

# Grundlagen von E-Mail Verschlüsselung & Signatur

**Informationsveranstaltung  
Informationssicherheit**  
19. November 2009, Wien

Priv.-Doz. Dr. Rene Mayrhofer  
eSYS Informationssysteme GmbH / Gibraltar

<http://www.esys.at>  
[rene.mayrhofer@gibraltar.at](mailto:rene.mayrhofer@gibraltar.at)

# eSYS Informationssysteme GmbH

## Tätigkeitsschwerpunkte

- **IT-Consulting**
  - Kompetenzschwerpunkt Security
- **IT-Security**
  - Firewalls, E-Mail-Security, VPN, Bandbreitenmanagement, Antivirus, Verschlüsselung, etc.
  - Durchführung von Forschungsprojekten
- **IT-Services und Outsourcing**
  - Microsoft Gold Certified Partner
  - Linux
- **Softwareentwicklung**
  - .NET
  - Java

Gründung 2002, derzeit 12 Mitarbeiter, Tendenz steigend

# Sprecher: Rene Mayrhofer

## Akademische Qualifikation

- Studium **Technische Informatik** an JKU Linz, 1998-2002
- **Doktorat** der technischen Wissenschaften an JKU, 2002-04
- **Habilitation** (*venia docendi*) für Praktische Informatik, Universität Wien, März 2009
- Über 30 Publikationen, Teilnahme an über 5 Forschungsprojekten (Leitung von 2), Lehre an JKU Linz, Universität Wien, Lancaster University (UK), FH Hagenberg

## Praxiserfahrung zum Thema Informationssicherheit

- Projekt- und Produktleitung „**Gibraltar Firewall**“ seit Sommer 1999
- Verschiedene Projekte zur Verbesserung oder Überprüfung von Netzwerksicherheit in Unternehmensnetzwerken (einschließlich Versicherungen)
- Entwicklung des „**OpenUAT**“ Toolkits zur Authentifizierung von neuen/mobilen Geräten
- Design von Authentifizierungsprotokollen und verschlüsselten Datenbanken
- Technologieerfahrungen mit Smart Cards, Hardware Crypto-Tokens, Bürgerkarte, Antivirus-Engines, Mobilgeräten, div. VPNs, OS-Sicherheitsmaßnahmen, Email-Sicherheit, Sicherheitsmaßnahmen auf Source-Code-Ebene (Secure Coding Practices), etc.

# Emails sind wie Postkarten

## Frei lesbar

- Unverschlüsselt, kein „Umschlag“
- Kann während der gesamten Übermittlungskette gelesen werden

## Nicht unterschrieben

- Keinerlei Überprüfbarkeit des Absenders
- Leicht im Nachhinein änderbar

## Durch nicht vertrauenswürdige Instanzen übermittelt

- Infrastruktur durch Dritte betreut

## Billig

# Schwächen werden ausgenützt

## Phishing

- Emails mit gefälschtem Absender
- Ziel: Empfänger soll bestimmte Aktion ausführen, z.B. Login-Daten in gefälschten Webserver eingeben

## Spionage

- Emails werden entweder bei Übermittlung oder im Benutzerpostfach von nicht berechtigten Personen gelesen
- Ziel: Erlangen von privaten/geheimen Daten

## Missachtung der Privatsphäre

## Und sehr viele mehr!

# Beispiel für Phishing-Email



The image shows a screenshot of a phishing email. On the left is a yellow vertical bar with the Postbank logo. The main content is on a light blue background. The text is in German and uses a mix of bold and regular fonts to mimic a real bank communication. It includes a salutation, a paragraph of text with a mouse cursor pointing to a word, a URL, a warning not to reply, and a footer with a copyright notice.

**Postbank**

**Sehr geehrte Kundin Sehr geehrter Kunde**

Wir sind gezwungen, Ihnen folgendes mitzuteilen. Im Zusammenhang mit häufiger wiederholten Angriffen auf die Portale der PostBanken ist die Direktion der PostBank zur Entscheidung gekommen, eine vollständige Zwangserneuerung der Informationen über Ihre Konten vorzunehmen. Sie müssen das nachfolgende Link befolgen und die Angaben zum Zugriff von Ihrem Konto ändern. Auf Grund der entstandenen Situation wollen wir auf Ihr Verständnis und Zusammenarbeit hoffen, weil es der beste Weg ist, ihre Konten zu sichern.

<https://banking.postbank.de/app/welcome.do>

Antworten Sie bitte auf diesen Brief nicht. Die Briefe, die an diese Anschrift geschickt werden, werden nicht beantwortet.  
Um Hilfe zu bekommen,  
Kommen Sie auf Ihr PostBank konto und tippen Sie oben auf der beliebigen Seite ein.

