

TELETRUST Deutschland e.V.

Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik
www.teletrust.de



TeleTrust Deutschland e.V.

zur

**Evaluierung der EG-Signatur-Richtlinie 1999/93/EG
(EGSRL)**

31. Juli 2003

TeleTrust Deutschland e.V.
Chamissostraße 11
99096 Erfurt

Tel +49 361 3460531
Fax +49 361 3453957
E-Mail info@teletrust.de

Gemäß Artikel 12 der EGSRL überprüft die Europäische Kommission die Durchführung der EGSRL und erstattet dem Europäischen Parlament und dem Rat darüber Bericht. Bei dieser Überprüfung ist unter anderem festzustellen, ob der Anwendungsbereich der EGSRL angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Der Bericht umfasst insbesondere eine Bewertung der Harmonisierungsaspekte auf der Grundlage der gesammelten Erfahrungen. Gegebenenfalls sollen dem Bericht auch Vorschläge für Rechtsvorschriften beigelegt werden.

Dieser Prozess wurde von der Europäischen Kommission mit der Vergabe einer Studie eingeleitet. In Ergänzung dieser Studie werden die interessierten Kreise zur Abgabe von Stellungnahmen bis zum 31. August 2003 aufgefordert.

In der Vorbereitung einer deutschen Stellungnahme zu dieser Evaluierung der Richtlinie hat die Bundesregierung TeleTrusT Deutschland e.V. um Stellungnahme zu folgenden Fragen gebeten:

1. Wo sehen Sie Vorteile der Einführung und Umsetzung der EGSRL in Deutschland?
2. Wo sehen Sie Probleme der Einführung und Umsetzung der EGSRL in Deutschland?
3. Sehen Sie notwendigen Änderungsbedarf der EGSRL?

TeleTrusT legt im nachstehenden die Grundgedanken für **eine anwendungsoffene und praxisbezogene Umsetzung** der europäischen Richtlinie in Deutschland dar.

Begleitung und Entwicklung der gesetzgeberischen Aktivitäten zur Schaffung von Grundlagen für die Anwendung elektronischer Signaturen war Schwerpunkt der Diskussionen in der AG1 von TeleTrusT in den vergangenen Jahren. Mit fachkundigen Stellungnahmen sowie intensiver Beteiligung an Anhörungen der gesetzgebenden Organe hat sich TeleTrusT zu Wort gemeldet. Neben dieser eher gesetzgeberischen Tätigkeit kommen in anderen Arbeitsgruppen und Projekten von TeleTrusT zusätzliche weitere Aspekte hinzu, die für vertrauenswürdige Informationsverarbeitungs- und Kommunikationsprozesse wichtig sind. Hierzu zählt beispielsweise die Standardisierung, zu der TeleTrusT mit ISIS-MTT einen wichtigen Beitrag geleistet hat, und auch das Projekt der European Bridge CA. In diesem Zusammenhang sind auch

die Best Practices für sicheren E-Commerce zu nennen, die von TeleTrusT entwickelt wurden und der Öffentlichkeit mittlerweile zur Verfügung stehen.

Einen weiteren Gesichtspunkt möchten wir dieser Stellungnahme voranstellen:

Ein wichtiges Ziel der europäischen Regelung von elektronischen Signaturen war eine intereuropäische Optimierung der elektronischen Geschäftsprozesse und deren Sicherung. Bei der Diskussion und Umsetzung der EGSR trat jedoch eine Fixierung auf das elektronische Dokument an die Stelle dieses Ziels. Bei den zukünftigen Diskussionen zur EGSR und zu eventuellen neuen Gesetzgebungsinitiativen auf nationaler wie auf europäischer Ebene muss der Blick weiter gefasst werden und auch in Richtung gesicherter Prozesssteuerungen gehen.

Diese Erfahrung möchten wir in der anstehenden Evaluierung der Richtlinie einbringen. Wir stehen gerne für Rückfragen zur Verfügung und sind bereit, in künftige Evaluierungs- und Anhörungsverfahren im Bereich der elektronischen Signatur einbezogen zu werden. Unsere Anregungen werden wir auch unmittelbar in die Analyse des Ist-Zustandes durch die Universität Leuven einbringen.

