Adrian Rufener

Sicherer Mailverkehr: eine Frage der Professionalität

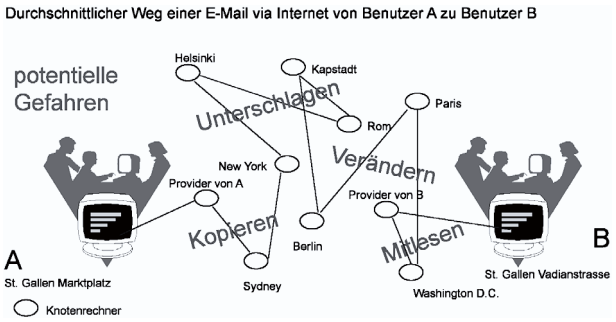
Stichworte : sicher kommunizieren, sicherer Mailverkehr, digitale Signatur, Verschlüsselung

I. Ausgangslage

Der zunehmende Einsatz moderner Kommunikationsmittel im Kanzleialltag sowie in unserer Gesellschaft hat dazu geführt, dass immer mehr Daten auf elektronischem Weg, insbesondere per E-Mail, SMS oder MMS übermittelt werden. Die elektronische Post hat der Informationsgesellschaft bedeutende Impulse und Produktivitätsvorteile gebracht. Sie ist praktisch, schnell, und fast jeder ist damit erreichbar. Ob Verträge, Strategiepläne oder persönliche Dokumente: In Windeseile erhalten Kunden oder Geschäftspartner Informationen mit elektronischer Post. Die Datenübertragung per E-Mail erfolgt heute in aller Regel ohne entsprechende Sicherheitsvorkehrungen. Die Mails werden im Klartext versandt, d.h. bildlich gesprochen werden elektronische Ansichtskarten vermailt.

II. Risiken des E-Mail-Verkehrs

Ein wesentlicher Unterschied zwischen dem elektronischen Versand von Daten und dem herkömmlichen Versand per Post besteht darin, dass der Absender elektronischer Mitteilungen im Voraus nicht weiss, welchen Weg seine «Post» nehmen wird. Vermeintlich «lokaler» und «nationaler» E-Mail-Verkehr wird sehr oft international abgewickelt, d.h. ein E-Mail von einem Absender in St. Gallen (Marktplatz) an einen Empfänger in St. Gallen (Vadianstrasse) kann durchaus über einen oder mehrere im Ausland (auch in Übersee) stehende Mailserver geleitet werden. Sodann können verschiedenste Transporteure (Provider) involviert sein. Die Provider sind aufgrund gesetzlicher Bestimmungen, die im europäischen Raum in etwa gleich sind, verpflichtet, den – auch bloss durchlaufenden – Mailverkehr während der Dauer von mindestens 6 Monaten[1] zu speichern. Aus Kostengründen und weil technisch einfacher, werden nicht bloss die gesetzlich vorgeschriebenen sogenannten Header-Daten gespeichert, aus welchen hervorgeht, wer mit wem gemailt hat, sondern die vollständigen E-Mails samt Anhängen.



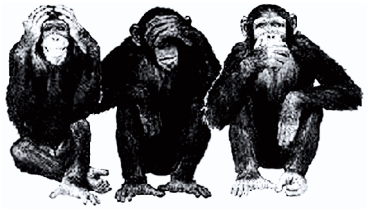
In technischer Hinsicht besteht die Möglichkeit, mit geringem Aufwand den E-Mail-Verkehr (ausserhalb abgeschotteter Firmengrenzen) nach Informationen zu durchsuchen. Dass sich das Durchforsten des Mailverkehrs bzw. des Internets für Kriminelle wirtschaftlich lohnen kann, haben die bekannt gewordenen Attacken auf Server, welche Kreditkarteninformationen enthielten, gezeigt.[2] Aus dem Gesagten und der vorstehenden Grafik folgt, dass nicht geschützte Mails sowohl in Bezug auf den Absender und den Inhalt verändert werden können, die Vertraulichkeit nicht gewahrt ist und zudem die Zustellung des Mails verhindert werden kann. Aus dem Bericht des Europäischen Parlamentes zum Abhörsystem «Echelon» vom Juli 2001[3] geht hervor, dass der Mailverkehr auch von Staaten systematisch durchsucht wird und unter anderem Industriespionage zugunsten der eigenen Industrie betrieben wird. Im Bericht wird deshalb empfohlen, den Mailverkehr zu schützen.