**2005 PostBank Inc.c**  
Alle Rechte vorbehalten. Handelsmarken und Brands sind Eigentum von ihren Besitzern.

# Transportsicherheit für Emails

## **SMTP-TLS** für Transportsicherheit **zwischen Email-Servern**

- Wird von den meisten aktuellen Servern unterstützt
- Muss meist nicht gesondert aktiviert oder eingerichtet werden  
Ausnahme: X.509 Zertifikat für Server erforderlich
- „Opportunistic security“: Server gibt mit Begrüßungsmeldung Unterstützung von TLS bekannt, wenn beide Seiten OK, dann im nächsten Schritt aktiviert
- Sicherheit nur gegen ausgewählte Gefährdungen
  - Abfangen/Mitlesen von Emails auf Transportweg (Provider)
  - Schutz der gesamten Nachricht inkl. SMTP Envelope
- **Keine Sicherheit** gegen Angriffe auf Mailbox der Benutzer!

# Sicherung der Nachrichten

Nachrichtensicherheit = **End-to-End Security** (Ende-zu-Ende Sicherheit)  
(fast immer – siehe spätere Erklärungen zu PGP Email Gateway)

- **Email-Client des Senders** verschlüsselt und/oder signiert
- **Email-Client des Empfängers** entschlüsselt und/oder prüft
- Sicherheit gegen andere Gefährdungen als bei Transportsicherheit
  - Nur „innerer“ Teil der Nachricht geschützt
  - Dafür nicht von Servern abhängig und mit jedem Provider möglich
- **Keine Sicherheit** der SMTP Envelope
  - Angriffe auf Privatsphäre (wer kommuniziert wann wie oft mit wem) weiter möglich

# Verschlüsselung ist kein Generalrezept

## Sicherheitsmaßnahmen müssen auf Gefahren eingehen

- Verschlüsselung hilft nicht gegen Fälschung des Absenders
- Verschlüsselung muss an der richtigen Stelle erfolgen, um einen bestimmten Angriff abzuwehren
- Digitale Unterschrift muss nicht unbedingt gegen Modifikation schützen, sondern wiederum an der richtigen Stelle erfolgen
  - DKIM-Signaturen gegen Fälschung von Absender-Domains
  - S/MIME, OpenPGP bzw. PGP/MIME gegen Fälschung des Inhalts
- **Weder Verschlüsselung noch Signatur hilft gegen Analyse von Verkehrsdaten laut aktueller Rechtslage (Sicherheitspolizeigesetz)!**  
Einzige Gegenmaßnahme gegen diese Gefahr: **Mix-Netzwerke**

# Grundbegriffe aus der Kryptographie

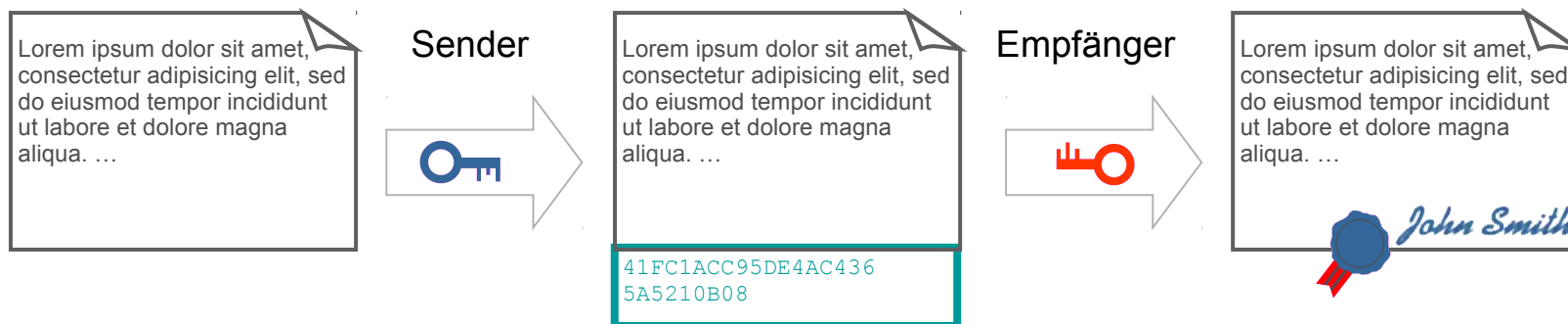
## Verschlüsselung

- 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

# Rechtsgültige Signaturen / Bürgerkarte

## Sichere/Qualifizierte Signatur

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

## Unterschied zur „gewöhnlichen“ elektronischen Signatur

- Speicherung des digitalen
- Starke Bindung des digitalen
- Maßnahmen

## Verwendung aus Beispiel

- Chipkarte + PIN für Erstellung einer Signatur und Entschlüsselung  
**Muss zum Zeitpunkt der Signatur vorliegen und unmittelbar verwendet werden!**
- Prüfung von Signaturen und Verschlüsselung ohne Chipkarte
- Problem Zeitstempeldienst

