

Zur Problematik der Existenz mehrerer heterogener Trust-Service-Infrastrukturen

Philip Tauschek*

Bei der Abgabe optimistischer Wachstumsprognosen bzgl. des Markts für Trustcenter-Leistungen wird die Problematik der Existenz mehrerer heterogener Trust-Service-Infrastrukturen (TSI) verkannt. Sie führt zur Verunsicherung der Teilnehmer und erschwert das für Systemgüter so wichtige Erreichen der kritischen Masse. Es ist zu erwarten, dass die Heterogenität

der TSI auch in Zukunft erhalten bleibt und daher mit einem schnellen durchschlagenden Erfolg der Trustcenter-Branche nicht zu rechnen ist.

1 Einleitung

Bei TSI handelt es sich um Systemgüter. Bei solchen ist das Erreichen der so genannten kritischen Masse von hoher Relevanz. Unter der kritischen Masse versteht man die Mindestanzahl der über eine Systemtechnologie zusammengebundenen Nutzerschaft, die überschritten werden muss, bevor ein nachhaltiger und ausreichender Nutzen zur Gewinnung weiterer Adopter aus dem System heraus selbst entwickelt werden kann [Schoder 1995]. Das nicht zeitnahe Erreichen der kritischen Masse kann zu negativen Rückkopplungseffekten führen, die sich darin äußern, dass nur wenige Akteure das Systemgut nutzen und somit seine Attraktivität weder ausreicht, neue Teilnehmer zu gewinnen, noch die bestehenden Teilnehmer zu halten. Existieren mehrere heterogene, um Teilnehmer konkurrierende TSI nebeneinander, so erschwert dies das Erreichen der kritischen Masse für jede einzelne der TSI. Es wird hier die These aufgestellt, dass auch in Zukunft eine Vielzahl unterschiedlicher TSI nebeneinander existieren werden. In Hinblick

auf die Problematik des Erreichens der kritischen Masse bleibt das Engagement im Trustcenter-Geschäft somit ein riskantes Spiel. Die Gründe für die aufgestellte These werden im Folgenden erläutert.

2 Unterschiedliche Rechtssysteme und politische Interessen

Die unterschiedlichen Rechtssysteme und politischen Interessen einzelner Länder sind nur schwer miteinander zu vereinbaren [vgl. Bizer 1998; ICC 1997]. Wenn eine Einigung überhaupt erfolgt, dann nur über das Zulassen von etlichen Ausnahme- und Sonderregelungen, wie die EU-Signaturrechtlinie zeigt. Sie schafft als Kompromissformel eine Regelungsvielfalt, auf deren Grundlage eine Vielzahl EU-signaturrechtlinienkonformer, aber untereinander unverträglicher Zertifizierungssysteme in Europa möglich sind [vgl. Welsch/Bremer 2000]. Entsprechend pessimistisch sind Hoffnungen auf einheitliche Rege-

*Institut für Bankinformatik und Bankstrategie
an der Universität Regensburg
[philip.tauschek@wiwi.uni-regensburg.de]

lungen im Hinblick auf die gegenseitige rechtliche Anerkennung digitaler Signaturen zwischen EU- und Nicht-EU-Staaten zu bewerten.

Insbesondere ist problematisch, dass TSI-Technologien nicht überall in Europa und weltweit der gleiche Stellenwert zugemessen wird [vgl. Servida 1998], d.h. einige Länder sind hinsichtlich der Findung eines Konsens nur wenig motiviert.

3 Normungsprozesse überdauern die Aktualität der Technik

Die Konformität von TSI zu bestimmten rechtlichen Rahmenwerken wie das deutsche Signaturgesetz oder die EU-Signaturrichtlinie impliziert keineswegs einheitliche technische Eigenschaften. Letztere müssen vielmehr durch technische Normungsprozesse erzielt werden. Diese sind jedoch bereits auf nationaler Ebene sehr langwierig. Zum einen konkurrieren häufig die einzelnen Aktivitäten miteinander und werden nicht zielgerichtet koordiniert, zum anderen zeigen viele betroffene Unternehmen und Einrichtungen eine abwartende Haltung und sind oft nicht zum Einsatz eigener Ressourcen bereit [vgl. Bahnke 1999]. Nachdem die nationalen Normungsorganisationen die inländischen Aktivitäten und Positionen gebündelt haben, bringen sie diese in internationale Normungsprozesse ein. Die lange Dauer des Abgleichs der eingebrachten Arbeiten steht in einem drastischen Widerspruch zu den immer kürzer werdenden Innovationszyklen der Technik [vgl. Bahnke 1999]. Internationale Normen sind folglich bei ihrer Verabschiedung aus technischer Sicht oft schon wieder veraltet, was dazu führt, dass viele Unternehmen auf aktuelle nationale Normen zurückgreifen.

