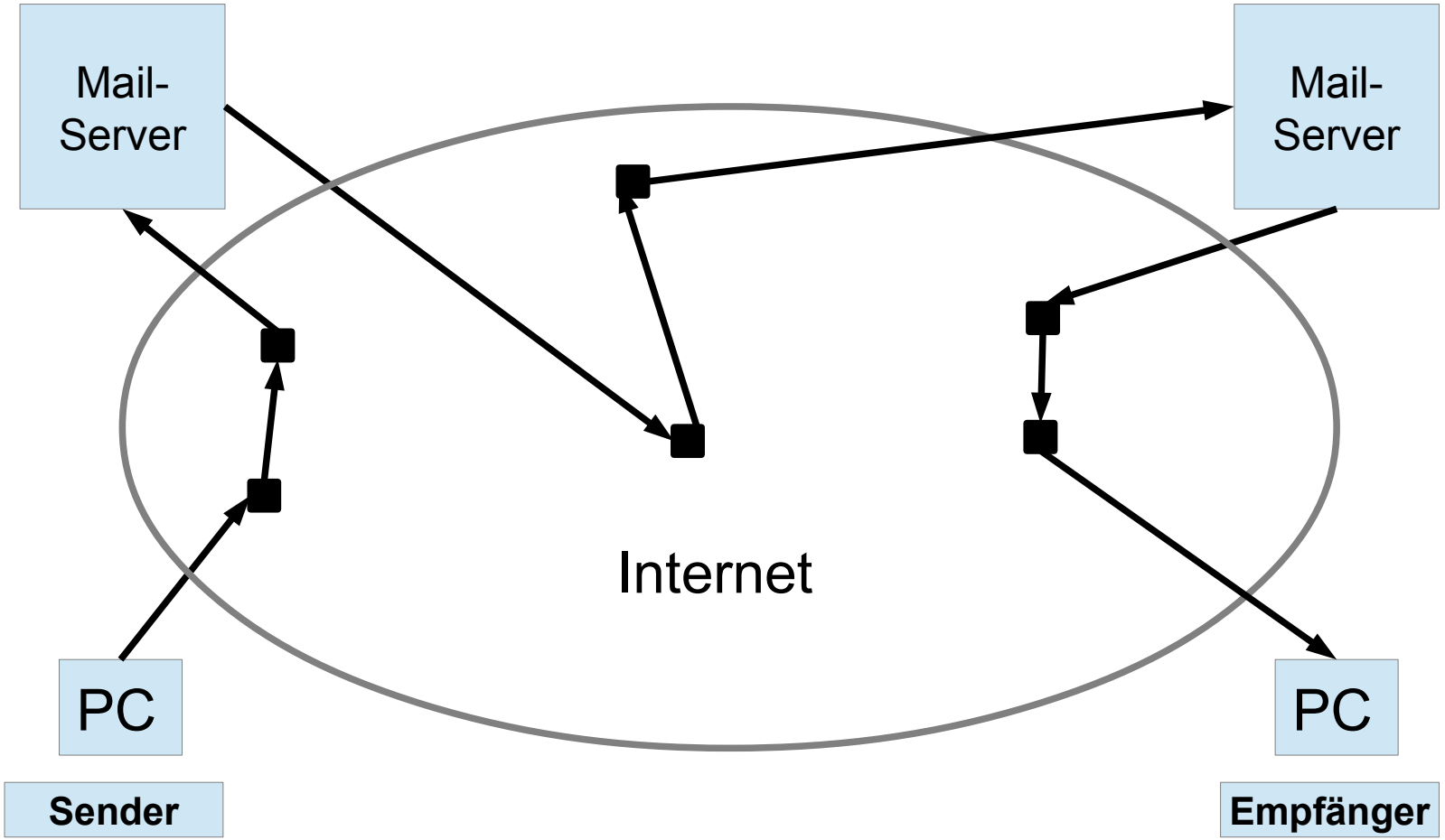
Die Idee des Jahres 2013: Kommunikation verschlüsseln

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

Burkhard Wald ■ 22.11.2013

Kommunikationsschema bei Email



Verschlüsselung ist ...

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

Verschlüsselung der Server-Server-Verbindung

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- 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