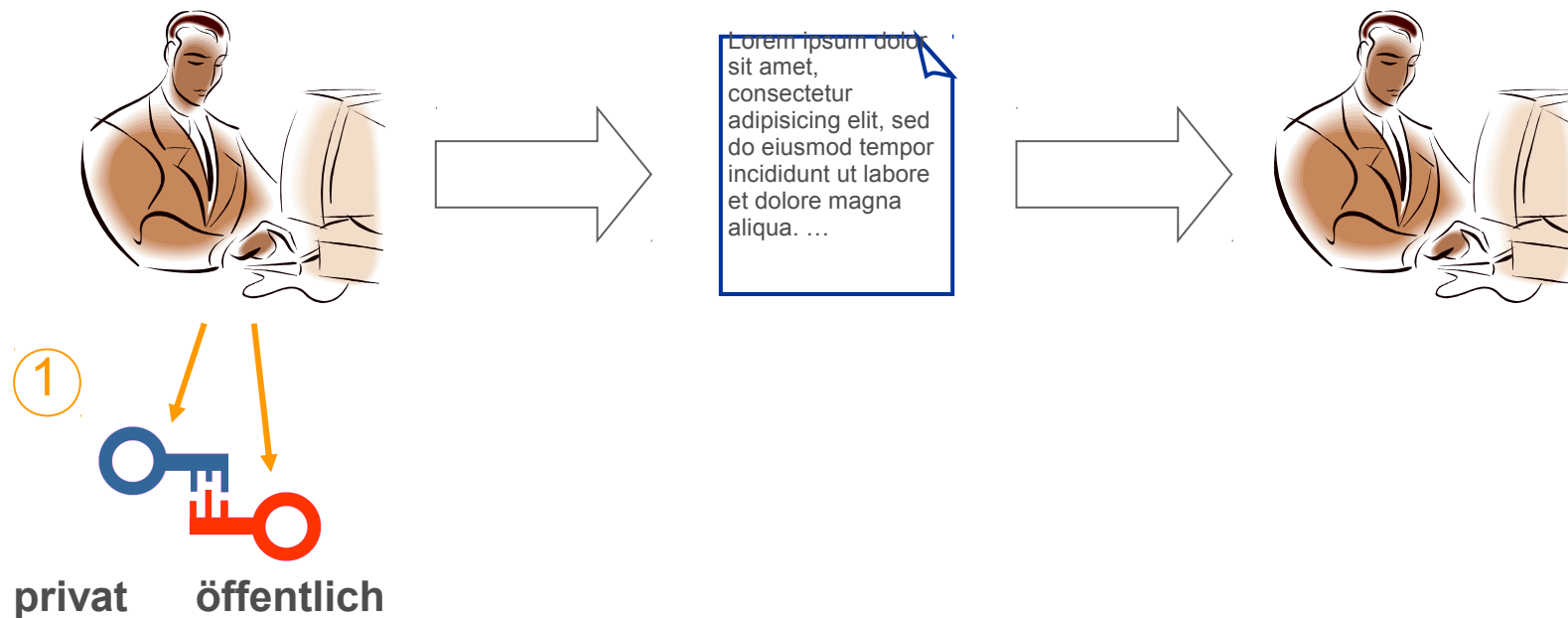


# Email-Signatur mit Standard-Clients

## Standards zur Signatur und Verschlüsselung von Emails

- **PGP/OpenPGP**
- **S/MIME**

## Verwendung digitaler Signaturen mit Standard-Software: OpenPGP

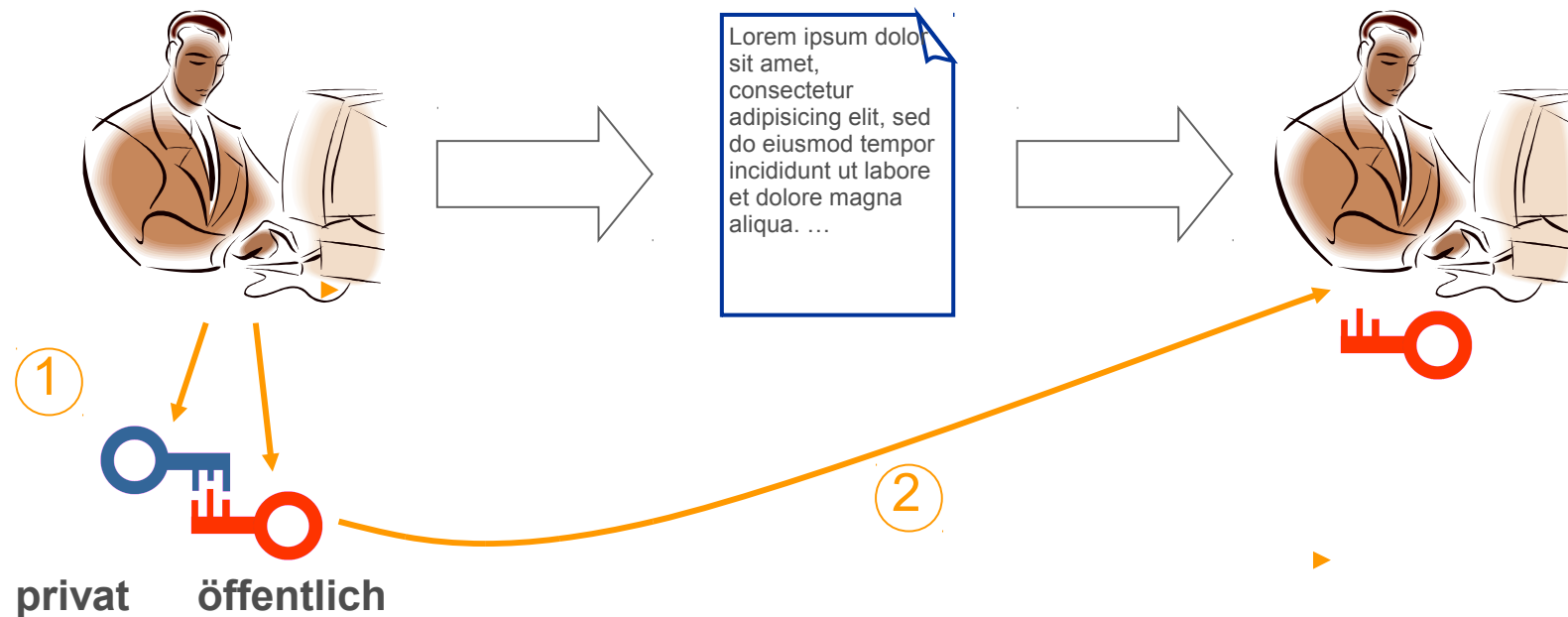


# Email-Signatur mit Standard-Clients

## Standards zur Signatur und