Antworten von TeleTrusT:

1. Frage:

Wo sehen Sie Vorteile der Einführung und Umsetzung der EGSRL in Deutschland?

2. Frage:

Wo sehen Sie Probleme der Einführung und Umsetzung der EGSRL in Deutschland?

Eine sachgerechte Beurteilung dieser beiden Fragen – die gemeinsam vorgenommen werden soll – kann nicht ohne Blick auf die mit der EGSRL verfolgten Ziele erfolgen. Diese sind hinlänglich bekannt, sollen aber dennoch noch einmal kurz zusammengefasst werden:

- Wesentliches Ziel der Richtlinie ist es, den europäischen Markt für interoperable Zertifizierungsdienstleistungen und Signaturprodukte zu öffnen.
- Die Richtlinie soll zu einer Harmonisierung der Bestimmungen zu elektronischen Signaturen inkl. der Rechtsfolgeregelungen in allen EU Mitgliedstaaten führen.
- Die Richtlinie hat den Grundsatz der Nicht-Diskriminierung von elektronischen und handschriftlichen Unterschriften festgelegt.

Es ist ein Verdienst der Richtlinie, den nationalen gesetzgeberischen Blick erweitert zu haben und den Rahmen für eine grenzüberschreitende Tätigkeit von Zertifizierungsdiensteanbietern (ZDA), einheitliche Grundlagen für die Zulassung, die Haftung, den Betrieb und die Sicherheitsbestimmungen von ZDA geschaffen zu haben.

Die Richtlinie hat einen flexiblen, aber auch ausfüllungsbedürftigen Rechtsrahmen für die nationalen Gesetzgebungen zu elektronischen Signaturen vorgegeben.

Für Deutschland war es von Bedeutung, dass die bereits im SigG 1997 vorgesehene Evaluierung dieses Gesetzes sowie seine Anpassung entsprechend der EGSRL zum Anlass genommen wurde, endlich auch die Rechtsfolgeregelungen für elektronische Signaturen vorzunehmen. Heute verfügen wir über einen gesetzlichen Rahmen für viele

relevanten Formen rechtswirksamen Handelns im elektronischen Geschäftsverkehr in Wirtschaft und Verwaltung sowie im Privatsektor. Allerdings betrifft die gesetzliche Regulierung im Schwerpunkt einen nur schmalen Bereich rechtswirksamen Handelns. Er bezieht sich zudem häufig explizit auf die Rahmenbedingungen für elektronische Signaturen gemäß §15 SigG 2001 und wirft damit zwangsläufig Fragen der technischen Interoperabilität von Komponenten und Diensten sowie der gegenseitigen Anerkennung im europäischen Rahmen auf. Praktisch ist diese Regulierung für die Bereiche des E-Commerce und die Geschäftsbeziehungen zwischen Unternehmen kaum von Bedeutung. Die Warnfunktion im Verbraucherbereich beispielsweise lässt sich auch anders lösen.

TeleTrust begrüßt ausdrücklich, dass die Umsetzung in den genannten nationalen Regelwerken zügig und in engem zeitlichen Zusammenhang zu den bereits verabschiedeten gesetzlichen Grundlagen erfolgte. Damit wurde die Bedeutung der elektronischen Signaturen nachhaltig unterstrichen und ein für die in diesem Bereich tätigen Unternehmen wirtschaftlich wichtiges zusätzliches Anwendungsfeld für den Einsatz und die Nutzung elektronischer Signaturen eröffnet.

Insgesamt misst sich der Erfolg der EGSR aber an den real erreichten Ergebnissen, also dem wirklichen Markterfolg der elektronischen Signaturen. Der Erfolgsnachweis der EGSR wäre – gemessen an den Maßstäben für die Evaluierung – das Vorhandensein vieler praktischer und interoperabler Anwendungen von elektronischen Signaturen in Europa.

Das Fehlen deutlicher wirtschaftlicher Impulse für die ICT-Branche nach immerhin vier Jahren praktischer Umsetzung belegt aber leider trotz des Verbrauchs umfangreicher Ressourcen den **grundsätzlichen Misserfolg der EGSR**.