Enigma

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

Burkhard Wald

22.11.2013

Banalverschlüsselung mit einer „Époisses“

Quelle: b-eats.blog.de

Symmetrische Verschlüsselung

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

Asymmetrische Verschlüsselung

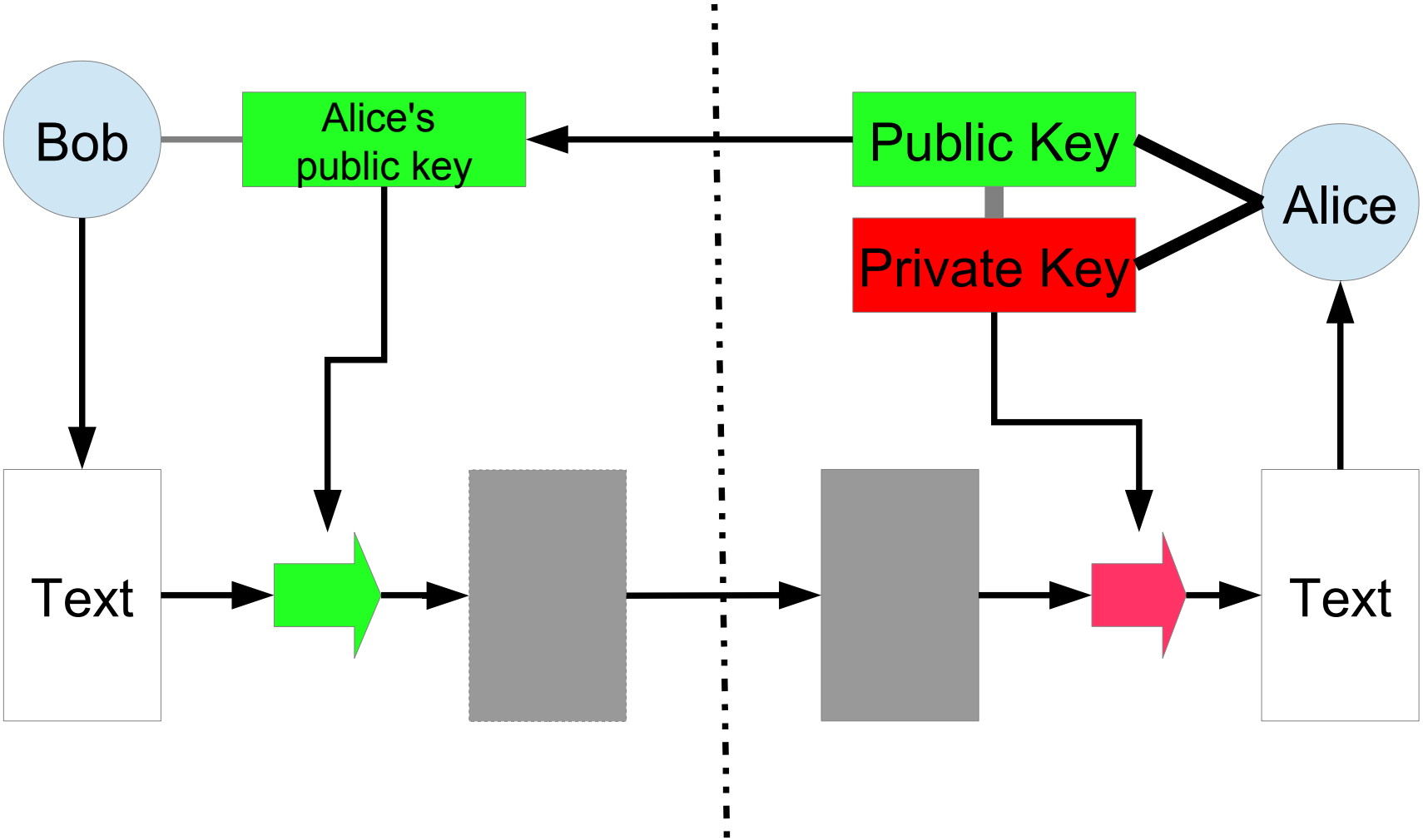
- Kann es das geben?
- Key a zum Verschlüsseln
  Key b zum Entschlüsseln
- Verfahren Va und Vb sind nicht effizient umkehrbar
- Verfahren Va und Vb sind zueinander inverse math. Funktionen.
- Aus aus b kann a nicht effizient berechnet werden
- Schlüssel b kann öffentlich sein.
- Antwort = Ja: Verfahren: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

RSA basiert auf dem Faktorisierungsproblem

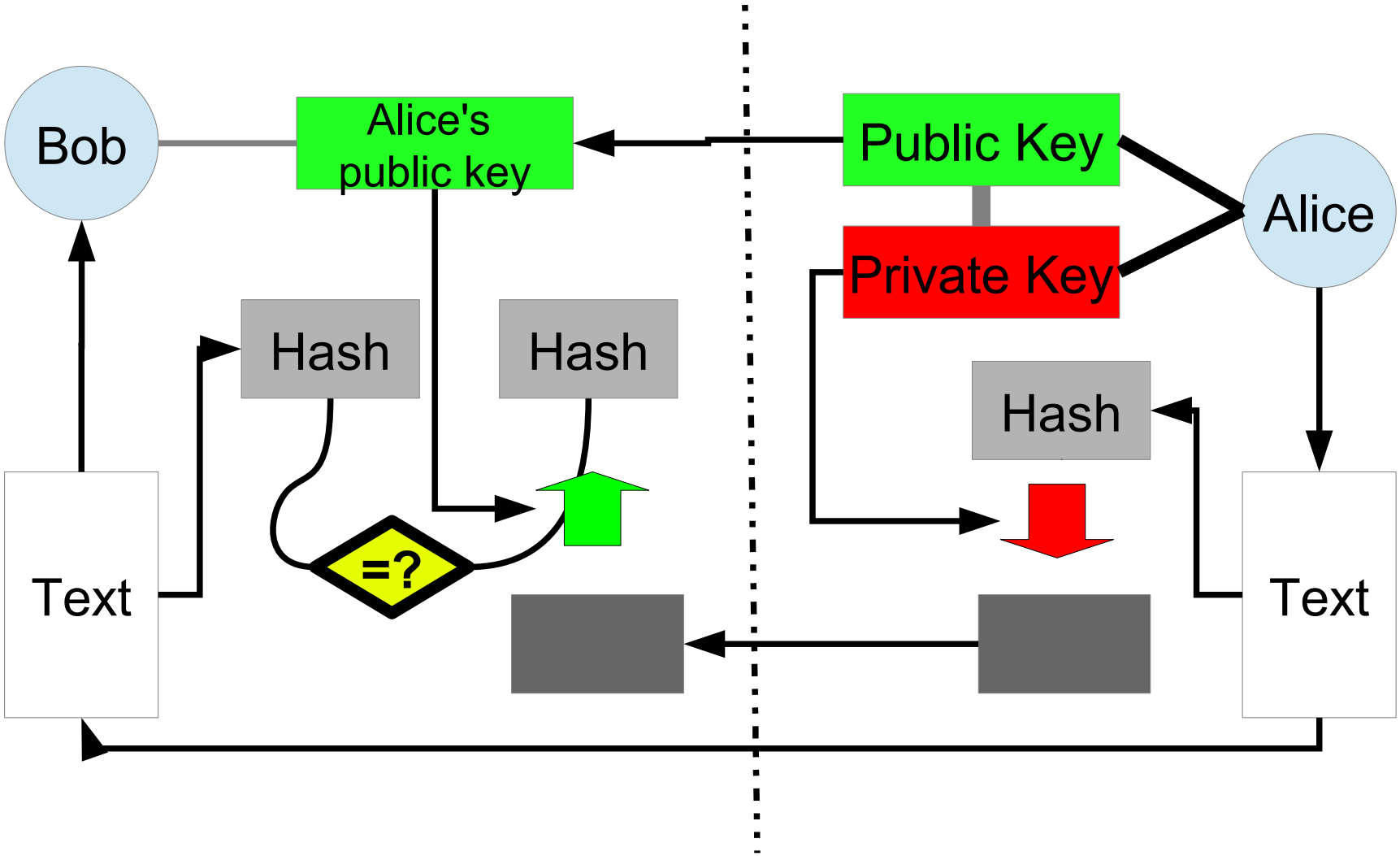

- ```
  > echo 107*113 | bc
  12091
  ```
- ```
  > echo 398075086424064937397125500550386491199064\
  362342526708406385189575946388957261768583317 *\
  472772146107435302536223071973048224632914695 30\
  209711645985217113052071125636359039752 7 | bc

  188198812920607963838697239461650439807163563379\
  417382700763356422988859715234665485319060606504\
  743045317388011303396716199692321205734031879550\
  656996221305168759307650257059
  ```
- **RSA-Challange-576**
- **Dezember 2003 von Jens Franke und Thorsten Kleinjung vom Mathematischen Institut in Bonn und dem Institut für Experimentelle Mathematik in Essen gefunden**