Verschlüsselung von Emails

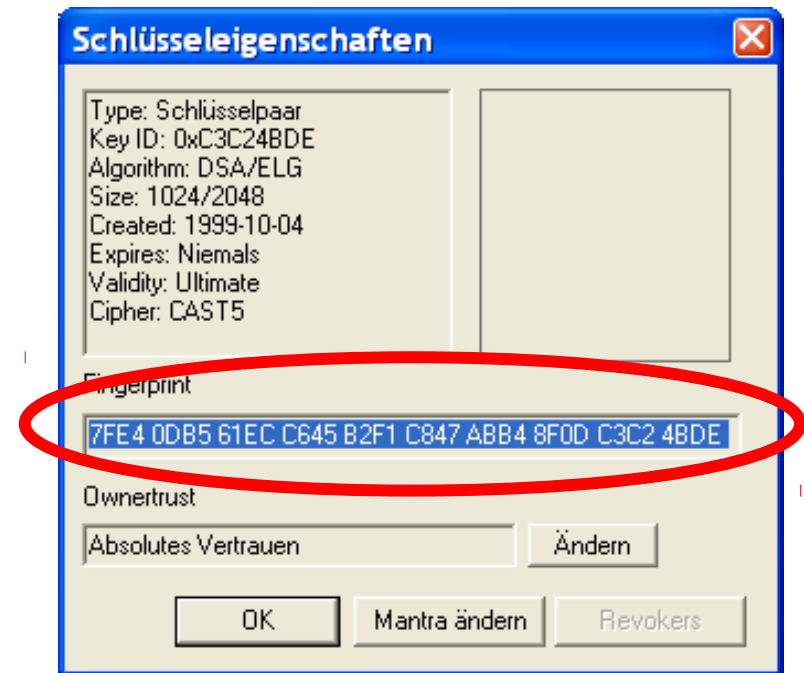
- **PGP/OpenPGP**
- **S/MIME**

## Verwendung digitaler Signaturen mit Standard-Software: OpenPGP



# Problem der Schlüsselüberprüfung

- Wie weiß der Empfänger, dass er mit dem Absender kommuniziert, der er vorgibt zu sein?
- Oder: Woher weiß ich, welcher Schlüssel zu Person XYZ gehört?



