Trusted Computing und Wettbewerbsrecht – Entwicklung einer IT-Sicherheitsarchitektur unter den Bedingungen des EG-Kartellrechts

Vortrag im Workshop 3 (Regulierung und Selbstregulierung)

bei der Jahrestagung 2004 der Deutschen Gesellschaft für Recht und Informatik e. V.

Hannover, 8. Oktober 2004

Andreas Neumann
Zentrum für Europäische Integrationsforschung

Ausgangslage

Das Problem

- (Das Vertrauen in die) Sicherheit von Systemen setzt (Vertrauen in) deren Integrität voraus.
- Die Systemintegrität wird durch Schadprogramme – Viren, Trojaner etc. – bedroht.
- Geschäftsmodelle, die auf Mechanismen der digitalen Rechteverwaltung (Digital Rights Management, DRM) basieren, setzen ebenfalls einen bestimmten Systemzustand voraus, in dem die vorgesehenen Nutzungsbeschränkungen beachtet werden.

„Die Entwicklung mobiler Breitbanddienste umfasst Firmen- und Verbraucheranwendungen mit persönlichen und sensiblen Daten. Diese Transaktionen erfordern ein zuverlässiges, sicheres Identifizierungs- und Authentifizierungsverfahren.“

Mitteilung der Kommission: „Mobile Breitbanddienste“, KOM (2004) 447, S. 9

Problem: Es existiert keine einfache Methode zur Überprüfung der Integrität von Hard- und Softwarekomponenten.

Ausgangslage

Mögliche Ebenen der Problemlösung

- Die Systemintegrität wird durch Schadprogramme – Viren, Trojaner etc. – bedroht.

=> Berührt primär Allgemeininteresse an sicherer IT-Infrastruktur.

Erforderlichkeit hoheitlicher (regulatorischer) Maßnahmen?

- Geschäftsmodelle, die auf Mechanismen der digitalen Rechteverwaltung (Digital Rights Management, DRM) basieren, setzen ebenfalls einen bestimmten Systemzustand voraus, in dem die vorgesehenen Nutzungsbeschränkungen beachtet werden.

=> Berührt primär unternehmerisches Einzelinteresse an Erwerbsmöglichkeiten.

Koordinierung durch privatwirtschaftliche Maßnahmen?

Koordinative Standardisierung

Trusted Computing Platform Alliance

Januar 1999: Gründung der Trusted Computing Platform Alliance (TCPA) durch Compaq, Hewlett-Packard, IBM, Intel und Microsoft.

11.10.1999: Bekanntmachung eines ersten Spezifikationsentwurfs und Öffnung der TCPA für andere Unternehmen.

22.02.2002: Veröffentlichung von Version 1.1b der TCPA-Spezifikationen.

Anfang 2003: Die TCPA hat mehr als 200 Mitgliedsunternehmen.

Koordinative Standardisierung

Trusted Computing Group

08.04.2003: Gründung der TCPA-Nachfolgeorganisation Trusted Computing Group (TCG) durch AMD, Hewlett-Packard, IBM, Intel und Microsoft als nicht gewinnorientierte Gesellschaft nach dem Recht des US-Staates Oregon, Beitritt von zehn weiteren Unternehmen; u. a. Nokia, Philips, Sony und VeriSign.

02.10.2003: Version 1.2 der TCG-TPM-Spezifikationen wird veröffentlicht.

Heute: Die TCG hat 79 Mitgliedsunternehmen; besondere Arbeitsgruppen bereiten u. a. TCG-Spezifikationen für PDAs (Leitung: Sony) und Mobiltelefone (Leitung: Nokia) vor; mehrere Millionen TCG-konforme Rechnersysteme wurden bereits verkauft.

„TCG develops and promotes open industry standard specifications for trusted computing hardware building blocks and software interfaces across multiple platforms, including PC's, servers, ***PDA's, and digital phones.***"

