

[ITAS - Projekt PEZ](#)

[EZI-N Auswahl und Anmeldung bei EZI-L](#)

[\$&\$]

EZI-N - 1997 - Nr. 3 - Freitag - 14.11.1997

[!]

Inhalt

[\[3&1\]](#) Editorial

[\[3&2\]](#) Fernabsatz-Richtlinie der EU in Kraft

[\[3&3\]](#) Internet Tax Freedom Act vom Handelsausschuß
beschlossen

[\[3&4\]](#) ICC Richtlinie zum elektronischen
Geschäftsverkehr

[\[3&5\]](#) NTT aktiv mit Zahlungsverkehr im Internet

[\[3&6\]](#) Inkasso-System für Micropayments bei
germany.net?

[\[3&7\]](#) Literaturhinweis: Mehr zum Cyber Money

[\[3&8\]](#) Literatur- und Rezensionshinweis: Die Ware
Information

[\[3&9\]](#) Impressum

[3&1]

Editorial

Am 2. Oktober 1997 kündigte die Firma Pretty Good Privacy Inc. ihre PGP Business Security Suite an. Das amerikanische Wirtschaftsministerium hat inzwischen übrigens den Export dieser Software auch mit starker Kryptographie an Banken erlaubt. PGP for Business Security soll Unternehmen den Aufbau und das Management einer Public-Key-Infrastruktur erlauben. Soweit die pretty good news.

Zu diesem Paket gehört auch eine Komponente, "Policy Management Agent" genannt, mit der Betriebe oder Institutionen, die diese PGP-Version einsetzen, bestimmte "Sicherheitspolitiken" durchsetzen können, z.B., daß nur verschlüsselte E-mails nach außen gehen und daß jede E-mail zusätzlich noch mit einem "corporate message recovery key" verschlüsselt wird, der den Sicherheitsabteilungen bzw. der Firmenleitung im Falle eines Falles - man denke z.B. an das plötzliche Ausscheiden von Mitarbeitern aus dem Unternehmen - Zugriff auf die E-Mails der Mitarbeiter gestattet.

Am CMR (corporate message recovery), für viele die bad news schlechthin, setzte alsbald die Kritik an, die von Peter Wayner in der New York Times vom 3.10.1997 noch recht vorsichtig vermerkt wurde, dann aber - vor allem aber in einigen Mailinglists - an Heftigkeit rapide zunahm. Man sah in diesem optionalen CMR-Mechanismus einen Schritt auf dem Weg zum gesetzlich erzwungenen Zugriff der Regierung auf private Kommunikation ("mandatory governmental access to key", kurz GAK) und einen Angriff auf die Privatsphäre, oder, um es auf einen anderen Nenner zu bringen: Schützenhilfe für die Vertreter eines restriktiven Kryptographiegesetzes.

Phil Zimmermann, 1996 noch mit dem Norbert Wiener-Preis für "social responsibility in computing" ausgezeichnet und als Evangelist des "bottom up approaches" beim Aufbau von Zertifizierungsinfrastrukturen gefeiert, dem das deutsche Signaturgesetz noch zu staatslastig galt, wurde auf einmal zum geldgierigen Saulus gestempelt, der mit den dunklen Mächten, den Sicherheitsdiensten und den Protagonisten eines Kryptographiegesetzes, wenn nicht gar gemeinsame Sache mache, so doch zumindest Wasser auf deren Mühlen gieße.

Ohne hier klären zu können, inwieweit diese PGP-Version in der Konsequenz tatsächlich einen Freibrief zum "Abhören" der elektronischen Kommunikation von Betroffenen bedeutet und inwieweit bei der Kritik ein automatischer Reflex gegen jeden Anschein von Überwachungsstaat mitgespielt hat, scheint doch zweierlei ablesbar: Zum einen deutet der Fall darauf hin, daß Diskussionen im Internet noch leichter zu emotionalisieren sind als über die herkömmlichen Massenmedien und daß unter Umständen Hersteller, Anbieter und deren Produkte deshalb besonders drastisch einen plötzlichen Vertrauensschwund erleiden können. Zum anderen läßt sich vermuten, daß die sowieso schon unwahrscheinliche Option, eine allgemeine Sicherheitsinfrastruktur mittels eines "bottom up" Ansatzes - dafür stand PGP ja exemplarisch - aufzubauen, noch unwahrscheinlicher geworden ist.

