

The logo for ZiM (Zentrum für Innovationen und Management) features the letters 'ZiM' in a bold, blue, sans-serif font. The 'i' is lowercase and has a blue dot above it. The background is a dark blue gradient with several light blue speech bubbles of various sizes and orientations.The logo for 'Talk' features the word 'Talk' in a large, bold, red, italicized sans-serif font. Below it, the tagline 'WISSEN SCHAFFT IT' is written in a smaller, red, all-caps sans-serif font. The text is contained within a white speech bubble with a drop shadow, set against a dark blue background with other light blue speech bubbles.

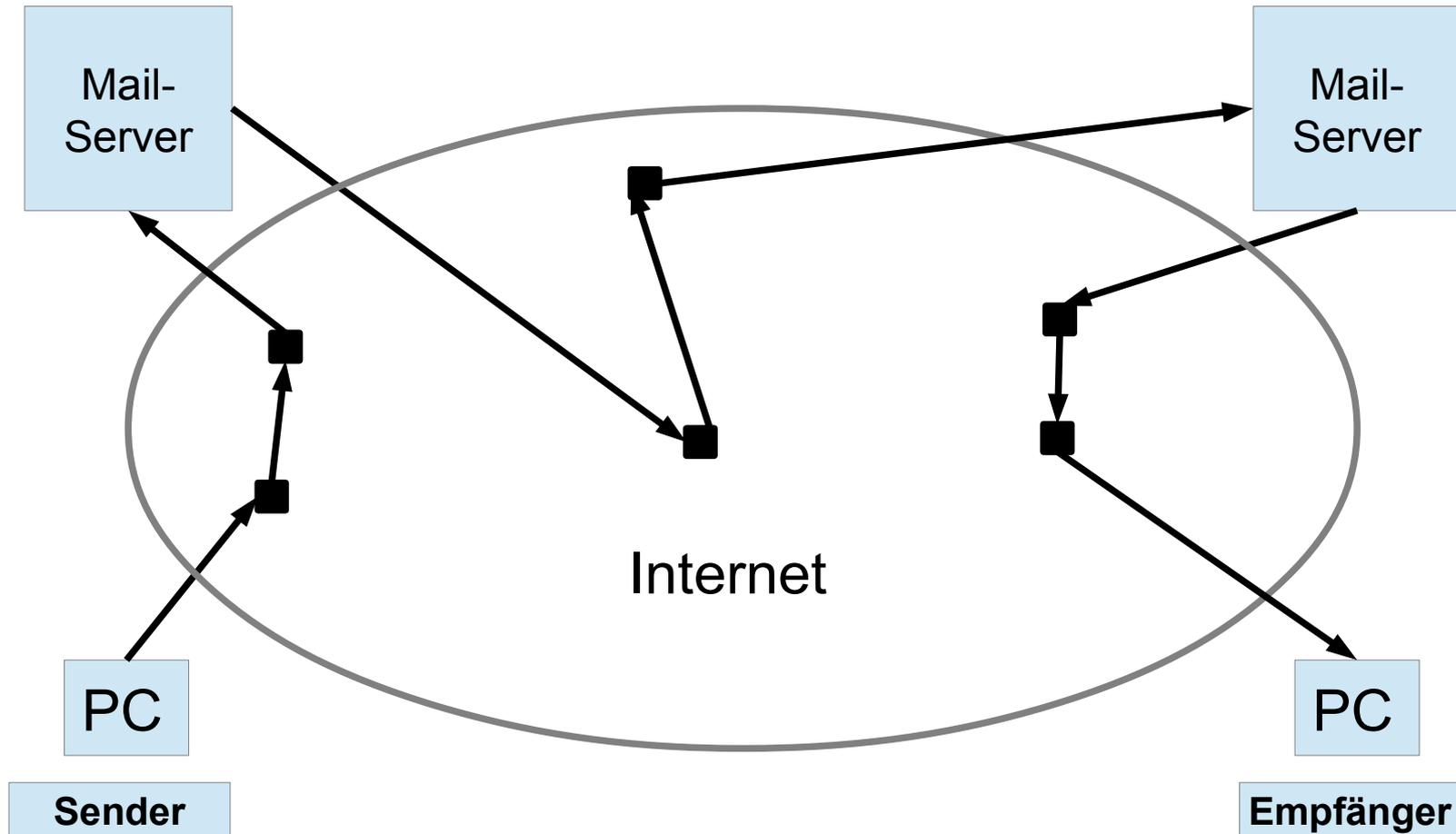
## ***Die Idee des Jahres 2013: Kommunikation verschlüsseln***

UNIVERSITÄT  
DUISBURG  
ESSEN

*Offen im Denken*

 Burkhard Wald ■ 22.11.2013

# Kommunikationsschema bei Email



- ... immer eine Vereinbarung zwischen zwei Kommunikationspartnern: Sender und Empfänger
- Client – Server
- Server – Server
- Client – Client
- End-To-End-Encryption (E2EE)

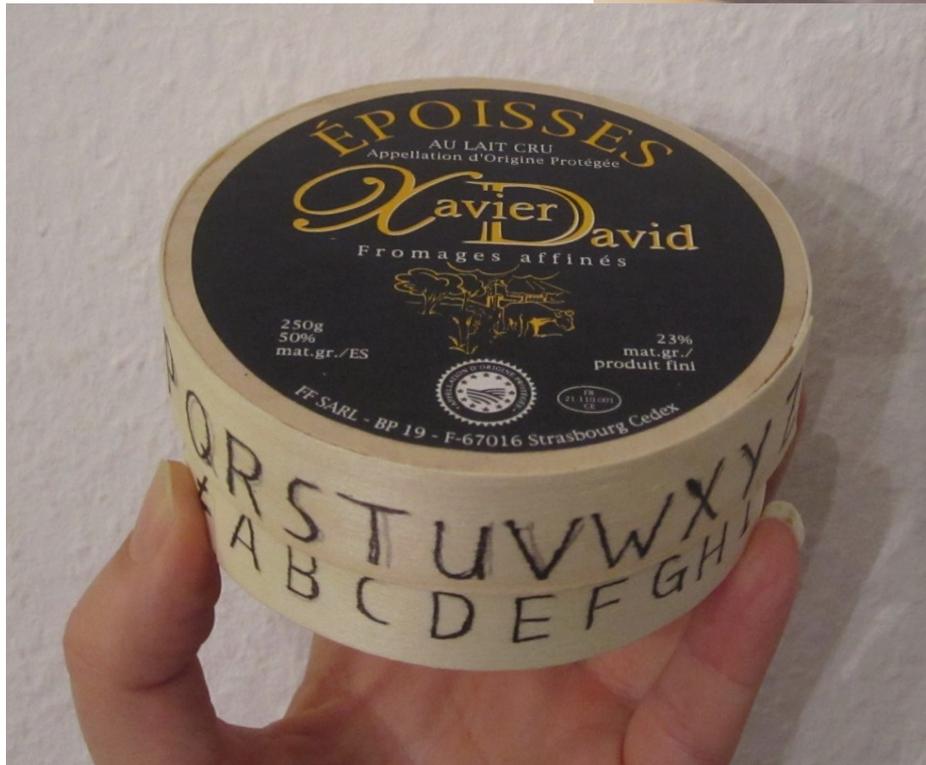
- **1 / 4** aller eingehenden Verbindungen
- **Nur 1 / 3** der eingehenden Mail werden zugestellt.
- **2 / 3** oder **3 / 4** der zugestellten Mails sind verschlüsselt übertragen worden
- **3 / 4** der ausgehenden Mail werden verschlüsselt übertragen
- **ZB. Bei gmx, web.de, google, t-online**
- **Nicht bei Yahoo, Hotmail**
- **Bei den Unis halbe-halbe**