<https://www.trustedcomputinggroup.org/home>

Technische Grundlagen

Zentrale Komponenten

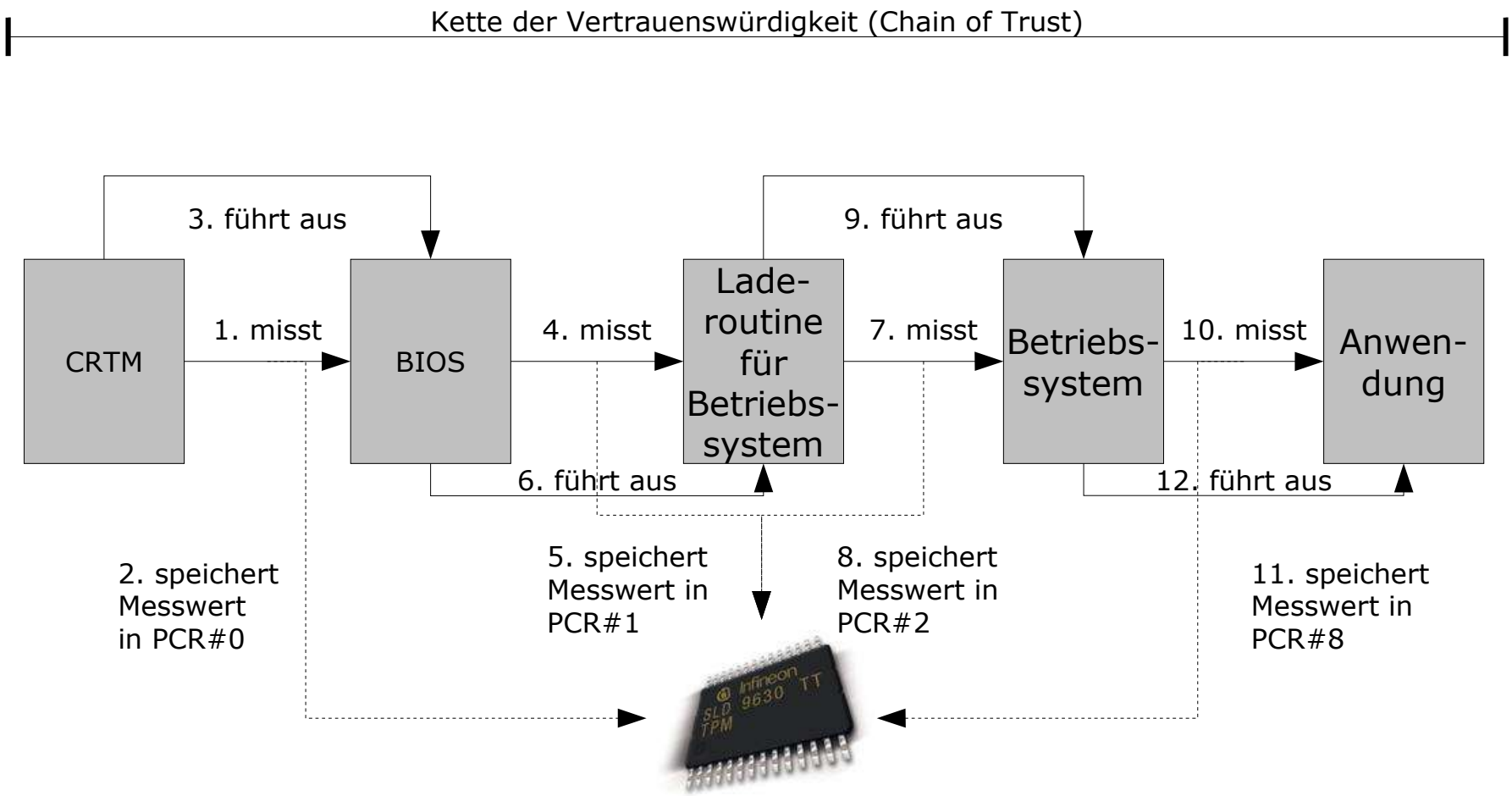
Trusted Platform Module (TPM): Ein Hardwaresicherheitsmodul, das fest an eine Rechnerplattform gebunden ist. Der TPM ist das „Herzstück" eines Trusted-Computing-Systems. Er verankert das auf Anwendungsebene in Anspruch genommene Vertrauen auf Hardware-ebene. Er erfüllt eine *Authentifizierungsfunktion* (Endorsement Keys, Attestation Identity Keys), eine *Kryptographiefunktion* (Erzeugung von Schlüsselhierarchien mit der Möglichkeit, Daten