TELETRUST Deutschland e. V.
Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
www.teletrust.de

24.04.2006

TeleTrusT-Vorschläge zum weiteren Vorgehen nach dem BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT Bericht über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 15.03.2006

Zielstellung der EG-Signaturrichtlinie 1999/93/EG

Sie wird deutlich in den der Richtlinie vorangestellten Erwägungsgründen

(4) Elektronische Kommunikation und elektronischer Geschäftsverkehr erfordern „elektronische Signaturen“ und entsprechende Authentifizierungsdienste für Daten. Divergierende Regeln über die rechtliche Anerkennung elektronischer Signaturen und die Akkreditierung von Zertifizierungsdiensteanbietern in den Mitgliedstaaten können ein ernsthaftes Hindernis für die elektronische Kommunikation und den elektronischen Geschäftsverkehr darstellen. Klare gemeinschaftliche Rahmenbedingungen für elektronische Signaturen stärken demgegenüber das Vertrauen und die allgemeine Akzeptanz hinsichtlich der neuen Technologien. Die Rechtsvorschriften der Mitgliedstaaten sollten den freien Waren und Dienstleistungsverkehr im Binnenmarkt nicht behindern.

(5) Die Interoperabilität von Produkten für elektronische Signaturen sollte gefördert werden. …

(8) Die rasche technologische Entwicklung und der globale Charakter des Internet erfordern ein Konzept, das verschiedenen Technologien und Dienstleistungen im Bereich der elektronischen Authentifizierung offensteht.

und Artikel 1, Abs.1 der Richtlinie:

„Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung beitragen. Sie legt rechtliche Rahmenbedingungen für elektronische Signaturen und für bestimmte Zertifizierungsdienste fest, damit das reibungslose Funktionieren des Binnenmarktes gewährleistet ist.“

1. Die EU-Richtlinie 1999/93/EG ist teilweise erfolgreich, sie hat ihr Ziel jedoch in wesentlichen Teilen verfehlt.

Grundlegendendes Ziel der Richtlinie 1999/93/EG war es, einen „Gemeinschaftsrahmen für die Verwendung elektronischer Signaturen“ zur allseitigen Nutzung zu schaffen, um eine Störung des europäischen Binnenmarktes im Bereich elektronischer Transaktionen zu verhindern.
Die grundsätzliche rechtliche Anerkennung elektronischer Signaturen ist in Europa (so auch in Deutschland) inzwischen weitgehend gegeben; das ist ein Erfolg.
Die nationalen Interpretationen und - darauf folgend - die spezifischen nationalen Regulierungen von Details „hochsicherer“ (qualifizierter) elektronischer Signaturen zeigen jedoch Unterschiede, die einen „Gemeinschaftsrahmen“ nicht haben entstehen lassen.
Insbesondere die qualifizierten elektronischen Signaturen (qElSig) führen nach über sechs Jahren seit Inkrafttreten der Signaturrichtlinie in Europa noch immer ein Schattendasein.

2. Vorauseilende Technikregulierung durch reale Anwendungsbezogenheit korrigieren – für innovative Entwicklungen.

TeleTrusT war bereits 1996/97 an der Entwicklung des ersten deutschen SigG (als Teil des IuKDG) beteiligt. Bereits vorher lagen Erfahrungen aus der Implementierung von PKI zunächst für E-Mail-Sicherheit vor. Von Anfang an hat TeleTrusT die Bemühungen um eine EU-weite Regulierung unterstützt. Dabei sollten ausschließlich Rahmenbedingungen für Trusted Third Parties, die öffentlich Zertifizierungsdienste anbieten, betroffen sein.
Die strenge einschränkende Orientierung der ersten deutschen Signaturgesetzgebung auf die Schriftform wurde von der Bundesnotarkammer eingebracht. Hinsichtlich der Interoperabilität von Angeboten wurden in Deutschland keine Anforderungen formuliert. Als Ergebnis der Umsetzung des ersten deutschen Signaturgesetzes von 1997 waren proprietäre Lösungen der Anbieter entstanden und - daraus resultierend - eine massive Abschreckung für die ohnehin mühsam zu überzeugenden Anwender.
TeleTrusT begrüßt ausdrücklich, dass die Europäische Kommission nunmehr „angesichts der Schwierigkeiten der gegenseitigen Anerkennung elektronischer Signaturen und der Interoperabilität“ den lange überfälligen Kontakt zu den Mitgliedsstaaten suchen wird, um Fragen zu folgenden Themen zu erörtern:

- unterschiedliche Umsetzung der Richtlinie;
- Klärung einzelner Artikel der Richtlinie;
- technische und Normungsaspekte;
- Probleme der Interoperabilität.