Verschlüsseln mit Public Key



Elektronische Unterschriften



Öffenliche Schlüssel

Schlüssel mit Schlüsselanhängern

Öffentliche Schlüssel

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

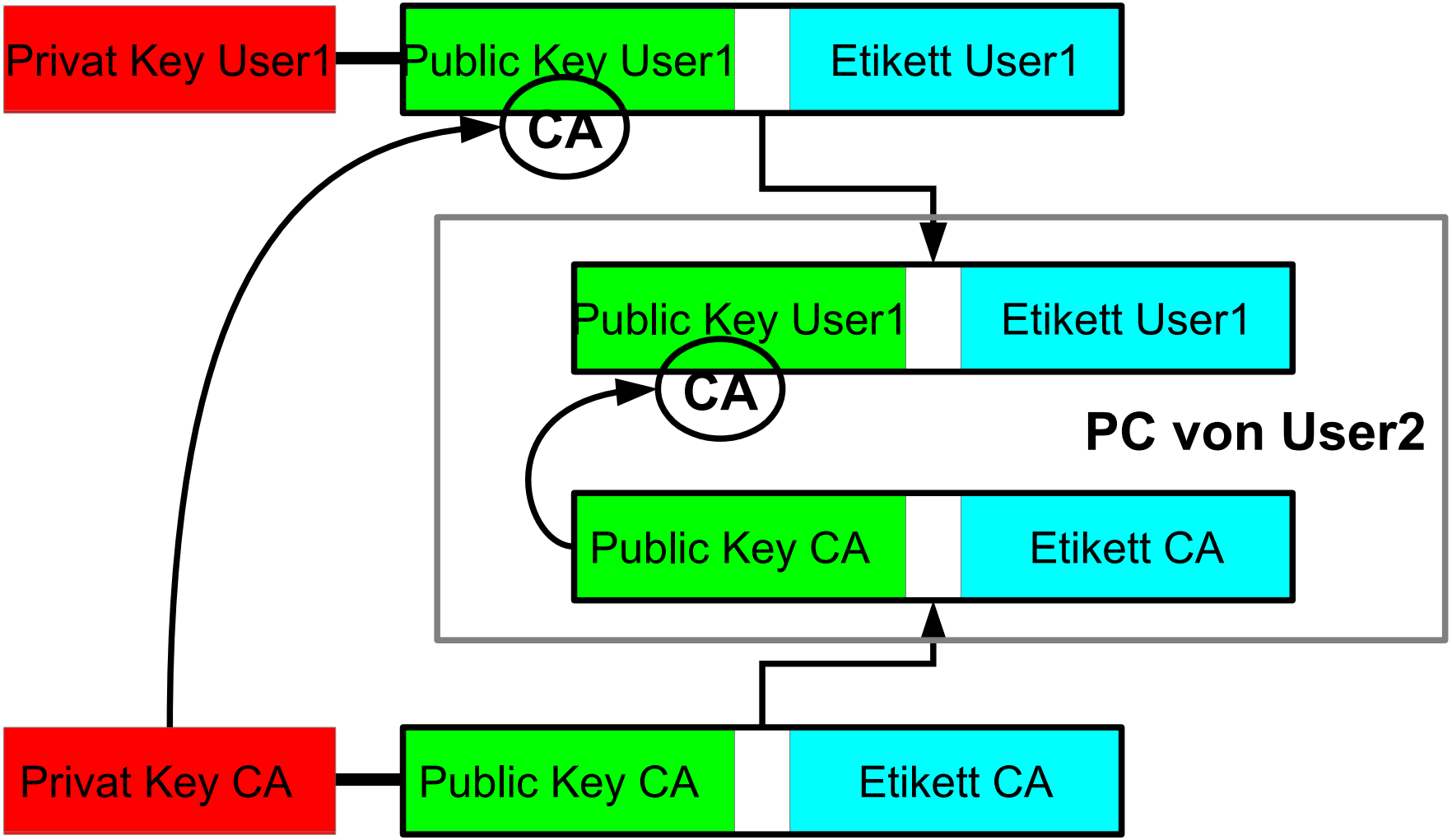
Wie entsteht das Vertrauen?

- **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)

Zwei Verfahren

- **1. PKI (public key infrastucture) 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

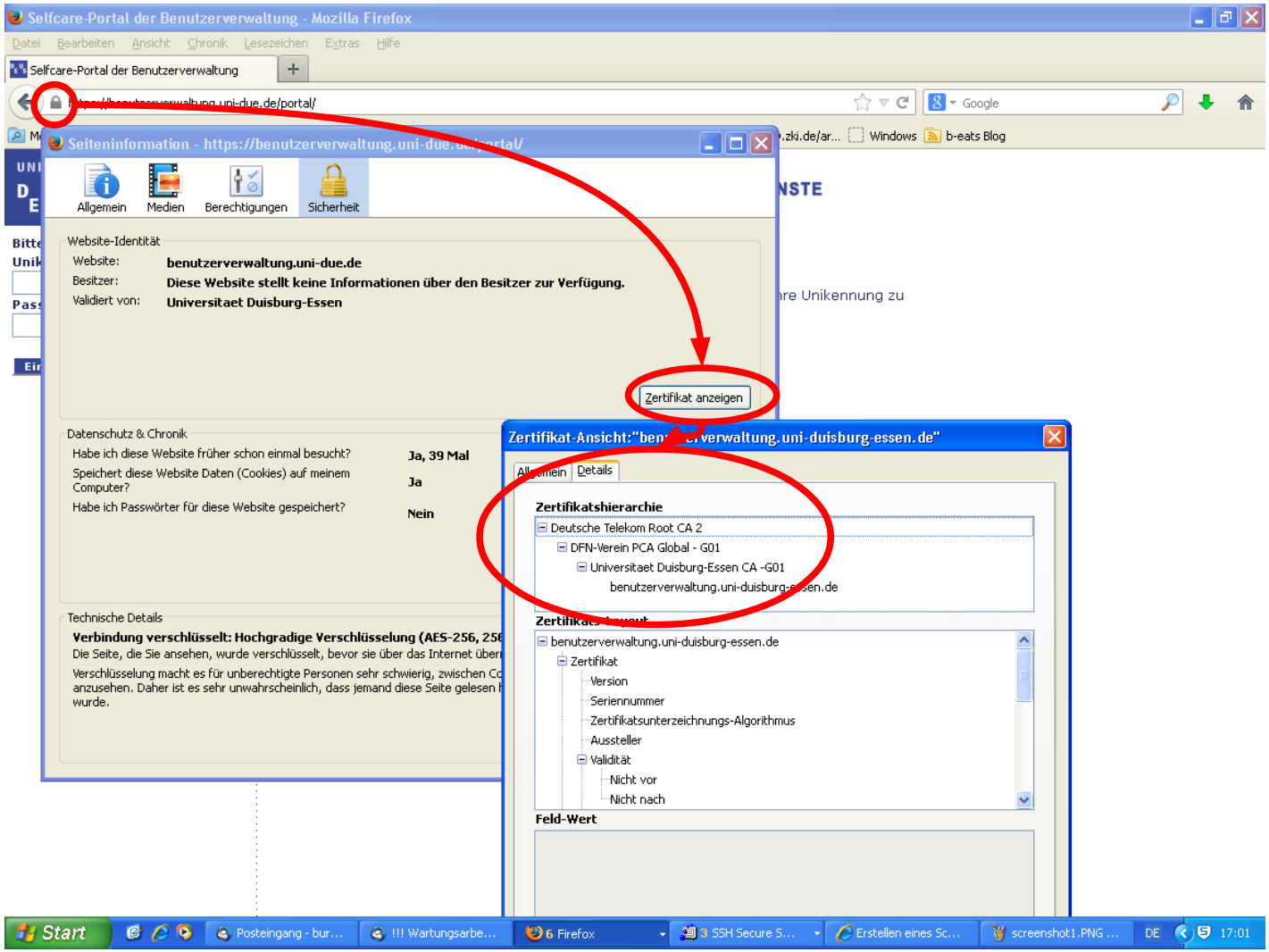
Zertifikate (X509)



Zertifikatsketten

- Browser-und Betriebssytem-Hersteller vertrauen wenigen Zertifizierungsstellen und bauen die öffenliche Schlüssel in ihre Software als vertrauenwürdig 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.

Zertifkatsketten 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.**

Was ist zu tun?

UNIVERSITÄT DUISBURG ESSEN

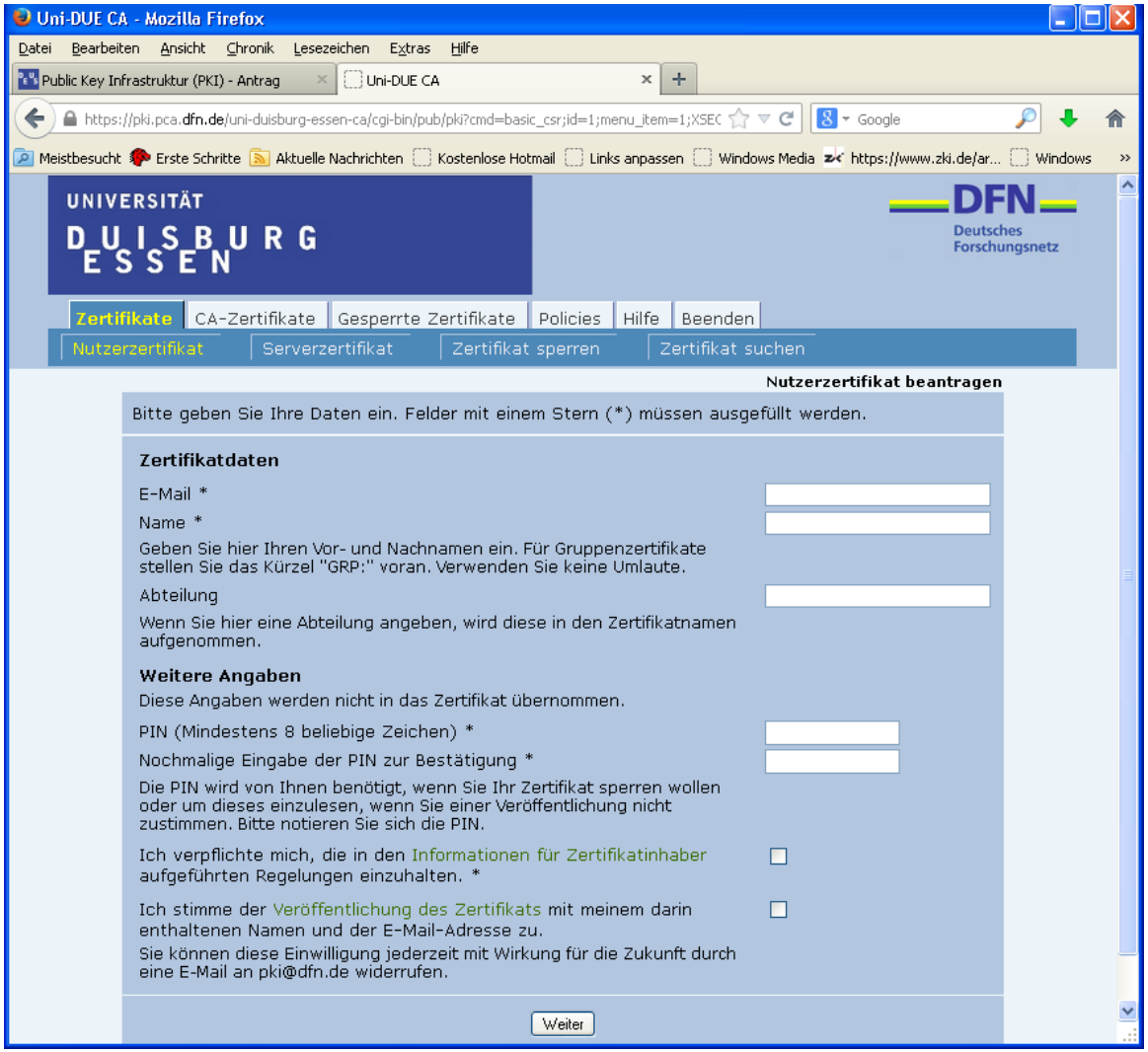
Offen im Denken

- 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.