an einen Systemzustand zu binden) und eine *Integritätsmessungsfunktion* (Speicherung und Zurverfügungstellung von Informationen zum Systemzustand in Plattformkonfigurationsregistern, den PCRs).

Core Root of Trust for Measurement (CRTM): Die Software, die unmittelbar nach dem Systemstart (und damit dem üblichen BIOS vorgeschaltet) ausgeführt wird.

TCG Software Stack (TSS): Die Schnittstelle zwischen Software (Firmware, Betriebssystem, Anwendungen etc.) und dem TPM.

Technische Grundlagen

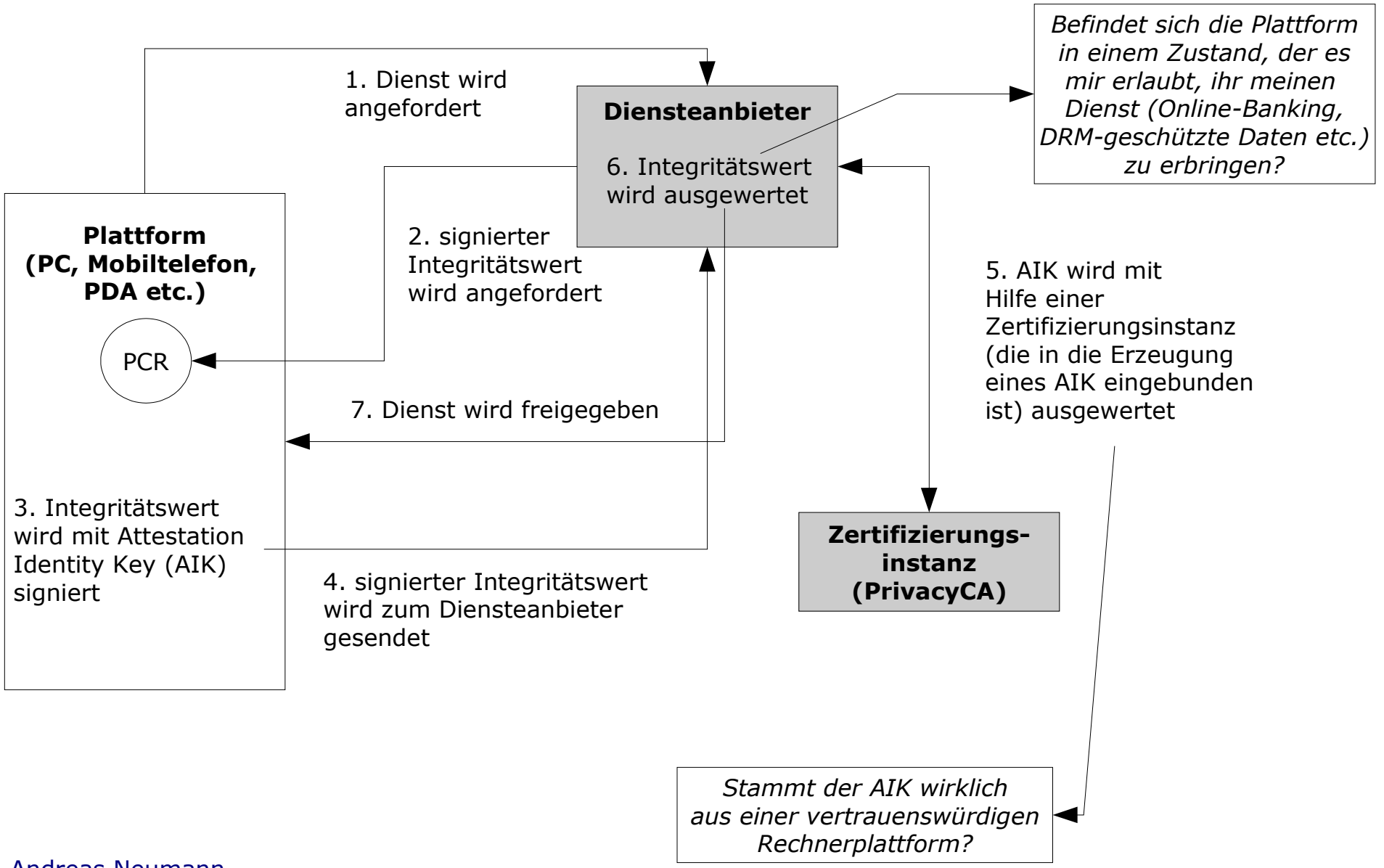
Integritätsmessung (Trusted Boot)