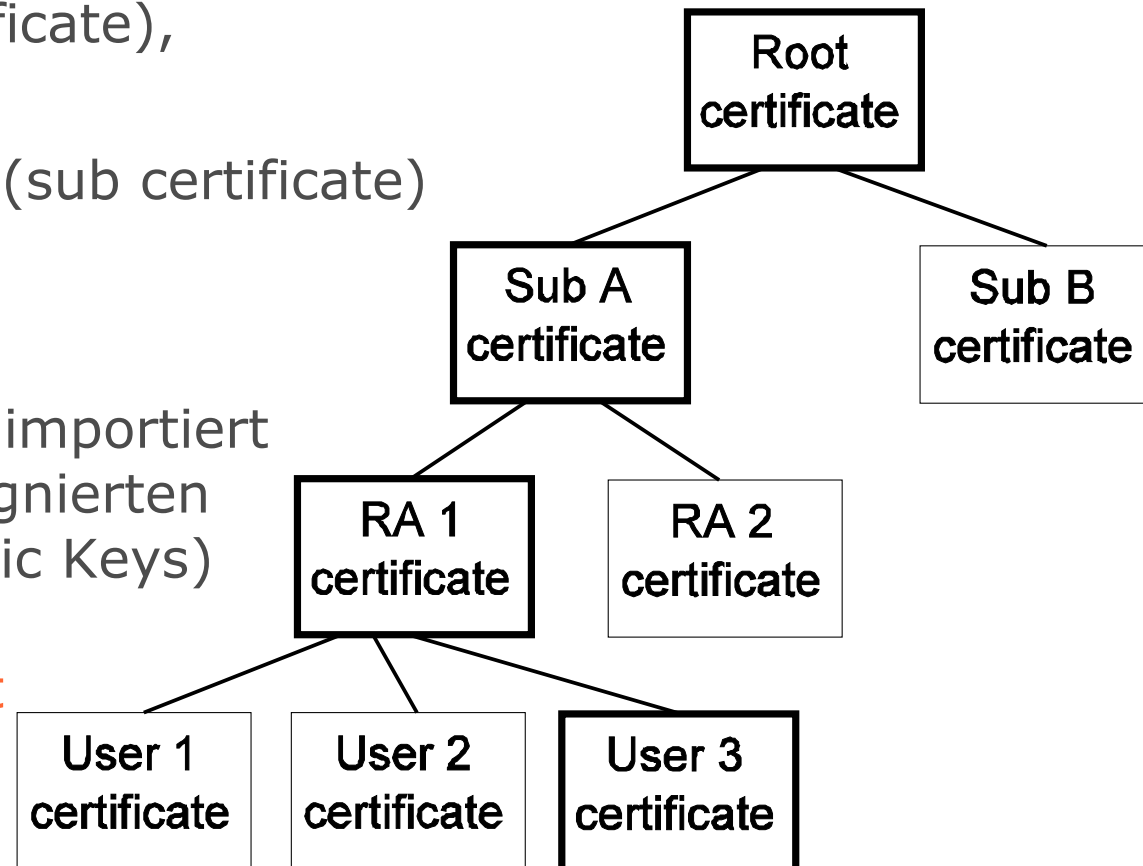
# Public Key Infrastructure

**PKI** Ziel: „**trusted third party**“ um Public Keys zu authentifizieren

- Ein Wurzelzertifikat (root certificate),  
z.B. **A-Trust für Bürgerkarte**
- signiert Unterzertifikatsstellen (sub certificate)
- diese signieren Zertifikate von Benutzern, Rechner, etc.
- Nur das Wurzelzertifikat muss importiert werden, damit alle darunter signierten Zertifikate (und damit die Public Keys) verifiziert werden können

**Aber: A-Trust nicht per default**

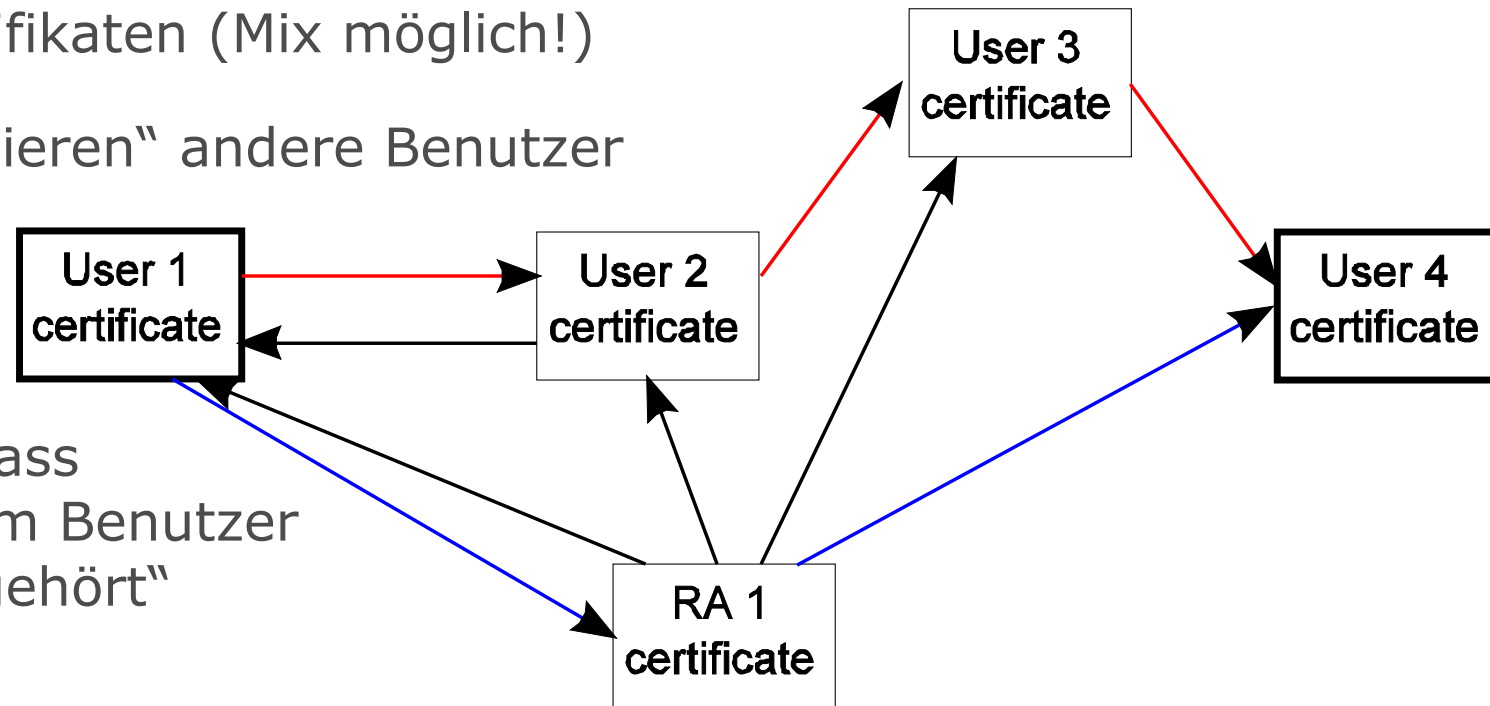
- Verschiedene Standards, X.509 am gebräuchlichsten