Hierin liegt die Chance für Deutschland, längst erkannte Diskrepanzen zwischen aus der Theorie definierten technischen und juristischen Rahmenbedingungen und praktischen Notwendigkeiten

bei der deutschen Umsetzung der Richtlinie 1999/93/EG abzubauen. Eine erfolgreiche Vorgehensweise kann darin bestehen, modifizierte Wirkbereiche der Richtlinie anzustreben, wie etwa:

- Die eindeutige Berücksichtigung der Juristischen Person und
- Die Orientierung auf Webservices und Identitäten von technischen Komponenten (Hard- und Software).

Der elektronische Rechtsverkehr zwischen natürlichen Personen mit dem Äquivalent zur Handunterschrift wird ein kleiner Bereich innerhalb der zukünftig benötigten PKI-Dienste bleiben.

3. Interoperabilität von Technik, Software und Diensten (inkl. deren Sicherheitsfunktionen) bringt Akzeptanz beim Anwender

In dem Bericht zur Anwendung der Richtlinie 1999/93/EG wird die Vermutung geäußert, dass eine Ursache für den nicht stärkeren Verbreitungsgrad fortgeschrittener Signaturen (inkl. qElSig, die als Teilmenge dazu gehören) in elektronischen Anwendungen am Markt „die fehlende technische Interoperabilität auf nationaler und grenzüberschreitender Ebene“ sein könnte, insbesondere hinsichtlich des Umstandes, dass man denen eine anwendungsübergreifende Verwendbarkeit zutraut.

Im gleichen Absatz wird auf die Schaffung von Interoperabilitätsnormen durch die EESSI (Europäische Initiative zur Normung elektronischer Signaturen) und vielfältige nationale Aktivitäten hingewiesen. Die ins Leben gerufenen Aktivitäten von CEN und ETSI haben viele neue Standards entstehen lassen, aber keine Wirkung bezüglich europäisch interoperabler Dienste oder Anwendungen gezeigt. Dagegen ist ISIS-MTT ein allgemein verfügbares Ergebnis der Profilierung internationaler Standards. Das Profil entstand auf Grundlage der langjährigen Erfahrungen von TeleTrusT bei der Implementierung von PKI-gestützten Anwendungen.

Bereits seit 1994/95 wurden von TeleTrusT die IETF-Standards PEM und S/MIME sowie X.509 profiliert, um die funktionale Interoperabilität von Produkten und Diensten zu erreichen. Mit **MailTrusT** hat TeleTrusT eine Spezifikation entwickelt, auf deren Basis der Aufbau von interoperablen PKI-orientierten Behörden- und Unternehmenslösungen in Deutschland möglich wurde. Das Konzept ist bis heute stabil und liegt dem erfolgreichen Netzwerk der **European Bridge-CA** zugrunde. Es leistet mit mehr als 600.000 Zertifikaten einen bedeutenden Beitrag zur Transaktionssicherheit zwischen Unternehmen, Banken und Behörden durch Anwendung von Chipkarten als Sicherheitstoken und digitalen Signaturen.

Um mit der Entwicklung und Anwendung von elektronischen Geschäftsprozessen Schritt zu halten und die Einheit von zertifikatsgestützten Anwendungen für Identifikation, Authentifizierung und Signaturen zu stärken, hat TeleTrusT gemeinsam mit T7 „**ISIS-MTT**“ entwickelt. ISIS-MTT ist ein Profil internationaler Standards – insbesondere auch von CEN und ETSI. Das ISIS-MTT-Konzept

ist mehrfach den ausgewiesenen Experten von ETSI zur Kritik vorgestellt worden. Alle Spezifikationen und auch das ISIS-MTT-Testbed sind öffentlich verfügbar und können kostenfrei benutzt werden. Eine Reihe von internationalen Anbietern hat bereits das ISIS-MTT-Konformitätssiegel erlangt.

TeleTrusT bietet den einschlägigen europäischen Gremien **sein Know-How an**, um Qualifizierte Elektronische Signaturen und die Zertifikate anderer Anwendungen mit dem Testbed auf Konformität zu testen. Nach unserer Überzeugung wird sich bestätigen, dass ISIS-MTT die relevanten internationalen Standards zuverlässig abbildet und interoperable Authentifizierungs- und Signaturfunktionen gewährleistet.