TeleTrust sieht hierzu eine Reihe von Gründen:

1. Problematik einer vorausseilenden Technikregulierung

Als Vorreiter in Europa hatte Deutschland bereits im Sommer 1997 ein Signaturgesetz (SigG) als Teil des Informations- und Kommunikationsdienstegesetzes (IuKDG) geschaffen. Auch Fachleute von TeleTrust waren daran voller Enthusiasmus beteiligt. Bereits Ende 1998 hatte TeleTrust jedoch

erkannt und in einem offenen Brief kommuniziert, dass der Versuch der vorausseilenden Technikregulierung im SigG 1997 nicht den gewünschten Effekt eines flächendeckenden Einsatzes digitaler Signaturen im elektronischen Geschäftsverkehr hatte:

„... TeleTrusT hält es für wünschenswert, dass das Signaturgesetz (bzw. die SigV) schnell in einigen Bestimmungen verändert wird, um bei seiner Umsetzung mehr Flexibilität hinsichtlich innovativer Lösungen und Kompatibilität zu globalen Standards zu erreichen. Das wird dazu beitragen, dass die Investitionen in diesem Bereich ein höheres Wirkungsfeld bekommen. ...“

Es ist festzustellen, dass auch in der EGSRL der Versuch einer „vorausseilenden Technikregulierung“ unternommen wurde, der naturgemäß nicht technikneutral sein kann.

2. Unterschiedliche Umsetzung der Richtlinie in EU-Mitgliedstaaten

Die EGSRL wurde von den Mitgliedsstaaten sehr unterschiedlich in nationales Recht umgesetzt. In Deutschland erfolgte dies beispielsweise nicht so, dass das Hauptziel der EGSRL, eine europaweite Harmonisierung, im Vordergrund stand. Die in der EGSRL vorhandenen Spielräume wurden vielmehr überwiegend dahingehend genutzt, um die Vorgaben des SigG 1997 möglichst unverändert in das SigG 2001 einfließen zu lassen. Als Beispiele aus dem SigG 2001 seien hier genannt:

- Die Bindung fortgeschrittener (und damit auch qualifizierter) elektronischer Signaturen allein an natürliche Personen; damit sind juristische Personen im Gesetzestext an dieser Stelle in Deutschland faktisch (wenn auch nicht wörtlich) ausgeschlossen, während andere EU-Mitgliedstaaten, vom weiteren Spielraum der EGSRL Gebrauch machend, elektronische Signaturen auch für juristische Personen zulassen.
- Die gegenüber der EGSRL einschränkende Definitionen (z.B. fortgeschrittene elektronische Signatur, Zertifizierungsdiensteanbieter)
- Die Zulassung von Pseudonymen in Verbindung mit elektronischen Signaturen: Elektronische Signaturen sollen in der Praxis zur Identifizierung von Personen und zur Authentifizierung bei Prozessen eingesetzt werden, in denen eine **verbindliche Zuordnung zu einem Urheber** wichtig ist. Ein Anspruch auf Pseudonymität oder gar Anonymität, wie er als

datenschutzrechtlicher Kern bereits im SigG 1997 geregelt war, widerspricht diesem praktischen Bedürfnis und sollte daher mit Blick auf die eigentlichen Geschäftsprozesse neu geregelt werden.

3. Fehlende marktwirtschaftliche Fokussierung der Umsetzung in Deutschland

Bei der Umsetzung der EGSRL in Deutschland wurde sehr viel Gewicht auf die Regulierung der qualifizierten Signatur mit freiwilliger Akkreditierung der ZDA gelegt und weniger auf die Berücksichtigung und Förderung anwendungsbezogener Signaturen, wie sie mittlerweile im europäischen Markt anzutreffen sind, z.B. auf dem Niveau der fortgeschrittenen Signaturen. Es hat sich als nachteilig erwiesen, dass das flexiblere „Baukastenprinzip“ bei den technischen Vorgaben der EGSRL zugunsten fest definierter Signaturqualitäten (einfach, fortgeschritten, qualifiziert, akkreditiert) im SigG 2001 aufgegeben wurde. Dies führte gemeinsam mit der vorbeschriebenen einseitigen Sichtweise zu vielen Fragen und Schwierigkeiten in der Praxis, die nach Ansicht von TeleTrust den geraden und schnellen Weg zu praxisbezogenen Lösungen verstellt hat