# Web of Trust

## Alternative zu PKI

- Kein einzelnes Wurzelzertifikat
- Keine Unterscheidung zwischen Benutzer- und Signaturzertifikaten (Mix möglich!)
- Benutzer „zertifizieren“ andere Benutzer



„Ich habe geprüft, dass dieser Public Key dem Benutzer mit diesem Namen gehört“

# Schlüssel-Widerruf

## Public Keys müssen unter Umständen widerrufen werden

- wenn Private Key kompromittiert wurde
- oder nicht mehr verwendet wird
- oder die zugeordnete Kennung zum Schlüssel ungültig wird (z.B. Erlöschen einer Email-Adresse, Ausscheiden eines Mitarbeiters aus dem Unternehmen, etc.)

## Möglichkeiten zum Widerruf

- Durch Ablauf der Lebenszeit von Zertifikaten
- Durch Certificate Revocation Lists (CRL)

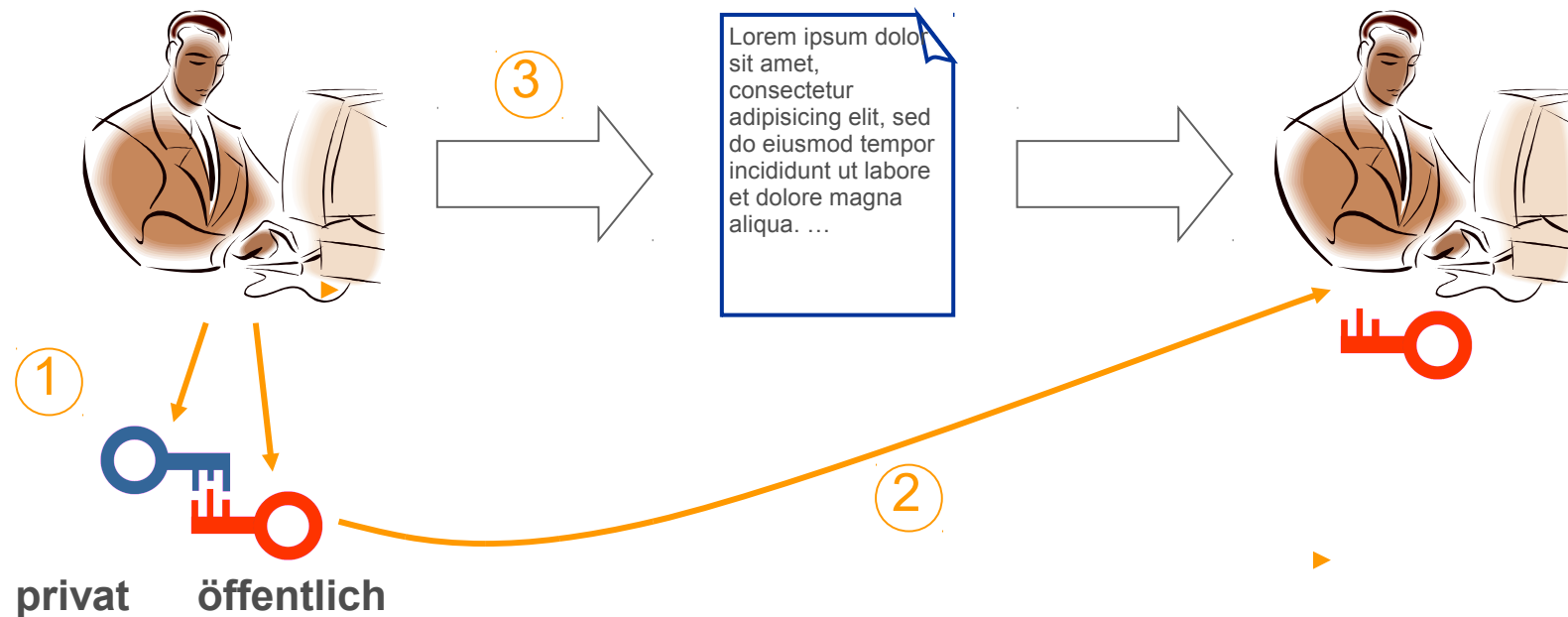
Nach wie vor eines der größten Probleme von PKIs, derzeit quasi ungelöst