- (griechisch, Rätsel)
- 1923
- 2. Weltkrieg
- Bildquelle: Wikimedia



# Banalverschlüsselung mit einer „Époisses“

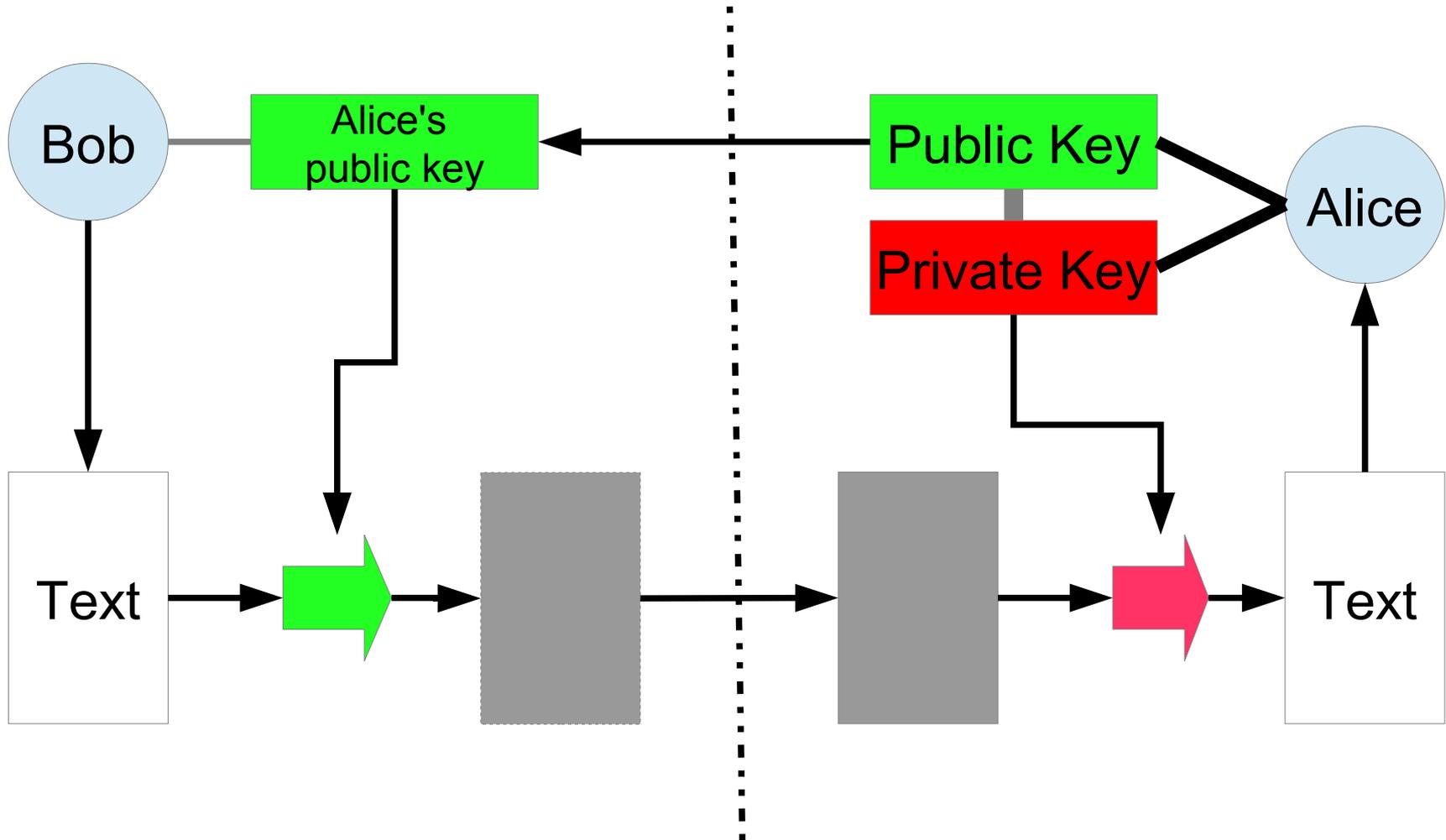


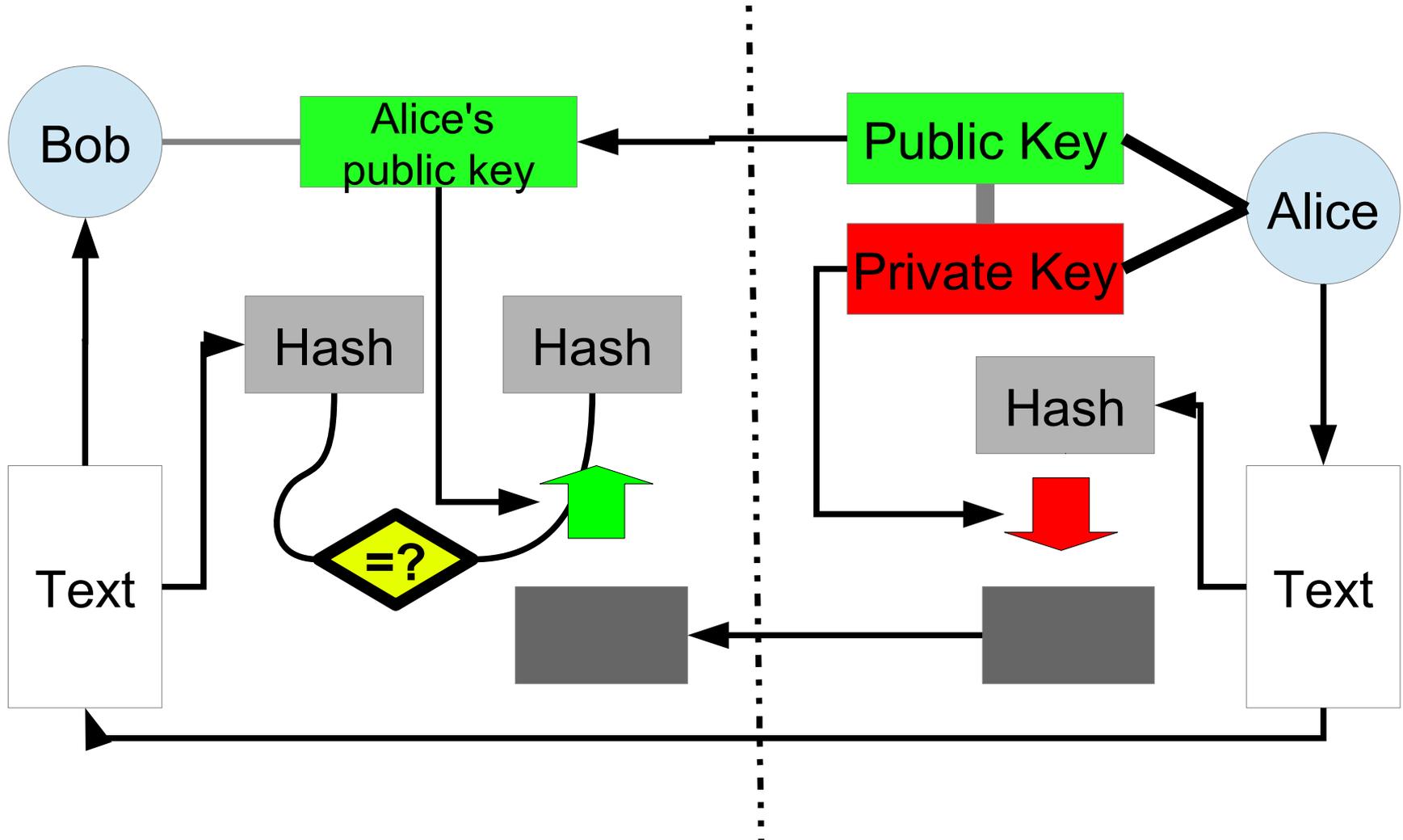
Quelle: [b-eats.blog.de](http://b-eats.blog.de)

- **Entschlüsselung = Verschlüsselung**  
- nur rückwärts.
- **Entschlüsselungs-Key = Verschlüsselungs-Key**
- **Problem: geheimer Schlüsselaustausch über einen unabhängigen Kanal.**
- **Verfahren: IDEA, DES3, AES, Blowfish, RC4**

- Kann es das geben?
- Key a zum Verschlüsseln  
Key b zum Entschlüsseln
- Verfahren  $V_a$  und  $V_b$  sind nicht effizient umkehrbar
- Verfahren  $V_a$  und  $V_b$  sind zueinander inverse math. Funktionen.
- Aus  $a$  und  $b$  kann  $a$  nicht effizient berechnet werden
- Schlüssel  $b$  kann öffentlich sein.
- Antwort = Ja: Verfahren: RSA

- `> echo 107*113 | bc`  
12091
- `> echo 398075086424064937397125500550386491199064\  
362342526708406385189575946388957261768583317 *\  
47277214610743530253622307197304822463291469530\  
2097116459852171130520711256363590397527 | bc`  
  
188198812920607963838697239461650439807163563379\  
417382700763356422988859715234665485319060606504\  
743045317388011303396716199692321205734031879550\  
656996221305168759307650257059
- **RSA-Challenge-576**
- **Dezember 2003 von Jens Franke und Thorsten Kleinjung vom Mathematischen Institut in Bonn und dem Institut für Experimentelle Mathematik in Essen gefunden**







