

Zusammenfassung

Die eMail, wie sie heute meist verwendet wird, entspricht rein technisch betrachtet etwa einer mit Bleistift geschriebenen Postkarte. Sie ist von jedem, der auf dem Transportweg Zugriff erlangen kann, zu lesen und eventuell auch zu verändern. Die Verschlüsselung und die elektronische Signatur haben uns als passende technische Lösung des Problems den Briefumschlag ermöglicht und warten auf ihren breiten Einsatz. Eine wichtige Voraussetzung für die wirkliche Vergleichbarkeit der elektronischen mit der herkömmlichen Post, ist aber auch die Nachweisbarkeit der Zustellung bzw. des Empfangs. Während die Rechtsprechung in einigen Fällen bereits das elektronische Postfach mit dem Pendant an der Hauswand gleichstellt hat, hinkt hier der zweifelsfreie Nachweis der Zustellung hinter her. Die nachfolgend beschriebenen Verfahren stellen Möglichkeiten dar, eine Reihe von Anscheinsbeweisen oder Indizien für die Zustellung einer eMail zu erzeugen. Abbildbar sind hier das „Einschreiben Einwurf“ und das „Einschreiben Rückschein“, nicht jedoch das „Einschreiben Eigenhändig“. Die Rechtsprechung müsste im Einzelfall entscheiden, wie die aus diesen Verfahren resultierenden Beweise zu bewerten sind.

1 eMail als Äquivalent zum herkömmlichen Brief

Das Internet mit seinen Diensten, das ursprünglich dem Militär und später der Wissenschaft vorbehalten war, versucht zunehmend Prozesse aus dem täglichen Leben und Arbeiten abzubilden. [NEU_00] Die Liste der Beispiele ist lang. Im vorliegenden Beitrag steht die eMail-Kommunikation als Äquivalent zur klassischen Postsendung im Zentrum.

1.1 Ausgangspunkt: Formen klassischer Postsendungen

Entsprechend der (Sicherheits-) Bedürfnisse und (Sicherheits-) Notwendigkeiten existieren bei der klassischen Postsendung verschiedene Formen, welche im vorliegenden Beitrag in drei Gruppen systematisiert werden: (1) die undokumentierte Zustellung, (2) die dokumentierte Zustellung und (3) die dokumentierte Zustellung und den dokumentierten Empfang. Die Postkarte und der klassische Brief zählen zur Kategorie der „undokumentierten Zustellung“. [DPO_04] Für die weiteren Betrachtungen ist es notwendig darauf hinzuweisen, dass die eigentliche Zustellung zwar undokumentiert erfolgt, dass aber der Brief und die Postkarte dann als zugegangen gelten, wenn sie in den Einflussbereich, sprich in den zur Empfängeradresse gehörenden Briefkasten gelangen. D.h. dass der Absender von einer Kenntnisnahme durch den Empfänger ausgehen kann. [STR_02] Das „Einschreiben Einwurf“ repräsentiert die Gruppe der „dokumentierten Zustellung“ in der Form, dass der Einwurf der Postsendung in den Briefkasten des Empfängers durch die Unterschrift des Zustellers dokumentiert ist. Eine „dokumentierte Zustellung“ kombiniert mit einem „dokumentierten Empfang“ wird ausschließlich durch die Formen Einschreiben, Einschreiben Rückschein und Einschreiben Eigenhändig gewährleistet, indem die Postsendung nur gegen Unterschrift an den Empfänger ausgehändigt wird. [DP_04]

1.2 Vergleich: elektronische und klassische Mailbox

Die zentrale Frage besteht nun darin, inwiefern die Formen der klassischen Postsendung nun auf die eMail-Kommunikations abgebildet werden können. Dies bedingt grundsätzlich, dass die eMail-Adresse als ein Äquivalent zur Postanschrift und, dass die Mailbox beim Provider als ein Äquivalent zum Briefkasten oder sonstiger physischer Empfangsvorrichtungen betrachtet werden kann. Beides ist der Fall, vorausgesetzt die bestimmte eMail-Adresse wurde beispielsweise von seiten eines Geschäftsmannes seinem Vertragspartner ausdrücklich als Korrespondenzadresse genannt. Die eMail gilt hierbei zu dem Zeitpunkt zugestellt, an dem gewöhnlicherweise mit „Leerung des

Briefkastens“ gerechnet werden kann. Bei Geschäftsleuten kann dies für den folgenden Vormittag erwartet werden. [STR_02]

Auf der Grundlage des letzten Absatzes, kann eine herkömmliche eMail unter bestimmten Voraussetzungen als zugestellt betrachtet werden, wenn sie das Postfach des Empfängers erreicht hat, wobei die Zustellung undokumentiert erfolgt.

1.3 Einsatzgebiete

Der herkömmliche Brief ist durch die klassische eMail im Internet bereits abgebildet. Die Frage ist: Gibt es Verfahren und Systeme, die eine dokumentierte Zustellung (wie etwa „Einschreiben Einwurf“ oder stärker Formen wie „Einschreiben Eigenhändig“) im eMail-Verkehr ermöglichen? Die Bestrebungen der Verwaltungen (G2C, G2B), die unter dem Stichwort „papierlose Behörde“ geführt werden, zeigen deutlich Einsatzgebiete für eine eMail im Sinne eines Einschreibens, d.h. die Notwendigkeit einer dokumentierten, nachweisbaren Zustellung oder gar eines dokumentierten Empfangs.

Diese Sicherheitsanforderung wird als Verbindlichkeit von Transaktionen (non repudiation) bezeichnet. [RAE_98] Während diese Forderung für den verbindlichen Versand bereits durch die elektronische Signatur erfüllt ist, gab es für den nichtabstreitbaren Empfang bisher keine Verfahren. Das Vorweisen eines Sendeprotokolls allein, erbringt nicht den Anscheinsbeweis für den Zugang. [HOE_02]

Einsatzfelder für einen dokumentierten Zustellungs- oder Empfangsvorgang lassen sich auch im Rahmen des elektronischen Geschäftsverkehrs finden (B2C): Man denke an den zunehmend an Bedeutung gewinnenden Bereich des Paid Content [IWW_03], d.h. der kostenpflichtigen digitalen Güter, deren Bezahlung meistens mittels Kreditkarte erfolgt (post-paid). In einem möglichen Szenario wäre es denkbar, dass der Käufer den Empfang des Content leugnet und die Belastung seiner Kreditkarte storniert. Ein weiteres mögliches Einsatzgebiet könnte bei dem Vorgang der Übermittlung von digitalen prepaid-Münzen beispielsweise innerhalb einer Peer-to-Peer-Transaktion liegen. [BET_99] Das „eCash-System“ der Deutschen Bank AG, (welches leider 2001 vom Markt genommen wurde) sah diesen Vorgang mittels eMail vor. [SHF_02] In Zukunft könnten solche Verfahren wieder an Bedeutung gewinnen. [KRE_01] In beiden Fällen wäre es für den Absender von Vorteil in einer Streitsituation den Empfang oder zumindest die Zustellung dokumentiert zu wissen.

2 Mögliche Lösungsansätze/Verfahren und Systeme

2.1 Einfache Lese- oder Empfangsbestätigung

Oberflächlich betrachtet, lässt sich die einfache Lese- oder Empfangsbestätigung in die Kategorie „Einschreiben mit Rückschein“ einordnen. Der Absender kann mittels des „Disposition-Notification-To-Header“ den UA (User Agent) des Empfängers zum Versenden einer Lesebestätigung auffordern. Diese Lesebestätigung ist jedoch optional und sollte auch nur nach ausdrücklicher Bestätigung durch den Empfänger abgesandt werden. [FAJ_98]

Vorteile:

- Das Verfahren ist in beinahe jedem verfügbaren UA implementiert. D.h. die technischen Voraussetzungen sind weitverbreitet.

Nachteile:

- Der Versand der Bestätigung ist optional; man kann dies nicht erzwingen. Es setzt die Kooperation des Empfängers voraus.
- Da solche Lesebestätigungen in der Regel keine elektronische Signatur tragen, sind sie als Anscheinsbeweis für den Empfang einer eMail leicht zu erschüttern. Eine solche Lesebestätigung kann sich der (vermeintliche) Absender mit geringem Aufwand selbst erstellen

bzw. bereits eingegangene Lesebestätigungen zu seinen Gunsten (z.B. Datum und Uhrzeit) verändern.

Eine solche Lesebestätigung könnte durchaus als Zustell- bzw. Empfangsnachweis gelten, sofern sie eine fortgeschrittene elektronische, vielleicht sogar eine qualifizierte Signatur trägt. Um den Erfordernissen eines klassischen „Einschreibens mit Rückschein“ zu genügen, dürfte die Mail jedoch ohne das vorherige Absenden der Lesebestätigung (dann eigentlich Empfangsbestätigung) nicht geöffnet werden können.

2.2 Zustellbestätigungen (DSN)

Eine Kooperation des Empfängers ist nicht erforderlich, wenn die Bestätigung für die Zustellung der eMail in das Postfach des Empfängers mittels DSN (Delivery Status Notification) erfolgt. Diese Benachrichtigungen werden auf Anfrage durch den für das Postfach verantwortlichen MTA (Message Transfer Agent) generiert, sofern dieser den Versand von DSNs unterstützt. [MOO_96a] Beispiele für das Beauftragen von DSNs:

R: „Remote“ S: „Sender“

```
R: 220 Pure-Heart.ORG SMTP server here
S: EHLO Pure-Heart.ORG
R: 250-Pure-Heart.ORG
R: 250-DSN
R: 250 SIZE
S: MAIL FROM:<Alice@Pure-Heart.ORG> RET=HDRS ENVID=QQ314159
R: 250 <Alice@Pure-Heart.ORG> sender ok
S: RCPT TO:<Bob@Big-Bucks.COM> NOTIFY=SUCCESS,DELAY ORCPT=rfc822;Bob@Big-
Bucks.COM
R: 250 <Bob@Big-Bucks.COM> recipient ok
S: RCPT TO:<Carol@Ivory.EDU> NOTIFY=FAILURE ORCPT=rfc822;Carol@Ivory.EDU
R: 250 <Carol@Ivory.EDU> recipient ok
S:RCPT TO:<Dana@Ivory.EDU> NOTIFY=SUCCESS,FAILURE
ORCPT=rfc822;Dana@Ivory.EDU
R: 250 <Eric@Bombs.AF.MIL> recipient ok
S: RCPT TO:<Fred@Bombs.AF.MIL> NOTIFY=NEVER
R: 250 <Fred@Bombs.AF.MIL> recipient ok
```

Listing 1 aus [ASS_01]

Diese Benachrichtigung bestätigt den „Einwurf“ in das Postfach nicht jedoch das Abrufen der eMail.

Vorteile:

- Das Verfahren erfordert keine Kooperation des Empfängers.
- Es dokumentiert die tatsächliche Speicherung der eMail in das Postfach des Empfängers.

Nachteile:

- nicht alle MTAs unterstützen DSNs für erfolgreiche Zustellungen - eigene Untersuchungen ergaben eine Quote von etwa 54%
- die Bestätigungsmail enthält einen Null-Absender [MOO_96a]
- unsigniert, fälschbar, veränderbar (siehe Lesebestätigung)

Die Anforderung einer solchen Benachrichtigung ist bisher auch nur in wenigen UAs implementiert. Hier gibt es meist nur Unterstützung für die klassische Lesebestätigung.

2.3 Treuhändische Zwischenspeicherung und Abholung

Wesentlich sicherer in Bezug auf die Beweiskraft sind die Verfahren bei denen die Entgegennahme und Zustellung von eMails mit einer von einer dritten Stelle digital signierten Bestätigungsmail

dokumentiert wird. Solche Treuhandverfahren nehmen die eMail vom Absender entgegen, speichern diese zwischen und setzen den Empfänger per eMail in Kenntnis, dass im Treuhand-Mail-System eine Nachricht für ihn hinterlegt worden ist. In dieser eMail werden die zum Abruf der Nachricht benötigten Zugangsdaten hinterlegt oder mit dem Empfänger vorher vereinbart (letzteres erfordert die [unwahrscheinliche] Registrierung durch den Empfänger). Ruft der Empfänger die für ihn zwischen gespeicherte eMail mit Hilfe dieser Zugangsdaten ab, wird dieser Vorgang dem Absender bestätigt. Je nach Anbieter kann der Absender somit eine Bestätigung für das Absenden, die Benachrichtigung des Empfängers als auch für das letztendliche Abrufen der eMail erhalten. Diese Bestätigungen können durch den Treuhänder elektronisch signiert sein.

Vorteile:

- Die Zustellung der eMail wird durch einen unparteiischen Dritten bezeugt.
- Es gibt für den Empfänger keine Möglichkeit die Nachricht zu lesen, ohne das der Empfänger benachrichtigt wird.
- Das Verfahren stellt keinerlei erweiterte Anforderungen an den Nutzer als der gewöhnliche eMail-Verkehr.

Nachteile:

- Es handelt sich dabei um kommerzielle Anbieter, d.h. das Verfahren ist meist kostenpflichtig.
- Die Kooperation des Empfängers bei jeder einzelnen Nachricht muss vorausgesetzt werden.
- Der Empfang der Benachrichtigung über die neue eMail kann der Empfänger genauso bestreiten.
- Der Inhalt der Benachrichtigungsmail ist unverschlüsselt, d.h. die zum Abruf der eMail erforderlichen Zugangsdaten könnten von Dritten gelesen werden, um diese dann selbst für das Herunterladen und lesen der Nachricht zu verwenden. In diesem Fall erhält der Absender eine Bestätigung, obwohl der eigentliche Empfänger die Nachricht nicht zwangsläufig selbst abgerufen hat.

Einordnung: Einschreiben mit Rückschein.

2.4 Durchleitung und Protokollierung

2.4.1 Protokollierung der Übertragung

Ein weiterer Ansatz wäre die fortlaufende Protokollierung des gesamten Weges, den eine eMail vom Absender bis zum Empfänger nimmt. Dabei kann sowohl die Entgegennahme der eMail vom Absender durch den ersten MTA als auch die Weiterleitung an den als MX-Eintrag gelisteten MTA der Empfängeradresse aufgezeichnet werden. Der Absender erhält dabei eine Bestätigung über den Zeitpunkt des Absendens, den Zeitpunkt der Weiterleitung, einen Mitschnitt des Handshakes zwischen den beteiligten Mail-Servern sowie eine Kopie seiner Nachricht in einer fortgeschritten elektronisch signierten eMail. Der Absender wählt dabei einen entsprechenden MTA (der eine solche Bestätigung ermöglicht) als seinen Postausgangs-Server aus.

2.4.2 Zusätzliche Sicherheit durch VRFY und DSN

Bei dem oben genannten Verfahren ist im Einzelfall nicht sichergestellt, dass die Entgegennahme der eMail, durch den als MX-Eintrag gelisteten MTA, tatsächlich dem Einwurf in das Postfach des Empfängers entspricht. Dies ist z.B. dann der Fall, wenn der MTA nicht überprüfen kann, ob das (angesprochene) Postfach tatsächlich existiert. Um das Verfahren abzusichern, kann hier auf das VRFY (Verify) Kommando des SMTP-Protokolls zurückgegriffen werden. Die Anwendung des Befehls innerhalb der SMTP-Session kann die Existenz des Nutzers prüfen:

Example of Verifying a User Name

Either

```
S: VRFY Smith
R: 250 Fred Smith <Smith@USC-ISIF.ARPA>
```

Or

```
S: VRFY Smith
R: 251 User not local; will forward to <Smith@USC-ISIQ.ARPA>
```

Or

```
S: VRFY Jones
R: 550 String does not match anything.
```

Or

```
S: VRFY Jones
R: 551 User not local; please try <Jones@USC-ISIQ.ARPA>
```

Or

```
S: VRFY Gourzenkyinplatz
R: 553 User ambiguous.
```

Listing 2: Auszug aus [POS_82]

Zusätzlich wird in [KLE_01] der Returncode 252 (Cannot VRFY user, but will accept message and attempt delivery) definiert, der beispielsweise dann zurückgegeben werden soll, wenn die Echtheit der Adresse nicht überprüft werden kann, der Mailserver die Nachricht aber dennoch entgegen nehmen würde. Etwa 28% der in Deutschland befindlichen SMTP-Server unterstützen das Kommando „VRFY“. Aus Sicherheitsgründen wird diese Funktion jedoch gern zusammen mit dem „EXPN“ (Expand) Befehl deaktiviert, um möglichst wenig Informationen über die lokalen Mailboxen oder Mailinglisten preiszugeben [KLE_01]. Weitere Sicherheit können die unter 2.2. behandelten DSNs ermöglichen. Abweichend ist hier jedoch ein Verfahren zu verwenden, welches nicht standardisiert ist. In diesem Fall fügt der protokollierende (erste) MTA einen Return-Receipt-To-Header (vgl. [MOO_96b] und [PAL_97]) in die Nachricht ein und veranlaßt damit den letzten MTA zur Erzeugung einer Zustellbestätigung, die jedoch nicht an den Absender, sondern an ein zum System des ersten (protokollierenden) MTA gehörenden Empfänger geschickt wird. Die Empfängeradresse für diese DSN wird dabei für jede weitergeleitete eMail dynamisch generiert. Auf diese Weise kann die eingehende Bestätigung einer zuvor weitergeleiteten eMail zugeordnet werden, ohne dass der Absender diese DSN von sich aus in das System injizieren kann (er kennt den zu seiner eMail dynamisch generierten Empfänger für die DSN nicht, es sei denn er hört die Kommunikation zwischen MTA 1 und MX-Eintrag ab). Das Versenden von Zustellbestätigungen an Empfänger, die nicht dem ursprünglichen Absender entsprechen, ist jedoch (wenn auch nach [MOO_96b] verbreitet verwendet) nicht standardisiert.

2.4.3 Protokollierung des Lesevorgangs

Zusätzlich ist es denkbar, eine im HTML-Format generierte eMail mit einem versteckten externen Link auf eine „blinde“ Imagesource zu versehen, wobei der Aufruf dieses Bildes ebenfalls dynamisch durch den ersten MTA generiert wird. Der Link verweist auf einen Webserver, der ebenfalls zum System des protokollierenden MTA gehört und ist der jeweils weitergeleiteten eMail zugeordnet. Beispiel für einen solchen Link:

```
<html>
<body>
Text der eMail (Mahnbescheid etc ...)
<!--versteckter Link: //-->

</body>
</html>
```

Beim Öffnen der eMail durch den Empfänger wäre es dadurch möglich, den http-request zum Laden der eingefügten Image-Source zu protokollieren und damit das Öffnen der eMail nachzuweisen.

2.4.4 Bestätigungen an den Absender

Der Absender kann bei der Nutzung dieses Verfahrens im Idealfall folgende Bestätigungen erhalten:

- Die Übermittlung der eMail an den protokollierenden MTA sowie das Handshake-Protokoll der Weiterleitung an den als MX-Eintrag der Empfängeradresse gelisteten MTA, nebst genauer Zeit und Inhalt seiner eMail.
- Den Eingang der DSN vom für das Postfach des Empfängers verantwortlichen MTA.
- Das Öffnen der eMail durch den Aufruf des versteckten Link.
- Alle diese Bestätigungsmails können fortgeschritten elektronisch signiert sein.

2.4.5 Bewertung

Vorteile:

- Es ist keine Kooperation des Empfängers notwendig.
- Die Zustellung und das Lesen (2.4.3) der eMail wird durch einen unparteiischen Dritten bezeugt.
- Das Verfahren stellt keinerlei erweiterte Anforderungen an den Nutzer als der gewöhnliche eMail-Verkehr.

Nachteile / Einschränkungen:

Allgemein:

- Das Verfahren benötigt einen unabhängigen Dritten als Betreiber und kann daher kostenpflichtig sein.

1. Variante:

- Die Bestätigung der erfolgreichen Weiterleitung an den MX-Eintrag des Empfängers stellt im Einzelfall nicht sicher, dass die eMail tatsächlich im Postfach des Empfängers gespeichert wurde. Hier ist beim Bestreiten zu untersuchen, ob der nächste Mail-Server sich bereits im Einflussbereich des Empfängers befindet oder in welchen Fällen ein „Einwurf“ in das Postfach des Empfängers letztendlich fehlgeschlagen sein könnte.

2. Variante:

- Wie bereits unter 2.2 erwähnt, unterstützen nicht alle MTAs das Versenden von DSNs oder den Befehl „VRFY“. Dies bedeutet, dass eine solche Bestätigung ausbleiben kann, was jedoch nicht das Versagen der Zustellung an den Empfänger impliziert. Zudem ist das hier verwendete Verfahren vom Standard abweichend.

3. Variante:

- Der Aufruf des versteckten Links allein reicht nicht aus, um das Öffnen der Mail durch den intendierten Empfänger beweisen zu wollen, da dies ebenfalls durch mitlesende Dritte geschehen kann.

3 Vorstellung eines Prototypen

SLITE IT-Security betreibt für das unter 2.4.1 vorgestellte Verfahren einen Prototypen. Es ist in naher Zukunft eine Erweiterung um die Funktionen aus 2.4.2 und eventuell 2.4.3 geplant, um die Aussagefähigkeit der Bestätigungsmail zu erhöhen. Das System „Mail-Evidence“ steht derzeit für jeden, der sich einmalig registriert, zum Test offen. Derzeit werden nur maximal 20 KB große eMails mit maximal einem Empfänger pro Nachricht unterstützt. Das System ermöglicht die SSL verschlüsselte Übertragung von Nachrichten bis zum nächsten MTA (MX-Eintrag der Empfängerdomain). Das Absenden einer Nachricht erfordert die Übermittlung von Nutzernamen und

Passwort (wird bei der Registrierung vergeben), um Missbrauch auszuschließen. Der Absender erhält nach Weiterleitung seiner eMail eine Bestätigungsmail, welche das Protokoll der Sitzung mit dem Mailserver des Empfängers sowie eine Kopie seiner originalen eMail enthält. Diese Bestätigung ist insgesamt mit GPG Signatur versehen und kann als Einlieferungsbeleg, Inhaltsbezeugung und (eventuell) als Zustellnachweis gelten.

4 Diskussion des Verfahrens

4.1 Verwendung von GPG oder anderen Signaturverfahren

Die Verwendung der elektronischen Signatur für die Bestätigungsmails stellt sicher, dass der vermeintliche Absender sich seinen Rückschein oder Einlieferungsbeleg nicht selbst erstellt oder abändert. Die hohen Anforderungen der Signaturverordnung schließen jedoch weitgehend die Verwendung der qualifizierten elektronischen Signatur aus. Nach europäischer Signaturrechtlinie (1999/93/EG) ist jedoch festgelegt, dass eine elektronische Signatur nicht nur allein deshalb als unwirksames Beweismittel erklärt werden kann, weil es sich nicht um eine qualifizierte Signatur handelt. Das vorgestellte Verfahren setzt für die Unterzeichnung der Bestätigungsmails GPG (GNU Privacy Guard) ein, welches eine fortgeschrittene elektronische Signatur ohne PKI erstellen kann [BKS_02].

4.2 Web Bugs als Lesenachweis?

Kontrovers zu diskutieren, ist sicher die Methode, über sogenannte Web Bugs eine Lesebestätigung zu erzwingen. Üblicher Weise werden diese versteckten Images in SPAM dafür verwendet, die Echtheit von eMail Adressen zu prüfen, die Wirkung von bestimmten Werbebotschaften zu analysieren und um festzustellen, wer auf eine Werbe-eMail reagiert und ob bzw. nach welcher Zeit er die beworbene Webseite besucht [ROT_99]. Der Zweck, für den diese Methode hier eingesetzt werden soll, greift sicher weniger in die Privatsphäre ein, als dies bei den zu SPAM-Zwecken benutzten Web Bugs der Fall ist. Dennoch besteht auch hier die Gefahr des Missbrauchs, da es nicht nur möglich ist herauszufinden, ob die eMail gelesen wurde, sondern auch wann, wie oft und mit welchem eMail-Programm.