Quelle: Infineon Technologies AG
<http://www.infineon.com/cmc_upload/images/029/049/tpm_chip_2.jpg>

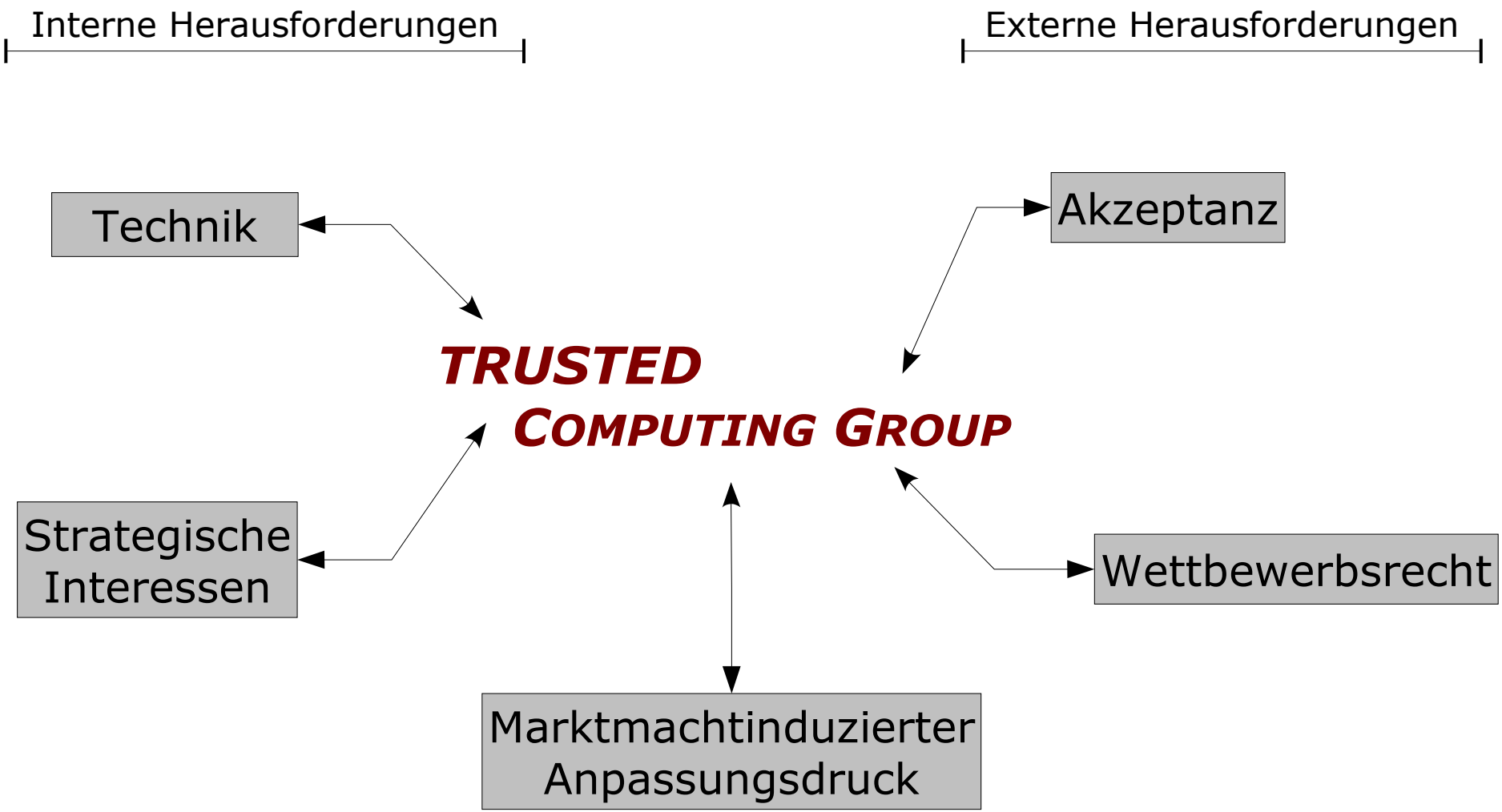
Technische Grundlagen

Plattformattestierung



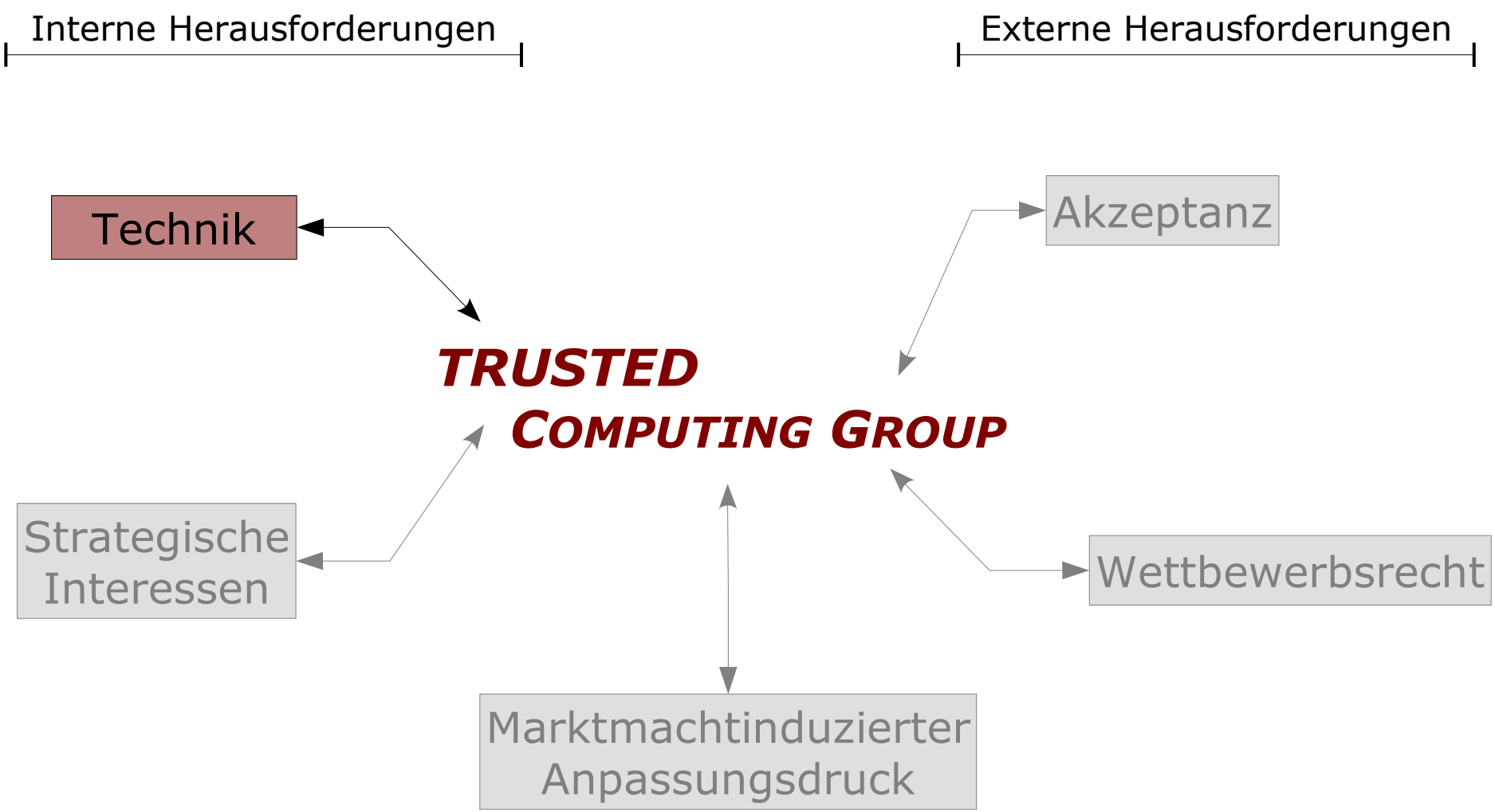
Herausforderungen

Übersicht



Herausforderungen

Technik



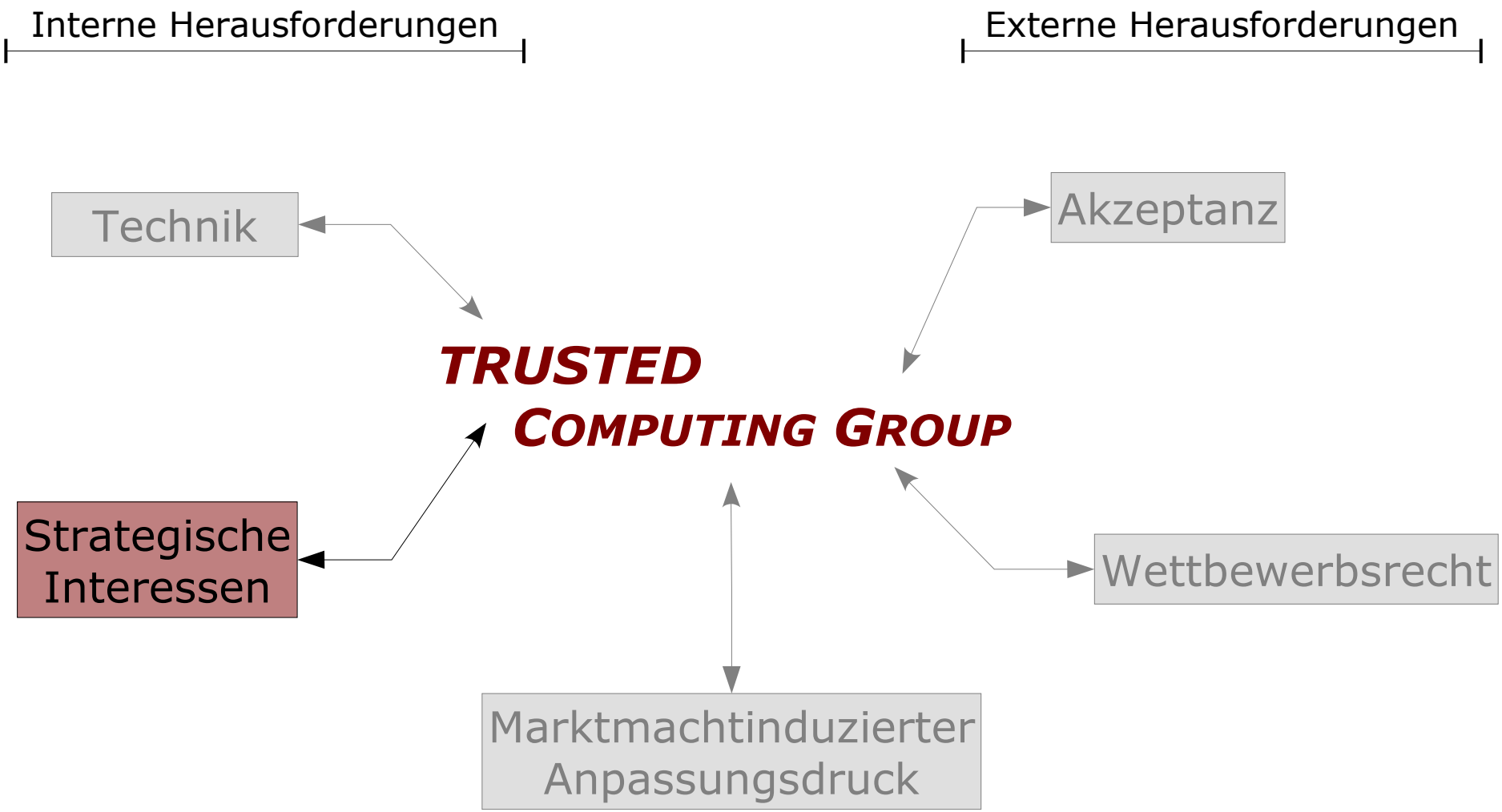
Herausforderungen

Technik

- Kontinuierliche Messung des Systemzustandes ist technisch sehr aufwendig.
  - Es werden Verfahren entwickelt, welche die manipulationssichere Messung des Systemzustandes auch zu einem beliebigen Zeitpunkt nach dem Systemstart erlauben.
- Vertrauenswürdige Systemumgebungen sind auf Software angewiesen.
  - Die Entwicklung einer „Killerapplikation“ steht noch aus.
  - Insbesondere fehlt ein „Trusted Computing“-Betriebssystem. Die Zukunft von Microsofts NGSCB ist unsicher, andere Lösungen (PERSEUS) bislang praktisch kaum relevant.