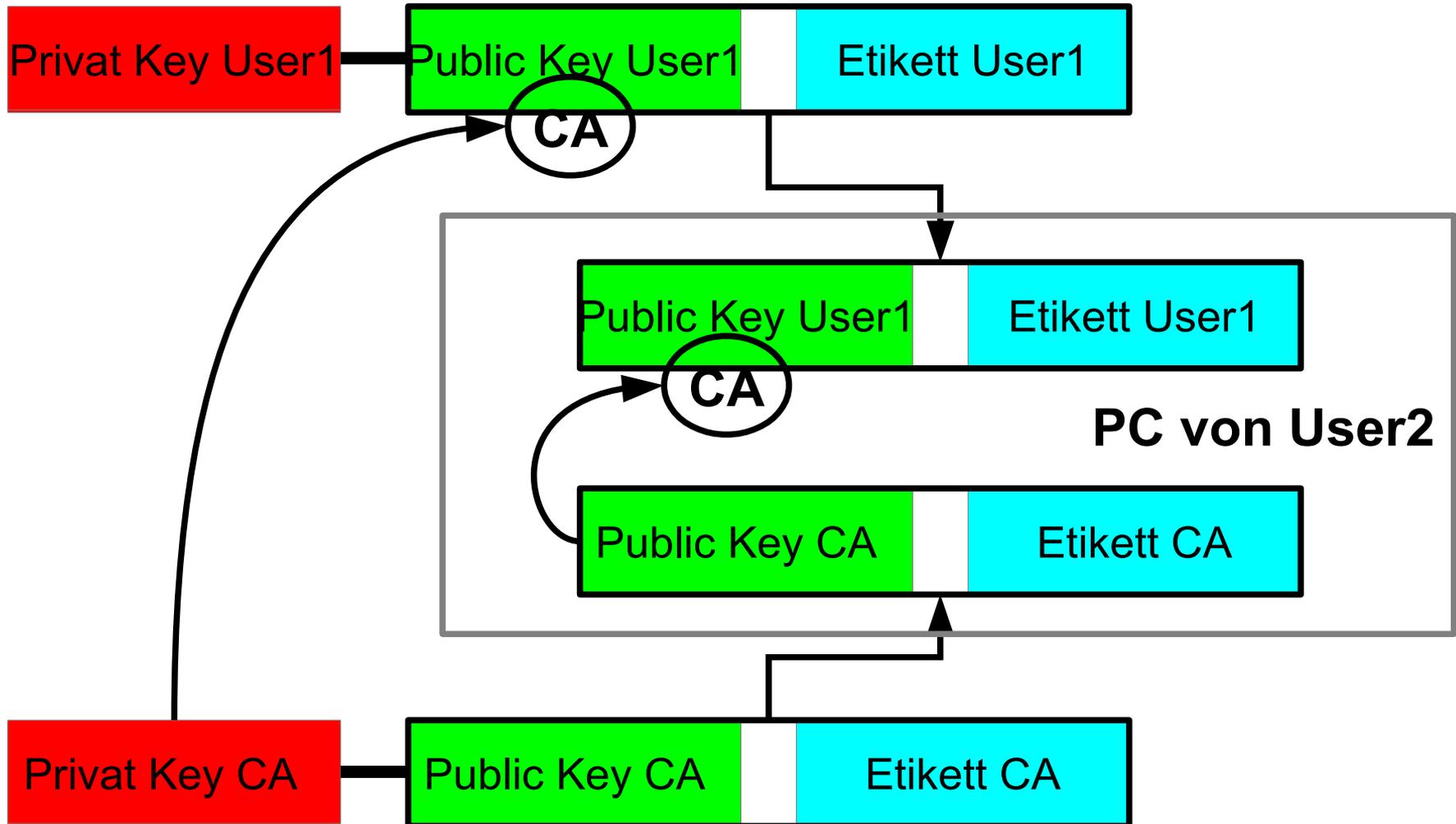
# Schlüssel mit Schlüsselanhängern



- **Sind öffentliche Schlüssel praktikabel?**
- **Auf jeden Schlüssel muss ein Etikett kleben.**
- **Kann man den Etiketten vertrauen?**
- **Lösung: Zertifikate und Fingerprints**

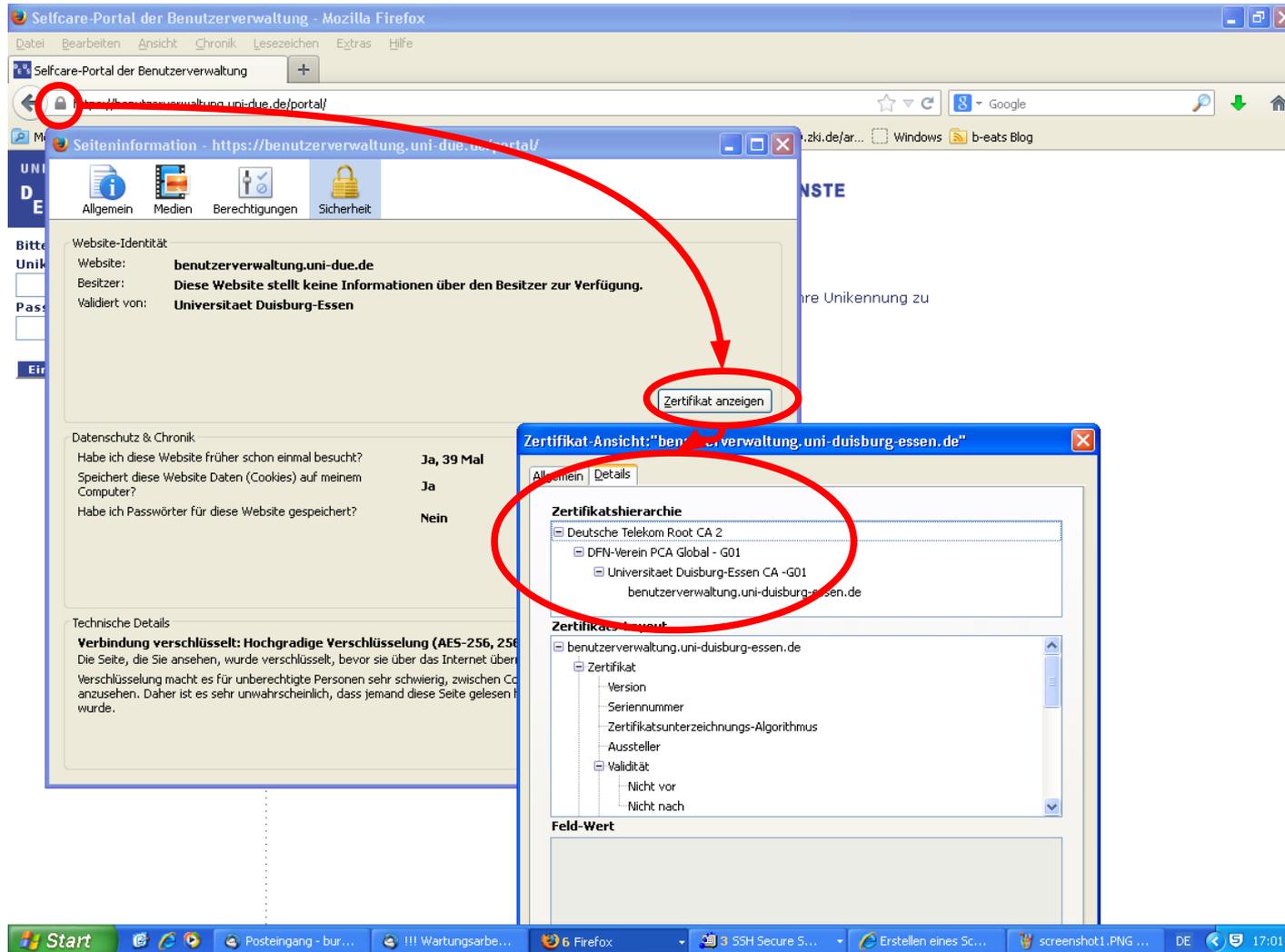
- **Mathematische Verfahren**
  - (symmetrische Verschlüsselung, Public Key, Hash-Verfahren (Fingerprints), Zufallszahlen)
- **Formate und Protokolle**
  - (Dateiformate, Kommunikations-Protokolle)
- **Anwendungsverfahren**
  - (PGP/GPG, S/MIME)
- **Software**
- **Handhabung**
  - (Schlüsseltausch, PKI)

- **1. PKI (public key infrastructure) mit X509-Zertifikaten.**
  - SSL/TLS (Verschlüsselung auf einer Transportschicht-ebene)
  - Gleiche Verfahren für Server-Server, Client-Server und Client-Client
  - Organisierter Verbund von Zertifizierungsstellen
- **2. PGP/GPG.**
  - Spezielle Software erforderlich
  - Vertrauen entsteht durch Direktkontakt und nicht durch Infrastruktur von Institutionen.
  - Es gibt trotzdem ein Konzept der Vertrauensweitergabe



- **Browser-und Betriebssystem-Hersteller vertrauen wenigen Zertifizierungsstellen und bauen die öffentliche Schlüssel in ihre Software als vertrauenswürdig ein: sogenannte Root-Zertifizierungsstellen**
- **Die Root-Zertifizierungsstellen stellen Zertifikate für die Schlüssel von untergeordneten Zertifizierungsstellen aus**
- **Die Kette geht weiter bis zum User- oder Serverzertifikat.**

# Zertifikatsketten ansehen



- **SSL, TLS**
- **HTTPS, IMAPS, LDAPS,**
- **STARTTLS**
- **Serverzertifikate nutzen die gleiche PKI**
- **Zwei Aspekte**
  - Bin ich mit dem richtigem Server verbunden?
  - Datentransfer verschlüsseln (in beiden Richtungen)
- **Der Server-Key reicht.**

- **Key erzeugen und Zertifikat beantragen**
- **PDF ausdrucken und unterschreiben**
- **Bei CA mit Personalausweis erscheinen**
- **Zertifikat erhalten und im Browser einbinden.**
- **Schlüssel und Zertifikat als Datei exportieren**
- **Schlüssel und Zertifikat in Mailprogramm importieren**
- **Schlüssel und Zertifikat mit Mailkonto verbinden**
- **Elektronische Unterschrift unter eigener Mail ist möglich.**
- **Empfangene verschlüsselte Mail kann entschlüsselt werden.**

# Schlüsselerzeugungen und Zertifikat beantragen

The screenshot shows a Mozilla Firefox browser window with the Uni-DUE CA website. The page title is "Uni-DUE CA" and the URL is "https://pki.pca.dfn.de/uni-duisburg-essen-ca/cgi-bin/pub/pki?cmd=basic\_csr;id=1;menu\_item=1;XSEC". The page features the University of Duisburg-Essen logo and the DFN (Deutsches Forschungsnetz) logo. A navigation menu includes "Zertifikate", "CA-Zertifikate", "Gesperrte Zertifikate", "Policies", "Hilfe", and "Beenden". Below this, there are tabs for "Nutzerzertifikat", "Serverzertifikat", "Zertifikat sperren", and "Zertifikat suchen". The main content area is titled "Nutzerzertifikat beantragen" and contains a form with the following sections:

**Zertifikatdaten**

Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (\*) müssen ausgefüllt werden.

E-Mail \*

Name \*

Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:" voran. Verwenden Sie keine Umlaute.

Abteilung

Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen aufgenommen.

**Weitere Angaben**

Diese Angaben werden nicht in das Zertifikat übernommen.

PIN (Mindestens 8 beliebige Zeichen) \*

Nochmalige Eingabe der PIN zur Bestätigung \*

Die PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen oder um dieses einzulesen, wenn Sie einer Veröffentlichung nicht zustimmen. Bitte notieren Sie sich die PIN.

Ich verpflichte mich, die in den [Informationen für Zertifikatinhaber](#) aufgeführten Regelungen einzuhalten. \*

Ich stimme der [Veröffentlichung des Zertifikats](#) mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu.

Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an [pki@dfn.de](mailto:pki@dfn.de) widerrufen.

# Schlüssel und Zertifikat exportieren

The screenshot shows the Mozilla Firefox interface with the 'Einstellungen' (Settings) window open to the 'Zertifikate' (Certificates) tab. The 'Zertifikate anzeigen' button is highlighted. A red arrow points from this button to the 'Zertifikat-Manager' window, which is open to the 'Ihre Zertifikate' tab. In the 'Zertifikat-Manager' window, the 'Burkhard Wald' certificate is selected, and the 'Sichern...' (Export) button is highlighted. Red circles and arrows indicate the sequence of actions: clicking the 'Einstellungen' menu, navigating to 'Zertifikate', clicking 'Zertifikate anzeigen', opening the 'Zertifikat-Manager', selecting the 'Burkhard Wald' certificate, and clicking 'Sichern...'.

Willkommen an der Universität Duisburg-Essen - Mozilla Firefox

https://www.uni-due.de

UNIVERSITÄT DUISBURG-ESSEN

Einstellungen

Allgemein | Tabs | Inhalt | Anwendungen | Datenschutz | Sicherheit | Sync | Erweitert

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

Automatisch eins wählen  Jedes Mal fragen

Zertifikate anzeigen | Wiederholung | Kryptographie-Module

**Zertifikat-Manager**

Ihre Zertifikate | Personen | Server | Zertifizierungsstellen | Andere

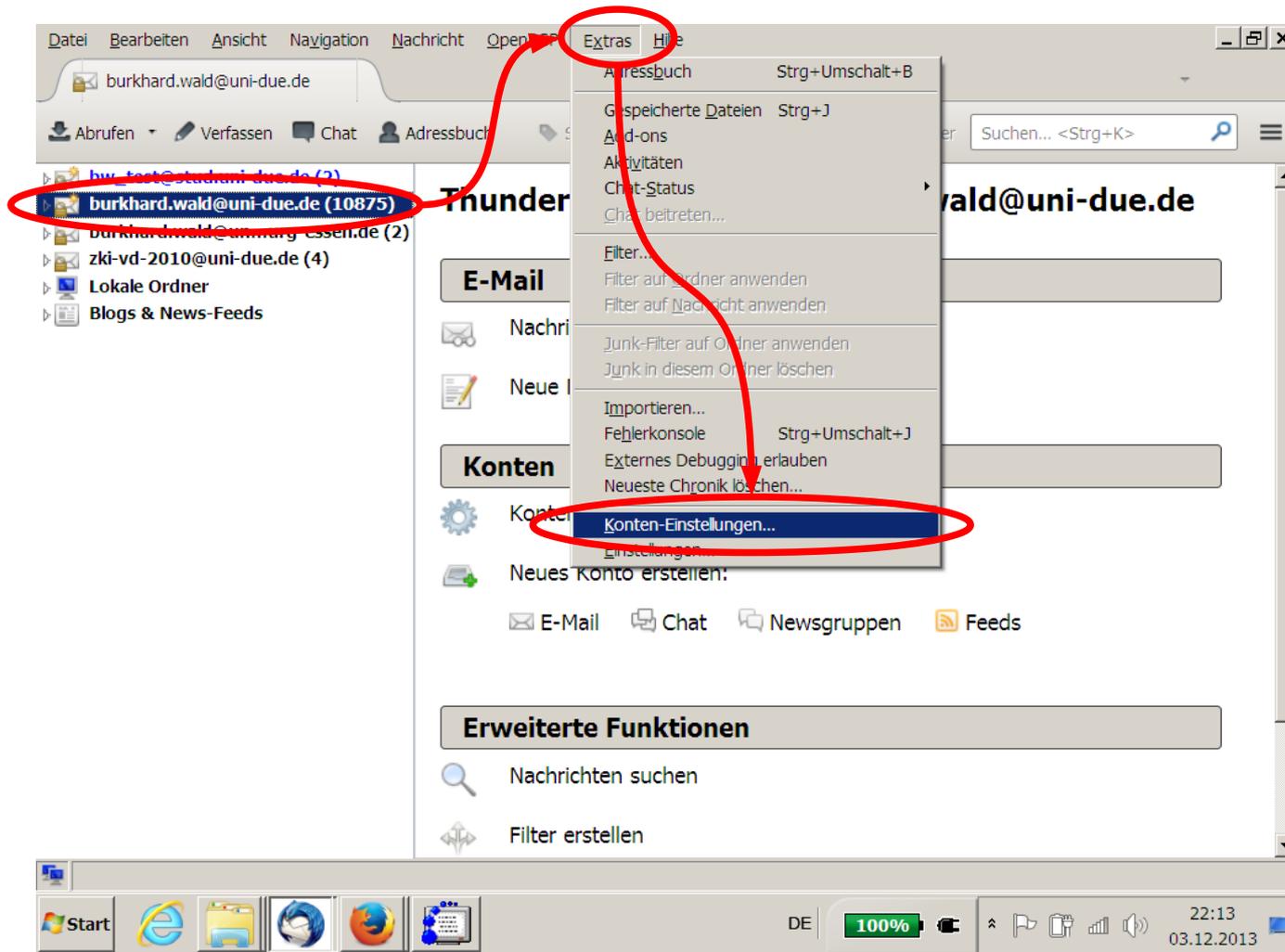
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:

Zertifikat	Kryptographie-Modul	Seriennummer	Läuft ab am
Universität Duisburg-Essen			
Burkhard Wald	Software-Sicherheitsmodul	11:A9:3C:04	22.03.2014

Ansehen... | Sichern... | Alle sichern... | Importieren... | Löschen...

OK

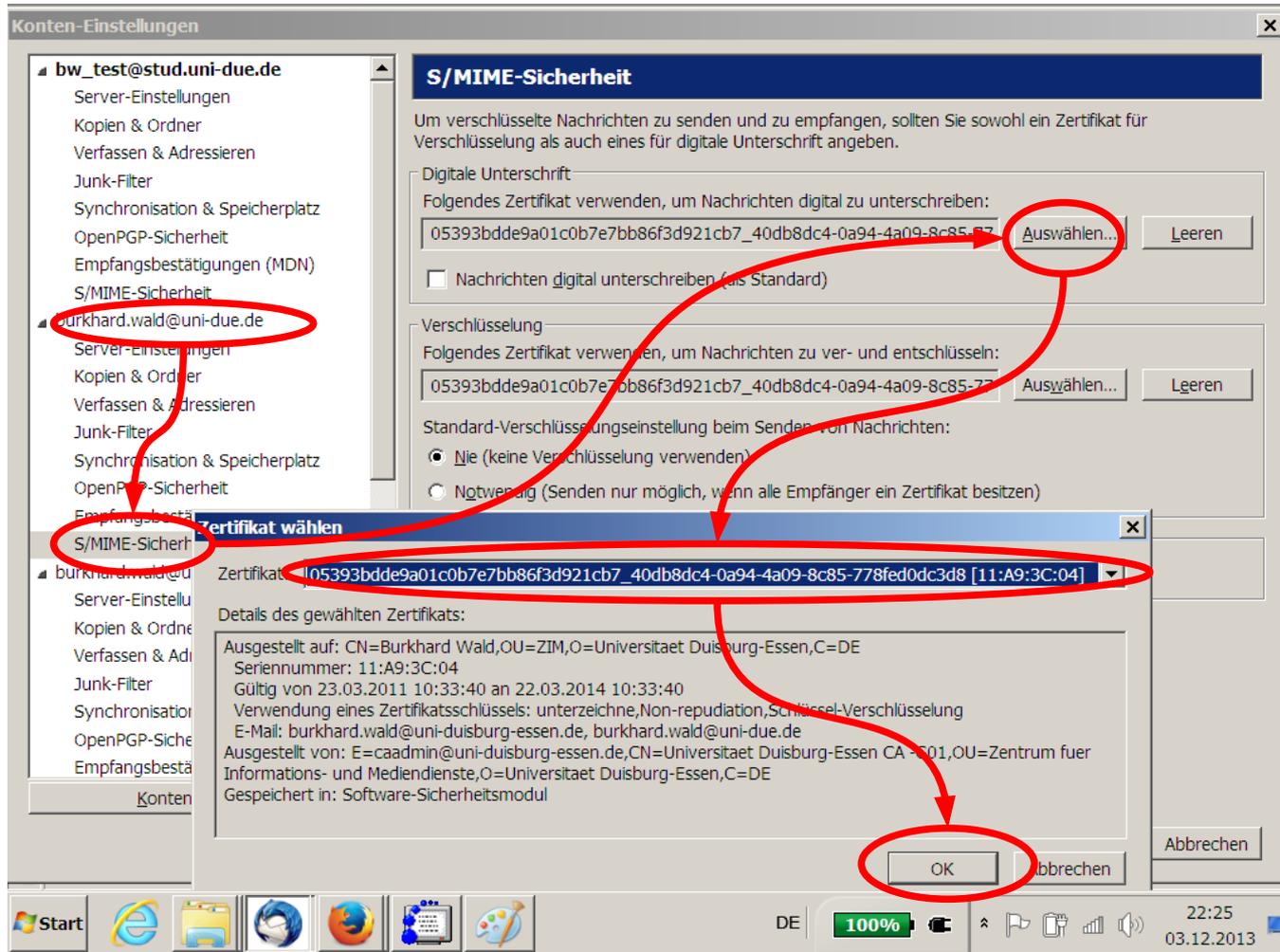
# Konteneinstellung im Thunderbird



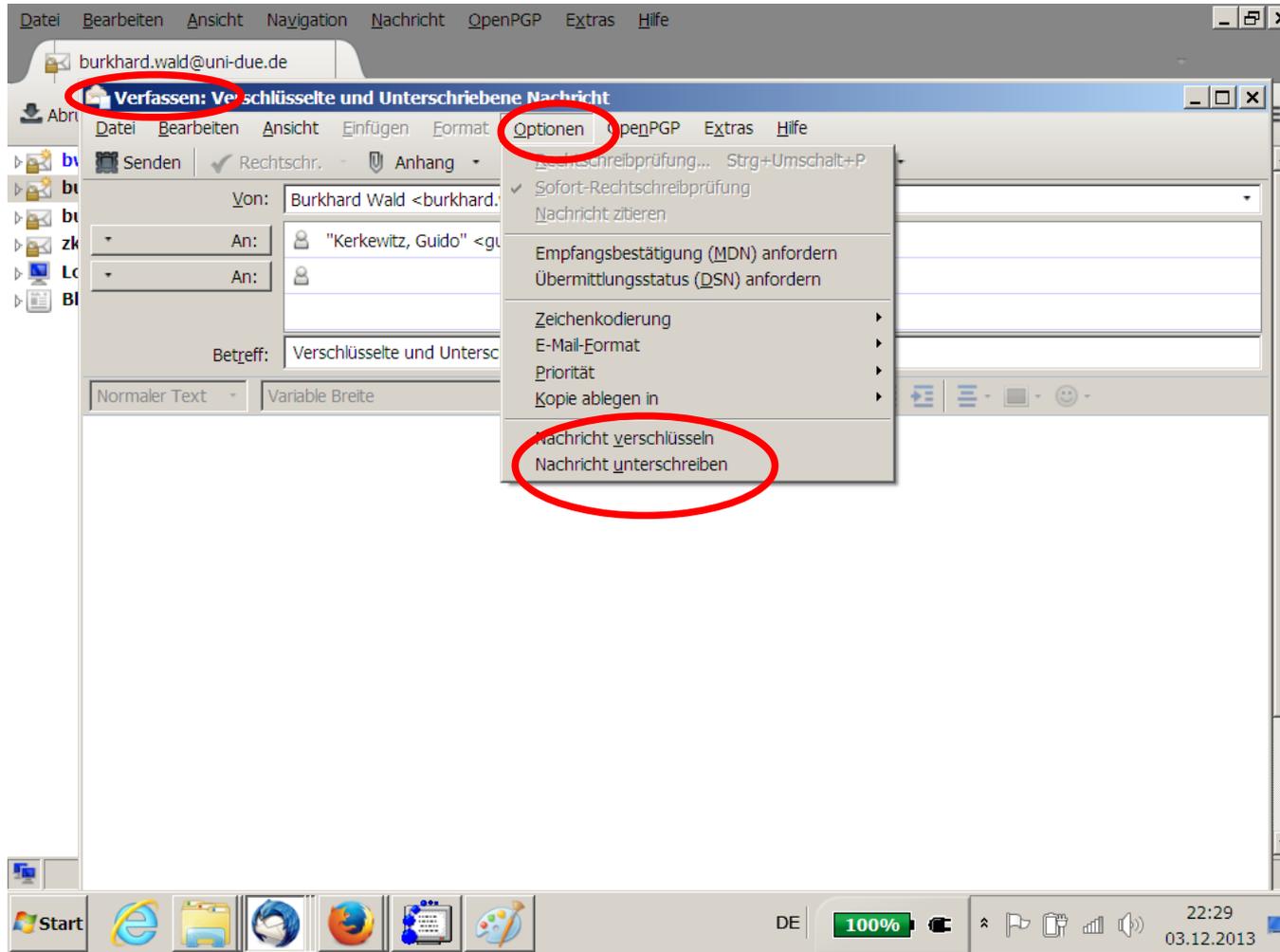
# Importieren eines Schlüssels in Thunderbird

The screenshot shows the 'Konten-Einstellungen' (Account Settings) window for the account 'burkhard.wald@uni-due.de'. The 'S/MIME-Sicherheit' (S/MIME Security) section is selected in the left sidebar. The main pane shows the 'S/MIME-Sicherheit' settings, including 'Digitale Unterschrift' (Digital Signature) and 'Verschlüsselung' (Encryption) options. A red circle highlights the 'S/MIME-Sicherheit' option in the sidebar, and another red circle highlights the 'S/MIME-Sicherheit' section in the main pane. A red arrow points from the sidebar to the main pane. Below the main pane, the 'Zertifikat-Manager' (Certificate Manager) window is open, showing a list of certificates. A red circle highlights the 'Importieren...' (Import...) button. A red arrow points from the 'Importieren...' button back to the 'S/MIME-Sicherheit' section in the main pane. The 'Zertifikat-Manager' window shows a table of certificates:

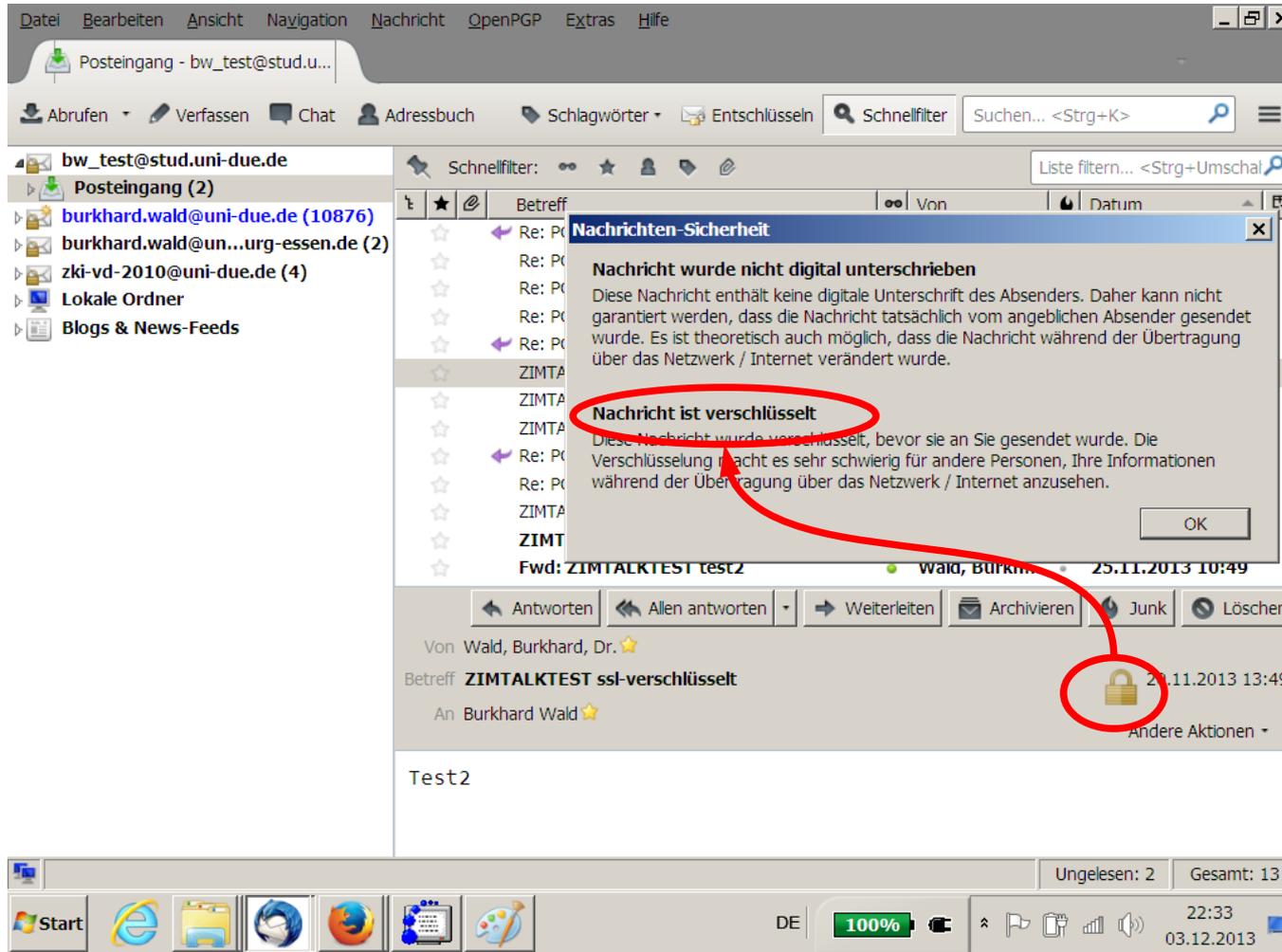
Zertifikatsname	Kryptographie-Modul	Seriennummer	Läuft ab am
Universitaet Duisburg-E...			
Burkhard Wald	Software Sicherheitsmodul	11:A9:3C:04	22.03.2014