4 Integrierbarkeit der Trustcenter-Leistungen in die Anwendungen

Unterschiedliche Anwendungen stellen unterschiedliche Anforderungen an die TSI. Soll z.B. eine Person aus einem Beglaubigungsträger bestimmte Angaben direkt entnehmen, so müssen die Daten in einer für Menschen interpretierbaren Form vorliegen [vgl. BSI-Sigl-A1 1999]. Ganz andere Bedingungen sind gegeben, wenn die Auswertung der Beglaubigungsträger ausschließlich von Maschinen erfolgen soll. Der Erfolg einer TSI-Anwendung hängt entscheidend davon ab, wie gut sich die bereitgestellten Basis- und Zusatzleistungen in sie integrieren lassen. Entsprechend muss die Konzentration auf bestimmte konkrete Anwendungen bereits maßgeblich in der Policy verankert sein [vgl. Keus 2000]. In diesem Zusammenhang stellt Welsch [1999] fest: „Es ist zu bezweifeln, ob es gelingen wird, eine einheitliche Sicherungsinfrastruktur für verschiedene Anwendungen aufzubauen. [...] Die Infrastruktur müsste die Authentifizierung von Maschinen und Diensten, die Authentifizierung und Integritätssicherung von Dokumenten und schließlich die Authentifizierung der digitalen Identität von Personen zulassen.“

5 Verwendung unterschiedlicher Sicherheitsstufen

Die derzeit am Markt existierenden TSI weisen sehr unterschiedliche Sicherheitsniveaus auf. Aus mehreren Gründen macht die Beibehaltung dieser Verschiedenartigkeit durchaus Sinn, was einer Vereinheitlichung von TSI entgegensteht.

Der Einsatz von Trustcenter-Leistungen steht im Spannungsverhältnis des gebotenen Mehrwerts, des in sie gesetzten Vertrauens und der Kosten. Nur bei einem aus Sicht der Anwender günstigen Verhältnis dieser Faktoren werden diese die neuen Technologien benutzen. Durch die Möglichkeit, auf unterschiedliche Sicherheitsstufen zurückgreifen zu können, kann je nach Anwendung eine Anpassung an das tatsächliche Gefähr-

dungspotenzial erfolgen und eine praktikable Lösung gefunden werden, welche die Kernanforderungen „einfache Bedienbarkeit“, „Implementierbarkeit“, „ausreichendes Sicherheitsniveau“ und „vernünftige Kosten“ weitgehend erfüllt. Bislang hat sich eine solche pragmatische Vorgehensweise bei der Einführung von neuen Technologien bewährt [vgl. Welsch 1999; Lacoste/Weber 1999].

Ein weiterer Vorteil unterschiedlicher Sicherheitsstufen liegt in der durch sie gegebenen Möglichkeit zur geeigneten Realisierung der Warnfunktion einer Unterschriftgabe. Wenn heute jemand sagt „Bitte unterschreiben Sie hier“, dann wird durch die Art der zu leistenden Unterschrift keine Aussage über das Gewicht der mit der Unterzeichnung verbundenen Folgen gemacht. Unter den freundschaftlichen Brief an einen Schulfreund wird die gleiche handschriftliche Unterschrift gesetzt wie unter den Kaufvertrag eines Kraftfahrzeugs. Diesbezüglich entsteht bei dem Ersatz der handschriftlichen Unterschrift durch die digitale Signatur die Möglichkeit zur Differenzierung. Wird bei einem bestimmten Vorgang vom Anwender wegen rechtlicher Anforderungen die Erstellung einer digitalen Signatur mit einer sehr hohen Sicherheitsstufe verlangt, so erfolgt hierdurch implizit die Aussprache einer Warnung.