Herausforderungen

Strategische Interessen



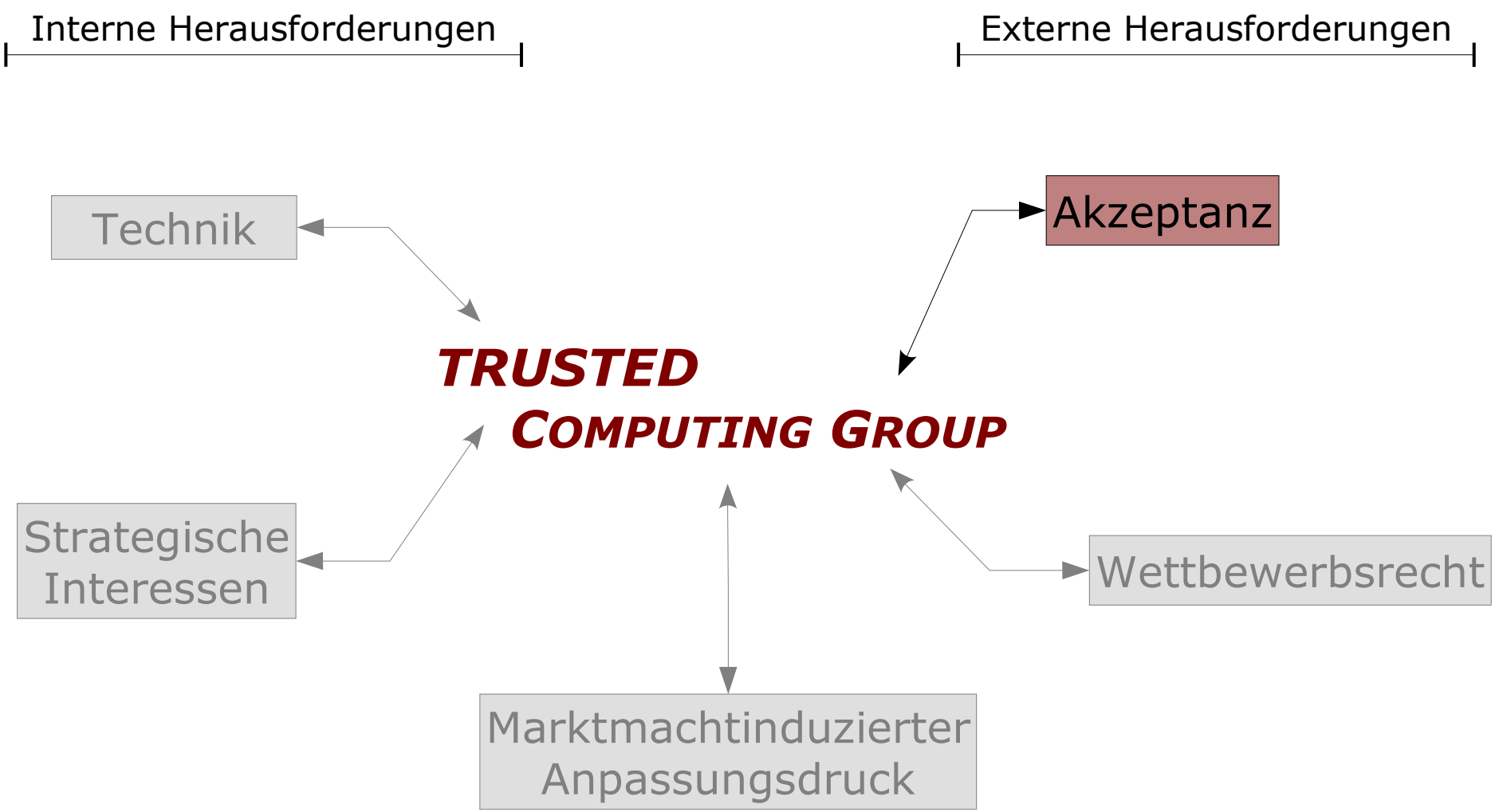
Herausforderungen

Strategische Interessen

- Manche Mitgliedsunternehmen stehen im Wettbewerb zueinander.
  - Diese Unternehmen haben Anreize, die Spezifikationen an ihren unternehmensspezifischen technischen Lösungen auszurichten, um wettbewerbliche Vorteile zu erlangen.
  - Verzögerung der Standardisierungsarbeit bzw. Entwicklung polymorpher Standards.
- Zur Implementierung bestimmter TCG-Spezifikationen ist der Rückgriff auf patentgeschützte technische Verfahren erforderlich.
  - Zwar besteht eine Selbstverpflichtung der TCG-Mitglieder, sich untereinander zur Implementierung der Spezifikationen benötigte Lizenzen einzuräumen (GSR-Politik), dies aber zu vernünftigen und nicht diskriminierenden Bedingungen (also entgeltlich).
  - Zusätzliches Interesse an einer Beeinflussung der Standardisierungsarbeit unter primär betriebswirtschaftlichen und nicht technischen Aspekten.