4. Die Richtlinie hat die Differenzierung von nationalen Sichtweisen gestärkt

Bei der Umsetzung der Richtlinie 1999/93/EG bis 2001 kamen unterschiedliche nationale Maßstäbe zum Tragen. Die in der Signaturrichtlinie vorhandenen Spielräume wurden dahingehend genutzt, auch die bis dahin vorhandenen deutschen Regelungen möglichst unverändert bestehen zu lassen. Ein typisches Beispiel hierfür ist die deutsche Entsprechung des unter 2.3.2. des Berichts definierten „Unterzeichners“ (im deutschen SigG: „Signaturschlüsselinhaber“):

> „ „Unterzeichner“ im Sinne der Richtlinie ist „eine Person, die eine Signaturerstellungseinheit besitzt und die entweder im eigenen Namen oder im Namen der von ihr vertretenen Stelle oder juristischen oder natürlichen Person handelt“. Obwohl die Richtlinie nicht feststellt, dass sich die elektronische Signatur auf eine natürliche Person beziehen muss, kann der Unterzeichner einer qualifizierten elektronischen Signatur (Artikel 5 Absatz 1 der Richtlinie) nur eine natürliche Person sein, da diese Form der Unterschrift als einer handschriftlichen Unterschrift gleichwertig gilt(7)“.

Die Theorie, dass es sich beim Unterzeichner nur um eine natürliche Person handeln könne, wird in der Fußnote (7) des Berichts

> „Die Beschränkung der Verwendung fortgeschrittener elektronischer Signaturen auf natürliche Personen zeigt, dass zahlreiche Regulierungsbehörden elektronische Signaturen lediglich als elektronische Äquivalente herkömmlicher handschriftlicher Unterschriften ansehen. Doch werden digitale Signaturen meist ausschließlich zur Verstärkung der Authentizität und Integrität einer Nachricht benutzt, ohne das Ziel oder die Absicht, im herkömmlichen Sinne zu unterschreiben. Darauf hat bei der formlosen Konsultation etwa auch der Internationale Strafgerichtshof hingewiesen.“

durch die Praxis widerlegt. Nicht die Willenserklärung des signierenden Menschen ist hinsichtlich der Anwendungshäufigkeit bei elektronischen Kommunikationen und Transaktionen signifikant sondern die Authentizität und Integrität der elektronisch übermittelten oder gespeicherten Daten. Bedingt durch die einseitige Zweck-Orientierung elektronischer Signaturen auf „Willenserklärungen natürlicher Personen“ sowie einen bilateralen elektronischen Rechtsverkehr

zwischen natürlichen Personen (Ende-zu-Ende), haben auch in Deutschland die umfangreiche Regulierung sowie deren juristische Interpretation und die daraus entwickelten Anforderungen zu einer völlig starren Angebotsstruktur geführt. Typisch sind dabei u.a. lange Entwicklungszeiten, hohe Kosten und die Vorstellung, die Anwendungen hätten sich an die angebotenen Signaturfunktionalitäten anzupassen und nicht umgekehrt. Die willkürlichen Vorgaben für die Technologie sowie ihre rechtlich-organisatorische und arbeitsteilige Umsetzung erfolgten ohne Verifizierung durch Markt und Wettbewerb. Dieses Missverhältnis spiegelt sich auch im vorliegenden Bericht der Europäischen Kommission wider.

TeleTrusT warnt ausdrücklich vor einer Erweiterung dieser Vorgehensweise in Richtung der Schaffung von neuen Betätigungsfeldern für Juristen, z. B. durch Regulierung von Diensten zur Prüfung elektronischer Signaturen!

5. Wirkung der EU-Richtlinie auf andere Rechtsvorschriften

Unter 4. in dem Bericht werden Auswirkungen der Richtlinie auf andere Rechtsvorschriften beschrieben, unter 4.1. insbesondere auf die EU-Richtlinie 2001/115/EG (vom 20.12.01 … mit dem Ziel der Vereinfachung, Modernisierung und Harmonisierung der mehrwertsteuerlichen Anforderungen an die Rechnungstellung).

In 4.1., Absatz 2 heißt es:

> „… gemäß der Richtlinie dürfen die Mitgliedstaaten die Unterzeichnung von Rechnungen nicht vorschreiben. …“

Die Spielräume der Formulierungen in der Richtlinie 2001/115/EG wurde von den Mitgliedsstaaten sehr unterschiedlich genutzt. Entsprechend groß ist die Bandbreite der nationalen Anforderungen an die geforderten Qualitäten für Authentizität und Integrität von elektronischen Rechnungen.

6. Vom Kopf auf die Füße

Das unter 5. beschriebene Beispiel beschreibt deutlich, unter welcher Sichtweise die nationalen Umsetzungen der Richtlinie 1999/93/EG vorgenommen wurde – nämlich jeweils nach innen gekehrt!