In der dritten Nummer von EZI-N wird in etwa gleichgewichtig von Dokumenten zum E-Commerce und neuen Zahlungssystemen berichtet, ergänzt von zwei Literaturhinweisen. Wie immer, würden wir uns wünschen, daß Nachfragen, kritische Kommentare und Diskussionsbeiträge zu EZI-N an die Mailliste EZI-L gerichtet werden.

[i]

-> Presseerklärung vom 2.10.1997 - PGP Business Security Suite: Complete Security Solution Protects Email And Digital Assets From The Desktop To The Internet <http://www.pgp.com/newsroom/>

-> Peter Wayner: PGP Offers New Encryption Software for Corporations. CyberTimes (New York Times) vom 3.10.1997 unter <http://www.nytimes.com/> (Anmeldung erforderlich) suchbar

[A]

Knud Böhle

[\[^\]](#)

[3&2]

Fernabsatz-Richtlinie der EU in Kraft
/Europa/elektronischer Handel/Verbraucher

Die Richtlinie über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz ist im Amtsblatt der EU am 4.6.1997 verkündet worden. Mit "Fernabsatz" sind alle Vertragsabschlüsse ohne gleichzeitige körperliche Anwesenheit der Vertragsparteien gemeint. Inhalt dieser Verträge sind die Lieferung von Waren oder Dienstleistungen. Zu den "Fernkommunikationstechniken" im Sinne dieser Richtlinie zählen u.a. Drucksachen und Standardbriefe, Pressewerbungen mit Bestellschein, telefonische Kommunikation mit Personen und Automaten, elektronische Post, Hörfunk und Fernsehen, Telefax.

Die Richtlinie gilt nicht für Verträge, die sich auf Finanzdienstleistungen beziehen. Ausnahmeregelungen gibt es auch für den Verkauf aus Automaten und für die regelmäßige bzw. zu einem bestimmten Zeitpunkt zu erbringende Lieferung von Lebensmitteln.

Die Richtlinie bestimmt in Artikel 4, in welcher Art und Weise und in welchem Umfang der Verbraucher vor Abschluß des Vertrages über die Vertragsinhalte unterrichtet werden muß. Die Richtlinie regelt in Artikel 6, daß der Verbraucher innerhalb von sieben Werktagen ohne Angabe von Gründen den Vertragsabschluß widerrufen kann. Artikel 10 sieht für die Nutzung bestimmter Kommunikationstechniken im Fernabsatz eine vorherige Zustimmung der Verbraucher vor (z.B. Voice-Mail- Systeme). Artikel 14 eröffnet die Möglichkeit für die Mitgliedsländer, auch strengere Bestimmungen zu erlassen. So könnte beispielsweise der Vertrieb von Arzneimitteln im Fernabsatz durch einzelne Mitgliedsländer unterbunden werden.

Die Mitgliedsländer müssen die Richtlinie innerhalb von drei Jahren in nationales Recht umsetzen.

[Q]

Computer und Recht, Heft 9, 1997, S. 575-579

[i]

-> Im WWW findet sich die Richtlinie in elf Sprachen unter <http://europa.eu.int/en/comm/dg24/cad.html>.

-> Die Verbraucherschutzpolitik der Kommission wird im WWW unter der Adresse <http://europa.eu.int/en/comm/dg24/spc.html> dargestellt.

[^]

[3&3]

Internet Tax Freedom Act vom Handelsausschuß beschlossen
/USA/Politik/elektronischer Handel/Steuern

Ein Gesetzentwurf des demokratischen Senators Ron Wyden wurde im Handelsausschuß des Senats gebilligt und soll nächstes Jahr im Plenum des Senats behandelt werden. Dieser Entwurf eines "Internet Tax Freedom Act" soll verhindern, daß in den nächsten fünf Jahren neue Steuern auf den Internet-Handel erhoben werden. Bereits bestehende Steuern werden durch den Gesetzentwurf nicht tangiert.