Herausforderungen

Akzeptanz



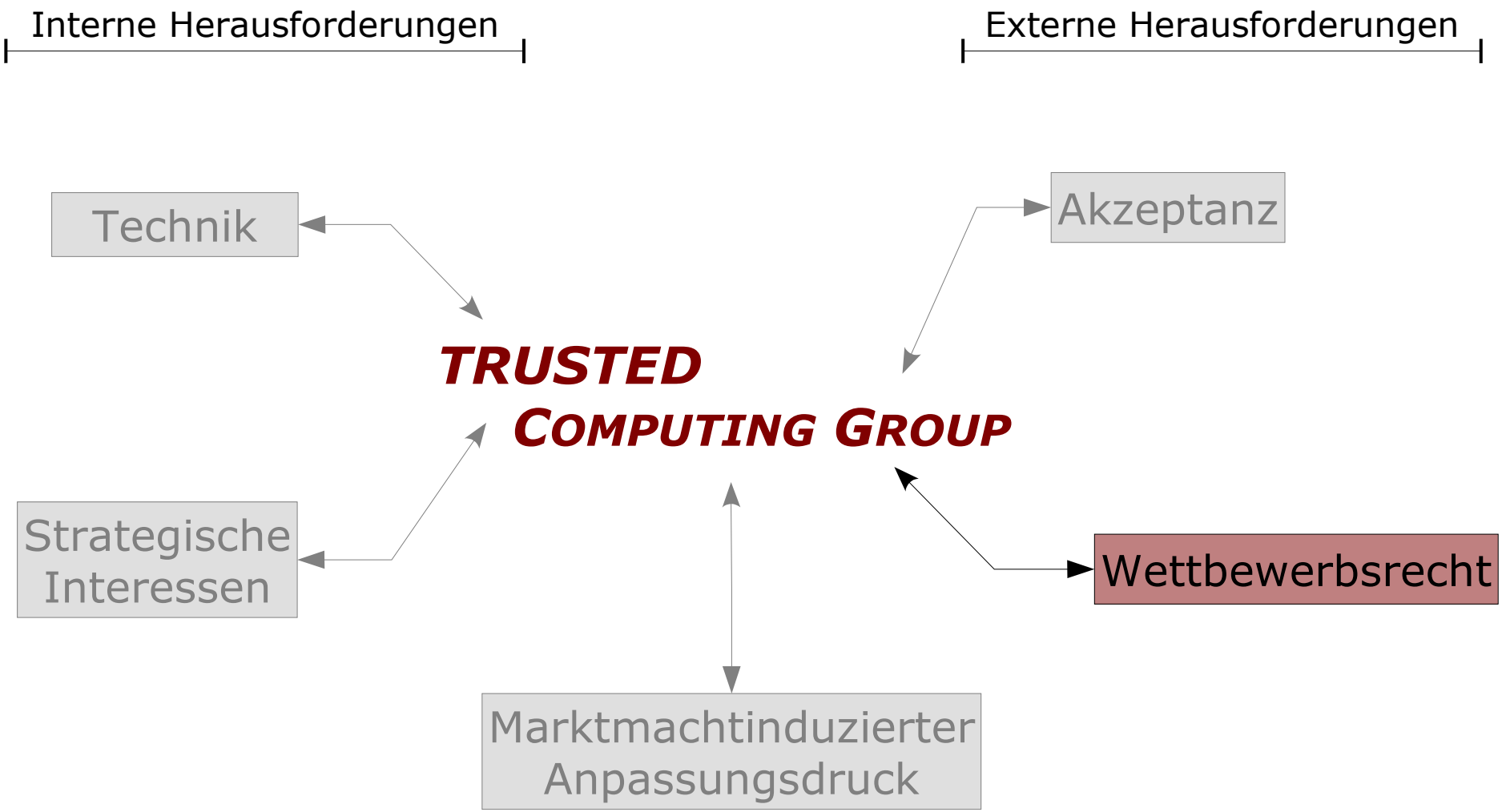
Herausforderungen

Akzeptanz

- Nach wie vor ist das Hauptanwendungsfeld von „Trusted Computing“ unklar.
  - Viel spricht dafür, dass die Industrie im Verbraucherbereich den Anwendungsschwerpunkt bei DRM-Geschäftsmodellen sieht (vgl. z. B. die Entwicklung sicherer Kommunikationspfade zu Ausgabemedien), so dass insoweit nachfragerseitig Unklarheit über den Nutzen der Technologie besteht (Recht auf Privatkopie? Kontrollverlust?).
  - Jedenfalls zunächst dürfte „Trusted Computing“ daher vor allem in Firmen- und Behördenlösungen zum Einsatz gelangen.
- Verbreitet bestehen auch datenschutzrechtliche Bedenken.
  - Die TCG hat den aktiven Dialog z. B. mit der Art. 29-Gruppe gesucht.
  - In Version 1.2 der TPM-Spezifikationen wurde die *Option* eines Verfahrens der direkten anonymen Bestätigung (Zero-Knowledge-Protokoll) vorgesehen.

Herausforderungen

Wettbewerbsrecht



Herausforderungen

Wettbewerbsrecht

- Die IT-Branche ist eine Netzwirtschaft.
  - Positive Netzexternalitäten – der Nutzen des Netzes wächst mit dem Anschluss eines neuen Teilnehmers auch für die bisherigen Teilnehmer – können zu einem Marktversagen in Form eines „Netzvorteils" führen.
  - Der Netzvorteil kann zu einer Markteintrittsbarriere werden – konkurrierende technische Lösungen müssen nicht nur „besser" sein als die etablierte Netztechnologie, sondern auch den Netzvorteil überwinden.
  - Wenn TCG-Kompatibilität zum faktischen Standard für Rechnerplattformen (ggf. beschränkt auf bestimmte Teilmärkte) werden sollte („Opt-in-Mythos"), kommt daher der Kontrolle über den Standard aus wettbewerblicher Sicht entscheidende Bedeutung zu.
  - Relevant sind somit vor allem die Bedingungen der Mitgliedschaft (Möglichkeit der Beeinflussung der Spezifikationen, des Erwerbs technischen Wissens und der früheren Berücksichtigung neuer Spezifikationen) und die Voraussetzungen für den Erwerb zur Implementierung benötigter Lizenzen.

Herausforderungen

Wettbewerbsrecht

- Art. 81 Abs. 1 EG verbietet kooperative Wettbewerbsbeschränkungen.
  - Die TCG-Mitgliedschaftsbedingungen nahmen bis vor kurzem keine Rücksicht auf wirtschaftliche Kenngrößen (Umsatz etc.) der Unternehmen.
  - Die Rechte der untersten Mitgliedskategorie (Adopter Members) sind im Wesentlichen auf eine Teilnahme an der GSR-Politik beschränkt.
  - Die Bedingungen der Mitgliedschaft beschränk(t)en damit tendenziell die Wettbewerbsmöglichkeiten kleiner und mittlerer Unternehmen.
  - Mittlerweile erlaubt die TCG Unternehmen mit weniger als 100 Beschäftigten die Mitgliedschaft als „Adopter Member" für $1.000 (statt $7.500). [Erfolg der wettbewerbspolitischen Diskussion(?)]