- Es hat im Ergebnis in Deutschland zu einer **Vielzahl von Signaturprofilen** geführt, die zudem in unterschiedlichen Gesetzen Eingang gefunden haben und nun ihrerseits den klaren und eindeutigen Praxisbezug und die von der Industrie gewünschte Leitlinie vermissen lassen.
- Aus unserer Sicht hat diese Umsetzung für **wenig Durchlässigkeit des deutschen Marktes für europäische Anbieter** gesorgt. Die europäische Komponente der Zertifizierungsdienste und die damit fehlende durchgängige Einheitlichkeit der Infrastrukturen fehlt heute. Die nach deutschem Recht pauschale Anerkennung der EGSRL entsprechender, der deutschen Umsetzung jedoch nicht genügender ausländischer Signaturen widerspricht einerseits (theoretisch) dem Gleichbehandlungsgrundsatz und scheitert andererseits (praktisch) an Interoperabilitätsproblemen. Ebenso ist die gewünschte Angebotsvielfalt von ZDA anderer Mitgliedsstaaten in nationalen Märkten nicht gegeben, was auch daran liegen mag, dass die zentrale Komponente des Registrierungsdienstes vor Ort von den nationalen zuständigen Aufsichtsbehörden des Herkunftslandes nicht erfasst werden kann.

- Es hat sich erwiesen, dass die Konzentration auf den höchstmöglichen Signaturstandard und die damit für den Verbraucher verbundenen **Kosten am Markt keine Akzeptanz** finden. Für den Geschäftserfolg der ZDA ist es inzwischen maßgeblich, die ganze Bandbreite von Zertifizierungsdiensten anzubieten. Für verschiedene, durch die Geschäftsprozesse des Kunden bestimmte, Anforderungen und ihnen zugrunde liegende gesetzliche Vorgaben können so angemessene Lösungen angeboten werden.
- Leider wird in Deutschland bei öffentlichen Diskussionen des öfteren der Eindruck erweckt, nur die für Anwendungen im formgebundenen Bereich vorgesehenen Instrumentarien elektronischer Signaturen seien vertrauenswürdig. Damit wurde und wird Unsicherheit gegenüber alternativen Lösungen, deren Zulässigkeit im Gesetz ausdrücklich bestätigt ist, erzeugt und ihre Verbreitung im stark überwiegenden Bereich formfreien Handelns verhindert.
- Der elektronische Signaturen betreffende Aufgabenschwerpunkt der Regulierungsbehörde für Telekommunikation und Post (RegTP) muss den wirtschaftlichen Erfordernissen angepasst werden. Er ist von der alleinigen, technologieorientierten Umsetzung des §15 SigG (Akkreditierung von ZDA) hin zu einer vertrauensbildenden Begleitung (Aufsicht) aller Diensteanbieter für qualifizierte elektronische Signaturen zu verschieben.

Aus der Sicht von TeleTrusT wäre es daher wünschenswert, nicht nur die rechtlichen und technischen Fragen – von denen einige noch nicht geklärt sind – in der **europäischen Praxis** zu analysieren und einer pragmatischen Lösung zuzuführen. Auch die betriebswirtschaftlichen Fragen sind auf europäischer Ebene eingehender zu berücksichtigen, um so den potentiellen Einsatz elektronischer Signaturen und die notwendige **europäische Interoperabilität** zu verbessern. Chancen dafür bieten sich durch die ersten Impulse seit der Gründung des Signaturbündnisses in Deutschland. Hierzu zählt eine genaue Marktbeobachtung und das Feedback der Markterfahrungen in die gegenwärtigen Diskussionen.

3. Frage:

Sehen Sie notwendigen Änderungsbedarf der EGSRL?