III. Disclaimer als Problemlösung?

In der Praxis behelfen sich die Unternehmen und wir Anwälte oft mit dem Anbringen von «Disclaimern» (Enthaftungserklärungen). Solche Erklärungen können allenfalls dazu dienen, das Unbehagen des Absenders beim Versand vertraulicher Informatio-

1 Vgl. die Regelungen im BÜPF (SR 780.1).
2 Auch die UBS/Birkenfeld Affäre beruht auf abgehörten/gelesenen E-Mails/Faxen und SMS von Birkenfeld.
3 Bericht vom 11. Juli 2001 über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) [2001/2098 (INI)]; A5–0264/2001.

nen zu vermindern und sich vor allfälligen strafrechtlichen Sanktionen und der Geltendmachung zivilrechtlicher Ansprüche zu schützen. Mit dem Anbringen von Disclaimern wird jedoch der Inhalt der elektronischen Post weder vertraulicher (immer noch Versand im Klartext) noch wird sichergestellt, dass Unbefugte keine Kenntnis vom Mailinhalt erhalten und diese Kenntnisse verwenden.



Disclaimer:

Wir machen Sie darauf aufmerksam, dass der E-Mail-Verkehr grundsätzlich nicht sicher ist. Die Integrität und Vertraulichkeit der Informationen, die über E-Mail versendet werden, sind zu keiner Zeit gewährleistet. Wir lehnen daher jegliche Haftung für Schäden ab, die aus der Verwendung des E-Mail-Verkehrs entstehen können. Die in diesem E-Mail enthaltenen Informationen sind für den exklusiven Gebrauch durch den Empfänger bestimmt und möglicherweise vertraulich. Alle Personen die dieses E-Mail erhalten, aber nicht Empfänger oder Mitarbeiter des Empfängers sind, werden informiert, dass die Benutzung sowie die Veröffentlichung, Reproduktion oder das Weiterleiten dieser Information untersagt ist. Wenn Sie dieses E-Mail aufgrund eines Fehlers erhalten haben, bitten wir Sie, uns dies per Mail oder telefonisch so schnell wie möglich mitzuteilen und das Mail zu löschen.
Herzlichen Dank

This message is being sent by or on behalf of a lawyer; it is intended for the exclusive use of the individual or entity that is the named addressee and may contain information that is privileged or confidential or otherwise legally exempt from disclosure. If you are not the named addressee, you are not authorised to print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify us immediately by e-mail, discard any paper copies and delete all electronic files of the message.

IV. Absicherung des Mailverkehrs mit technischen Mitteln

Die dargelegten Sicherheitsrisiken führen zur Erkenntnis, dass schützenswerte Informationen durch einen vom Absender bis zum Empfänger durchgehenden, vom Zugriff durch unbefugte Personen geschützten Prozess abgesichert werden sollten. Zur schützenswerten Kommunikation zählen etwa die Vorbereitung und Abwicklung eines Rechtsgeschäftes (z.B. Unternehmenskauf bzw. Verkauf), der Austausch von Geschäftsgeheimnissen, die Übermittlung von Finanzinformationen oder kursrelevanten Informationen sowie von Personaldaten wie z.B. Lohndaten an Versicherungsgesellschaften. Dabei gibt es keinen Unterschied zwischen einzelnen Berufsgeheimnisträgern und Unternehmen. Dies gilt namentlich für uns Anwälte. Meines Erachtens mutet es sehr seltsam an, wenn wir grossen Wert auf unser Berufsgeheimnis legen und gleichzeitig unsere Kunden verpflichten wollen (ausdrücklich oder stillschweigend), in ungeschützten Mailverkehr einzuwilligen. Niemand von unserem Berufsstand käme auf die Idee unseren Kunden zu erklären, dass wir Geschäftsbriefe nicht in einen Briefumschlag stecken, sondern als Postkarte versenden. So wie wir Briefe in Couverts verpacken, muss es auch zumutbar sein, Mails mittels geeigneter technischer Hilfsmittel zu schützen.

Der Mailverkehr kann im Wesentlichen mit zwei Vorgehensweisen sicherer ausgestaltet werden. Einerseits können sogenannte digitale Signaturen zum Signieren/Verschlüsseln von Mails verwendet werden. Anderseits besteht die Möglichkeit, den Mailverkehr über eine sogenannte Secure E-Mail-Plattform abzuwickeln.

1. Signieren/Verschlüsseln von E-Mails mit digitalen Signaturen (auf Stufe Benutzer)

Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder der Identität des Absenders. Elektronische Signaturen werden wie Identitätskarten oder Reisepässe von vertrauenswürdigen Dritten[4] verwaltet und ausgegeben, den sogenannten Anbieterinnen von Zertifizierungsdiensten (in der Schweiz derzeit: Swisscom Solutions AG, SwissSign AG [Schweizerische Post], QuoVadis Trustlink Schweiz AG, Bundesamt für Informatik)[5]. Dabei ist der Identifikationsprozess zur Erlangung der digitalen Signatur mit demjenigen zur Ausstellung einer Identitätskarte vergleichbar. Die rechtlichen Grundlagen zur Ausstellung von digitalen Signaturen (elektronische Identitäten) enthält das Bundesgesetz über die elektronische Signatur (ZertES)[6]. Zertifikate nach Art. 2 ZertES (fortgeschrittene elektronische Signaturen) erfüllen folgende Anforderungen (mehr zum Thema digitale Signaturen unter: *www.quovadisglobal.ch* oder *www.swisssign.ch*):

1. Sie sind ausschliesslich der Inhaberin oder dem Inhaber zugeordnet.
2. Sie ermöglichen die Identifizierung der Inhaberin oder des Inhabers.
3. Sie werden mit Mitteln erzeugt, welche die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann.
4. Sie werden mit den Daten, auf die sie sich beziehen, so verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Mit einem fortgeschrittenen elektronischen Zertifikat können E-Mails signiert und/oder verschlüsselt werden. Das Signieren

4 «Certificate Authority» = «CA».
5 Vgl. *http://www.seco.admin.ch/sas/00 229/00 251/index.html?lang=de.*
6 SR 943.03.

funktioniert auch, wenn der Empfänger über kein Zertifikat verfügt; um ein E-Mail zu entschlüsseln, muss auch der Empfänger über ein Zertifikat verfügen. Die gängigen E-Mail-Programme erleichtern den Nutzern das Signieren bzw. Verschlüsseln durch entsprechende Schaltflächen und Symbole.

		
Schaltflächen in Outlook 2003 «Nachricht digital signieren»/«Nachrichten und Anlagen verschlüsseln»	Signiersiegel im empfangenen E-Mail	Verschlüsselungssiegel im versandten E-Mail

Die Vorteile der Verwendung von fortgeschrittenen digitalen Zertifikaten besteht darin, dass das E-Mail samt Inhalt «End-to-End» verschlüsselt ist, d.h. der Mailinhalt (inkl. Anhänge) auf dem gesamten Transportweg vom Absender bis zum Empfänger von Dritten nicht eingesehen werden kann. Um das verschlüsselte E-Mail zu öffnen, benötigt sowohl der Absender als auch der Empfänger einen USB-Token. Dieses Gerät sieht aus wie ein Memory-Stick und hat die Funktion eines Tresorschlüssels. Der Nutzer muss das/den USB-Token im PC einstecken und sich dann mit einem PIN-Code authentifizieren – analog zur Zahlenkombination eines Tresors.

Der Nachteil der Mailverschlüsselung mit digitalen Zertifikaten besteht darin, dass sowohl der Absender als auch der Empfänger über digitale Zertifikate verfügen müssen. Ein weiterer Nachteil besteht darin, dass der Mailverkehr bis ins Mailprogramm des Empfängers verschlüsselt ist und verschlüsselte Mails immer nur mit dem digitalen Zertifikat des Inhabers des Mailkontos geöffnet werden können. Dies gilt beispielsweise auch für verschlüsselte Mails, welche in der Mandatsverwaltungssoftware abgelegt werden. Zudem wird normalerweise ein Serverseitiges Filtern gegen Viren oder Spam verunmöglicht. Insbesondere höherwertige Verschlüsselungszertifikatslösungen erlauben es nicht private Entschlüsselungs-Schlüssel aus dem USB-Token zu extrahieren. Kanzlei interne Stellvertretungsprozesse zur Wahrung von Fristen (z.B. bei Krankheit oder Militärdienstabwesenheiten) werden dadurch stark beeinträchtigt bzw. bedingen oft die Weitergabe des Tokens inkl. des Passwortes für den Entschlüsselungs-Schlüssel, was üblicherweise einen Verstoss gegen die AGB's der CA darstellt und CA seitige Haftungsgarantien erlöschen lässt.

Dieser Lösungsansatz ist höchstens für den Einsatz in ganz kleinen Anwaltskanzleien zu empfehlen, wo der Nutzerkreis auf einen Anwalt und allenfalls eine Sekretärin beschränkt ist. Sobald mehrere Personen auf E-Mails zugreifen müssen, ist eine Signatur/Verschlüsselung auf Stufe Benutzer nicht zu empfehlen. Eine weitere Schwierigkeit liegt darin, dass Privatklienten und KMUs die technischen Voraussetzungen für einen sicheren Mailverkehr oft nicht haben.

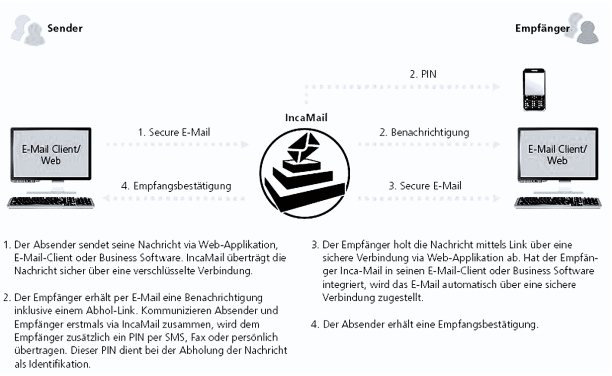
2. Signieren/Verschlüsseln von E-Mails mit digitalen Signaturen (auf Stufe Unternehmen)

Zur Optimierung der Abläufe sollte deshalb in grösseren Kanzleien (und anderen Unternehmen) der Verschlüsselungs- bzw. Entschlüsselungsprozess nicht individuell auf Stufe des einzelnen Mitarbeiters sondern zentral auf Stufe des Mailservers erfolgen. Intern stehen die Mails immer im Klartext zur Verfügung – was natürlich einen entsprechenden technischen Schutz der unternehmensinternen Kommunikationsinfrastruktur gegen das Eindringen von aussen erfordert. E-Mails, welche die Unternehmenssphäre verlassen, sind dagegen gesichert. Auf dem Markt sind diverse Lösungen verfügbar, welche diese Funktionalität aufweisen [z.B. Totemo *(www.totemo.ch)*, SEPPmail (www.seppmail.ch), PGP Universal Gateway Email *(www.pgp.com)*, Zertificon *(www.zertificon.de)*, etc.]. Die Funktionsweise der erwähnten Softwarelösungen ist mehr oder weniger identisch: Die versendeten Mails verbleiben solange im Herrschaftsbereich der Kanzlei, als sie der Mailempfänger noch nicht abgeholt hat oder der Appliance kein Verschlüsselungs-Zertifikat des Empfängers bekannt ist. Zur Abholung bzw. zum Empfang stehen dem Mailempfänger verschiedene Möglichkeiten offen. Beispielsweise können die E-Mails mit einer digitalen Signatur verschlüsselt übermittelt werden, es kann ein verschlüsseltes PDF als Anhang eines (nicht notwendigerweise verschlüsselten) E-Mails versandt werden, oder der Empfänger kann über seinen Browser sicheren Zugang zur Sphäre des Senders (z.B. mit dem https-Protokoll) erhalten. Die letztere Lösung hat den Vorteil, dass die Nachricht den geschützten Bereich des Senders nie verlässt.

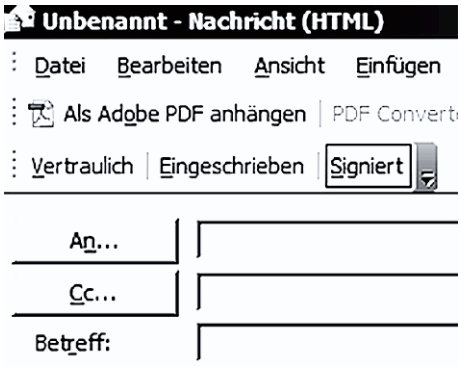
Es gilt jedoch zu berücksichtigen, dass beim Einsatz einer solchen Lösung (gilt auch für die unter Kapitel IV.1. dargestellte «End-to-End»-Verschlüsselung) die sogenannte Beziehungsvertraulichkeit nicht gewahrt ist, d.h. wohl ist der Mailinhalt samt Anhängen verschlüsselt, nicht jedoch der Betreff sowie die Absender- und Empfängeradresse. Weil Anwälte (aber auch Banken, Ärzte usw.) auch die Geschäftsbeziehung zum Klienten als solche nicht offenlegen dürfen, entbindet eine Verschlüsselung der E-Mails nicht davon, die Zustimmung des Klienten zur Kommunikation per E-Mail einzuholen. Diese Einwilligung ist jedenfalls dann erforderlich, wenn reger Mailverkehr zwischen Anwalt und dem Klienten besteht, somit Aussenstehende auf den Bestand eines Mandatsverhältnisses schliessen könnten bzw. können. Gateway-Lösungen sollten nur von einem in solchen Fragen spezialisierten IT-Anbieter konfiguriert und in Betrieb genommen werden.

3. Verwendung einer firmenübergreifenden Secure-E-Mail-Plattform

Wer ohne Verwendung von digitalen Zertifikaten vertraulich E-Mails versenden möchte, dem steht die Nutzung einer Secure E-Mail-Plattform zur Verfügung. Die Funktionsweise von IncaMail (eine Plattform der Schweizerischen Post) kann der nachstehenden Grafik entnommen werden.[7]



Dank flexibler Integrationsmöglichkeiten,[8] kann der Mailversand in der Praxis benutzerfreundlich umgesetzt werden. Der Absender verfasst seine E-Mail in seinem Mailprogramm und wählt mittels Schaltflächen die gewünschte Übertragungsart an («Signieren» = E-Mail mit einer digitalen Signatur versehen; «Vertraulich» = Mailzustellung via Secure-E-Mail-Plattform; «Eingeschrieben» = Mailzustellung via Secure-E-Mail-Plattform, elektronisch eingeschrieben).



Ferner stellen IncaMail und Privasphere weitere Dienste zur Verfügung. So ist es möglich, elektronisch eingeschriebene E-Mails (analog: Einschreibebrief) zuzustellen.[9] Siehe dazu nachfolgend eine Einschreiben-Quittung von IncaMail.


SWISS POST

IncaMail Empfangsquittung

Absender:	"Kundendienst IncaMail" <incamail@post.ch>
Versandart:	Swiss Post Einschreiben
Betreff:	Vertrag
Gesendet:	16.02.2009 11:10
Transaktionsnummer:	72f11c8b40cee3df5f57186ee551f1d5c73ac59e

Empfänger	Status	Identifikation	Datum
incamail.noreply@post.ch	Abgeholt	Passwort	16.02.2009 11:10

Original E-Mail
Doppelklicken Sie auf nebenstehendes Bild um die Original E-Mail einzusehen.

Die Richtigkeit dieser Quittung bezeugt:

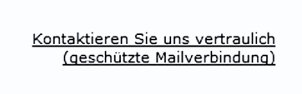
IncaMail

16.02.2009 11:10 CET

Digitally signed by pseudo. IncaMail
Date: 2009.02.16 11:10:51 GMT+01:00

Die Schweizerische Post
incamail@post.ch
www.incamail.ch

Andererseits ist es auch möglich, auf der eigenen Homepage einen Link auf ein sicheres Webformular zur Verfügung zu stellen.