Abkürzungen

B2B	Business to Business
B2C	Business to Consumer
DSN	Delivery Status Notification (Benachrichtigung über den Zustellstatus)
G2B	Government to Business
G2C	Government to Citizen
GPG	GNU Privacy Guard, ein Verschlüsselungsprogramm nach dem OpenPGP Standard
HTML	Hypertext Markup Language, eine Beschreibungssprache zum Erstellen von Dokumenten für das WWW
HTTP	Hypertext Transfer Protocol, Protokoll zum Übertragen von Webseiten u.a. Daten im WWW
KB	K-Byte, 1024 Byte = 8192 Bit
MTA	Message Transfer Agent (hier: ein Mailserver im Internet)
MX	Mail Exchanger, Adresse des für eine Domain zuständigen Mailservers
PKI	Public Key Infrastructure, Hierarchisches System von Zertifizierungsstellen für Signaturzertifikate
SPAM	Stupid Person's Advertisements, Unerwünschte Wurfungen als eMail
SMTP	Simple Mail Transfer Protocol, Protokoll zum Versenden von eMail
SSL	Secure Socket Layer, Verschlüsselungstechnologie
UA	User Agent, der eMail Client des Anwenders
WWW	World Wide Web, Dienst im Internet zur Anzeige und Verknüpfung von HTML Dokumenten

Literatur

- [ASS_01] Aßmann, C. (2001). How to get notified when an e-mail has been read/delivered? Unter: <http://www.sendmail.org/~ca/email/dsn.html> (abgerufen am 21.01.2004).
- [BET_99] Betz, S. (1999). Einweg-Token-Systeme am Beispiel des Ecash-Verfahrens von DigiCash. In: Thießen, F. (Hrsg.) (1999). Bezahlsysteme im Internet. Frankfurt, am Main. S. 179.
- [BKS_02] Baier, H; Klink, J; Straub, T. (2002). Digitale Signatur. Leitfaden zum Einsatz digitaler Signaturen. In: Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung. (Hrsg.) (2002). hessen-media Band 42. Wiesbaden. S. 24.
- [DPO_04] Deutsche Post AG. (2004). EINSCHREIBEN Unter: http://www.deutschepost.de/download/broschueren/Handling_Einschreiben.pdf (abgerufen am 20.01.2004)
- [FAJ_98] Fajman, R. (1998). An Extensible Message Format for Message Disposition Notifications. RFC 2298. S. 3-6
- [HOE_02] Hoeren, T. (2002). Grundzüge des Internetrechts. München. S 201.
- [IWW_03] Institut für Wirtschaftspolitik und Wirtschaftsforschung der Universität Karlsruhe – IWW (2003). Internet-Zahlungssysteme aus Sicht der Verbraucher. Ergebnisse der Online-Umfrage IZV6.
- [KLE_01] Klensin, J. (2001). Simple Mail Transfer Protocol. RFC 2821. S. 22
- [KRE_01] Krempl, S. (2001). eCash und Co: Das waren Kopfgeburten. Unter: <http://heise.de/tp/deutsch/inhalt/te/7477/1.html> (abgerufen am 15.01.2004)
- [NEU_00] Neumann, D. (2000). Die Rechtsnatur des Netzgeldes. Internetzahlungsmittel ecashTM. München. S. 5-8.
- [MOO_96a] Moore, K. (1996). SMTP Service Extension for Delivery Status Notifications. RFC 1891.
- [MOO_96b] Moore, K. (1996). An Extensible Message Format for Delivery Status Notifications. RFC 1894. S. 24
- [PAL_97] Palme, J. (1997). Common Internet Message Headers. RFC 2076. Anh. A
- [POS_82] Postel, J.B. (1982). Simple Mail Transfer Protocol. RFC 821. S. 9
- [RAE_98] Raeppele, M. (1998). Sicherheitskonzepte für das Internet. Heidelberg. S 5-7.
- [ROT_99] Rötzer, F. (1999). Nach den Cookies die Web Bugs. Unter: <http://www.heise.de/tp/deutsch/inhalt/te/5482/1.html>. (abgerufen am 15.01.2004)
- [SHF_02] Stroborn, K; Heitmann, A.; Frank, G. (2002). Internet-Zahlungssysteme in Deutschland: ein Überblick. In: Ketterer, K.-H.; Stroborn, K. (2002). Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven. Köln. S. 35
- [STR_02] Strömer, T.H. (2002). Online-Recht. Rechtsfragen im Internet. Heidelberg. S. 133-134