Kritik an diesen Plänen kommt von den betroffenen Bundesstaaten und Kommunen, die sich in ihrer Souveränität Steuern zu erheben eingeschränkt fühlen und um ihr Steueraufkommen fürchten, wenn immer mehr Geschäftsaktivitäten im Internet abgewickelt werden. Die US-amerikanische "National Governors' Association" (NGA) erklärte, daß diese Pläne zu einem Kollaps bei den derzeitigen Verkaufssteuern führen könnten, der für jede US- amerikanische Gemeinde spürbar wäre.

Ähnliche Pläne für ein Steuer-Moratorium im Internet werden von der amerikanischen Regierung, der OECD und in der EU verfolgt.

In den USA gibt es auf bundesstaatlicher und lokaler Ebene 30.000 Instanzen, die über Steuern entscheiden können. Wie die Süddeutsche Zeitung berichtete, wurden neue "Internet- Steuern" in den Bundesstaaten Colorado, Connecticut, Florida und Texas bereits eingeführt.

[Q]

-> Communications-related Headlines der Benton Foundation, 5.11.1997

-> STERN Newsletter Computer 44/97

-> Süddeutsche Zeitung, 4.7.1997, S. 22

[i]

-> Informationen von Senator Wyden zum Gesetzentwurf finden sich unter <http://www.senate.gov/~wyden/leg/cybtax.htm>.

-> Die Presseerklärung des Handelsausschusses des Senats findet sich unter <http://www.senate.gov/~commerce/press/105-169.htm>.

-> Mit den Anwendungsproblemen herkömmlicher Steuerregelungen im Internet befaßt sich aus kanadischer und US-amerikanischer Sicht Zak Muskowitch: Taxation of Internet Commerce, in http://www.firstmonday.dk/issues/issue2_10/muscovitch und aus deutscher Sicht Jens Bleuel und Marcus Stewen: Grundlegende Probleme einer Besteuerung von Internettransaktionen, erscheint in Wirtschaftsdienst 11/1997.

[^]

[3&4]

ICC Richtlinie zum elektronischen Geschäftsverkehr
/International Chamber of Commerce/Sicherheit
/elektronischer Handel

Die ICC (International Chamber of Commerce) mit Sitz in Paris hat am 6.11.1997 Empfehlungen für den sicheren elektronischen Geschäftsverkehr in offenen Netzwerken vorgelegt. Der Titel lautet: "General Usage in International Digitally Ensured Commerce", kurz GUIDEC. Das Papier wurde von einer Arbeitsgruppe im Rahmen des ICC Electronic Commerce Projektes entwickelt. Es richtet sich an Wirtschaft und Regierungen und versteht sich als "comprehensive statement of best practices for the emerging global infrastructure", wobei man sich stark macht für digitale Signaturen und eine Public-Key-Zertifizierungsinfrastruktur. Wichtige Bezugspunkte bei der Ausarbeitung waren die "Digital Signature Guidelines" der American Bar Association und das UNICTRAL "Model Law on Electronic Commerce". Das Papier will aber auch als Beitrag zu einer international eindeutig verwendbaren Terminologie verstanden werden. Der Eindeutigkeit fallen sowohl die Begriffe "Authentisierung" als auch "digitale Signatur", die zusammen durch ein Konzept von "ensure" ersetzt werden, zum Opfer.

Der entsprechende GUIDEC-Passus folgt:

1. Ensure

To record or adopt a digital seal or symbol associated with a message, with the present intention of identifying oneself with the message.

Clarification: "Ensure": In American usage, the term "authenticate" is often used to denote the act of identifying oneself with a message, but in European usage "authenticate" is more associated with the verification of a signature (see post). Furthermore, there is a fundamental difficulty in the concept of "digitally signing" a message, in that there are significant differences between a physical signature, and one effected through an electronic medium. The

most important difference is that most digital signatures rely upon a smartcard or some other storage facility in order to reproduce the algorithm necessary for securing the "signature" to the message with which it is to be associated. It then follows that if this storage facility is accessed by someone other than the person to whom it belongs, a message can be "signed" and appear to have originated from the owner, either with or without his consent. It is for this reason that we have employed the term "Ensure", which is defined by Webster's Universal College Dictionary as "1. To secure or guarantee. 2. To make sure or certain. 3. To make secure or safe, as from harm". It is exactly this which is being sought in an electronic message - to make it secure from subsequent alterations.