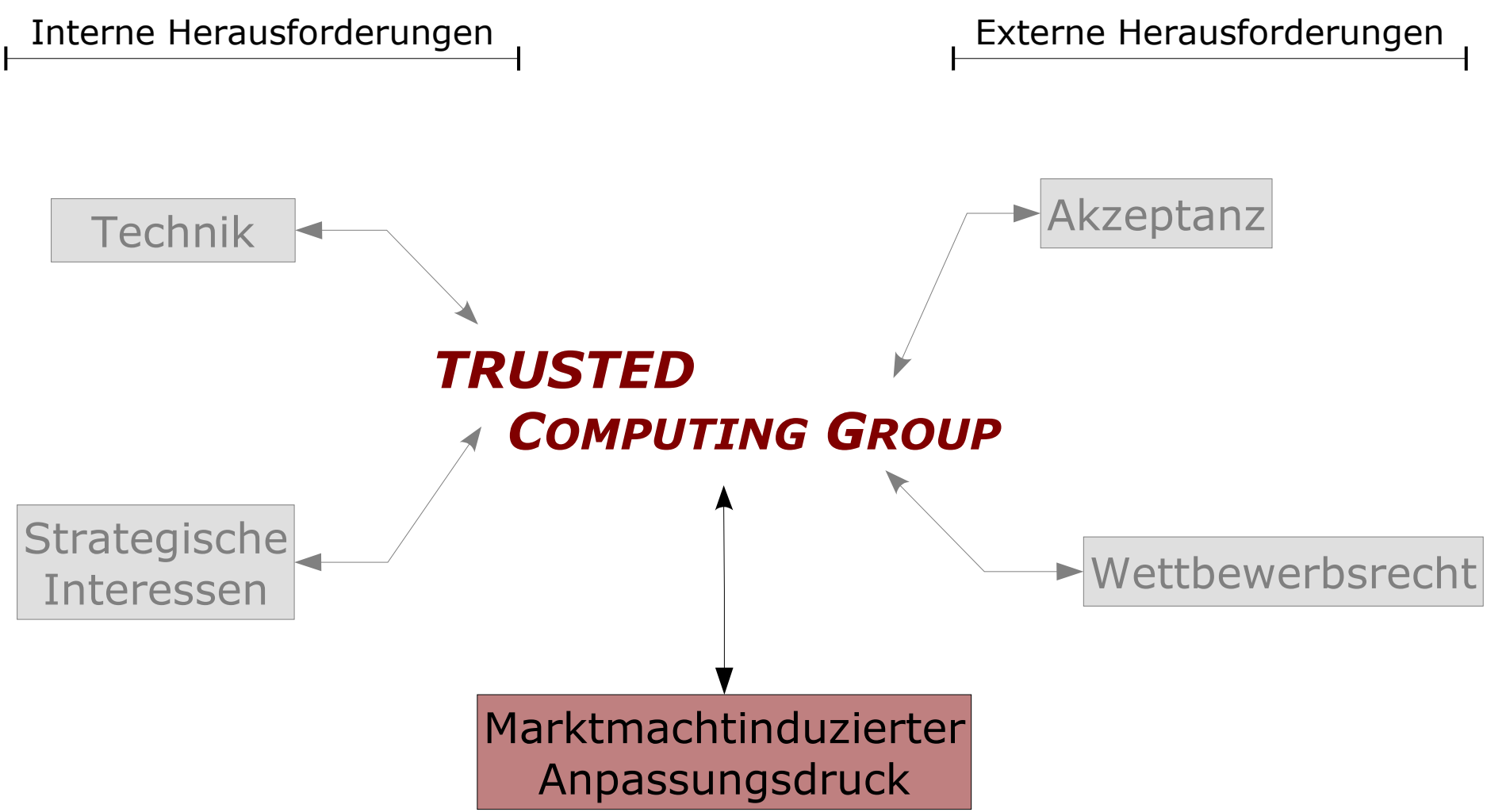
Herausforderungen

Wettbewerbsrecht

- Art. 81 Abs. 1 EG verbietet kooperative Wettbewerbsbeschränkungen (Fortsetzung).
  - Lizenznotwendigkeiten eröffnen eine weitere tendenzielle Beeinträchtigung der wettbewerblichen Möglichkeiten kleiner und mittlerer Unternehmen, da insoweit erhebliche Transaktionskosten entstehen. (Welche Patente bestehen? Zu welchen Konditionen können erforderliche Lizenzen erworben werden?)
  - Die Einrichtung eines Technologiepools könnte dieser strukturellen Benachteiligung entgegenwirken. (Dies entspricht einem Vorschlag der Bundesregierung; entsprechende Überlegungen seitens der TCG sind nicht bekannt.)
  - Es verbleibt ein erheblicher Wettbewerbsvorsprung der Gründungsunternehmen (auch bzgl. Patente).
  - Bei einem Verstoß gegen Art. 81 Abs. 1 EG besteht die Möglichkeit der Ausnahme nach Art. 81 Abs. 3 EG (Verbrauchernutzen?).

Herausforderungen

Marktmachtinduzierter Anpassungsdruck



Herausforderungen

Marktmachtinduzierter Anpassungsdruck

- Die praktische Relevanz von „Trusted Computing“ ist von der Verfügbarkeit entsprechender Software abhängig – insbesondere eines „Trusted Computing“-fähigen Betriebssystems.
- Faktisch ist die TCG daher jedenfalls im Massenmarkt auf eine Unterstützung durch Microsoft („Windows“) angewiesen.
- Microsoft ist Gründungsmitglied der TCG und eins von nur sieben Mitgliedern der „Promoter“-Stufe.
  - Microsoft konnte somit bereits grundlegende Weichenstellungen erheblich beeinflussen, obwohl die eigentliche Implementierung der TCG-Technologien in Hardwaremärkten erfolgt, und kann dies auch künftig.
- Bereits durch die Formulierung von Hardwareanforderungen einer „Trusted Computing“-Version von „Windows“ kann Microsoft entsprechenden Anpassungsdruck auf die TCG ausüben (vgl. NGSCB<->LaGrande).

Schluss

Fazit und Ausblick

- Die TCG sieht sich – mit noch offenen Erfolgsaussichten – zahlreichen internen und externen Herausforderungen gegenüber.
- Unklar ist zurzeit, ob eine Durchdringung bereits reifer Märkte glücken wird. Die Berücksichtigung TCG-konformer Systeme bei der (Massenmarkt-) Einführung neuer Technologien (UMTS, IT-Technologien für das vernetzte Auto etc.) erscheint insoweit potentiell erfolgsträchtiger.
- Die TCG könnte gleichermaßen zur Verbesserung der IT-Sicherheit beitragen wie auch neue Geschäftsmodelle (gerade auch für mobile Dienstleistungen) ermöglichen, auch wenn die private Regulierung (mit Blick auf den Nutzen für das Gemeinwohl) eher eine Nebenfolge der unternehmerischen Koordinierung ist.
- Ist TCG-Konformität erst einmal zu einem faktischen Standard geworden, verringern sich (faktisch) die Möglichkeiten (effizienter) hoheitlicher Regulierung. Daher ist *jetzt* auf die TCG einzuwirken.

Vielen Dank für Ihre Aufmerksamkeit!

Für weitere Informationen:

Andreas Neumann
Zentrum für Europäische Integrationsforschung
Abteilung A
Walter-Flex-Straße 3
53113 Bonn
Tel.: 02 28 / 73 49 33; Fax: 02 28 / 73 18 93
E-Mail: an@andreasneumann.de
WWW: http://www.andreasneumann.de; http://www.tkrecht.de

Schluss

Weiterführende Informationen

- Datenschutz und Datensicherheit, Heft 9/2004 (mit Beiträgen von *Brandl/Rosteck, Hansen, Koenig/Neumann, Kuhlmann, Kursawe, Sadeghi/Stüble/Pohlmann, Sailer/van Doorn/Ward, Sandl* und *Schallbruch*)
- *Koenig/Neumann/Katzschmann* (Hrsg.), Trusted Computing – Technik, Recht und gesellschaftspolitische Implikationen vertrauenswürdiger Systemumgebungen, 2004 (mit Beiträgen von *Bechtold, Grassmuck, Günnewig/Rannenberg/Sadeghi/Stüble, Koenig/Neumann, Kuhlmann, Kursawe, Pfitzner* und *Weis*)

- <http://cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml>