



Internet-Recht: Technische Grundlagen

23. April 2005, 9:00

RLB, Linz

Rene Mayrhofer

Institut für Pervasive Computing

Johannes Kepler Universität Linz, Austria

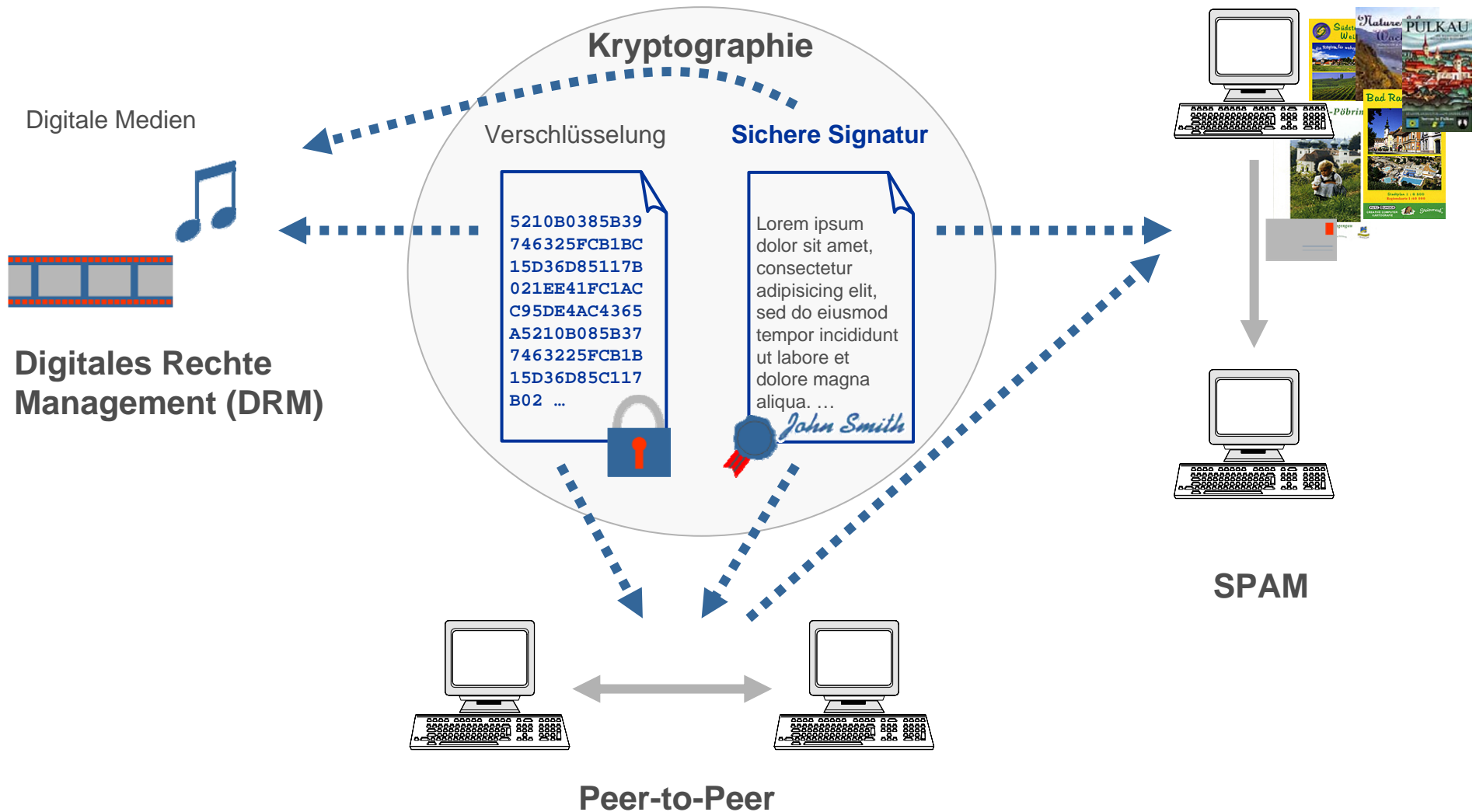
rene@mayrhofer.eu.org

Gibraltar Firewall Entwicklungsleiter

<http://www.gibraltar.at/>



Vortragsinhalt



Grundbegriffe aus der Kryptographie



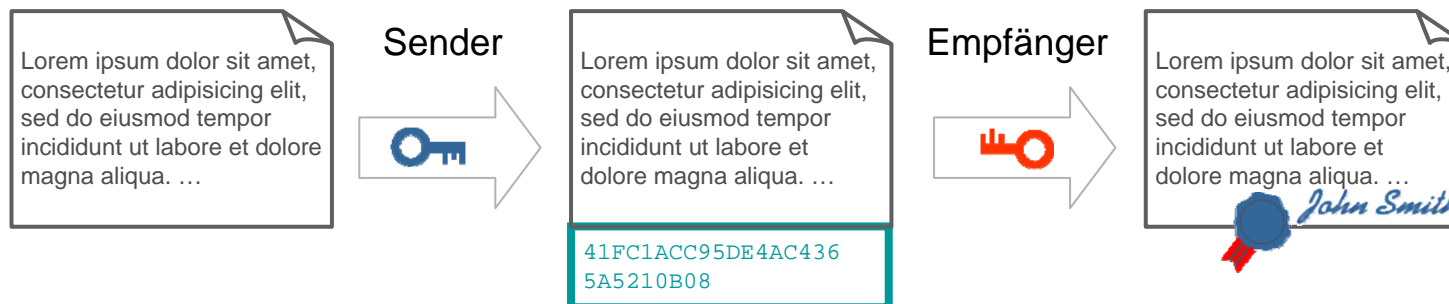
Verschlüsselung

- Löst das Problem der „**Vertraulichkeit**“ („Geheimhaltung“)



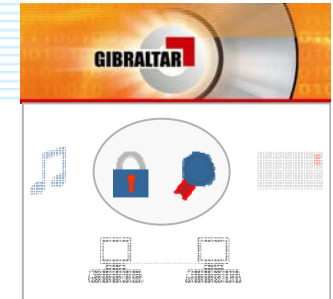
Digitale Signatur

- Löst primär das Problem der „**Integrität**“ und trägt bei zur Sicherung der „**Authentizität**“



Technische Lösung für „**Verbindlichkeit**“ und „**Authentifikation**“ sowie „**Autorisierung**“ nicht ausreichend ⇒ organisatorische Maßnahmen benötigt

Von der einfachen Signatur zur sicheren/qualifizierten



Sichere/Qualifizierte Signatur

- Benötigt **Chipkarte**
- Benötigt **Kartenleser** mit T
- Benötigt **Zertifikat**

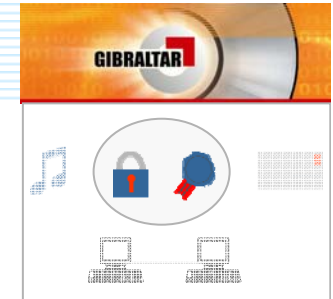
Unterschied zur „gewöhnlich

- Speicherung des digitalen
- Starke Bindung des digitalen
Maßnahmen



Verwendung aus Benutzersicht

- Chipkarte + PIN für Erstellung einer Signatur und Entschlüsselung
- Prüfung von Signaturen und Verschlüsselung ohne Chipkarte
- **Aber:** Problem Software-Verfügbarkeit!
- Problem Zeitstempeldienst

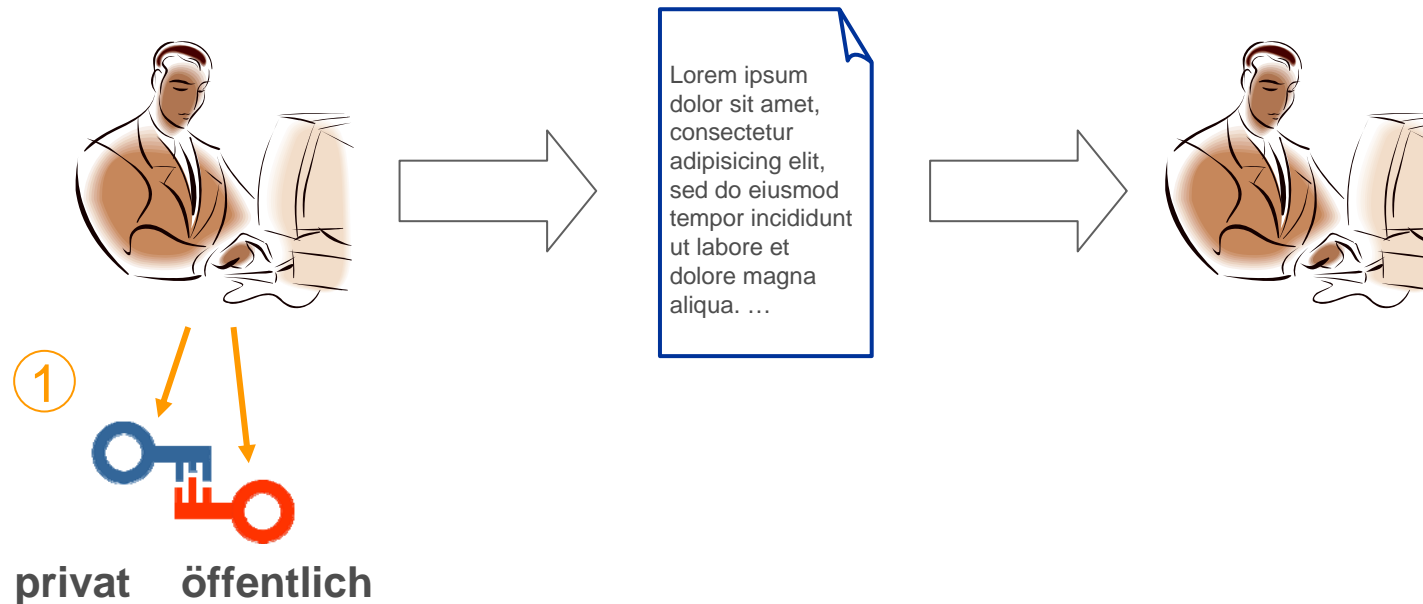


Aktuelle Email-Signaturen mit Standard-Software

Standards zur Signatur und Verschlüsselung von Emails

- PGP/OpenPGP
- S/MIME

Verwendung digitaler Signaturen mit Standard-Software: OpenPGP





Schlüsselverwaltung

File Edit View Key Groups Schlüsselserver GPG ?

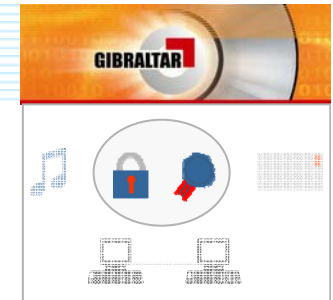
New... Edit Signieren Löschen Widerrufen Signaturen prüfen Zeige Vertrauenspfad Import via HTTP... Import... Export... Export Secret Key Eigenschaften Refresh Keys (Keyserver) Erneuere Schlüsselcache Signaturen überprüfen

Normal Experte Smartcard

User ID	Key ID	Algorithm	Validity	Trust	Creation
Alexander Stieglecker <...>	1024	DSA/ELG	[] Unknown	None	2000-07-13
Andreas Rottmann <rotti...>	1024	DSA/ELG	[] Unknown	None	2000-03-17
Christian Wagner <2:31...>	1024	RSA	[] Unknown	None	1996-01-05
Christoph Guger <cguge...>	1024/2048	DSA/ELG	[] Unknown	None	1998-05-18
Felix Schwenk <felix.sch...>	1024/2048	DSA/ELG	[] Unknown	None	2000-10-03
Florian Ortner <florian.ort...>	1024/2048	DSA/ELG	[] Unknown	None	2000-06-17
FRISK Software Internat...	1024	RSA	[] Unknown	None	1995-10-09
Gerfried Fuchs <alfie@d...>	1024/1024	DSA/ELG	[] Unknown	None	2000-02-15
Harald Radi <harald.radi...>	1024/2048	DSA/ELG	[] Unknown	None	2000-06-17
Marco Blum <marco.blum...>	1024/2048	DSA/ELG	[] Unknown	None	2001-05-20
Martin Maurer (Uni) <ma...>	1024/2048	DSA/ELG	[] Unknown	None	2001-12-10
Martin Maurer <martin.m...>	1024/2048	DSA/ELG	[E] Unkno...	None	1999-05-25
Michael Kumar <m.kuma...>	1024/2048	DSA/ELG	[] Unknown	None	2000-12-04
Michael Moerz <e96251...>	1024/2048	DSA/ELG	[E] Unkno...	None	2000-09-17
Michael Richardson (Ge...	1024	RSA	[] Unknown	None	2001-05-06
Mihaela Ionescu <Mihae...>	1024/2048	DSA/ELG	[] Unknown	None	1999-10-01
Rene Mayrhofer <rene.n...>	1024/2048	DSA/ELG	[R] Revok...	None	1998-05-19
Rene Mayrhofer <rene@...>	1024/2048	DSA/ELG	[] Unknown	Full	1999-10-04
Rene Mayrhofer <rmayr@...>	1024	RSA	[] Unknown	Full	1999-06-23
ViaNova <office@viano...>	1024/2048	DSA/ELG	[] Unknown	None	2001-04-09
Volker Christian <voc@...>	1024/1024	DSA/ELG	[] Unknown	None	2003-08-16

Groups

Standardschlüssel: c3c24bde 21 keys (2 secret keys)



Key Generation Wizard

Name und E-Mail Zuweisung

Jedes Schlüsselpaar muss mit einem Namen verknüpft sein. Am Namen und der E-Mail-Adresse erkennen Ihre Kommunikationspartner die Echtheit des Schlüssels.

Ihr Name

Mit der Verknüpfung einer E-Mail-Adresse mit Ihrem Schlüssel, ist die Auswahl des richtigen Schlüssels für Ihre Kommunikationspartner leichter!

Mail-Adresse

☐ Bevorzuge RSA

OK Cancel Expert

Schlüsselerzeugung

Mantra eingeben ☒ Hide Typing

OK Cancel

Key Generation - Progress Dialog

```

+++++.....+++++
+++++.....+++++
+++++.....+++++
.....>+++++<+++++.....+++++
+++++.....+++++
+++++.....+++++
+++++.....+++++
+++++.....+++++
+++++>.....+++++

```

GnuPG-Status

Schlüsselerzeugung abgeschlossen

OK



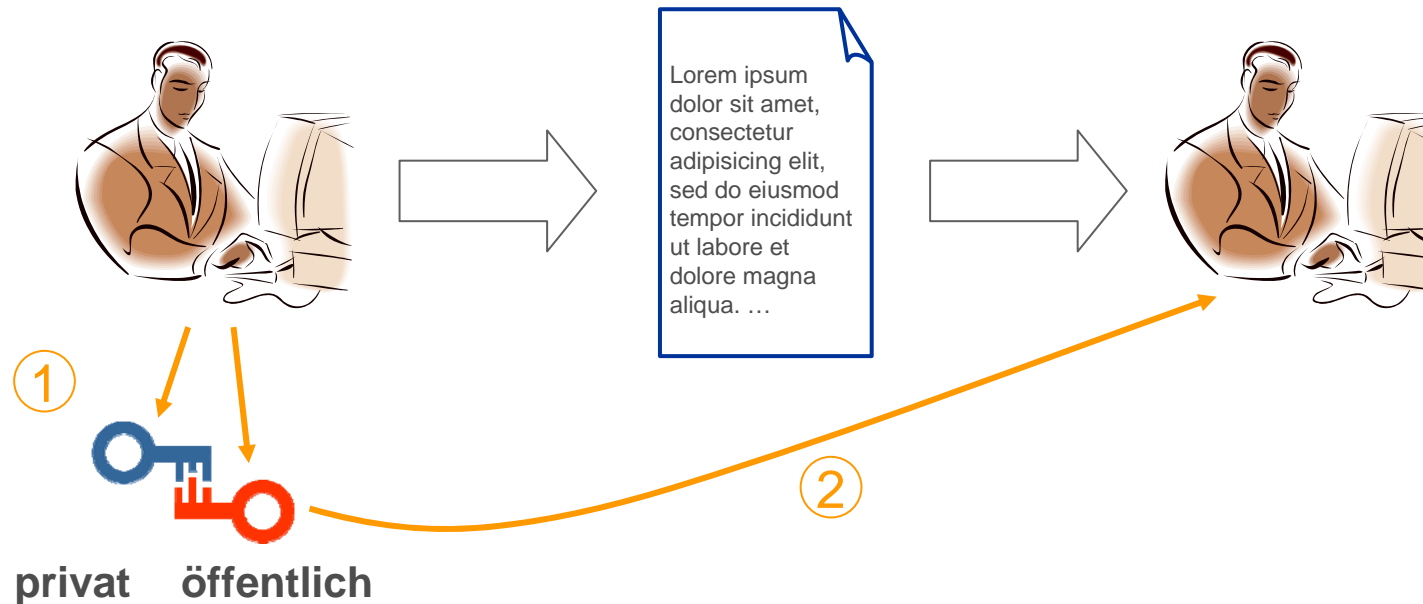


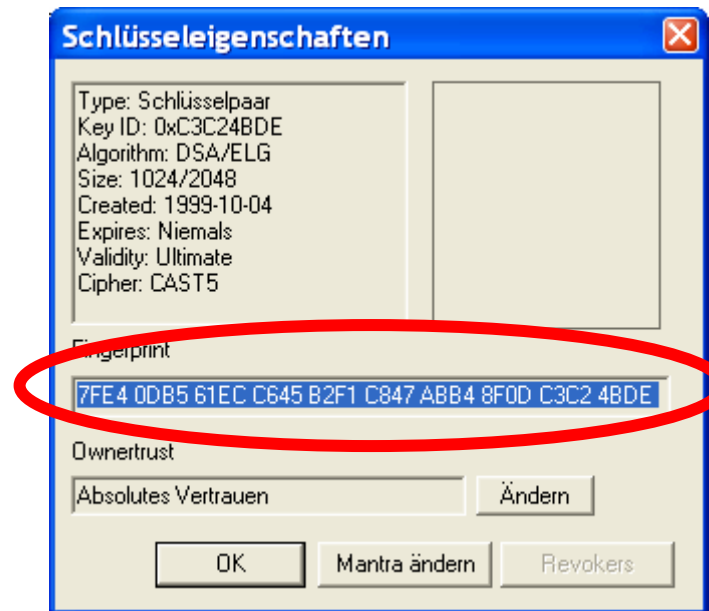
Aktuelle Email-Signaturen mit Standard-Software

Standards zur Signatur und Verschlüsselung von Emails

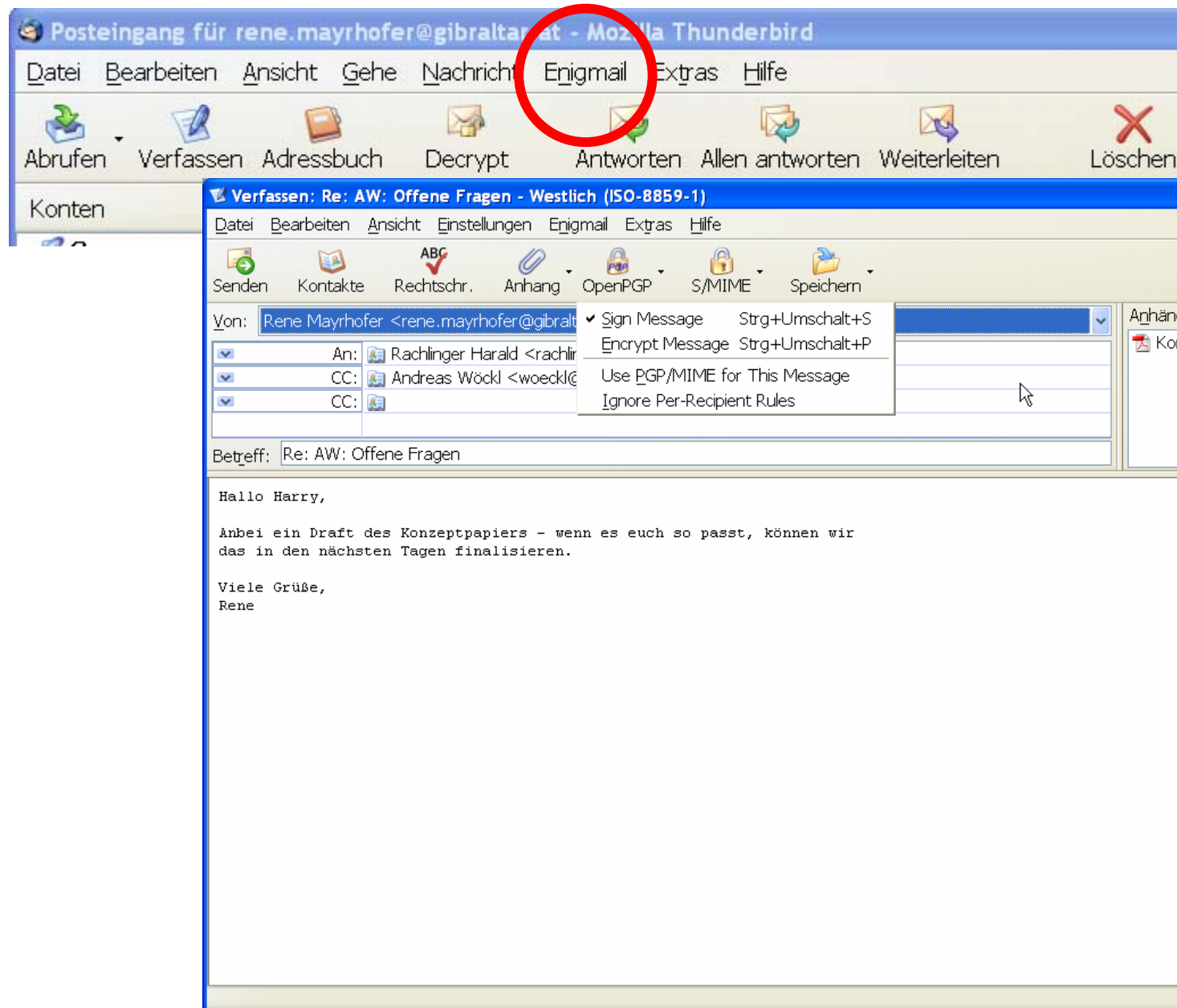
- PGP/OpenPGP
- S/MIME

Verwendung digitaler Signaturen mit Standard-Software: OpenPGP











Re: AW: Offene Fragen - KMail

Nachricht Bearbeiten Ansicht Optionen Anhängen Extras Einstellungen Hilfe

Standard 6 B i U

Identität: Standard (Standard) Beibehalten

An: Rachlinger Harald <rachlinger@powerdat.at>

Kopie an (CC): Andreas Wöckl <woeckl@esys.at>

Blindkopie an (BCC):

Betreff: Re: AW: Offene Fragen

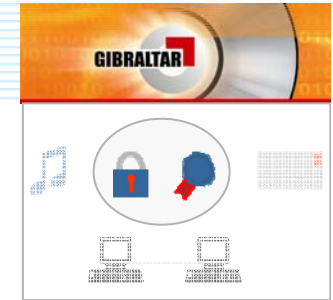
Hallo **Harry**,

Anbei ein **Draft** des Konzeptpapiers - wenn es euch so passt, können wir das in den nächsten Tagen **finalisieren**.

Viele Grüße,
Rene

Name	Größe	Kodierung	Typ	Verschlüsse	Signiere
Konzept.pdf	108,2...	base64	PDF-Dokument	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Spalte: 1 Zeile: 1

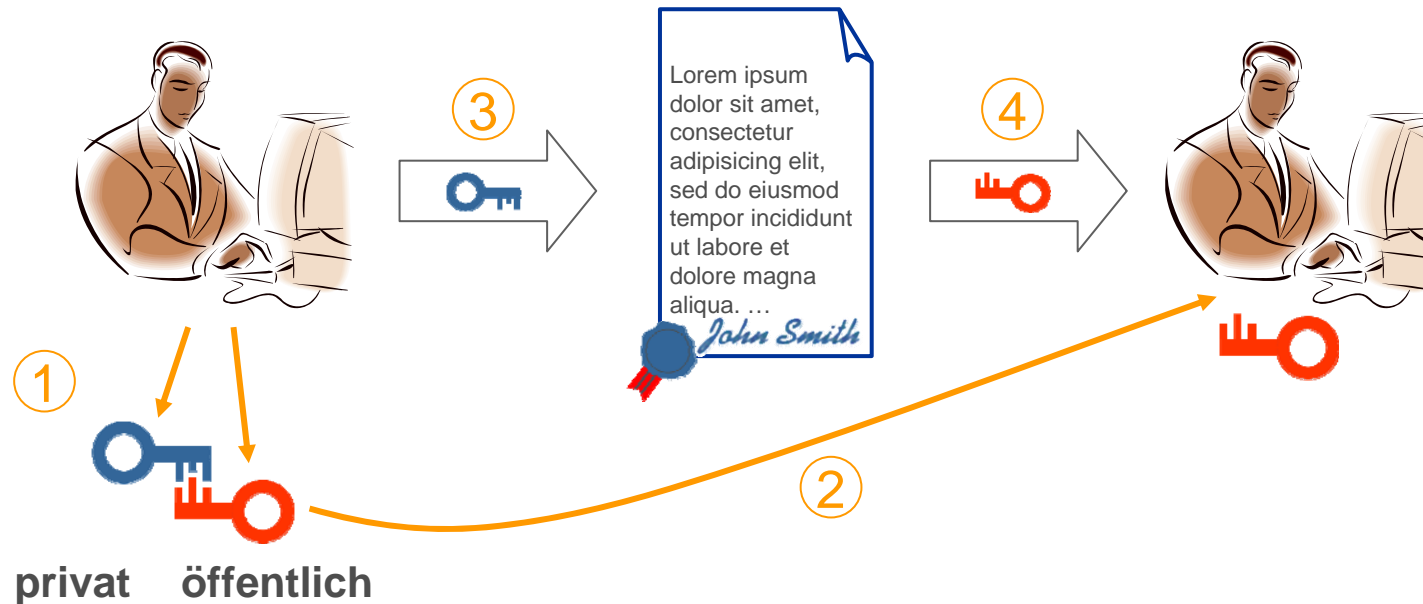


Aktuelle Email-Signaturen mit Standard-Software

Standards zur Signatur und Verschlüsselung von Emails

- PGP/OpenPGP
- S/MIME

Verwendung digitaler Signaturen mit Standard-Software: OpenPGP





Mailing-list für rene.mayrhofer@gibraltar.at - Mozilla Thunderbird

Datei Bearbeiten Ansicht Gehe Nachricht Enigmail Extras Hilfe

Abrufen Verfassen Adressbuch Decrypt Antworten Allen antworten Weiterleiten Löschen Junk Drucken Stopp

Konten Ansicht: Alle Betreff oder Absender

Jupiter

- Posteingang
- Entwürfe
- Vorlagen
- Gesendet
- Papierkorb
- 00-Old-Vi...-Address
- 01-SPAM
- 02-VIRUS
- Administrative
- Debian-Packages
- Fun
- Gibraltar
 - 00-Config
 - 00-TODO
 - 01-TOREAD
 - 02-TOFAQ
 - 03-IDEAS
 - Administrativa
 - Antivir
 - Build-System
 - Donations
 - Lizenz
 - Mailing-list
 - Mirrors
 - Preis
 - Redistributors
 - Staff
 - Webinterface
 - Webpage
 - Werbung
- Mailing-lists

Betreff	Absender	Datum
[Gibraltar-list] Migration of SMTP services (partially)...	Rene Mayrhofer	11.04.2005 14:40
[Gibraltar-list] Server migration during the next days	Rene Mayrhofer	11.04.2005 10:17
[Gibraltar-list] Gibraltar 2.2 USB version released (b...	Rene Mayrhofer	08.04.2005 23:40
Re: [Gibraltar-list] Gibraltar 2.2 released	Andreas Czerniak	08.04.2005 15:46
[Gibraltar-list] (no subject)	eddie bradbrook	08.04.2005 13:36
Re: [Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	08.04.2005 12:12
Re: R: [Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	08.04.2005 09:50
R: [Gibraltar-list] Gibraltar 2.2 released	Mario Moleri	08.04.2005 08:23
Re: [Gibraltar-list] Gibraltar 2.2 released	Kim Holburn	08.04.2005 03:36
[Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	07.04.2005 21:27
AW: [Gibraltar-list] Bayesfiltering	gibraltarSupport	16.03.2005 09:20
[Gibraltar-list] private license key request	mark jones	11.03.2005 23:57

Enigmail: Good signature from Rene Mayrhofer <rene.mayrhofer@gibraltar.at>
Key ID: 0xC3C24BDE / Signed on: 07.04.2005 21:27

Betreff: [Gibraltar-list] Gibraltar 2.2 released

Von: Rene Mayrhofer <rene.mayrhofer@gibraltar.at>

Antwort an: Gibraltar mailing list <gibraltar-list@gibraltar.at>

Datum: 07.04.2005 21:27

An: gibraltar-list@gibraltar.at

Hi all,

We are pleased to announce Gibraltar release 2.2. It significantly improves the speed of the web interface and solves a previous issue with license checks in high-bandwidth cases. An important change is the introduction of the tcp-window-tracking patch to the firewall code, which checks TCP connection much more thoroughly than before. This means more security against attacks, and therefore most likely more messages in the system log - these are to be expected and should not be taken as errors. You can find a more detailed explanation of these new checks at <http://www.netfilter.org/patch-o-matic/pom-submitted.html#pom-submitted-tcp-window-tracking> and

Anhänge: Teil 1.1.2 Teil 1.2

Ungelesen: 0 Gesamt: 3047

Jupiter/Posteingang/Gibraltar/Mailing-list - KMail

Datei Bearbeiten Ansicht Gehe zu Ordner Nachricht Extras Einstellungen Hilfe

Suchen: Status: Jeder Status

Betreff	Absender	Datum
[Gibraltar-list] Migration of SMTP services (partially) completed	Rene Mayrhofer	Montag - 14:40:54
?? [Gibraltar-list] Server migration during the next days	Rene Mayrhofer	Montag - 10:17:25
?? [Gibraltar-list] Gibraltar 2.2 USB version released (beta)	Rene Mayrhofer	08.04.2005 23:40
?? Re: [Gibraltar-list] Gibraltar 2.2 released	Andreas Czerniak	08.04.2005 15:46
?? [Gibraltar-list] (no subject)	eddie bradbrook	08.04.2005 13:36
?? Re: [Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	08.04.2005 12:12
?? Re: R: [Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	08.04.2005 09:50
?? R: [Gibraltar-list] Gibraltar 2.2 released	Mario Moleri	08.04.2005 08:23
?? R: [Gibraltar-list] Gibraltar 2.2 released	Kim Holburn	08.04.2005 03:36
[Gibraltar-list] Gibraltar 2.2 released	Rene Mayrhofer	07.04.2005 21:27
?? AW: [Gibraltar-list] Bayesfiltering	gibraltarSupport	16.03.2005 09:20
?? [Gibraltar-list] private license key request	mark jones	11.03.2005 23:57
?? [Gibraltar-list] Bayesfiltering	Christoph Fritsch	21.02.2005 14:17
?? Re: [Gibraltar-list] Cron <clamav@gibraltar> ... /usr/bin/freshclam 1.6.6 /usr/bin/freshcl	Rene Mayrhofer	16.02.2005 18:35

[Gibraltar-list] Gibraltar 2.2 released

Von: Rene Mayrhofer <rene.mayrhofer@gibraltar.at>
An: gibraltar-list@gibraltar.at
Datum: 07.04.2005 21:27

**Nachricht enthält Signatur von rene@mayrhofer.eu.org (Schlüssel-ID: 0xABB48F0DC3C24BDE).
Die Signatur ist gültig, und der Schlüssel ist vollständig vertrauenswürdig.**

We are pleased to announce Gibraltar release 2.2. It significantly improves the speed of the web interface and solves a previous issue with license checks in high-bandwidth cases. An important change is the introduction of the tcp-window-tracking patch to the firewall code, which checks TCP connection much more thoroughly than before. This means more security against attacks, and therefore most likely more messages in the system log - these are to be expected and should not be taken as errors. You can find a more detailed explanation of these new checks at <http://www.netfilter.org/patch-o-matic/pom-submitted.html#pom-submitted-tcp-window-tracking> and <http://www.netfilter.org/documentation/FAQ/netfilter-faq-3.html#ss3.16>

Another change is that freeswan has been replaced by its successor openswan, which uses compatible config files so that this replacement should not need any changes in current configurations.

There are also new options and smaller changes in the web interface, including:

- Options for set up of L2TP tunnels via IPSec, which are compatible with the

Beschreibung	Typ	Kodierung	Größe
[Gibraltar-list] Gibraltar 2.2 released	multipart/mixed	7bit	3,6 KB
▼ Textteil	multipart/signed	7bit	3,5 KB



Aktuelle Email-Signaturen mit Standard-Software

Standards zur Signatur und Verschlüsselung von Emails

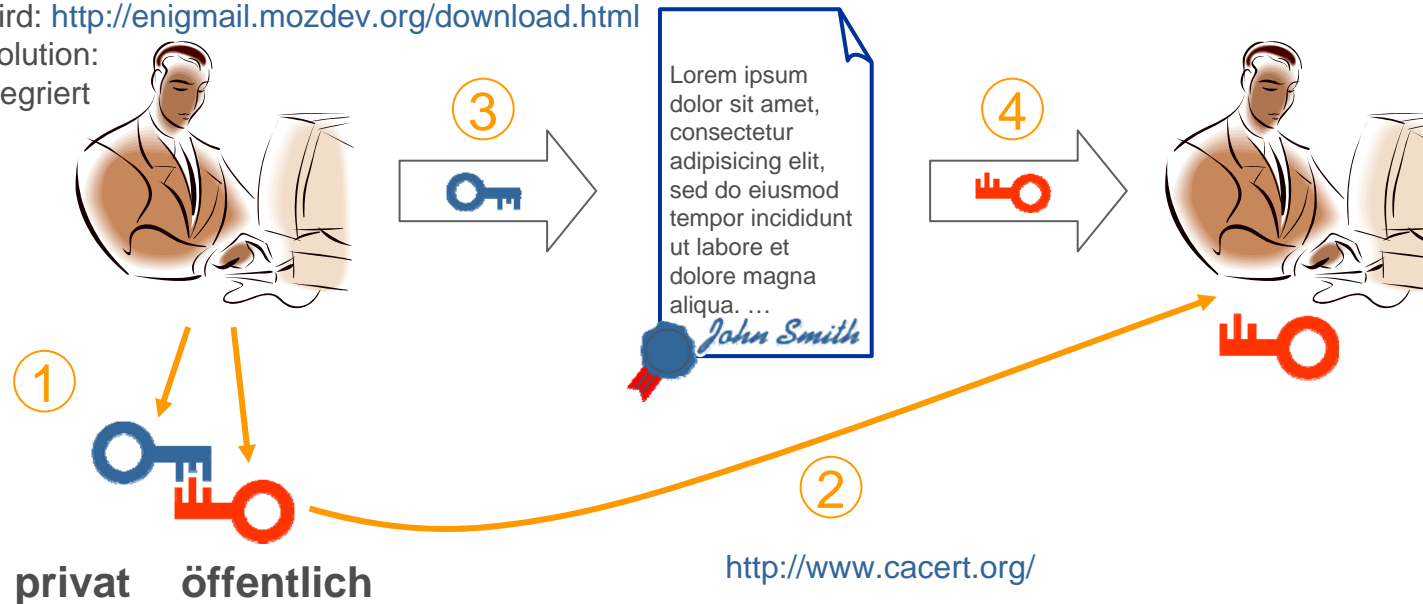
- PGP/OpenPGP
- S/MIME

Verwendung digitaler Signaturen mit Standard-Software: OpenPGP

Outlook: <http://www.equipmente.de/viewtopic.php?t=642>

Thunderbird: <http://enigmail.mozdev.org/download.html>

Kmail, Evolution:
bereits integriert



<http://www.equipmente.de/gnupt-int.exe>

Dokumentensignatur: Probleme mit dem aktuellen Betrieb



Erfordernisse laut <http://www.cio.gv.at/faq/Amtssignatur/>

Für das Aussehen der **Amtssignatur** gibt es keine verbindliche Regelung. Zur erleichterten Erkennbarkeit der Herkunft eines Dokuments von einer Behörde sieht das E-GovG im § 19 Abs. 3 vor, dass in der Darstellung zumindest folgende Komponenten zu visualisieren sind:

- die **Bildmarke** der Behörde,
- der ausstellende **Zertifizierungsdiensteanbieter** (Name und Herkunftsland) sowie die Seriennummer des Zertifikates, und
- der **Signaturwert** in BASE64 Codierung.

Beispiel „Änderung der Signaturverordnung“ auf

<http://ris1.bka.gv.at/authentic/index.aspx> bzw.

<http://ris1.bka.gv.at/authentic/index.aspx?page=doc&docnr=2>




BUNDESKANZLERAMT RIS - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://ris1.bka.gv.at/authentic/index.aspx?page=doc&docnr=2 Go ris.aco.at

Kostenlose Hotmail Links anpassen Windows Media Windows

Ihre Visitenkarte im Internet

 Ihr Informationsvorsprung im Umgang mit Ämtern und Behörden.

Jurbooks
Bücher zu
Recht und Steuern

BUNDESKANZLERAMT ÖSTERREICH ■ **BGBL AUTHENTISCH AB 2004**

HOME Auswahl RIS Info BGBl Handbuch BGBL HTML 1983 - 2003 BGBL PDF 1999 - 2003





➔ Abfrage ➔ Trefferliste ➔ Vorheriger Treffer ➔ Nächster Treffer ➔ Drucken

Fundstelle:
BGBl. II Nr. 527/2004

Typ: **Teil:** **Datum der Kundmachung:**
V II 2004-12-30

Kurztitel:
Änderung der Signaturverordnung

Texte:

Hauptdokument    

Titel:
Verordnung des Bundeskanzlers, mit der die Signaturverordnung geändert wird

Einbringendes Bundesministerium:
BKA
(Bundeskanzleramt)


Seitenanfang Impressum Kontakt

Fertig 0 error / 20 warnings Adblock



Bundeskanzleramt der Republik Österreich - Signaturprüfdienst - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe



Bundeskanzleramt der Republik Österreich

Signaturprüfdienst

Nachfolgend finden Sie das Ergebnis der Prüfung der eingereichten elektronischen Signatur.

Unterzeichner

Name	Christian Wregar
Organisationseinheit	Verfassungsdienst
Organisation	Bundeskanzleramt der Republik Österreich
Staat	AT

Aussteller des Zertifikats

Name	a-sign-corporate-light-01
Organisationseinheit	a-sign-corporate-light-01
Organisation	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Staat	AT

Informationen zum Zertifikat

Seriennummer	21221
Qualität	gewöhnliches Zertifikat

Prüfungen

Signatur	Die Überprüfung der Hash-Werte und des Werts der Signatur konnte erfolgreich durchgeführt werden.
Zertifikat	Eine formal korrekte Zertifikatskette vom Signatorzertifikat zu einem vertrauenswürdigen Wurzelzertifikat konnte konstruiert werden. Jedes Zertifikat dieser Kette ist zum in der Anfrage angegebenen Prüfzeitpunkt gültig.

Signierte Daten

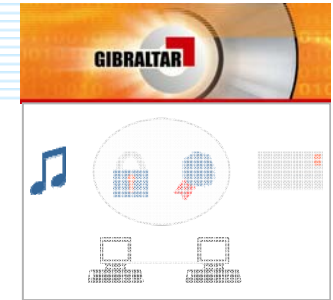
Datei Nr.1	Die Datei kann in einem eigenen Browser-Fenster angezeigt werden.
----------------------------	---

http://ris1.bka.gv.at/authentic/findbgbl.aspx?targetURL=http://10.102.11.14/mo... 0 error / 50 warnings Adblock

Dokument vom
16.4.2005

?

DRM: Digitales Rechte (Restriktionen) Management



Ziel

- Bindung von Mediendateien
- Einschränkungen bei der Verwendung

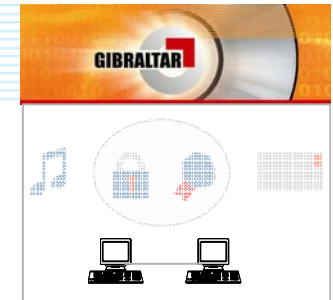
Methode

- Verschlüsselung
- Schlüssel wird an das System gebunden
- Beim Abspielen automatisch entschlüsselt
- Software kontrolliert Einschränkungen

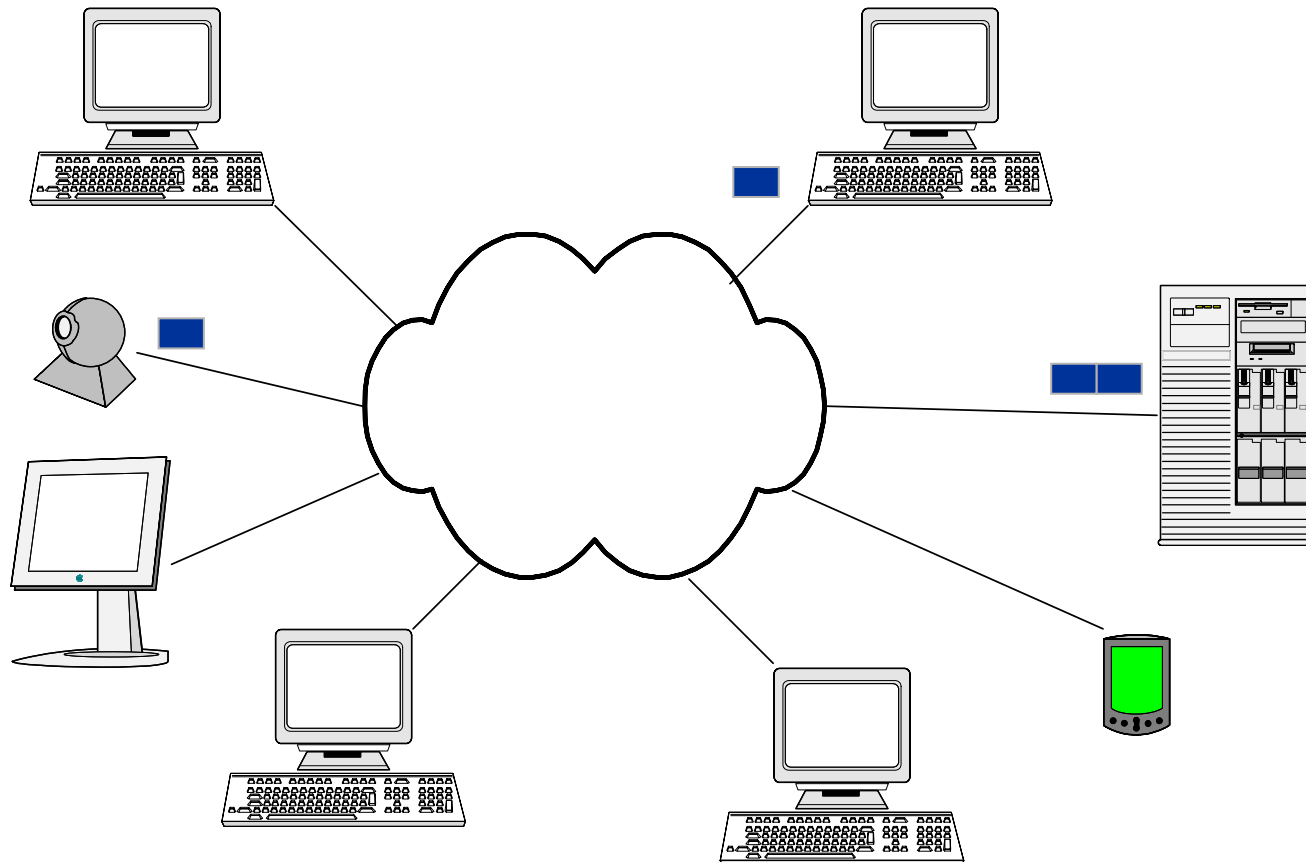
Probleme

- Privatkopie und Urheberrechtsabgabe
StF: BGBl. Nr. 111/1936, i.d.F. der UrhG-Novelle 2003: (1) Jedermann darf von einem Werk einzelne Vervielfältigungsstücke auf Papier oder einem ähnlichen Träger zum eigenen Gebrauch herstellen.
- Massive Akzeptanzprobleme

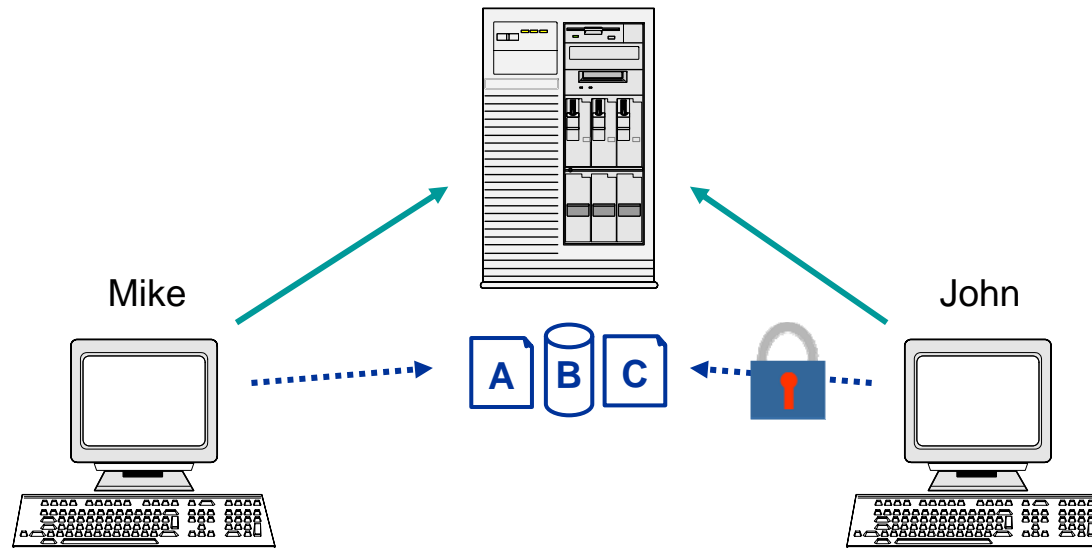
Peer-to-Peer als Technik



- Peer-to-Peer (P2P) bedeutet, dass kommunizierende Systeme **gleichberechtigte Teilnehmer** („Peers“) sind
- Idee ist nicht neu, das Internet ist grundsätzlich P2P!
- Es werden nur Datenpakete übertragen, jeder Teilnehmer ist **Empfänger und Sender**

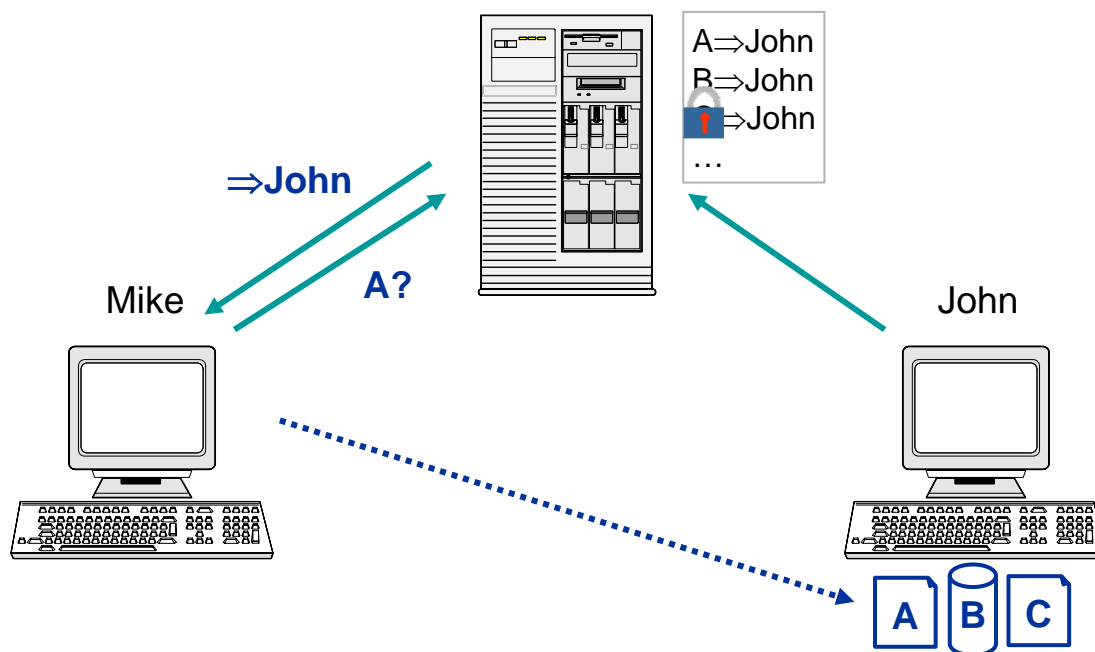


Generation 0: Server / Client

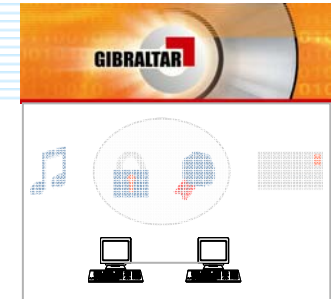


- Server hat Zugriff auf alle Informationen
- Umfangreiche zentrale Sperrmöglichkeiten
- Beispiele: **Dateiserver in lokalem Netzwerk**

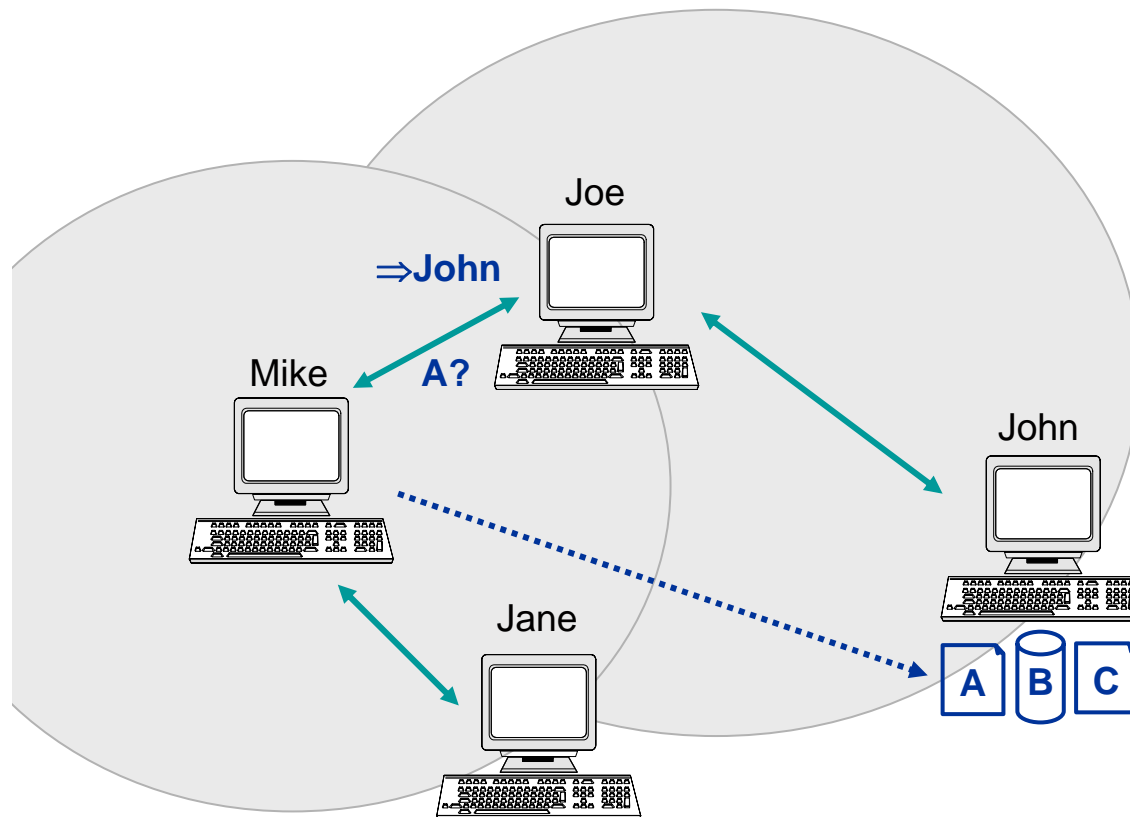
Generation 1: verteilte Daten, zentrale Suche



- Peers halten Daten, Server bietet Suche
- Server hat Zugriff auf alle Informationen
- Umfangreiche zentrale Sperrmöglichkeiten
- Beispiele: **Napster**, **Instant Messenger (ICQ, MSN, ...)**, **Internet-Telefonie**, **Video-Telefonie**, **Bittorrent**, ...

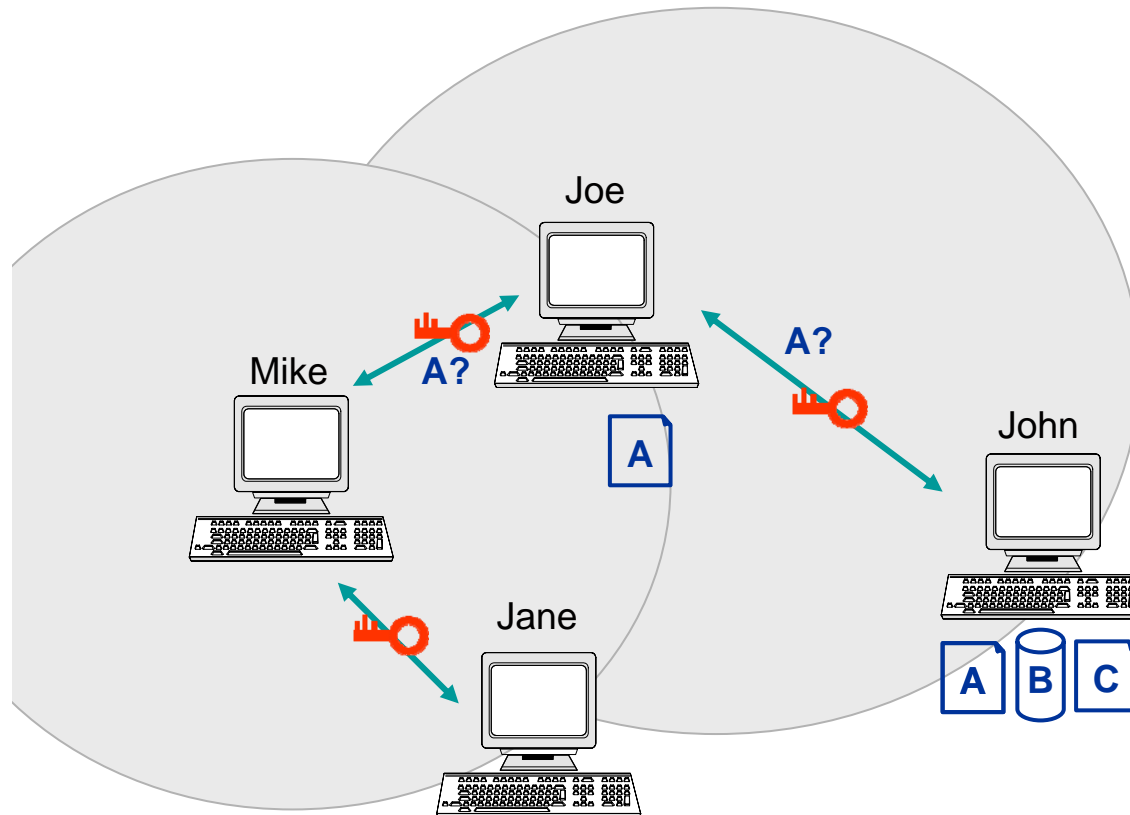


Generation 2: verteilte Daten, verteilte Suche

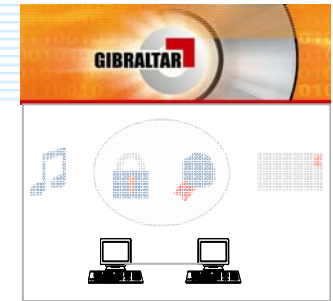


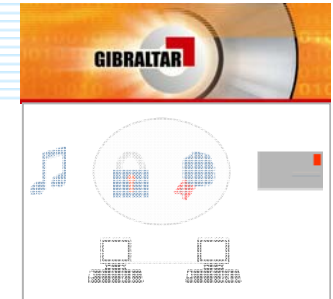
- Peers halten Daten, Suche zwischen Peers
- Peer hat Zugriff auf **eigene** Kommunikationsdaten
- Beispiele: **Kazaa**, **Gnutella**

Generation 3: Anonymität



- Wie Generation 2
- Aber:
 - **Verschlüsselung**
 - Suche und Transfer **indirekt**
- Beispiele:
 - Freenet** (Dateien),
 - Mixmaster** (Email),
 - Tor** (allgemein)

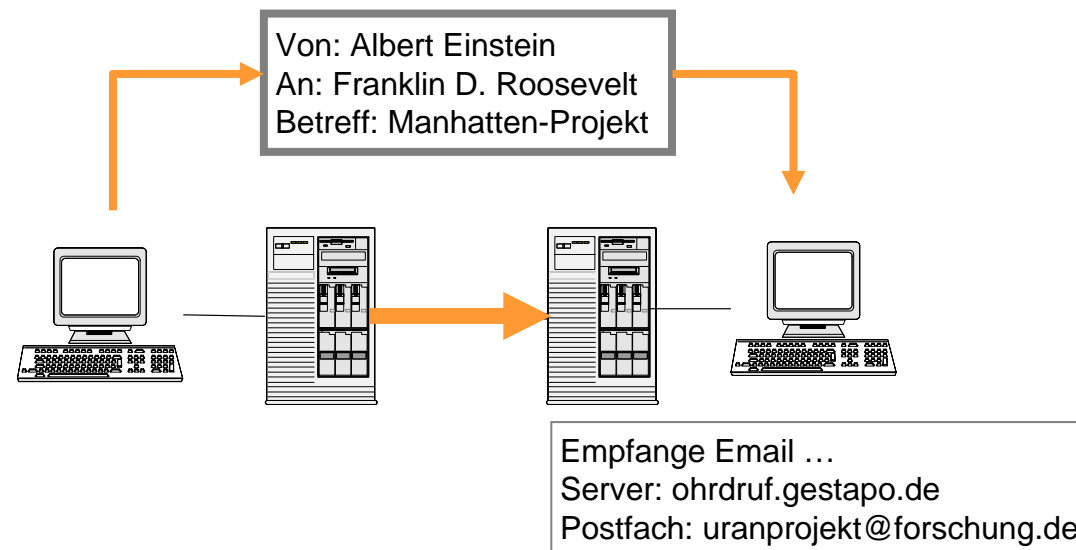




Identifizierung der Absender einer Email

Unterschied zwischen wirklichem Absender und angezeigtem Absender

- Absender unerwünschter Emails versuchen oft, ihre Identität zu Verschleiern



- Im Email-Programm angezeigte Absender und Empfänger können einfach gefälscht werden
- **Aber:** bei Zustellung einer Email zum empfangenden Email-Server werden Daten des Absenders registriert und in **Vorspann der Email, also im Umschlag**, eingetragen (Email-Header)



01-SPAM für rene.mayrhofer@gibraltar.at - Mozilla Thunderbird

Datei Bearbeiten Ansicht Gehe Nachricht Enigmail Extras Hilfe

Abrufen Verfasste

Konten

- Diss
- Junk-E-Mail
- Konferenzen
- Lehre: Algo1
- Lehre: Algo2
- Lehre: SE2
- Links
- Manet
- Organisatoris
- Pervasive 20
- Pervasive ...ceedings
- Pervasive ... Tutorials
- Pervasive 2005
- Pervasive mailing list
- Privat
- Silicon P2P
- SPAM

Jupiter

- Posteingang
- Entwürfe
- Vorlagen
- Gesendet
- Papierkorb
- 00-Old-Vi...-Address
- 01-SPAM (1236)

Symboleisten
Fensterlayout
Sortieren nach
Nachrichten
Themen
Kopfzeilen
Nachrichtentext
Anhänge eingebunden anzeigen
Schriftgrad
Zeichenkodierung
Nachrichten-Quelltext Strg+U
Nachrichten-Sicherheit

ten Allen antworten Weiterleiten Löschen Junk Drucken Stopp

Betreff oder Absender

Absender	Datum
vic55kuz@kuzin77.net	18:48
Mr liupeijin	13:15
Mr liupeijin	13:14
W.W	12:39
W.W	12:30
sales	12:21
MRS MARY JONES	17.04.2005 06:26
Ruthie Phelps	16.04.2005 18:05

Von: Mr liupeijin <liu_23peijin@mycity.com>
Datum: 13:15

Dear Sir/Madam,

I am Mr.Liu Peijin ,managinig Hubei Machinery&equipment Import&export Corporation(CMEC HUBEI CO.) we are a company who deal on mechanical equipment,hardware and minerals, electrical products, Medical & Chemicals,light industrial products and office equipment, and export into the Canada/America and Europe.

We are searching for representatives who can help us establish a medium of getting to our costumers in the Canada/America and Europe as well as making payments through you to us.

Please if you are interested in transacting business with us we will be glad.