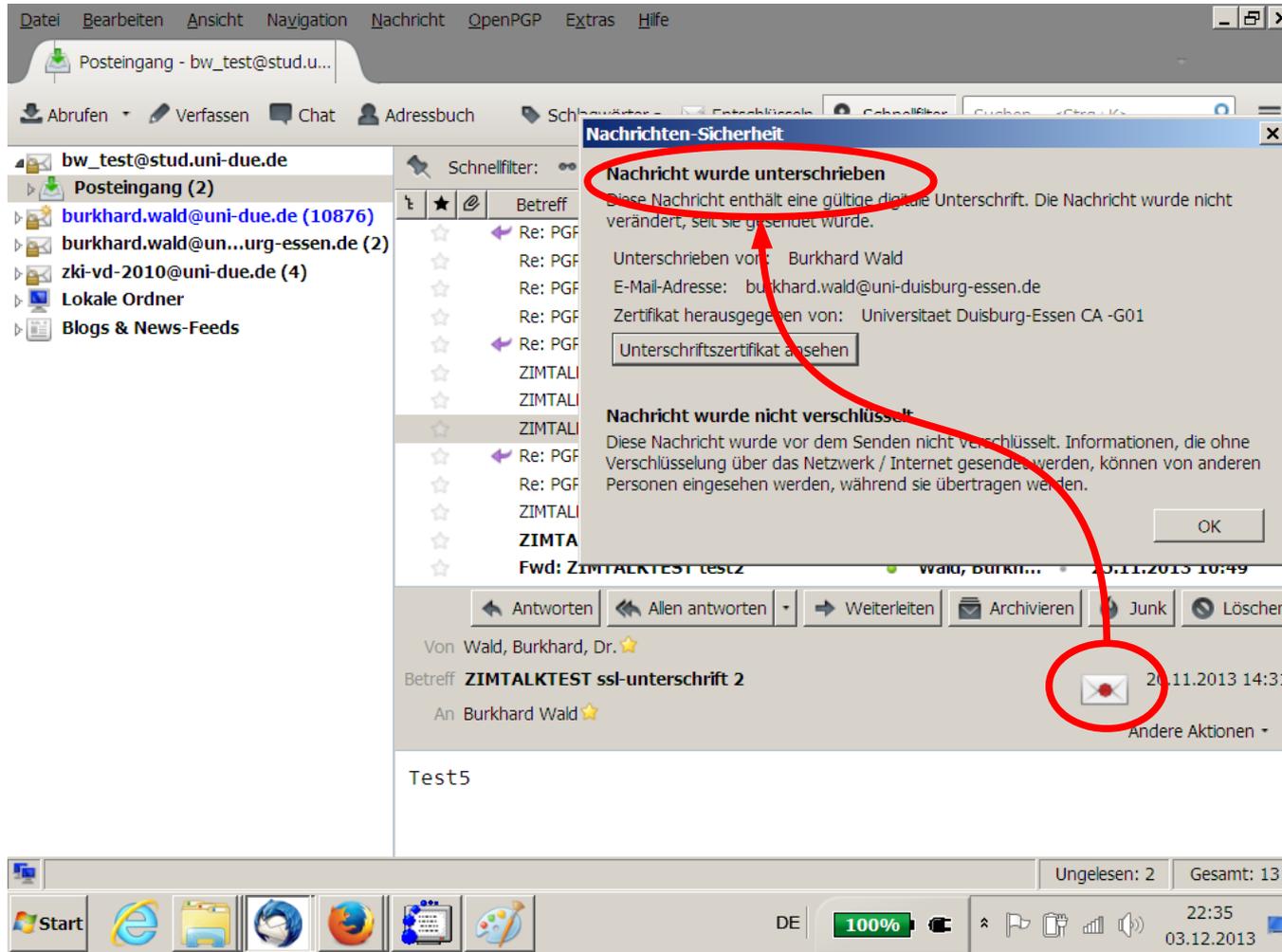


# Mail unterschreiben und/oder verschlüsseln

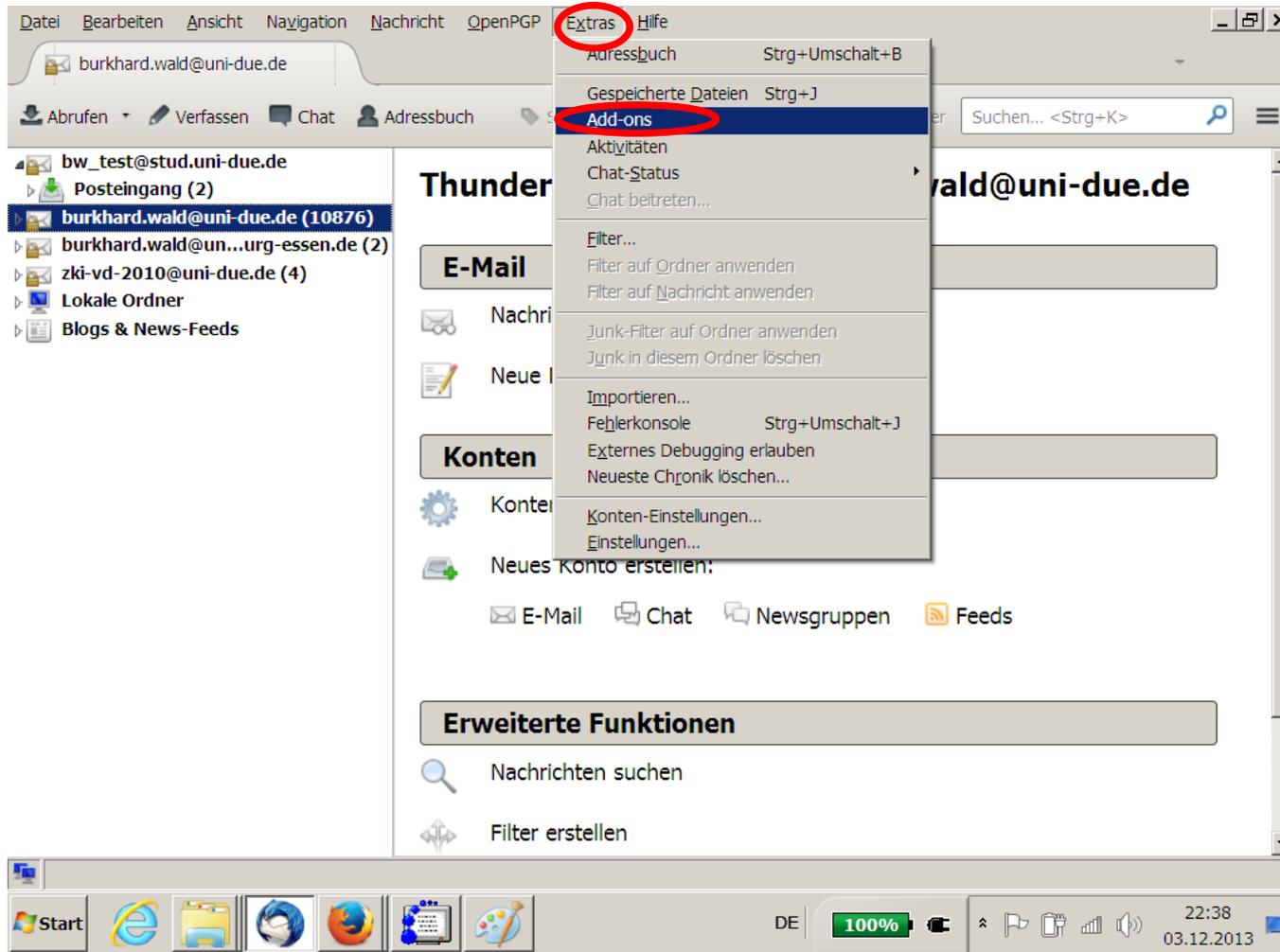


# Verschlüsselte Nachricht lesen

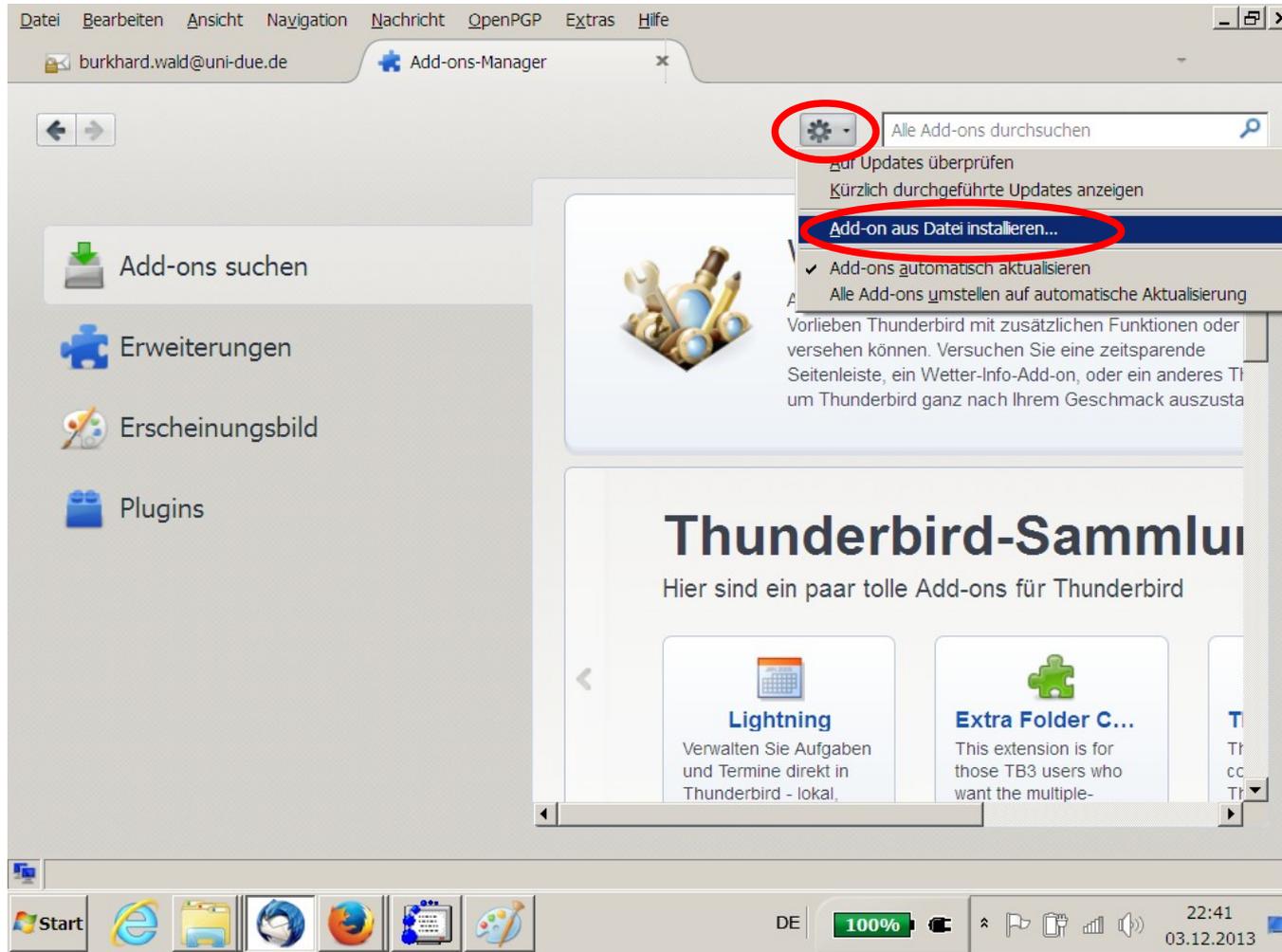




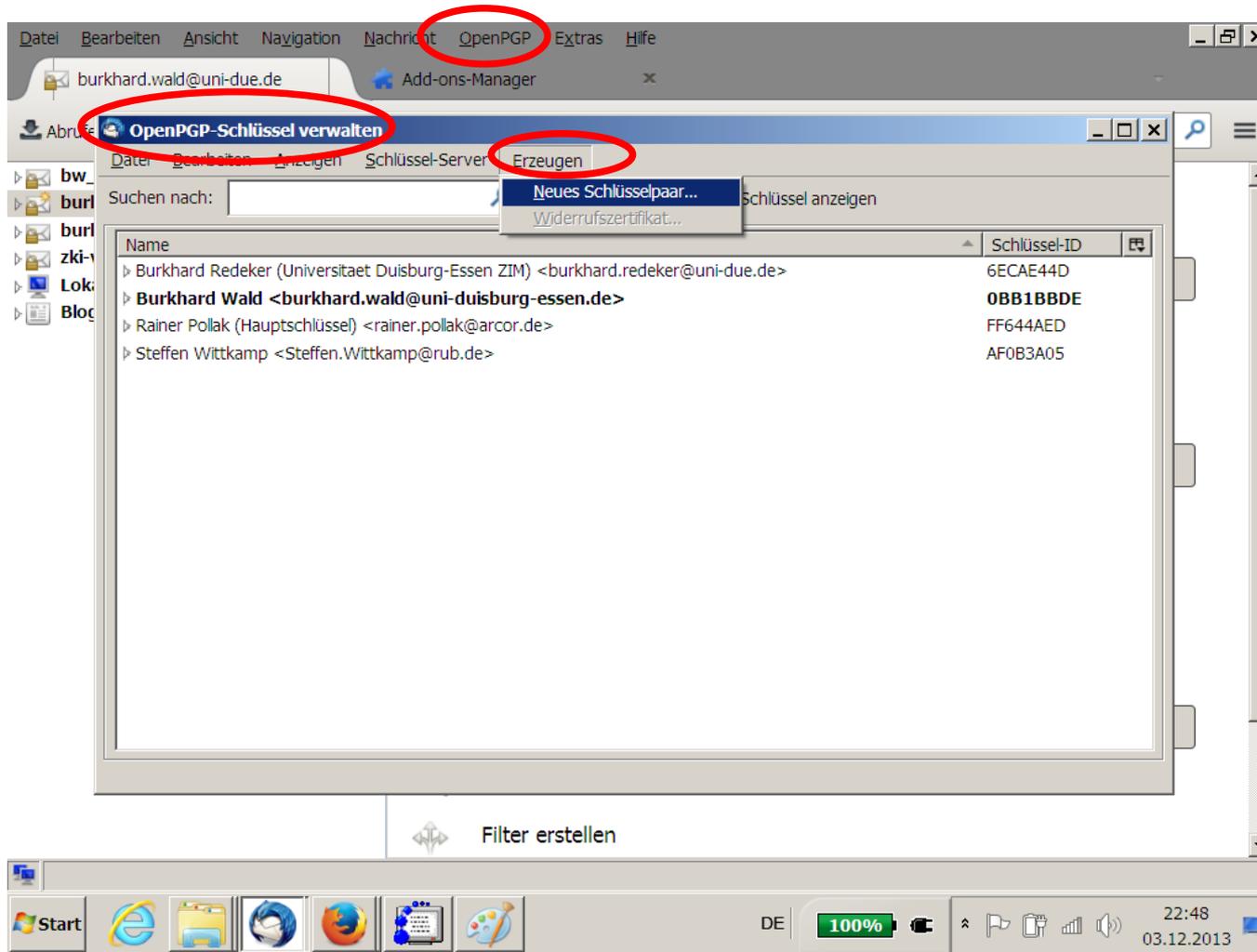
- **PGP (Pretty good Privacy)**