Kontaktieren Sie uns vertraulich
(geschützte Mailverbindung)

4. Beurteilung der zur Verfügung stehenden Lösungen

Der Verfasser dieses Artikels beschäftigt sich seit Jahren mit der Frage der Absicherung des Mailverkehrs im praktischen Kanzleialltag. Die vor mehreren Jahren durchgeführten Tests mit verschlüsselten Mails gemäss vorstehendem Kapitel IV.1. verliefen wenig erfolgreich, da die Mailempfänger entweder nicht bereit waren kostenlose Software zu installieren (GnuPG) oder eine digitale Signatur zu erwerben und einzusetzen. Kurz gesagt: Dieser Weg sollte wohl nicht beschritten werden.

Seit mittlerweile mehr als drei Jahren wickelt der Verfasser den sicheren Mailverkehr mittels einer digitalen Signatur oder über die Secure-E-Mail-Plattform von PrivaSphere ab. Die Erfahrungen v.a. mit der Secure-E-Mail Plattform sind positiv und die Zusammenarbeit mit PrivaSphere ist unkompliziert, lösungsorientiert und kundenfreundlich. IncaMail wurde von der Schweizerischen Post zusammen mit dem Technologiepartner PrivaSphere entwickelt und im Herbst 2008 lanciert.

IncaMail wird vom SAV zur Nutzung in Anwaltskanzleien empfohlen und anlässlich des Anwaltskongresses 2009 in Luzern im Workshop «Vertrauliche Daten elektronisch sicher übermitteln» vorgestellt werden.

Kanzleien einer gewissen Grösse oder solche Kanzleien, die Wert darauf legen, dass die Mails primär im eigenen Herrschaftsbereich verbleiben, sollten eine Lösung gemäss Kapitel IV.2. (mit) evaluieren. Beide Lösungen können empfohlen werden, wobei die Bereitschaft bestehen muss, eine Grundinvestition zu tätigen.

7 Mehr zum Thema unter: *www.incamail.ch* oder *www.privasphere.com.*
8 Die WinJur AG hat ein PlugIn für Outlook entwickelt, welches auch in den Lösungen von Totemo und SeppMail verwendet werden kann.
9 Wird am Schweizerischen Anwaltskongress 2009 am Samstag, 13. Juni, im Workshop «Vertrauliche Daten sicher elektronisch übermitteln», live gezeigt.

V. Umsetzung im Kanzleialltag

Die unter den vorstehenden Kapitel IV.2. und IV.3. vorgestellten Lösungen lassen sich mit angemessenem Aufwand in die IT-Umgebung mittlerer und grösserer Kanzleien integrieren. Für kleinere Kanzleien bietet sich IncaMail/PrivaSphere als Lösung an. Grössere Kanzleien sollten Softwarelösungen von Totemo, SeppMail, PGP in die Evaluation miteinbeziehen. Welche Lösung auch immer gewählt wird, die Softwarepartner sind kompetent und in der Lage, eine Lösung rasch in die bestehende IT-Umgebung zu integrieren.

VI. Elektronischer Behördenverkehr

Aufgrund der geltenden Regelungen ist derzeit ausschliesslich IncaMail im elektronischen Behördernverkehr (konkret: im Verkehr mit dem Bundesgericht) zugelassen.[10] Pendent sind die Zulassungsentscheide zum elektronischen Verkehr mit Verwaltungsbehörden.[11]

10 Reglement des Bundesgerichts vom 5. Dezember 2006 über den elektronischen Rechtsverkehr mit Parteien und Vorinstanzen (ReRBGer; SR 173.110.29).

11 Verordnung vom 17. Oktober 2007 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (SR 172.021.1).

VII. Verzicht auf sichere Mails als echte Alternative?

Der grundsätzliche Verzicht auf die Möglichkeit, unseren Klienten sicheren Mailverkehr anzubieten, ist meiner Ansicht nach keine Alternative. Wie erwähnt, würden wir Anwälte nie auf die Idee kommen, unsere Geschäftsbriefe mit einer Briefmarke zu versehen und auf einen Briefumschlag zu verzichten. Gleiches muss für den Mailverkehr gelten. Letztlich geht es meines Erachtens beim Entscheid des sicheren Mailverkehrs um eine Frage der Professionalität und des Ansehens unseres Berufsstandes und nicht, ob uns allenfalls ein Disclaimer vor Sanktionen oder zivilrechtlichen Ansprüchen bewahrt.