Please contact us for more information Subject to your satisfaction you will be

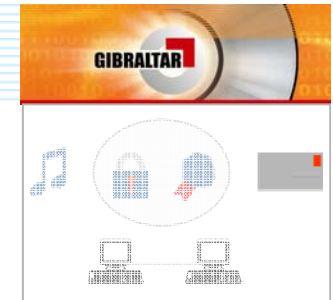
Ungelesen: 1236 Gesamt: 1716



Email-Umschlag

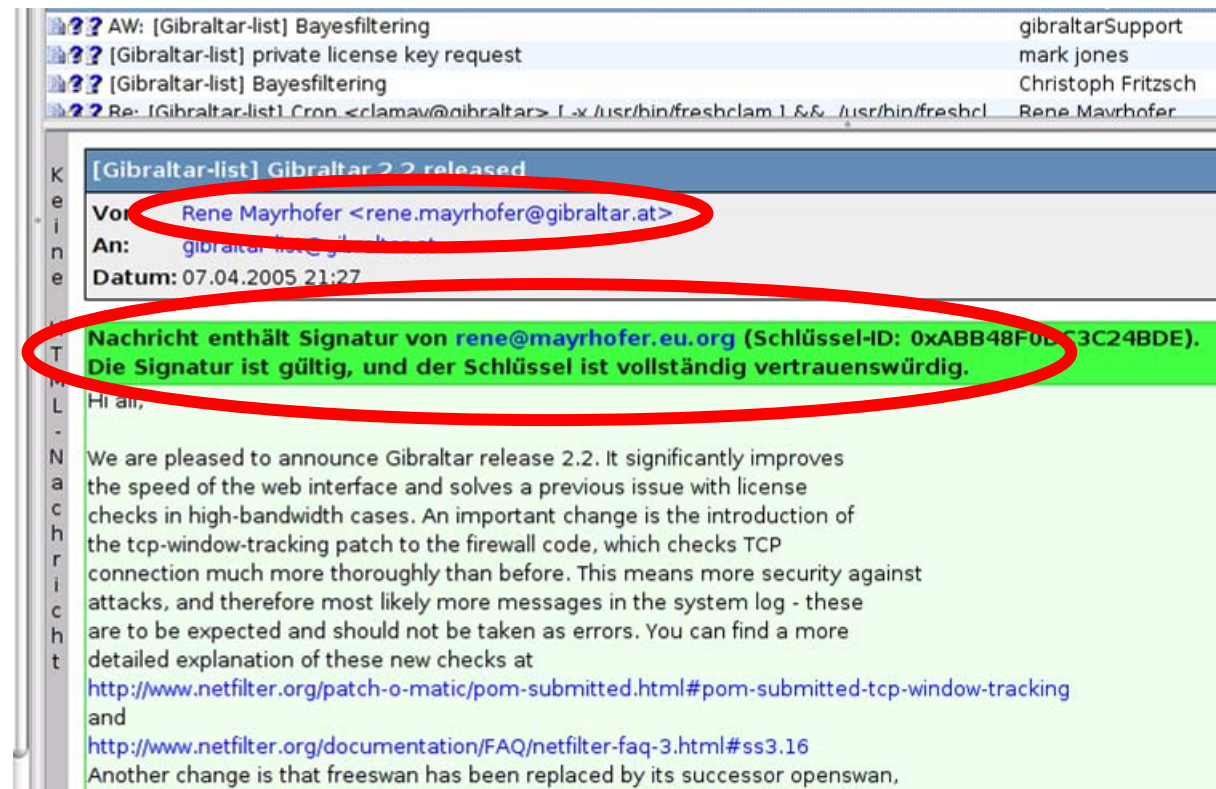


```
Return-Path: <nobody@s005.interlize.net>
X-Original-To: rene.mayrhofer@gibraltar.at
Delivered-To: rene.mayrhofer@gibraltar.at
Received: from localhost (jupiter [127.0.0.1])
    by jupiter.gibraltar.at (Postfix) with ESMTP id 2F97C180024B
    for <rene.mayrhofer@gibraltar.at>; Mon, 18 Apr 2005 13:22:30 +0200 (CEST)
Received: from jupiter.gibraltar.at ([127.0.0.1])
    by localhost (jupiter [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id 21172-06 for <rene.mayrhofer@gibraltar.at>;
    Mon, 18 Apr 2005 13:22:26 +0200 (CEST)
Received: from s005.interlize.net (s005.interlize.net [80.69.72.18])
    (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
    (No client certificate requested)
    by jupiter.gibraltar.at (Postfix) with ESMTP id 5F26D180153C
    for <rene.mayrhofer@gibraltar.at>; Mon, 18 Apr 2005 13:22:26 +0200 (CEST)
Received: from nobody by s005.interlize.net with local (Exim 4.44)
    id 1DNUDr-0001V9-7q; Mon, 18 Apr 2005 13:15:23 +0200
To:
From: Mr liupeijin <liu_23pei jin@mycity.com>
...
```

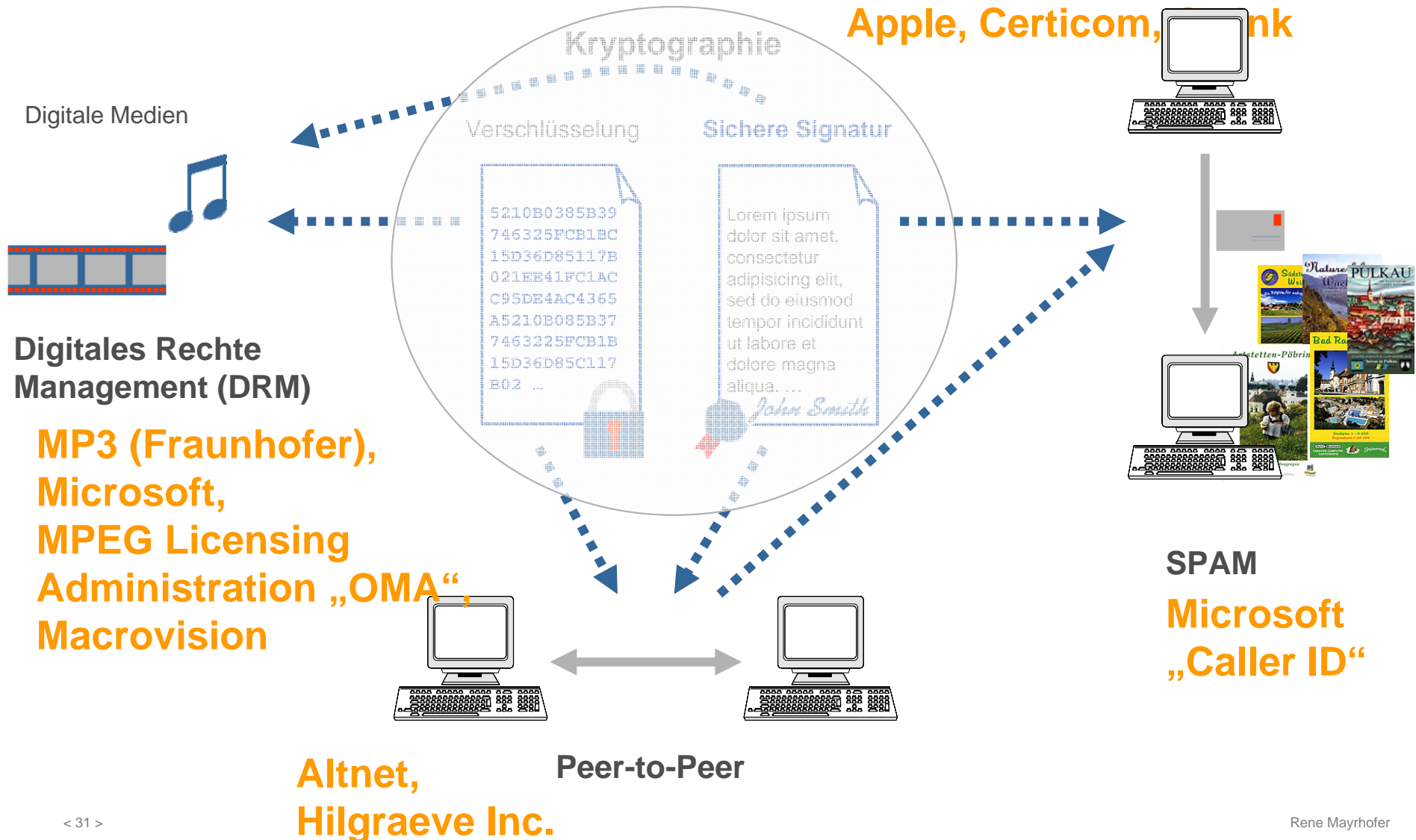
Verhinderung solcher Fälschungen?

- Administrative Maßnahmen auf Serverseite
- Digitale Signaturen



Auswirkungen von Software-

DH (ausgelaufen April 1997),
RSA (freigegeben September
2000), „Elliptic Curves“:
Apple, Certicom, Bank





Wie geht es weiter?





Vielen Dank für Ihre Aufmerksamkeit!



Folien: <http://www.gibraltar.at/>

Spätere Fragen: rene@mayrhofer.eu.org

OpenPGP Schlüssel: 0xC3C24BDE

7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE

Beglaubigtes S/MIME Zertifikat von cacert.org auf Anfrage.

Sichere Signatur mit Bürgerkarte sobald entsprechende (Open Source) Software für Linux verfügbar.