Die EGSRL hat ihr wirtschaftliches Ziel verfehlt. Die Marktentwicklung für Signaturanwendungen wurde nicht stimuliert.

Die EGSRL hat ihr juristisches Ziel nur zum Teil erreicht. In wesentlichen Details hat nationales Besitzstandsdenken die Umsetzung der EGSRL in national geltende Bestimmungen für elektronische Signaturen bestimmt und damit einer europaweiten Harmonisierung entgegen gewirkt.

Eine Änderung der EGSRL in Details sollte aber aus unserer Sicht ultima ratio sein; es sollte eher auf nationaler Ebene versucht werden, Änderungen durchzuführen und diese - wo notwendig - europäisch abzustimmen. Deutschland hat hier deutlichen Handlungsbedarf, wie wir bei der Beantwortung der Fragen 1 und 2 bereits dargelegt haben.

TeleTrusT ist der Ansicht, dass eventuelle Detailänderungen der Richtlinie Einführung und Umsetzung elektronischer Signaturen in Europa für die Dauer des Gesetzgebungsvorhabens auf der europäischen wie auch die Umsetzung auf nationaler Ebene ganz erheblich bremsen würden.

Wenn Änderungen trotzdem vorgenommen werden sollen, sieht TeleTrusT Änderungsbedarf, der sich zum einen auf rechtliche Vorgaben der Richtlinie, die zu verdeutlichen sind, und zum anderen auf den Prozess der sogenannten „co-regulation“, den die Richtlinien-systematik vorgibt und der sich in der Praxis als zu langsam und zu wenig flexibel erweist.

Die Erfahrung der TeleTrusT-Mitglieder bei der Einführung der elektronischen Signatur hat gezeigt, dass rechtliche und technische Vorgaben allein eine automatische flächendeckende Verbreitung elektronischer Signaturen nicht erreichen. Für einen erfolgreichen Einsatz der elektronischen Signatur in den Geschäftsprozessen wird ein komplettes Framework mit Workflow und Archivierung unter Berücksichtigung auch

betriebswirtschaftlicher Faktoren benötigt. Dies kann durch starre regulative Vorgaben nicht erreicht werden.

Aus den praktischen Erfahrungen von TeleTrusT-Mitgliedern haben sich insbesondere folgende Aspekte ergeben, die keinesfalls abschließend sind:

- Durch elektronische Signaturen können Geschäftsprozesse medienbruchfrei realisiert werden. Dies hat den wesentlichen Vorteil, dass sie schneller und effizienter gestaltet und somit erhebliche Kosten eingespart werden können. Deshalb sollen möglichst viele Anwendungen, beginnend im formfreien Bereich, der keinerlei Regulierung bedarf, mit der Funktionalität des elektronischen Signierens ausgestattet werden. Die Regelungen der Signaturverfahren im formgebundenen Bereich können national aber nur im **intereuropäischen Konsens** ausgefüllt werden. In der Praxis der Umsetzung der EGSRL sind die vorhandenen Spielräume stets unter Wahrung der Ziele der EGSRL und nicht zur Verfolgung eigener nationaler Interessen zu nutzen. Dem kann aus unserer Sicht nur durch eine **verstärkte und formalisierte Kooperation** der EU-Mitgliedstaaten begegnet werden, zum Beispiel im Rahmen der ENISA, deren Aufgaben entsprechend zu gestalten sind.
- Die Richtlinie ist in den Mitgliedstaaten sehr unterschiedlich umgesetzt worden. Dies haben die bislang gemachten Erfahrungen und verschiedene Studien gezeigt; zusätzlich wird die Richtlinie mittlerweile von einigen neueren Richtlinien (z.B. EU-Richtlinie für elektronische Rechnungen und MWSt, 2001/115/EC) referenziert. In der Praxis führt dies zur Anwendung der jeweiligen nationalen Gesetzgebung. Grenzüberschreitende Anwendungen – wie sie zum Beispiel im Bereich europäischer Unternehmen oder in Bereichen grenzüberschreitender Anwendungen aus **Kostenersparnis** erforderlich sind – werden durch die unterschiedlichen nationalen Umsetzungen teils verhindert und teils unnötig kompliziert. Hier muss nach Auswegen gesucht werden, die das Föderationsprinzip in der EG konstruktiver als bisher berücksichtigen.
- Bei der Implementierung von Signaturprozessen in die Abläufe des elektronischen Geschäftsverkehrs treten in der Praxis unterschiedlichste Anforderungen auf, denen durch innovative Lösungen zu entsprechen ist. Die durch den flexiblen Rahmen der EGSRL gegebenen Möglichkeiten sind bei

