auf die Plattform insgesamt, erkennt aber deutlich, dass die von der TCG entwickelten Module (insbesondere die TPMs) bedeutende Auswirkungen auf den künftigen Einsatz von Plattformen (gegenwärtig PCs bzw. Server, längerfristig jedoch auch persönliche digitale Assistenten (PDAs), Mobiltelefone usw.) in einer voll vernetzten Welt haben werden.

Die internationale Presse hat dieser Entwicklung ebenfalls große Beachtung geschenkt, nicht nur aufgrund der PR-Maßnahmen der TCG, sondern auch wegen der bedeutenden Diskussionsbeiträge einiger Datenschutzbehörden[2] und maßgebender Hochschulvertreter[3].

[2] Siehe hierzu Dokumente der CNIL, des Büros von Alexander Dix u. a.
[3] Siehe hierzu Arbeiten von Ross Anderson.

Die Datenschutzgruppe hat sich entschlossen, mit der TCG in einen Dialog einzutreten, und im Laufe des Jahres 2003 mehrere Treffen ihrer Taskforce Internet mit TCG-Vertretern zur Erörterung der technischen und rechtlichen Aspekte der TPM-Spezifikationen organisiert.
Die Datenschutzgruppe stellt mit Befriedigung fest, dass die TCG mehrere Vorschläge der Datenschutzgruppe in die Version 1.2 der Spezifikationen aufgenommen und eine Best Practices Group eingerichtet hat, die Empfehlungen zu den Datenschutzfragen abgeben soll.
Im vorliegenden Papier sollen einige der Themen angesprochen werden, die zusätzliche Beachtung verdienen und von der TCG weiter erörtert werden sollten.

Der Bewertung der Arbeiten der TCG in diesem Papier sind durch eine Reihe von Sachzwängen im Hinblick auf den gegenwärtigen Entwicklungsstand der Spezifikationen Grenzen gesetzt. Derzeit ist noch nicht absehbar, in welcher Weise von den Spezifikationen Gebrauch gemacht wird, welche Anwendungen oder Betriebssysteme entwickelt werden, welche Akteure beteiligt sein werden, welche Geschäftsmodelle etabliert werden usw. Ein weiteres Unsicherheitsmoment liegt in der Tatsache, dass die Spezifikationen weder zur Verwendung all ihrer Elemente noch zur Implementierung der in die Version 1.2 aufgenommenen neuen Systemmerkmale (Features) verpflichten. Nicht alle in den TPM-Spezifikationen von Version 1.2 definierten Funktionen werden in den einzelnen plattformspezifischen Komponenten implementiert werden.

Die vorliegende Thematik erfordert also noch weitere Arbeiten in der Zukunft; die Datenschutzgruppe wird die Entwicklungen, insbesondere im Hinblick auf spezifische Anwendungen, aufmerksam verfolgen.

Was ist die TCPA/TCG?
Die Aufgabe der TCG besteht nach eigenen Aussagen der Gruppe in der Entwicklung und Förderung offener, anbieterneutraler Industriestandardspezifikationen für der IT-Sicherheit dienende Baublöcke und Softwareschnittstellen für vielfältige Plattformen. Die TCG ist als Non-Profit-Vereinigung mit internationaler Mitgliedschaft eingetragen, die die Spezifikationen der TCPA als Arbeitsbasis übernommen hat.

Der Gruppe, einem Ad-hoc-Industriekonsortium, gehören viele bedeutende Akteure des Technologiebereichs nicht nur aus der Computerwelt, sondern auch aus anderen Disziplinen an. Interessant ist beispielsweise, dass sich Sony der Gruppe angeschlossen hat[4].

Auf der Spezifikation 1.1b der TCPA basierende Trusted Platform Modules (TPM) können derzeit von drei Anbietern bezogen werden: Atmel, Infineon und National Semiconductor. Außerdem sind jetzt einige TCG-konforme PC-Plattformen lieferbar: ThinkPad Notebooks und NetVista Desktops von IBM. Die Branche geht davon aus, dass in Kürze weitere hinzukommen.