[Q]

<http://www.iccwbo.org/guidec2.htm>

[i]

ICC (International Chamber of Commerce)

<http://www.iccwbo.org/>

[^]

[3&5]

NTT aktiv mit Zahlungsverkehr im Internet
/Japan/elektronische Zahlungssysteme/Internet
/Pilotversuch

Das Konzept des japanischen Telekommunikationsunternehmens NTT zum elektronischen Zahlungsverkehr im Internet sieht in der Kunde-Händler-Bank-Beziehung zwei Intermediäre vor: ein Ausgabeinstitut und eine Meldestelle. Will ein Kunde elektronisches Geld auf seiner Chipkarte speichern, so fordert er dies - auf elektronischem Wege natürlich - bei seiner Bank an, die ihm einen "Issue Request" zurückschickt, der dann beim Ausgabeinstitut gegen elektronisches Geld eingelöst wird. Das Ausgabeinstitut holt sich dann bei der Bank des Kunden den entsprechenden Betrag. Diese Transaktionen laufen selbstverständlich automatisiert ab, so daß der Kunde sich nicht um die einzelnen Schritte kümmern muß. Das Ausgabeinstitut garantiert die Einlösbarkeit des elektronischen Geldes, kontrolliert bankübergreifend die Ausgabe der elektronischen Geldeinheiten und fungiert als Verrechnungsstelle zwischen den beteiligten Banken. Die sogenannte Meldestelle vergibt pseudonyme Identifikationscodes an die Kunden, mit denen sie ihre Zahlungen anonym abwickeln können. Das digitale Geld besteht aus dem Nennwert, einer Seriennummer, dem Eigentumsnachweis aufgrund des Identifikationscodes und einer digitalen Unterschrift.

1998 sind zwei größere Pilotversuche in Japan geplant. Im ersten Versuch, unterstützt durch die Cyber Business Association, soll in erster Linie die Zuverlässigkeit elektronischer Zahlungen im Internet getestet werden. Der Versuch soll im Juli 1998 mit 10.000 Anwendern beginnen. Beim zweiten Versuch geht es um die Zusammenarbeit zwischen NTT und den großen japanischen Banken. Die praktische Anwendbarkeit und Sicherheitsaspekte stehen im Vordergrund. Rund 100.000 Teilnehmer sollen in 1.000 Akzeptanzstellen mit elektronischem Geld einkaufen können.

[Q]

Handelsblatt, 4.11.1997, S. 29

[\[^\]](#)

[3&6]

Inkasso-System für Micropayments bei germany.net?
/elektronische Zahlungssysteme/Micropayment/Internet-Service-Provider

Nach T-Online hat auch der Online-Dienst und Internet Service Provider germany.net ein Inkassosystem bzw. Mikropaymentsystem angekündigt, das nach einer Pressemeldung vom 30.8.1997 voraussetzt, daß der Kunde über die Teilnehmerkennung und eine Kopie seines Personalausweises bekannt ist - und seine Bankverbindung weitergibt. "Danach wird der Teilnehmer aufgefordert, ein persönliches Kennwort einzugeben, um die Daten zu verschlüsseln. Dadurch sind die Daten selbst germany.net nicht bekannt. Nach der Bestätigung der Bankverbindung und der nochmaligen Bestätigung durch das Passwort ist es möglich, auf das Kleingeldkonto Beträge zwischen 10 DM und 120 DM gutzuschreiben. Der Teilnehmer legitimiert zukünftig jede Transaktion mit seinem Kennwort. Bricht die gebührenpflichtige Übertragung ab, kann sie erneut und ohne weitere Gebühren aktiviert werden. Bei Beträgen, die 9,99 DM übersteigen, muß der Teilnehmer dem jeweiligen Anbieter der "Online-Waren" die Erlaubnis zur Abbuchung erteilen. Der Teilnehmer legitimiert diesen Vorgang wiederum durch die Eingabe seines persönlichen Kennworts.

Nach dieser 10 Wochen alten Ankündigung ist offenbar noch nichts passiert: auf den frei zugänglichen Seiten bei germany.net gibt es keinen aktuelleren Hinweis und auch in einem neueren Portrait des Online-Dienstes in der November-Ausgabe von Business Online ist mit keinem Wort von dem Micropaymentsystem die Rede. Auf Nachfrage bei callisto germany.net in Frankfurt hieß es ohne genauere Zeitangabe "demnächst", was vielleicht dem spanischen "mañana" nahekommt.

[Q]

<http://www.germany.net/info/presse/payperview.html>

[i]

-> Harald Lux und Ronald Wiltscheck: Vom Fernsehen abgucken. Business Online 11/97, S.32-33
-> Online Cash <http://www.intouch.de/zahlungssysteme/index.htm> Die Firma inTouch gibt (unregelmäßig) einen Newsletter Online Cash heraus, der im Internet kostenfrei abonniert werden kann und in der aktuellsten Ausgabe, der September-Nummer, eine Fülle von Meldungen - so an die 50 - enthält, die sich um elektronische Zahlungssysteme und E-Commerce drehen - darunter eine zum Micropaymentsystem von germany.net, die uns zum Nachrecherchieren veranlaßte.

[\[^\]](#)

[3&7]

Literaturhinweis: Mehr zum Cyber Money
/Deutschland/Literatur/elektronische Geldbörse/Akteure

In dem Buch von Sylvia Lukas, das Basisinformationen für "Manager bei Kreditinstituten, bei Handelsunternehmen und Dienstleistern" bereitstellen möchte, stehen - anders als vom Titel her vielleicht zu erwarten - elektronische Geldbörsen (nicht zuletzt die GeldKarte) im Vordergrund. Eine ganze Reihe von aktuellen Projekten werden kurz beschrieben und auch eine ganze Reihe von Firmen, die EDV-Lösungen für die

Kreditwirtschaft entwickeln, wie IKOSS VAN, Gemplus, Krone, Brokat und andere, werden mit ihren Produktlinien vorgestellt. Hier ist am ehesten das "Alleinstellungsmerkmal" dieses Buches gegenüber Konkurrenzangeboten zu suchen, während bei der Besprechung von Sicherheitskonzepten und der Darstellung von Zahlungskonzepten im Internet von einer eher schwachen Vorstellung zu sprechen wäre. Positiv ist die Konzentration auf deutsche Produkte und Projekte herauszustellen, die bei den Geldbörsenprojekten sinnvoll durch europäische Projekte ergänzt wird. Diese Fokussierung läßt einen gewissen Eindruck davon entstehen, was in Deutschland so läuft und ist auf jeden Fall einem internationalen Sammelsurium an Projekten und Zahlungssystemen vorzuziehen. Wer also mit relevanten deutschen Akteuren im Bereich elektronischer Zahlungssysteme bekannt gemacht werden will, dem wird hier ein gut gegliederter Einstieg geboten. Wer jedoch eigenständige Argumentationen, Interpretationen, Einschätzungen, Meinungsäußerungen sucht, der wird nicht auf seine Kosten kommen.

[i] Sylvia Lukas: Cyber Money, Künstliches Geld in Internet und Elektronischen Geldbörsen. Neuwied: Luchterhand 1997, 80.00 DM

[A]

Knud Böhle

[\[^\]](#)

[3&8]

Literatur- und Rezensionshinweis: Die Ware Information /Literatur/elektronisches Geld/Recht/PGP

Das Jahrbuch Telekommunikation und Gesellschaft, ist jetzt zum fünften Mal, diesmal mit dem Schwerpunkt "Die Ware Information..." und einem Special: "Internet" herausgekommen. Als besonders einschlägig im Kontext von EZI-N ist der Beitrag "Cyber Money ohne Bankenlobby" von Stephan Klein anzusprechen, der dem Interesse der Banken an digitalen Geldprodukten, vor allem der GeldKarte, nachgeht. Er zeigt, daß es für die Banken sowohl vorteilhaft ist, a) von Bar- auf Buchgeld umzustellen und b) nicht-digitale Zahlungsinstrumente wie Schecks, Überweisungen oder eben auch Bargeld durch digitale Formen zu ersetzen. Das Fazit lautet, daß die Kreditinstitute rational handeln, "wenn sie ihr Zahlungsverkehrsangebot, das auf Buchgeld basiert, optimieren, um so möglichst lange elektronisches Bargeld zu verhindern" (gemeint: Zentralbankgeld).