6 Probleme bei der Modifikation des Leistungsangebots

Die Modifikation des Leistungsangebots eines Trustcenters kann sich als schwierig erweisen, da solche Maßnahmen oft zu sicherheitsrelevanten Änderungen führen. Bspw. kann es erforderlich sein, dass neue Prozesse in bereits bestehende Abläufe integriert werden müssen und die Einbindung zusätzlicher technischer Komponenten notwendig ist [vgl. Keus 2000]. Derartige Änderungen führen leicht zur Notwendigkeit der erneuten Definition und Umsetzung des Sicherheitskonzepts. Ggf. muss auch eine erneute externe Akkreditierung erfolgen. In diesem Zusam-

menhang haben Trustcenter leidvolle Erfahrungen machen müssen, die zunächst nicht zu dem deutschen Signaturgesetz von 1997 konforme Trustcenter-Leistungen erstellt haben und später derartige Dienste anbieten wollten [vgl. Keus 2000].

Aus diesen Problemen bzgl. der Modifikation des Leistungsangebots resultiert eine gewisse Trägheit der Trustcenter, die einer Vereinheitlichung von TSI im Wege steht.

7 Fazit

Es wurde dargelegt, dass mit großer Wahrscheinlichkeit auch in Zukunft eine Vielzahl unterschiedlicher TSI nebeneinander existieren werden. Zum einen konkurrieren somit mehrere TSI um Teilnehmer, zum anderen führt die Heterogenität der TSI zur Verunsicherung potenzieller Anwender. Entsprechend bleibt es schwierig, für einzelne TSI eine kritische Masse an Teilnehmern zu erzielen. Ein Engagement am Trustcenter-Markt ist daher mit hohen Risiken verbunden. Allzu optimistische Wachstumsprognosen sind mit Vorsicht zu genießen.

Literaturverzeichnis

Bahnke, T. (1999): Begrüßung und Eröffnung. In: Beiträge des DIN-Workshops „Branchenübergreifende digitale Identität“, Tagungsband zum Workshop vom 04.-05.05.1999 in Berlin, S. 1f.

Bizer, J. (1998): Das deutsche Signaturgesetz. In: Digitale Signaturen: Ihre Rolle im Rechts- und Geschäftsverkehr. Tagungsband Deutsch-Japanischer Workshop vom 10.-11.09.1998 in Darmstadt, Deutsch-Japanischer Kooperationsrat für Hochtechnologie und Umwelttechnik, S. 100ff.

BSI (1999): Spezifikation für die Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV: Abschnitt A1 Zertifikate. Version 4.0.

ICC (1997): General Usage in International Digitally Ensured Commerce (GUIDEC).
<http://www.iccwbo.org/home/guidec/guidec.asp>.
Abruf am 18.04.2000.

Keus, K. (2000): Maßenwendungen für elektronische Unterschriften im Kontext nationaler und europäischer Anforderungen. In: Der Weg zur sicheren Informationstechnik: Aktuelle Beispiele, BSI, S. 77ff.

Lacoste, G./Weber, A. (1999): Gestaltung und Nutzen einer Sicherheitsinfrastruktur für globalen elektronischen Handel. In: Horster, P. (Hrsg.): Sicherheitsinfrastrukturen: Grundlagen, Realisierungen, rechtliche Aspekte, Anwendungen. Vieweg.

Schoder, D. (2000): Diffusion von Netzeffektgütern. In: Marketing ZFP, Nr. 1, Band 17, S. 18ff.

Servida, A. (1998): Digital Signature: Inventory of International Regulatory, Standardisation and Commercial Activities. Europäische Kommission.

Welsch, G. (1999): Stufenweise skalierbare Sicherheit für digitale Signaturen. In: Beiträge des DIN-Workshops „Branchenübergreifende digitale Identität“, Tagungsband zum Workshop vom 04.-05.05.1999 in Berlin, S. (3.2-1)ff.

Welsch, G./Bremer, K. (2000): Die europäische Signaturrichtlinie in der Praxis. In: DuD, Nr. 2, S. 85ff.

**Neues Buch in der Reihe
Bankinformatik-Studien:
Trust-Service-Infrastrukturen**

Autor: Dr. Philip Tauschek
Erscheinungsdatum: Mai 2002/Physica-Verlag

Nähere Informationen erhalten Sie:
Institut für Bankinformatik
und Bankstrategie an der
Universität Regensburg
D - 93040 Regensburg
Tel +49 (0)9 41/9 43-19 21
(Frau Andrea Rosenlehner)
Fax +49 (0)9 41/9 43-18 88