[4] Die Trusted Computing Platform Alliance (TCPA, Allianz für vertrauenswürdige Rechnerplattformen) wurde ursprünglich von Compaq, HP, IBM, Intel und Microsoft gebildet. Gegenwärtig sind AMD, HP, IBM, Intel und Microsoft die Träger („Promoters“) der TCG, zu denen voraussichtlich noch weitere hinzukommen. So genannte „Contributors“, darunter auch europäische Unternehmen, sind derzeit ATi Technologies, Atmel, Broadcom Corporation, Comodo, Fujitsu Limited, Gemplus, Infineon, Legend Limited Group, National Semiconductor, Nokia, MTRU Cyryptosystems, nVidia, Phoenix, Philips, Rainbow Technologies, Seagate, Shang Hai Wellhope Information, Sony, Standard Microsystems, STMicroelectronics, Texas Instruments, Ultimaco Software AG, VeriSign und Wave Systems. Darüber hinaus haben weitere Unternehmen wie z. B. Sun Microsystems ihr Interesse und die Absicht bekundet, sich der Gruppe anzuschließen.

Die TCG hat Spezifikationen für Hardwaresicherheitschips (TPM) erarbeitet. Diese Chips sollen der umfassenden Informatisierung und Vernetzung (Ubiquitous Computing) dienen, weshalb der Schwerpunkt der Bemühungen nach Angaben der Branche auf der Sicherung beliebiger Hardwareplattformen liegt. Die wichtigsten Ziele der TCG sind die Authentifizierung und die Erhöhung der Sicherheitsniveaus. Darüber hinaus sollen TCG-Produkte zur Realisierung von Computational Grids[5] beitragen.

Der TPM-Chip weist folgende Funktionalitäten auf:

- Public-Key-Funktionen: Generierung des Schlüsselpaares, Public-Key-Signatur, Verifizierung, Verschlüsselung und Entschlüsselung.

- Trusted-Boot-Funktionen: Platform Configuration Registers (PCR) speichern während der gesamten Bootsequenz Hash-Werte von Konfigurationsinformationen. Nach dem Booten können Daten (z. B. symmetrische Schlüssel für verschlüsselte Dateien) mithilfe eines PCR „versiegelt“ werden.

- Initialisierungs- und Verwaltungsfunktionen: Sie gestatten dem Eigentümer das Ein- und Ausschalten einer Funktionalität, das Zurücksetzen des Chips sowie die Inbesitznahme. Die neue Version der Spezifikationen bietet dem Eigentümer die Möglichkeit, eine Reihe von Funktionen auf den Nutzer zu übertragen.

Die TPM-Technik ermöglicht die Durchsetzung von Sicherheitsrichtlinien.

Die Entwicklung spezifischer Anwendungen ist noch in der Anfangsphase. Einige Beispiele für mögliche Anwendungen sind das Digital Rights Management (DRM)[6], die Next Generation Secure Computing Base (vormals Palladium) von Microsoft und die LaGrande-Technologie von Intel. Derzeit ist noch nicht voll absehbar, welche Anwendungsmöglichkeiten der TCG-Spezifikationen sich in der Zukunft ergeben könnten.

Die Datenschutzgruppe möchte betonen, dass die TCG, wie bereits in früheren Dokumenten[7] zu ähnlichen Sachverhalten festgestellt, zumindest für die technische Entwicklung des Projekts verantwortlich ist. Sie sollte zudem sicherstellen, dass die von ihr entwickelten Spezifikationen und Protokolle die Unternehmen, die nach ihnen verfahren, in die Lage versetzen, den Bestimmungen der Richtlinie[8] zu entsprechen.

Sowohl die Entwickler der technischen Spezifikationen als auch diejenigen, die effektiv Anwendungen oder Betriebssysteme herstellen bzw. implementieren, tragen die Verantwortung für die diesbezüglichen Datenschutzaspekte, wenn auch auf verschiedenen Ebenen. Wer die Anwendungen herstellt, vermarktet und nutzt, ist

---

5 Computational Grids sind Netzwerke, die die gemeinsame Nutzung, Selektion und Vereinigung einer breiten Palette weiträumig verteilter Rechnerressourcen (wie z. B. Supercomputer, Compute Clusters, Speichersysteme, Datenquellen, Instrumente, Humanressourcen) ermöglichen und sie als eine vereinte Ressource präsentieren.

6 Die Datenschutzgruppe will in naher Zukunft in diesem Bereich tätig werden.

7 Siehe z. B. das am 29. Januar 2003 angenommene Arbeitspapier zu Online-Authentifizierungsdiensten (WP 68).

8 Siehe auch Richtlinie 1999/5/EG über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität, ABl. L 91 vom 7.4.1999.

ebenfalls verantwortlich, insbesondere auch die Verarbeiter von Benutzerdaten, da sie normalerweise das letzte Glied in der Kette und diejenigen sind, die mit dem Benutzer interagieren.

Rechtlicher Rahmen

Die Datenschutzgruppe möchte betonen, dass die Arbeiten der TCG den Anforderungen der bestehenden europäischen Rechtsvorschriften Rechnung tragen sollten. Die Richtlinien 95/46/EG und 2002/58/EG sind die wichtigsten Rechtsakte zum Datenschutz im Allgemeinen bzw. im Bereich der elektronischen Kommunikation. Darüber hinaus sollten auch die einschlägigen Bestimmungen der Richtlinien über den elektronischen Geschäftsverkehr[9] und über elektronische Signaturen[10] berücksichtigt werden.

Im vorliegenden Zusammenhang kommt zahlreichen Grundsätzen der Datenschutzrichtlinie erhebliche Bedeutung zu. Die Datenschutzgruppe möchte vor allem nachdrücklich auf die Wichtigkeit des Grundsatzes der Verhältnismäßigkeit und des Grundsatzes der Notwendigkeit der Erhebung und Verarbeitung von Daten verweisen. Diese Prinzipien besagen, dass unter Abwägung der Grundrechte des Betroffenen gegen die Interessen der verschiedenen beteiligten Akteure so wenig personenbezogene Daten wie möglich verarbeitet werden sollten.
Aus den genannten Grundsätzen ergibt sich Folgendes für die Konzeption der neuen Protokolle und Geräte: Technik ist zwar an sich neutral, es sollte aber grundsätzlich darauf geachtet werden, dass die Anwendungen und die Konzeption der neuen Geräte datenschutzgerecht sind[11].

Die Datenschutzgruppe kennt und unterstützt die Arbeiten der Europäischen Kommission im Bereich der datenschutzfördernden Technologien (Privacy-Enhancing Technologies, PET) und legt der TCG nahe, die PET-Konzeption auch bei ihren weiteren Arbeitsschritten im Auge zu behalten.

Überlegungen zu den Auswirkungen der Arbeiten der TCG auf den Datenschutz
Da es hier um einen technologischen Kontext geht, der sich noch im theoretischen Aufbau befindet, möchte sich die Datenschutzgruppe auf einige allgemeine Überlegungen beschränken, die sich aus den derzeit in der Industrie gebräuchlichen Leitlinien ergeben

- Anwendungsumfeld

Bei allen Versuchen, die Auswirkungen der Arbeiten der TCG auf den Datenschutz zu analysieren, sollte zwischen den verschiedenen Umgebungen differenziert werden, in denen TCG-konforme Plattformen eingesetzt werden können:
- In Unternehmensumgebungen, insbesondere in Unternehmensnetzen, könnte die vorgeschlagene Infrastruktur der Erhöhung der Sicherheit dienen. Dabei ist zu beachten, dass Unternehmen dem TCG-Konsortium zufolge die wichtigste Zielgruppe unter den Käufern/Benutzern des Systems sind.

---

9 Richtlinie 2000/31/EG vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), ABl. L 178 vom 17.7.2000.

10 Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1.2000.

11 Siehe hierzu die am 30. Mai 2002 angenommene Stellungnahme 2/2002 über die Verwendung eindeutiger Kennungen bei Telekommunikationsendeinrichtungen: das Beispiel Ipv6 (WP 58).

- Aufseiten der Verbraucher ist weniger offenkundig, worin der Vorteil für die Benutzer des Systems liegt. Die TCG könnte für gewisse aus Benutzersicht wünschenswerte Verbesserungen hinsichtlich des Speicherschutzes und der Möglichkeit zur Verwendung digitaler Pseudonyme für Transaktionen sorgen. TPM-basierte Anwendungen könnten aber auch zum Nachteil der Benutzer eingesetzt werden, z. B. von der Contentindustrie, um die Kontrolle über Verbreitung und Nutzung von digitalem Content (einschließlich Software) zurückzugewinnen, die sie mit dem Aufkommen von Internet und Peer-to-Peer-Anwendungen verloren hat.

- Wahlfreiheit beim Einsatz von TPM

In den TPM-Spezifikationen wird zwischen der Rolle des Eigentümers und der Rolle des Nutzers unterschieden. Im privaten Bereich hat dies keinerlei Auswirkungen, da eine Privatperson sowohl der Eigentümer als auch der Nutzer wäre, in Unternehmen kann die Unterscheidung jedoch gewisse Probleme aufwerfen.
In einer Unternehmensumgebung wäre der einzelne Arbeitnehmer der Nutzer, während der Arbeitgeber der Eigentümer wäre. Der Arbeitgeber kann Entscheidungen treffen, die sich auf den einzelnen Arbeitnehmer und die Menge ihn betreffender Daten, die verarbeitet werden, auswirken. In solchen Fällen hat der Eigentümer (Arbeitgeber) für die Unterrichtung und einen angemessenen Schutz der Nutzer zu sorgen.

In dieser Hinsicht hat die Version 1.2 der Spezifikationen durch die Aufnahme eines Systems, mit dem Entscheidungen bezüglich der Anwendung der verschiedenen Funktionen des TPM delegiert werden, gewisse Fortschritte gebracht, der Eigentümer hat aber weiterhin die oberste Kontrolle und kann entscheiden, ob er bestimmte Schlüsselfunktionen delegieren will oder nicht. Infolgedessen kann man nicht sagen (wie dies einige TCG-Unternehmen auf ihren Websites oder in ihren offiziellen Äußerungen tun), dass sich der Einzelne die Möglichkeit hat, über für die Nutzung des Systems entscheidet und völlig frei wählen kann.

Außerhalb des Unternehmensbereichs besteht derzeit noch die Möglichkeit, sich für oder gegen die Benutzung einer Plattform mit einem TPM zu entscheiden, wobei man sich allerdings fragt, wie lange das so bleibt. Der von einer derart starken Vertretung der Industrie propagierte TPM-Einsatz dürfte zum De-facto-Standard werden, zu einer notwendigen Voraussetzung für die Teilhabe an der Informationsgesellschaft. Dies könnte sich nicht nur im Bereich des Datenschutzes, sondern auch in Bezug auf andere Menschenrechtsaspekte wie etwa die Redefreiheit auswirken.

- Information der Benutzer

Wegen der technischen Komplexität TPM-basierter Systeme ist schwer vorstellbar, dass der Durchschnittsbenutzer in der Praxis in der Lage sein wird, die Informationen über die Systeme zu verstehen und in voller Sachkenntnis, in klarem Bewusstsein der Konsequenzen, über ihre Nutzung zu entscheiden. Die Datenschutzgruppe fordert die TCG auf sicherzustellen, dass die Benutzer einfache und klar verständliche Informationen erhalten, und – was noch wichtiger ist – dafür zu sorgen, dass in allen Fällen ausreichender Schutz gewährleistet ist, unabhängig von etwaigen Schritten, die der Benutzer zu unternehmen hat.

- Sicherheitsmerkmale

Die TPM-Spezifikationen sehen positive Sicherheitsmerkmale vor. Sicherheit und Integrität sind natürlich wichtige Aspekte, die auch in Zusammenhang mit der Datenschutzrichtlinie relevant sind. Die Datenschutzgruppe fragt sich jedoch, ob das Sicherheitsniveau im Einzelfall auf die spezifischen Verwendungen des Systems

„abgestimmt“ werden kann. Der Sicherheitsgrad sollte letztlich den potenziellen Risiken entsprechen, die je nach Situation unterschiedlich sind: So ist z. B., wenn ein Benutzer online auf seine medizinische Akte zugreifen will, mehr Sicherheit erforderlich, als wenn sich jemand auf einer News-Website registrieren lassen will.

- Datenschutz durch externe Zertifizierung oder Anonymisierung

Um die Übermittlung von Identifizierungsdaten und damit die Bestimmung des Benutzerprofils durch Dritte zu beschränken, sieht die TCG die Möglichkeit zur Einschaltung einer Trusted Third Party (TTP) vor, die die Identität des Benutzers gegenüber dem Dritten bestätigt, ohne sie jedoch offen zu legen.
Die Rolle der Trusted Third Party (TTP), von der TCG auch Privacy Certification Authority genannt, bedarf eingehender Überlegungen. Eine starke Datenkonzentrationen birgt immer zusätzliche Risiken, weshalb für ausreichende Vorsichtsmaßnahmen gesorgt werden sollte. In Bezug auf TPMs existieren Szenarien, bei denen eine einzige TTP riesige Mengen von Authentifizierungsinformationen kontrolliert.
Version 1.2 der Spezifikationen bietet die Möglichkeit, ohne TTP auszukommen und sich stattdessen der Direct Anonymous Attestation (DAA) zu bedienen, mit deren Hilfe der Benutzer einen so genannten Attestation Identity Key (AIK) generieren kann, ohne dafür den eindeutig identifizierenden Genehmigungsschlüsssel (Endorsement Key, EK) präsentieren zu müssen[12]. Die Datenschutzgruppe betrachtet dies als Verbesserung, weist jedoch darauf hin, dass die Wahl zwischen TTP und DAA auf der Anwendungsebene getroffen wird; die derzeit vorliegenden Spezifikationen lassen noch beide Funktionen zu.

Die DAA ist mithin eine zusätzliche Option, kein Standardmerkmal des Systems in allen Fällen. Die Datenschutzgruppe vertritt die Auffassung, dass die Einführung der DAA-Funktionalität[13] eine Verbesserung darstellt, möchte jedoch darauf hinweisen, dass in Fällen, in denen ein Bezug zur Identität des Benutzers hergestellt werden kann oder Benutzerprofile erstellt werden können, nicht mehr von Anonymität die Rede sein kann[14]. Sie empfiehlt der TCG, sich für einen äußerst datenschutzfreundlichen bzw. datenschutzfördernden Gebrauch dieser Funktionalität einzusetzen: möglichst weit gehende Verwendung so genannter „random bases“ und, wenn ein Zurückrufen des TPM und so genannte „name bases“ notwendig sind, Beschränkung der Verwendung ein und derselben „name base“ auf den kürzestmöglichen Zeitraum.

Die Datenschutzgruppe möchte nachdrücklich auf die wichtige Rolle verweisen, die das Vertrauen bei TPM-basierten Systemen spielt. In der gesamten Kette beteiligter Akteure – vom Entwickler der Spezifikationen bis hin zum Anbieter der Anwendungen und zum Einrichter des Systems vor Ort - sollte Vertrauen herrschen. Dem Datenschutz sollte in allen Phasen des Prozesses Rechnung getragen werden.

Punkte, die zusätzliche Berücksichtigung in den von der TCG zu erarbeitenden Leitlinien und optimalen Praktiken verdienen

---

12 Die DAA bietet eine alternative Methode zum TTP-Verfahren zur Feststellung der Gültigkeit eines AIK. Sie bedient sich der Zero-Knowledge-Proof-Verschlüsselungstechnik und stellt die Gültigkeit des AIK fest, ohne die EK-Daten gegenüber dem Identity Provider auszuweisen.

13 Mangels praktischer Erfahrung mit der Funktionsweise von Zero-Knowledge-Proof-Systemen ist es auch schwer zu beurteilen, wie die DAA in der Praxis funktionieren wird.

14 Siehe Erwägung 26 der Präambel der Datenschutzrichtlinie.

Die Datenschutzgruppe begrüßt die Einrichtung einer Best Practices Group innerhalb der TCG, die sich mit den anstehenden Datenschutzproblemen befassen und diesbezügliche Leitlinien und optimale Praktiken entwickeln soll.

Dieser Gruppe kommt eine entscheidende Rolle im Hinblick auf eine datenschutzgerechte Umsetzung der TCG-Spezifikationen zu. Die Datenschutzgruppe fordert die Best Practices Group auf, sich insbesondere mit folgenden Themen zu befassen:

- Aufgabe der Trusted Third Party (Privacy CA): Welche Stelle wird als TTP fungieren, worin wird ihre Aufgabe bestehen? Die Best Practices Group könnte Leitlinien für die einzurichtenden Sicherheitsmechanismen vorgeben. Wenn die TTP ihren Sitz in Europa hat, muss sie die einschlägigen europäischen Datenschutzvorschriften erfüllen. Außerdem sollten die Bestimmungen der Richtlinien über den elektronischen Geschäftsverkehr und über elektronische Signaturen beachtet werden.

- Nutzung der DAA-Funktionalität: Die Best Practices Group sollte sich für die „random base“ als bevorzugte Option einsetzen, sofern nicht nachweislich eine besondere Notwendigkeit zur Verwendung einer „name base“ besteht. Wenn eine „name base“ notwendig ist, sollte sie nur kurzzeitig verwendet werden, um zu vermeiden, dass über längere Zeit Benutzerprofile angelegt werden können. Die Benutzer sollten zudem umfassend informiert werden. Die Best Practices Group könnte eine Reihe von Beispielen für verschiedene Dienste und die Einsatzmöglichkeiten der DAA im jeweiligen Kontext ausarbeiten, um die anstehenden Probleme zu verdeutlichen und die wichtigsten Fragen aufzuzeigen, die behandelt werden sollten.

- Bereitstellung der erforderlichen Benutzerinformationen: Die Informationen sollten vollständig und leicht verständlich sein und den Benutzern auf verschiedenen Ebenen vermittelt werden. Dabei besteht eine Kette der Verantwortung, die von den Entwicklern der Spezifikationen bis zu den Herstellern, den Entwicklern neuer Betriebssysteme oder Anwendungen, deren Anbietern usw. reicht. Die Verwendung von TPMs sollte für die Benutzer klar ersichtlich sein, vor allem auf der Anwendungsebene.
Die Datenschutzgruppe befürchtet, dass es wegen der technischen Komplexität TPM-basierter Systeme für den Durchschnittsbenutzer äußerst schwierig sein könnte, die Implikationen und Konsequenzen bestimmter vorgesehener Systemmerkmale zu überblicken, und legt der TCG dringend nahe, für die Erstellung von Informationspaketen in klarer und einfacher Sprache zu sorgen, die es ermöglichen, die TPM-Technik und die damit verbundenen Verantwortlichkeiten vollständig zu verstehen.

- Notwendige Kontrolle und Durchsetzung der Datenschutzanforderungen im Implementierungsprozess: Die Datenschutzgruppe ist sich der Tatsache bewusst, dass die TCG keine vollständige Kontrolle der Erfüllung der Datenschutzvorschriften bei den Anwendungen gewährleisten kann, hielte jedoch die Einführung von Systemen, durch die eine gewisse Kontrolle der Umsetzungen der Spezifikationen „eingebaut“ wird, für sehr sinnvoll. Im Dialog mit den Mitgliedern der TCG wurde die Entwicklung eines Logo- oder Zertifizierungsprogramms für TCG-konforme Produkte vorgeschlagen.
Die Datenschutzgruppe möchte der TCG nahelegen, derartige Möglichkeiten zu erkunden und Empfehlungen und Leitlinien zu entwickeln, die die Unternehmen dazu anregen, die Spezifikationen in datenschutzgerechter bzw. datenschutzfördernder Weise umzusetzen. Dabei sollte dem spezifischen Charakter der europäischen Rechtsvorschriften in diesem Bereich besondere Beachtung geschenkt werden.

Fazit

Die Datenschutzgruppe stellt mit Befriedigung fest, dass die TCG mehrere Vorschläge der Datenschutzgruppe in die Version 1.2 der Spezifikationen aufgenommen und eine Best Practices Group eingerichtet hat, die Empfehlungen zu den Datenschutzfragen abgeben soll. Sie ersucht die TCG, sich mit den in diesem Papier angesprochenen Problemen auseinander zu setzen und nicht nur datenschutzgerechte, sondern auch datenschutzfördernde Merkmale in das System aufzunehmen.

Die TCG-Spezifikationen haben bisher kaum Anwendung in der Praxis gefunden und werden in der Zukunft möglicherweise abgeändert. Einige der Einsatzmöglichkeiten der TPM-Technik sind noch nicht ausgewiesen und über viele Fragen wird erst auf der Anwendungsebene entschieden. Neue Funktionalitäten dürften eher in anderen Plattformen als PCs, etwa in Mobiltelefonen, PDAs usw., eingerichtet werden. Auf der Ebene der Dienste und Anwendungen herrscht mithin große Ungewissheit.

Die Datenschutzgruppe wird daher die Entwicklungen weiterverfolgen, um sich zu vergewissern, dass den Bestimmungen der Datenschutzrichtlinie Rechnung getragen wird. Sie ersucht die TCG, der Datenschutzgruppe regelmäßig über weitere Fortschritte und die Entwicklung von Anwendungen und insbesondere über die Arbeit der Best Practices Group und des Board of Advisors Bericht zu erstatten.

Geschehen zu Brüssel, am 23. Januar 2004
Für die Arbeitsgruppe
Der Vorsitzende
Stefano RODOTA