Schlüsselerzeugen und Zertifikat beantragen

UNIVERSITÄT DUISBURG ESSEN

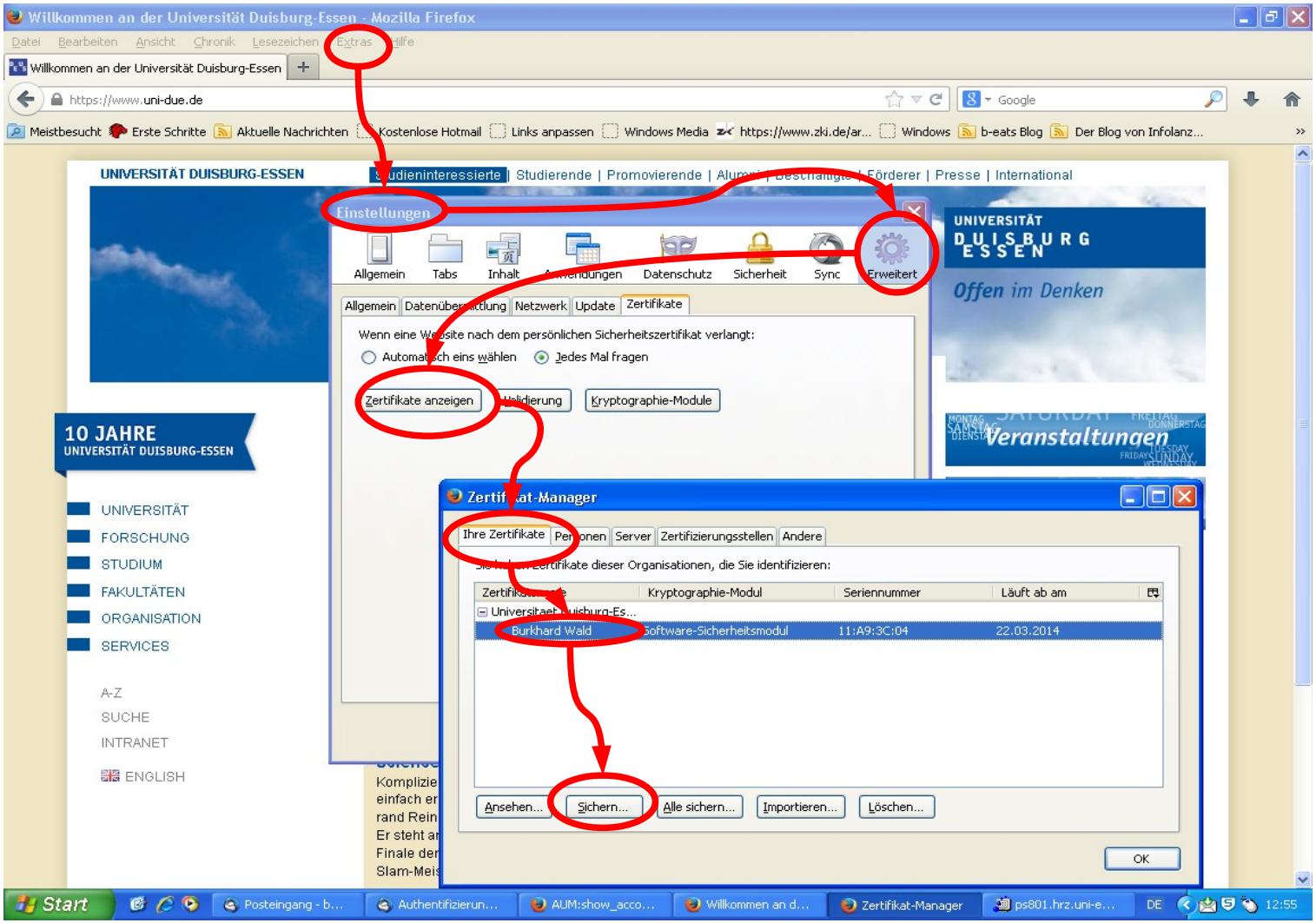
Offen im Denken