R. Grimm ergänzt diesen Beitrag kompetent mit Ausführungen zur Rechts- und Zahlungssicherheit im Internet. Zum einen stellt er auf "technische Herausforderungen an offene Kommunikationsnetze" ab, zum anderen überlegt er, inwieweit Sicherheit in offenen Netzen durch Maßnahmen der Selbstorganisation (a la PGP) und inwieweit sie nur durch zentral gesteuerte Sicherungsverfahren erbracht werden kann, um schließlich "für ein ausgewogenes Verhältnis zwischen staatlichen Regelungen und Selbstschutz der Bürger" zu plädieren.

Eine ausführliche Rezension des Jahrbuchs wird in der neuesten Ausgabe der TA-Datenbank-Nachrichten, der Zeitschrift des Instituts für Technikfolgenabschätzung und Systemanalyse, abgedruckt, ist aber schon jetzt online verfügbar.

[i]

->Kubicek, H.; Klumpp, D.; Müller, G.; Neu, W.;
Raubold, E.; Rossnagel, A. (Hrsg.): Jahrbuch
Telekommunikation und Gesellschaft 1997. Die Ware
Information - Auf dem Weg zu einer
Informationsökonomie, R.v. Decker's Verlag: Heidelberg
1997, 98.-- DM. Die Homepage zum Jahrbuch
<http://www.jtg-online.de/>

-> Knud Böhle: Die Masse könnt ihr nur durch Masse
zwingen. Rezension. TA-Datenbank-Nachrichten Nr. 3/4,
6. Jahrgang - November 1997 [http://www.itas.fzk.de
/deu/TADN/TADN397/butag.htm#butag3](http://www.itas.fzk.de/deu/TADN/TADN397/butag.htm#butag3)

[A]

Knud Böhle

[\[^\]](#)

[3&9]

Impressum

[\$&\$]

EZI-N Elektronische Zahlungssysteme im Internet
Newsletter - 1997 - Nr. 3 - Freitag - 14.11.1997
<http://www.itas.fzk.de/deu/projekt/pez/ezin.htm>

Herausgegeben im Rahmen des Projekts Elektronische
Zahlungssysteme (PEZ), ein im Auftrag des
Bundesministeriums für Bildung und Forschung (BMBF)
durchgeführtes Projekt des Instituts für
Technikfolgenabschätzung und Systemanalyse(ITAS) im
Forschungszentrum Karlsruhe.

Erscheint vierzehntägig freitags.
Redaktion Knud Böhle und Ulrich Riehm.

EZI-N wird per E-Mail verteilt im Rahmen der
Diskussionsliste EZI-L. Um an EZI-L teilzunehmen,
schicken Sie eine E-Mail an:

majordomo@listserv.fzk.de
mit dem Text
subscribe EZI-L.

Außerdem finden sich alle Nummern von EZI-N auf dem
PEZ- Bereich unseres ITAS-WWW-Servers unter

<http://www.itas.fzk.de/deu/projekt/pez/ezin.htm>

EZI-N ist mit den begrenzten Möglichkeiten der Mail-
Kommunikation gestaltet für eine nichtproportionale
Schrift (z.B. Courier) und eine Zeilenbreite von 60
Zeichen.

Die vollständige, unveränderte und nichtkommerzielle
Weitergabe von EZI-L ist gestattet. Ausschnitte nur
mit vollständiger Herkunftsbezeichnung. Alle sonstigen
Verwertungsrechte liegen bei PEZ.

Knud Böhle und Ulrich Riehm
Institut für Technikfolgenabschätzung
und Systemanalyse(ITAS)

Forschungszentrum Karlsruhe - Technik und Umwelt
Postfach 3640 76021 Karlsruhe
Tel.: +49 (0) 721 / 608 - 22989
Fax.: +49 (0) 721 / 608 - 24806
Mail: boehle@itas.fzk.de oder riehm@itas.fzk.de

WWW: <http://www.itas.fzk.de/deu/projekt/pez.htm>
[\[^ \]](#)

[\$ & \$]

Stand: 18.08.1998 - Kommentare und Bemerkungen an die
[Redaktion](#)