- **OpenPGP, GnuPG, gpg, gpg4win**
- **Enigmail (Add-On für Thunderbird)**
- **Public-Key-Server**
- **Fingerprints**
- **Keys vertrauen**
- **Signieren von Keys**
- **Signierern vertrauen (Web of Trust)**



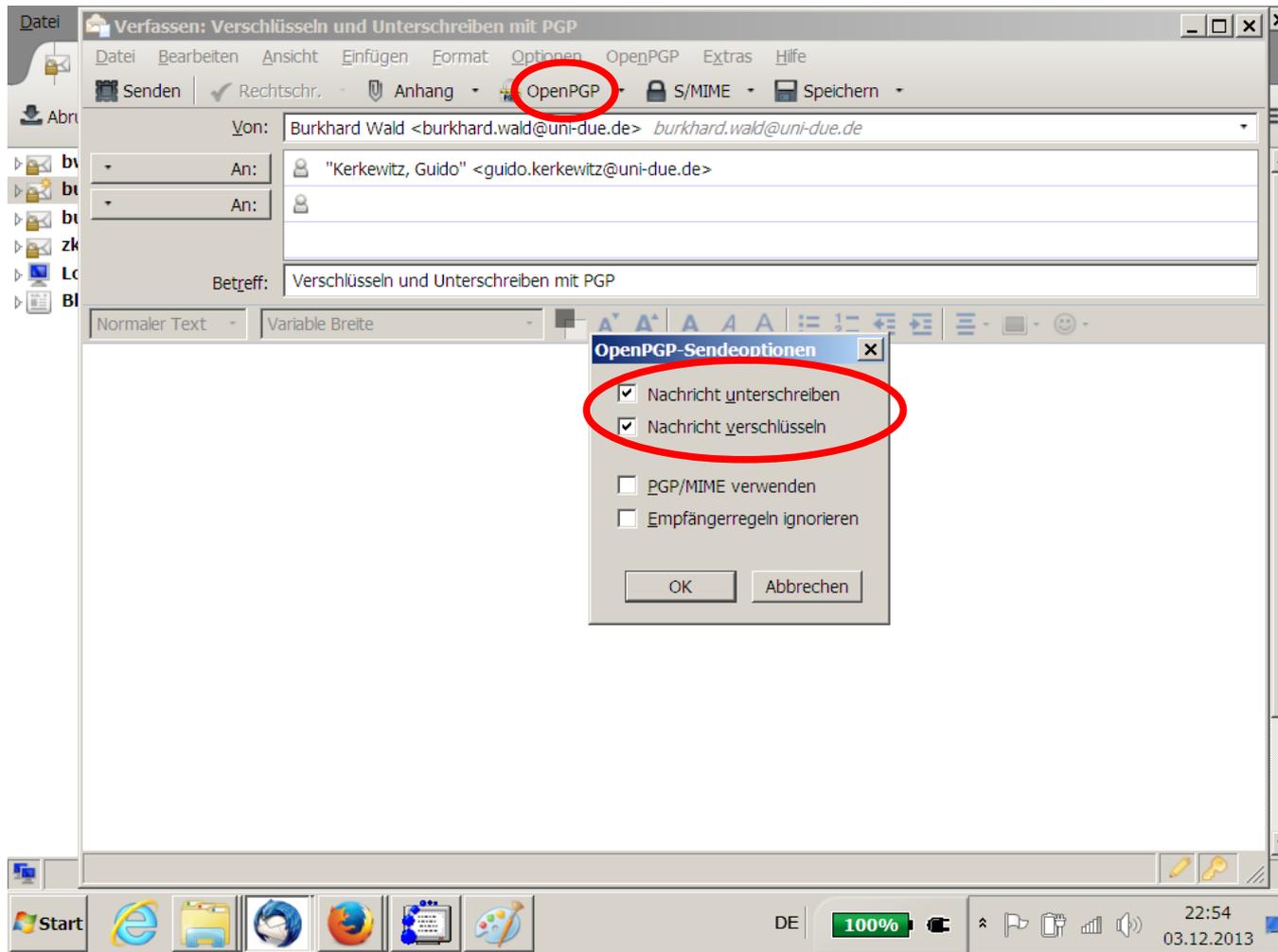
# Enigmail-Add-On aus Datei installieren



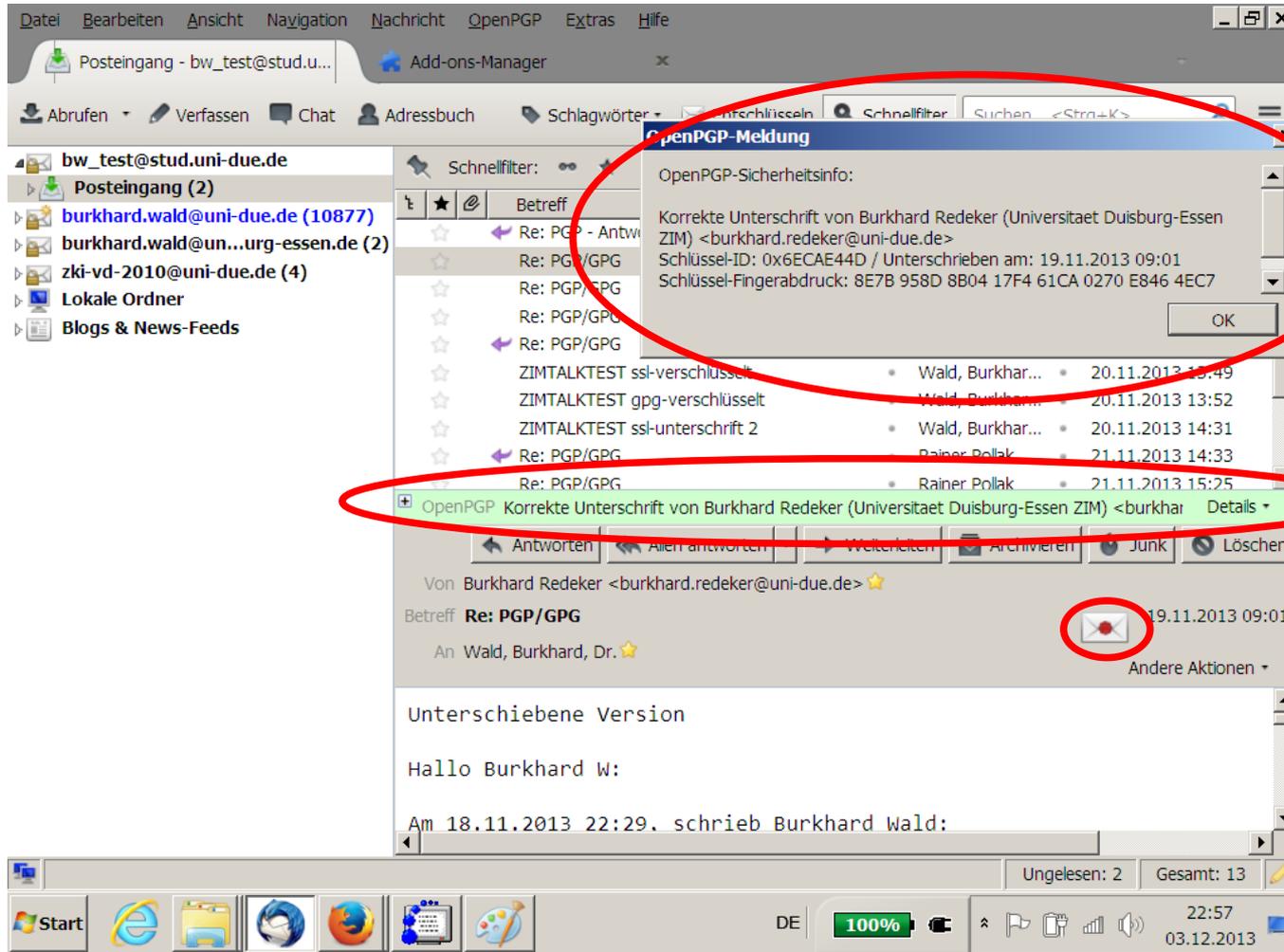
# PGP-Schlüssel erzeugen und verwalten

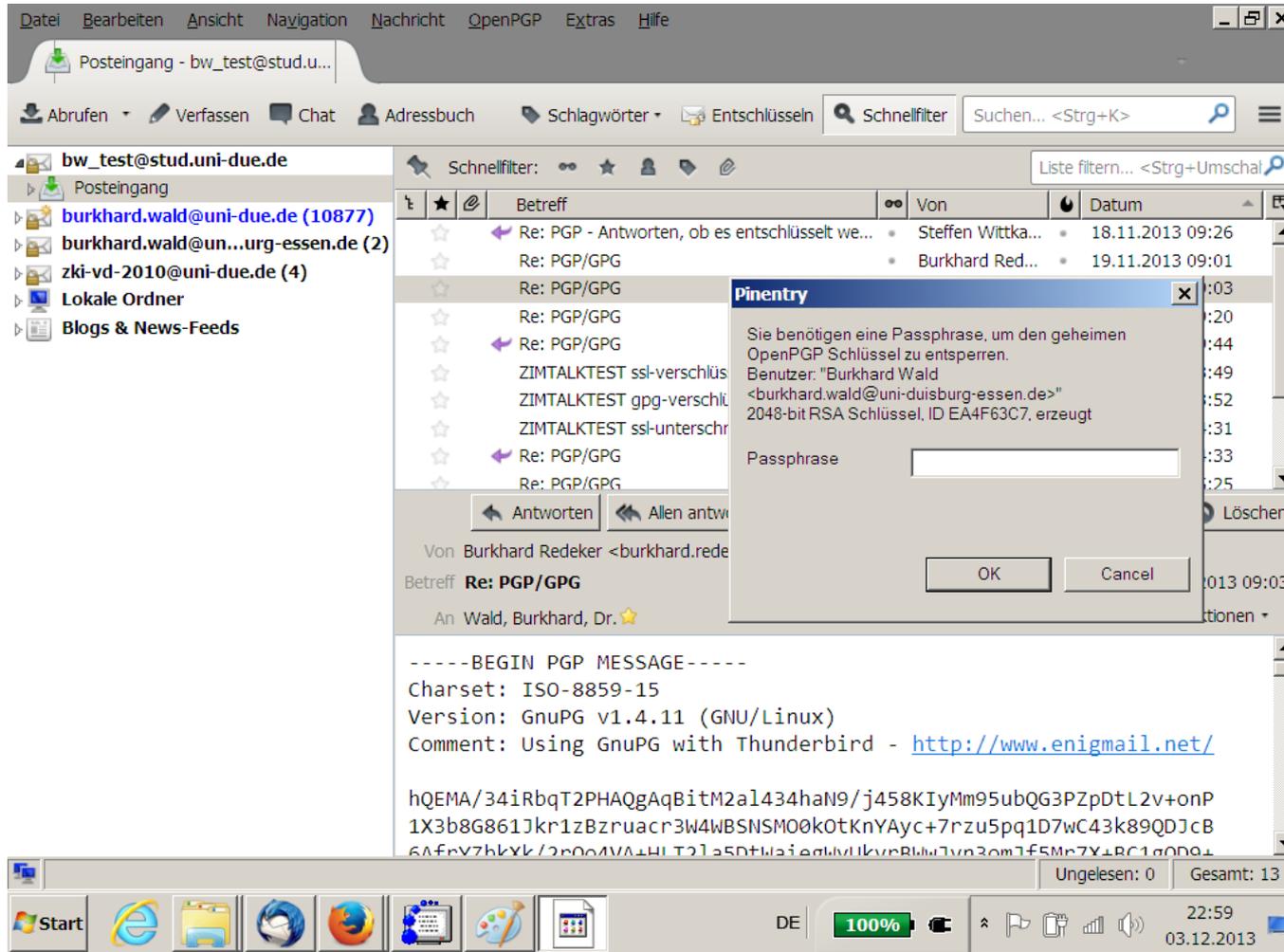


# Nachricht verschlüsseln und/oder unterschreiben



# Unterschiedene Nachricht





- **SSL, S/MIME, X509, PKI**
  - Außer ein Standard-Mailprogramm ist keine Software erforderlich
  - Antrag bei Zertifizierungsstelle erforderlich
- **PGP/GPG**
  - Spezielle Software muss installiert werden
  - Keine Bürokratische Hürden
- **Die Entscheidung für eine der Varianten müssen beide Kommunikationspartner gemeinsam treffen.**
- **Achtung: Niemand kann ungewollt verschlüsselte Emails empfangen**

**Vielen Dank!**

- 25.10.2013 - Andreas Bischoff  
**ARM für Raspberry Pi, Phone Tablet und Server**
- 22.11.2013 – Burkhard Wald:  
**Die Idee des Jahres 2013: Kommunikation verschlüsseln**
- 20.12.2013 – Andreas Michels  
**Menschenbilder im Informationszeitalter**
- 24.01.2014 – Stefan Helker  
**Entwicklung einer mobilen Webanwendung**
- 21.02.2014 – Daniel Biella  
**Home automation und Datenvisualisierung**
- 21.03.2014 – Sandrina Heinrich & Steffi Engert  
**iPad in der Lehre**

14:00 Uhr  
Duisburg LE  
105