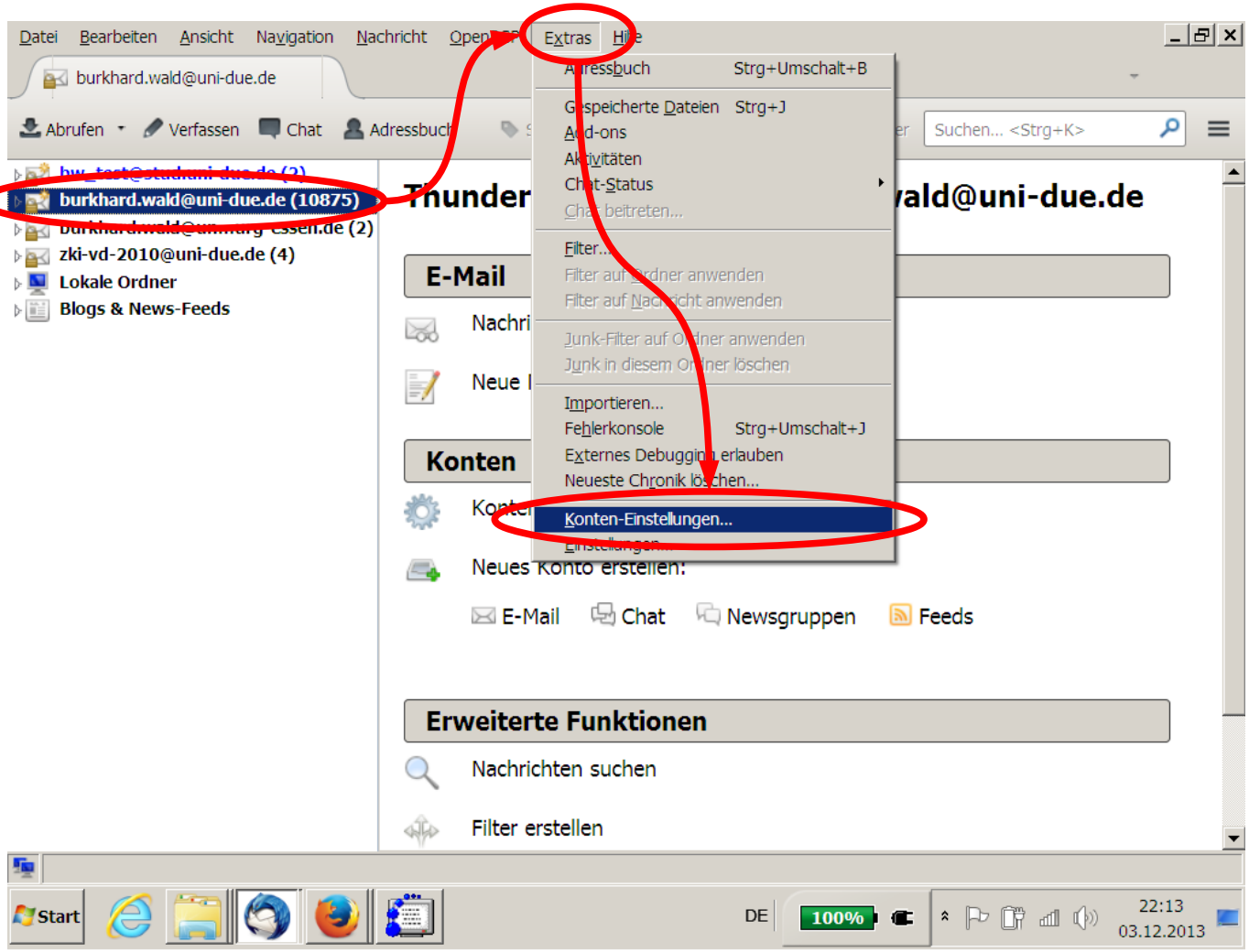
Schlüssel und Zertifikat exportieren

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken



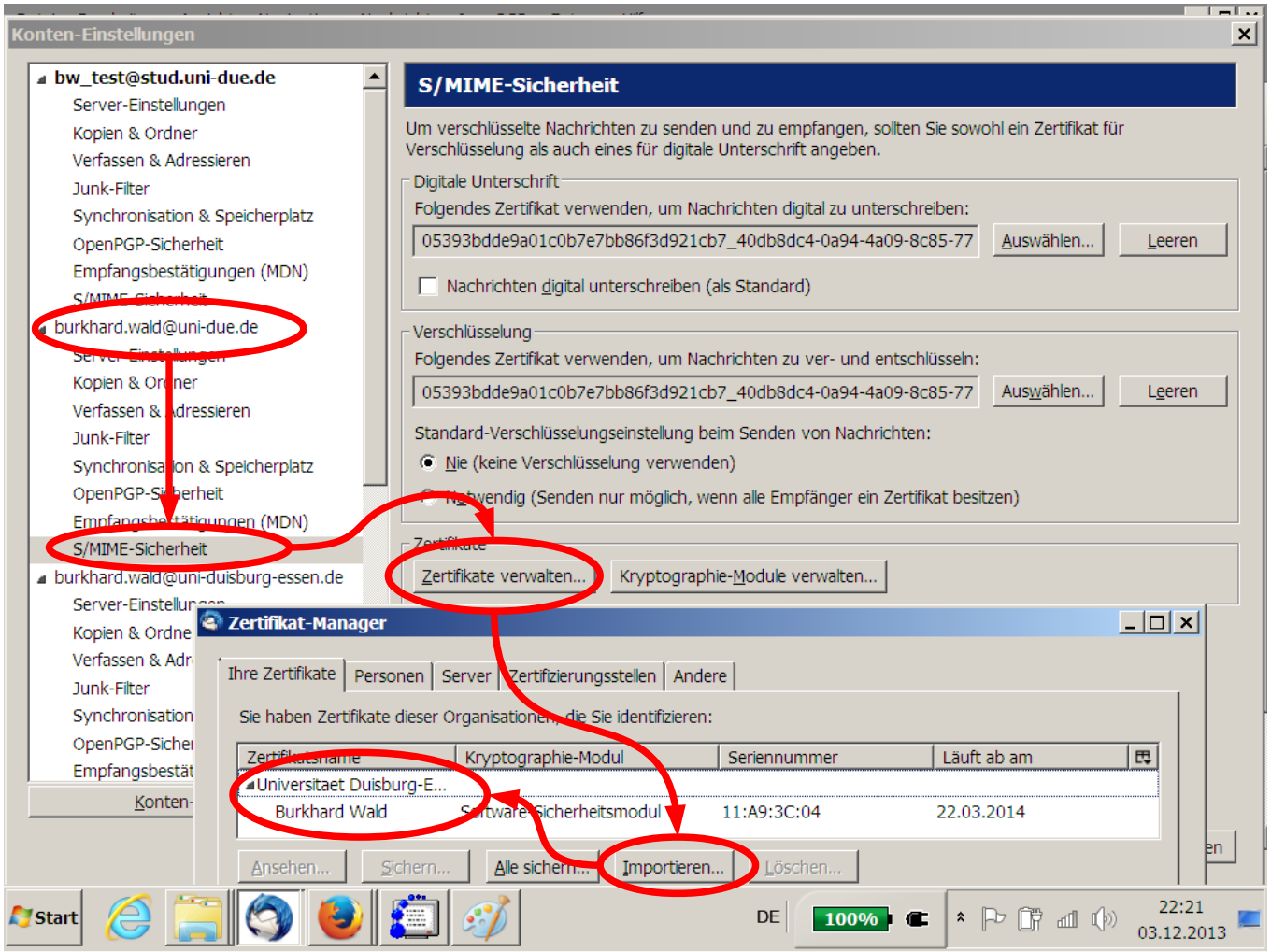
Konteneinstellung im Thunderbird



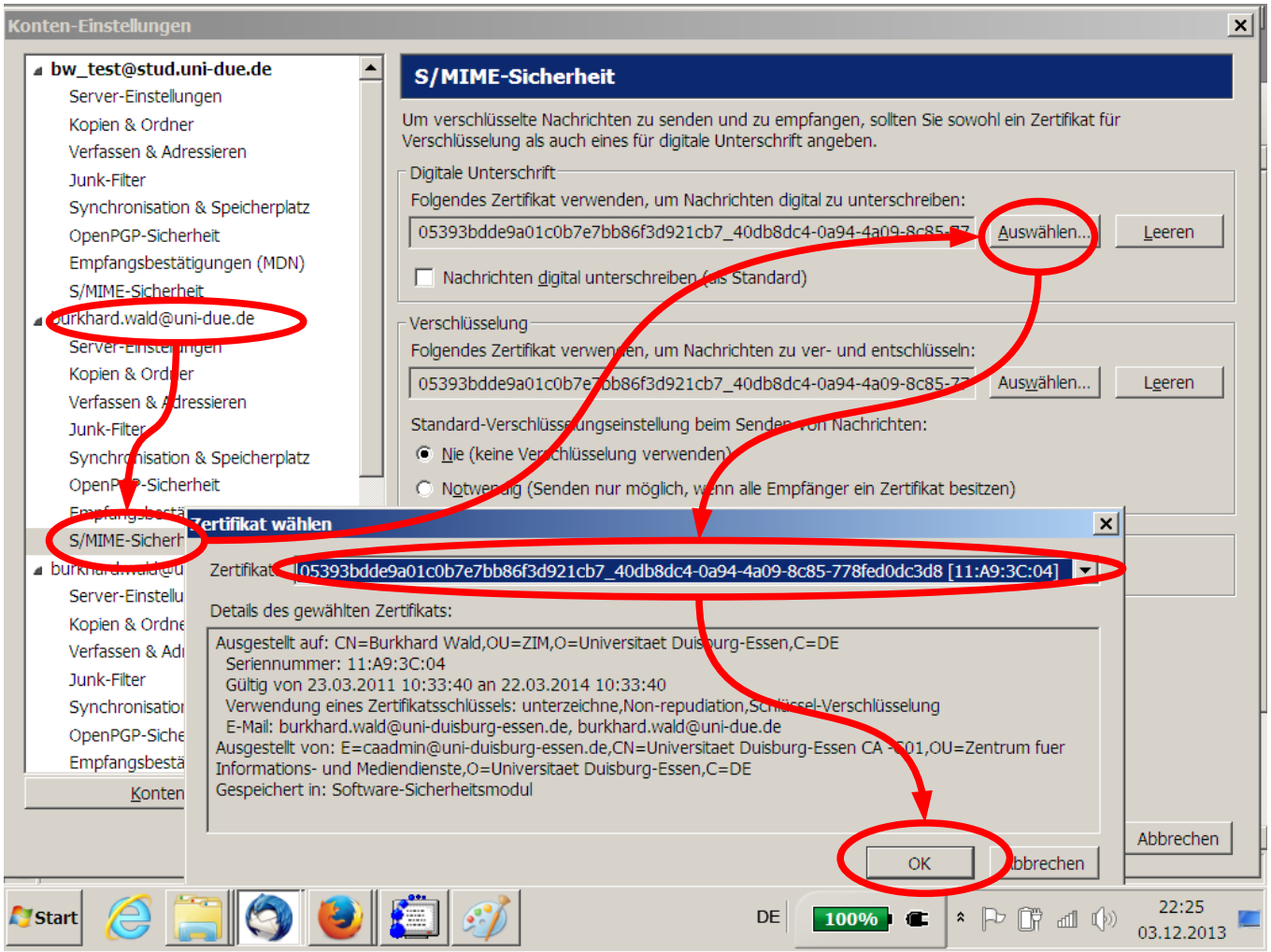
Importieren eines Schlüssels in Thunderbird