# Email-Signatur mit Standard-Clients

## Standards zur Signatur und Verschlüsselung von Emails

- **PGP/OpenPGP**
- **S/MIME**

## Verwendung digitaler Signaturen mit Standard-Software: OpenPGP



# Signieren mit Outlook



# Signieren mit Thunderbird

The screenshot displays the Mozilla Thunderbird interface. The main window is titled 'Posteingang für rene.mayrhofer@gibraltar.at - Mozilla Thunderbird'. The 'Enigmail' menu item in the top menu bar is circled in red. Below it, the 'Verfassen' (Compose) window is open, showing a draft email titled 'Verfassen: Re: AW: Offene Fragen - Westlich (ISO-8859-1)'. The 'Enigmail' menu is open, showing options: 'Sign Message (Strg+Umschalt+S)', 'Encrypt Message (Strg+Umschalt+P)', 'Use PGP/MIME for This Message', and 'Ignore Per-Recipient Rules'. The email header shows 'Von: Rene Mayrhofer <rene.mayrhofer@gibraltar.at>', 'An: Rachlinger Harald <rachlir...>', and 'CC: Andreas Wöckl <woeckl...>'. The subject is 'Re: AW: Offene Fragen'. The email body contains the text: 'Hallo Harry, Anbei ein Draft des Konzeptpapiers - wenn es euch so passt, können wir das in den nächsten Tagen finalisieren. Viele Grüße, Rene'. An attachment named 'Konzept.pdf' is visible in the right-hand pane.

# Signieren mit Kmail/Kontakt

The screenshot shows the KMail email client window titled "Re: AW: Offene Fragen - KMail". The toolbar contains various icons, with the "Signieren" (Sign) icon (a blue envelope with a signature) circled in red. Below the toolbar, the email header fields are visible: "Identität: Standard (Standard)", "An: Rachlinger Harald <rachlinger@powerdat.at>", "Kopie an (CC): Andreas Wöckl <woeckl@esys.at>", "Blindkopie an (BCC):", and "Betreff: Re: AW: Offene Fragen". The main body of the email contains the text: "Hallo Harry,", "Anbei ein Draft des Konzeptpapiers - wenn es euch so passt, können wir das in den nächsten Tagen finalisieren.", and "Viele Grüße, Rene". At the bottom, there is a table of attachments:

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

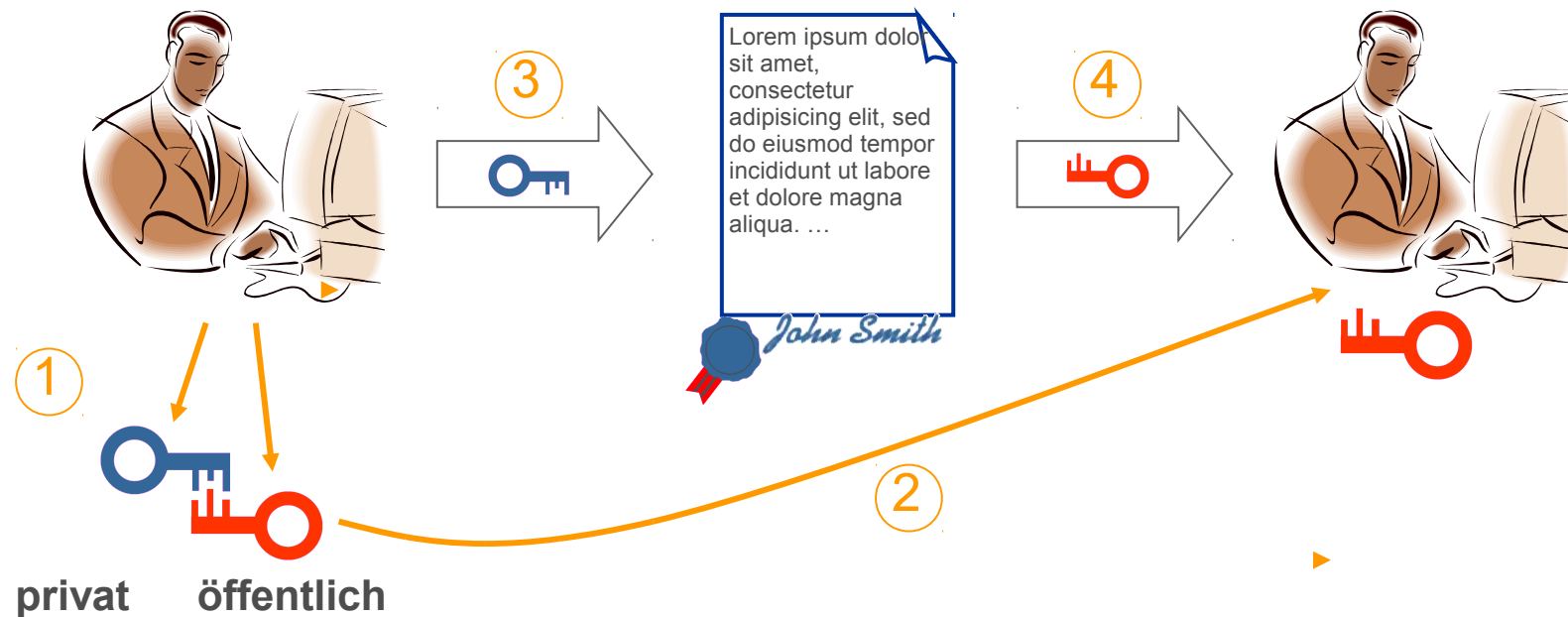
The "Signieren" checkbox in the table is also circled in red. The status bar at the bottom right indicates "Spalte: 1 Zeile: 1".