diesen Implementierungen soweit wie nötig auszuschöpfen; sich daraus ergebende neue Instrumentarien (Produkte, Lösungen, Dienstleistungen) sind in die Konzepte einzuordnen und anzuerkennen. Die Implementierung muss bestimmt werden durch Zweckorientiertheit, nicht durch vorausseilende Technikregulierung.

- Nach wie vor herrscht eine große Unsicherheit bei den Anwendern durch immer neue regulatorische Anforderungen oder Änderungen bestehender Verordnungen: So wird zum Beispiel zur Betrachtung des Dokumentes, das ein Anwender mit einer qualifizierten elektronischen Signatur signieren möchte, eine Anzeigekomponente benötigt. Diese soll z.B. laut RegTP mindestens E2 "hoch" evaluiert sein, was in dieser Form weder im Signaturgesetz noch in der Signaturverordnung zu finden ist. In der Anlage zur Verordnung zur elektronischen Signatur, Anlage 1 Nr.1 (zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2) besteht keine Veranlassung Anzeigekomponenten zu evaluieren. Allerdings, laut Aussage der RegTP, wird die Verordnung abgeändert und die Anlage 1 Nr.1 bezieht sich auf § 11 Abs. 3, § 16 Abs. 2, § 17 Abs. 2, § 17 Abs. 3 -1 und 2. Damit müssten auch Anzeigekomponenten evaluiert werden. Nun stellt sich natürlich die Frage, ob man von der jetzigen Signaturverordnung ausgeht oder von der zukünftigen, ob man sich in Deutschland dem Ziel der EGSR wieder nähern oder sich von ihm gar noch weiter entfernen will.
- Die Richtlinie sollte daher nach unserer Auffassung die **europäische Zertifizierung** von Produkten für elektronische Signaturen ermöglichen ohne sie vorzuschreiben. Dies ist zwar in der Richtlinie durch Art. 3 Abs. 5 angelegt und ist jetzt auch in einer ersten Entscheidung der EU Kommission vom 14.07.2003 umgesetzt worden. Dies ist im Kern ein richtiger Ansatz, müsste aber aus unserer Sicht auf weitere Komponenten ausgedehnt werden. Damit würden zahlreiche Unsicherheiten bei Anbietern, die ihre Signaturprodukte nicht nur für einen nationalen Markt, sondern für den europäischen Markt anbieten, genommen.
- Der bereits angesprochene Grundsatz der „**co-regulation**“ bedeutet, dass vor allem bei technologisch geprägten Rechtssetzungen auf der europäischen Ebene sich diese mit wesentlichen Prinzipien begnügt und die technische Ausgestaltung den anerkannten Standardisierungsgremien ETSI, CEN,

CENELEC und ihren jeweiligen nationalen Mitgliedsorganisationen anvertraut wird. Dieser Weg ist im Ansatz richtig, führt jedoch zu erheblichen Verzögerungen bei der Umsetzung und Verabschiedung der gefundenen Standards. Hier wäre es wünschenswert, wenn klare und einfache Verfahren geschaffen würden, die transparente und rasche Verfahren erlauben würden. Aus Sicht von TeleTrusT wäre es dabei wichtig, nationale Entwicklungen, zum Beispiel ISIS-MTT, mit einzubeziehen.

Erfurt, 31. Juli 2003

gez. Prof. Dr. Helmut Reimer

Geschäftsführer
TeleTrusT Deutschland e.V

gez. RA Stefan Engel-Flehsig

Leiter der TeleTrusT-Arbeitsgruppe
„Juristische Aspekte einer verbindlichen
Kommunikation“