Entscheidend für den Erfolg der Richtlinie ist jedoch das Umgekehrte – die Gestaltung nationaler Rahmenbedingungen bei allen europäischen Partnern, die die Kommunikations- und Transaktionssysteme über Staatsgrenzen hinweg für alle potentiellen Teilnehmer öffnet, also auch auf die Interoperabilität mit Lösungen ausländischer Anbieter abgestellt ist.

7. „Signatur sucht Anwendung“ ist keine zielführende Strategie

In dem Bericht zur Anwendung von 1999/93/EG wird deutlich gemacht, dass elektronische Signaturen seit 1999 durchaus in vielen Anwendungen (insbesondere Transaktionsanwendungen) am Markt eingesetzt werden. Relativ selten stützen sich die Signaturen dabei jedoch auf PKI-

Dienste (fortgeschrittene Signaturen) und noch seltener wurden durch die PKI-Dienste dafür qualifizierte Zertifikate ausgestellt (qElSig).

Als weitere Ursache für die nur schwache Verbreitung elektronischer Signaturen sieht der Bericht:

> „… dass die **Archivierung** elektronisch unterzeichneter Dokumente als zu komplex und unsicher gilt. Gesetzliche Verpflichtungen zur Aufbewahrung von Dokumenten bis zu 30 Jahre lang erfordern kostspielige und umständliche Technologien und Verfahren, um die Lesbarkeit und die Verifizierung während eines solch langen Zeitraums sicherzustellen."

Gesetzlich vorgeschrieben ist die differenziert dauerhafte Aufbewahrung von Dokumenten (Aufbewahrungs- und Verjährungsfristen). Dies geschieht in Archiven. Die Dauerhaftigkeit der Aufbewahrung impliziert die Integrität der enthaltenen Informationen, die sowohl Urheberschaft als auch Inhalt des Dokuments betreffen.

Keine elektronische Signatur ist in der Lage, die Integrität der Information eines elektronischen Dokuments zu schützen – also deren Verletzung zu verhindern. Elektronische Signaturen können ggf. lediglich anzeigen, dass eine Integritäts-Verletzung vorliegt – aber noch nicht einmal welche. Insofern ist infrage zu stellen, ob elektronische Signaturen überhaupt besonders gut zur Archiv-Sicherung geeignet sind. Mit der regulatorischen Vorgabe der „Archivierungsfestigkeit" von elektronischen Dokumenten und dem Konzept des Erneuerns von Signaturen nach Maßgabe der Sicherheit von Parametern der verwendeten Algorithmen sind Anwenderbereiche aller Kategorien überfordert. Möglicherweise können andere innovative physikalische Verfahren für die Archivierung elektronischer Dokumente viel wirksamer sein. In diesem Fall wäre auch die Endlos-Diskussion darüber, ob die letztlich im Archiv verifizierbaren elektronischen Dokumente tatsächlich originär vorliegen, gegenstandslos (Eine elektronisch signierte Datei müsste möglicherweise im Verlauf der Jahre mehrfach übersignierten und als so veränderte Datei wieder abgespeichert werden).

Um künftig einen europäischen Markt mit interoperablen Produkten und Dienstleistungen für Identifikation, Authentifizierung und Signaturen entstehen zu lassen, sind Anwendungen von grundsätzlicher Bedeutung.

Aus der Sicht von TeleTrusT sind hier europaweite Regelungen für elektronische Rechnungen und die Vergabe von öffentlichen Aufträgen sowie ein verbindliches Konzept für Dokumente der Europäischen Kommission mit elektronischen Signaturen und auch die Realisierung von IDABC geeignete Maßnahmen.

In allen Fällen sind keineswegs nur die Vorgaben des Artikels 5.1 der Richtlinie 1999/93/EG durch PKI-Services zu erfüllen, sondern es sind elektronische Signaturen aller Kategorien zu berücksichtigen.

Wie von der Europäischen Kommission in ihrem Bericht angeregt, wird TeleTrusT gerne seine vielfältigen Erfahrungen mit pragmatischen Konzepten und ihrer praktischen Umsetzung in die erneute Erörterung von Fragen der Interoperabilität von Signatur-Anwendungen einbringen und dadurch zu neuen Impulsen für ihre verstärkte Implementierung beitragen. Der praktischen Erprobung grenzüberschreitend wirksamer interoperabler Produkte und Dienste ist dabei gegenüber der weiteren Standardisierung der Vorzug zu geben.