# Email-Signatur mit Standard-Clients

## Standards zur Signatur und Verschlüsselung von Emails

- **PGP/OpenPGP**
- **S/MIME**

## Verwendung digitaler Signaturen mit Standard-Software: OpenPGP



# Prüfen mit Thunderbird

**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	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
[Gibraltar-list] Bayesfiltering	Christopher...	21.03.2005 14:17

**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

# Prüfen mit Kmail/Kontakt

The screenshot shows the KMail interface with the following details:

- Left Panel (Folder List):** Shows a tree view of folders. The 'Gibraltar' folder is expanded, and 'Mailing-list' is selected, containing 30 messages.
- Message List:** A table of messages with columns 'Betreff', 'Absender', and 'Datum'. The selected message is:
 

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
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
[Gibraltar-list] Bayesfiltering	Christoph Fritsch	21.02.2005 14:17
Re: [Gibraltar-list] Cron <clamav@gibraltar> I... /usr/bin/freshclam.1 && /usr/bin/freshcl	Rene Mayrhofer	16.02.2005 18:35
- Message Content:** The selected message is titled '[Gibraltar-list] Gibraltar 2.2 released'. The header shows:
 

Von: Rene Mayrhofer <rene.mayrhofer@gibraltar.at>  
An: gibraltar-list@gibraltar.at  
Datum: 07.04.2005 21:27
- Signature Verification:** A green bar with a red oval highlights the following text:
 

**Nachrichte enthält Signatur von rene@mayrhofer.eu.org (Schlüssel-ID: 0xABB48F0DC3C24BDE). Die Signatur ist gültig, und der Schlüssel ist vollständig vertrauenswürdig.**
- Main Text:** The email body contains the following text:
 

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
- Bottom Panel:** Shows a table with columns 'Beschreibung', 'Typ', 'Kodierung', and 'Größe'.
 

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

# Client-less Nachrichtensicherheit

## Einbindung von Clients ohne Sicherheits-Plugins

- in Unternehmensnetzen oft unnötig, da Clients kontrolliert werden können
- S/MIME sowie OpenPGP bzw. PGP/MIME Unterstützung entweder schon eingebaut oder für alle wichtigen Clients vorhanden: **Outlook, MacOS/X Mail, Thunderbird, Evolution, Kmail**
- **Problem** derzeit: **Mobile Clients (Smartphones) und Webmail**
- **Problem** mit Schlüssel-Management auf Clients über Unternehmensgrenzen hinweg (innerhalb des eigenen Netzwerk leicht über interne Certificate Authority und automatischem Rollout lösbar)

Mögliche Lösung: zentrales Sicherheits-Gateway für Emails

# Beispiel: PGP Universal Gateway Email

- In SMTP-Kette eingebunden bzw. direkt mit internem Email-Server
- **Verwaltet Schlüssel für Benutzer direkt am Gateway**, Clients müssen diese nicht kennen
- Über Policies gesteuert, welche Emails beim Senden verschlüsselt und/oder signiert werden sowie welche Prüfungen beim Empfangen durchgeführt werden
- Clients arbeiten unverändert weiter
- Externe / unternehmensfremde Benutzer entweder über **Web-Gateway** angebunden (Login am eigenen Gateway zum Abrufen der Emails) oder durch Versenden von **verschlüsselten PDF-Anhängen**
- **Problem mit externen Schlüsseln weiter ungelöst**

# Probleme mit Server-geprüften Signaturen

**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**

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

**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:** V **Teil:** II **Datum der Kundmachung:** 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**

<a href="#">Datei Nr.1</a>	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



# Points to take away

- Email-Sicherheit braucht **Verschlüsselung und Signatur**
- Sicherheitsmaßnahmen müssen den Gefahren entsprechen
- Nachrichtensicherheit ist mit den meisten aktuellen Email-Clients bereits möglich oder einfach nachrüstbar
- Integration in Single-Signon Umgebungen am einfachsten per Smartcard bzw. Crypto-Tokens möglich
- Hauptproblem ist Schlüssel- bzw. Zertifikatsverwaltung
- Zentrale Gateways können bei mobilen und externen Benutzern helfen (Webzugriff), aber Schlüsselmanagement nach wie vor schwierig

# Danke für Ihre Aufmerksamkeit!

Folien: <http://www.mayrhofer.eu.org/presentations>

eSYS Informationssysteme GmbH  
Steinhüblstraße 1  
4800 Attnang-Puchheim  
Tel: +43 720 702 845  
Fax: +43 7674 21 495  
office@esys.at

OpenPGP Schlüssel: 0xC3C24BDE  
7FE4 0DB5 61EC C645 B2F1 C847 ABB4 8F0D C3C2 4BDE