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken



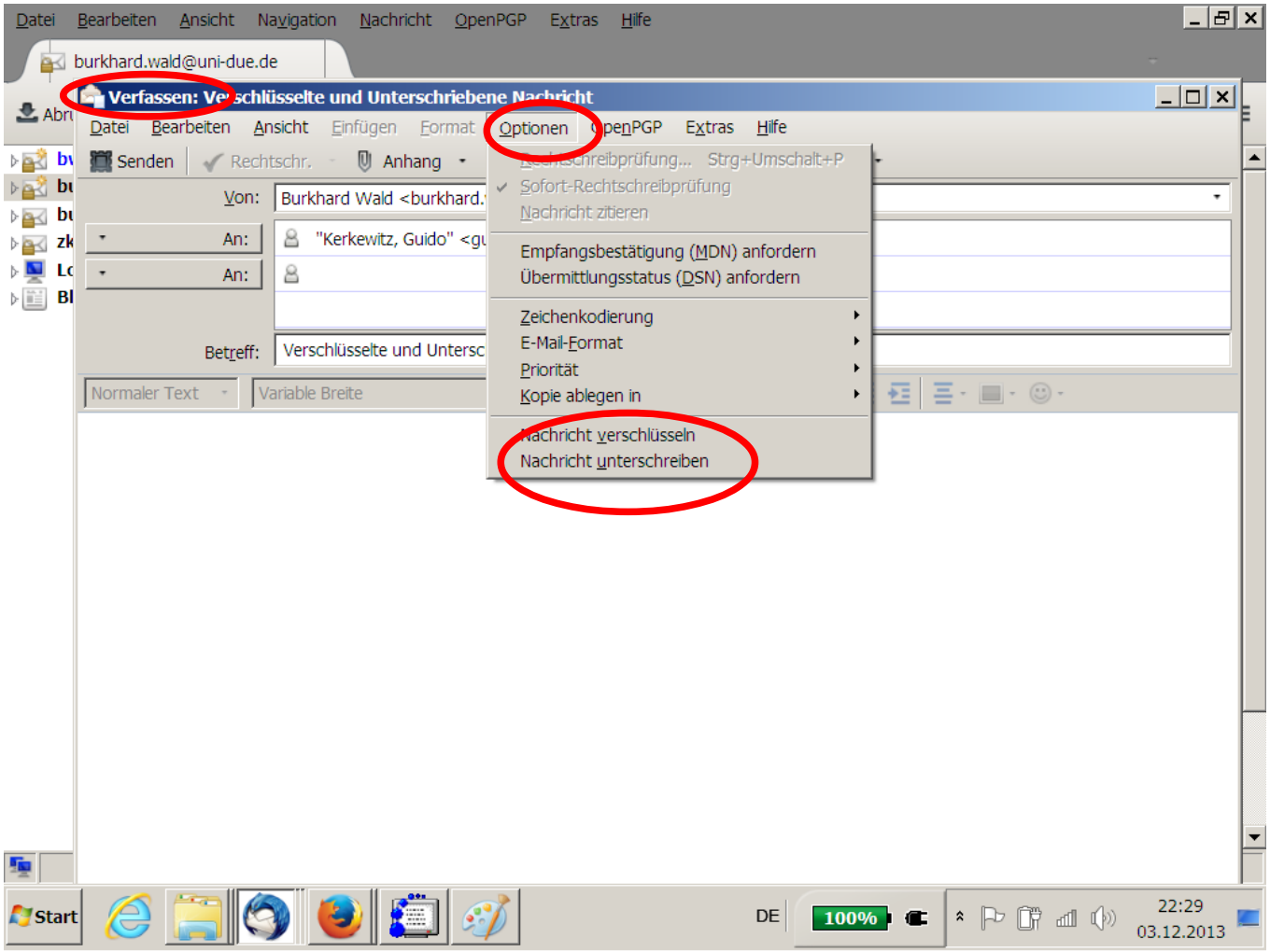
Schlüssel im Konto aktivieren



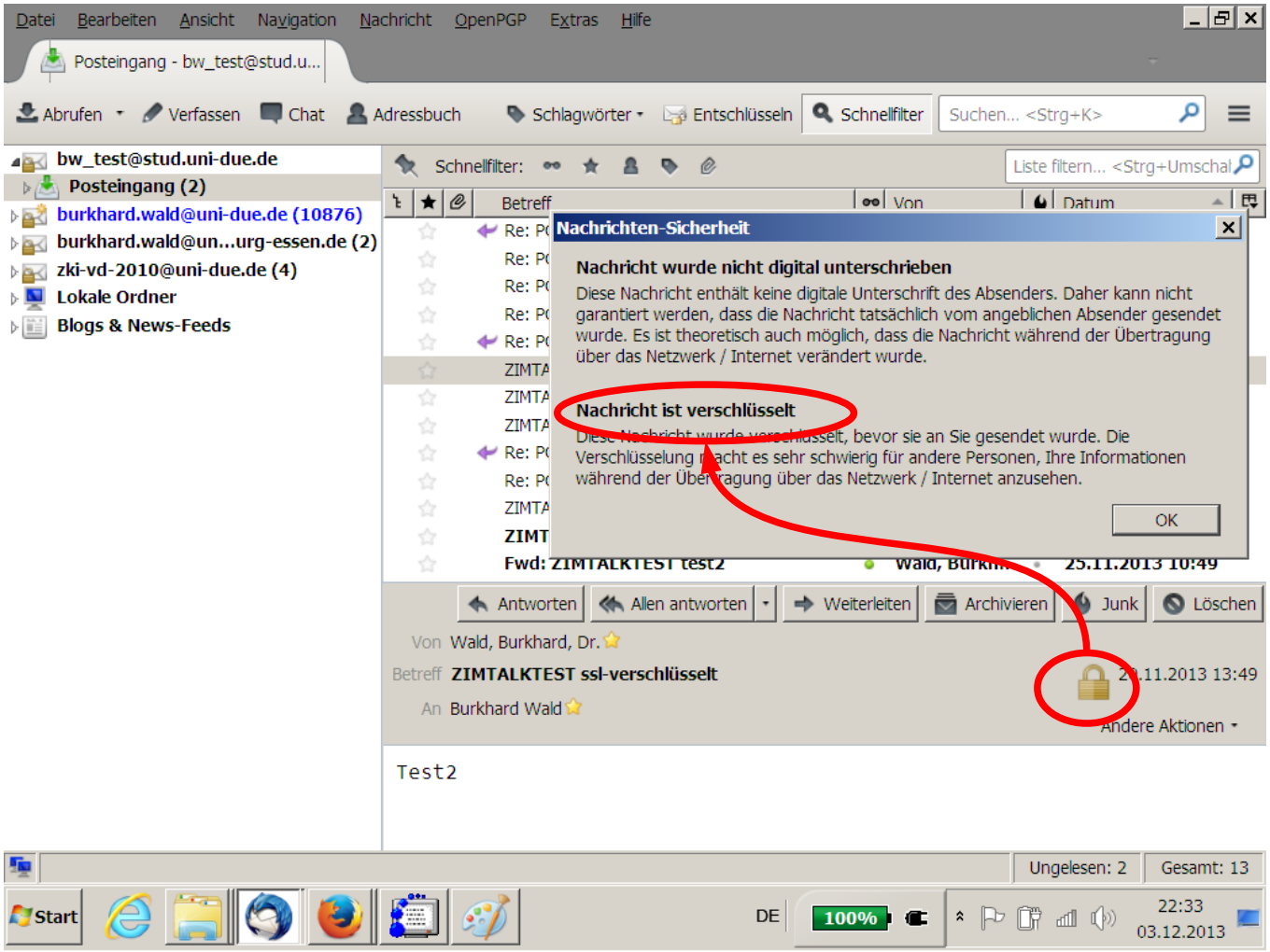
Mail unterschreiben und/oder verschlüsseln

UNIVERSITÄT DUISBURG ESSEN

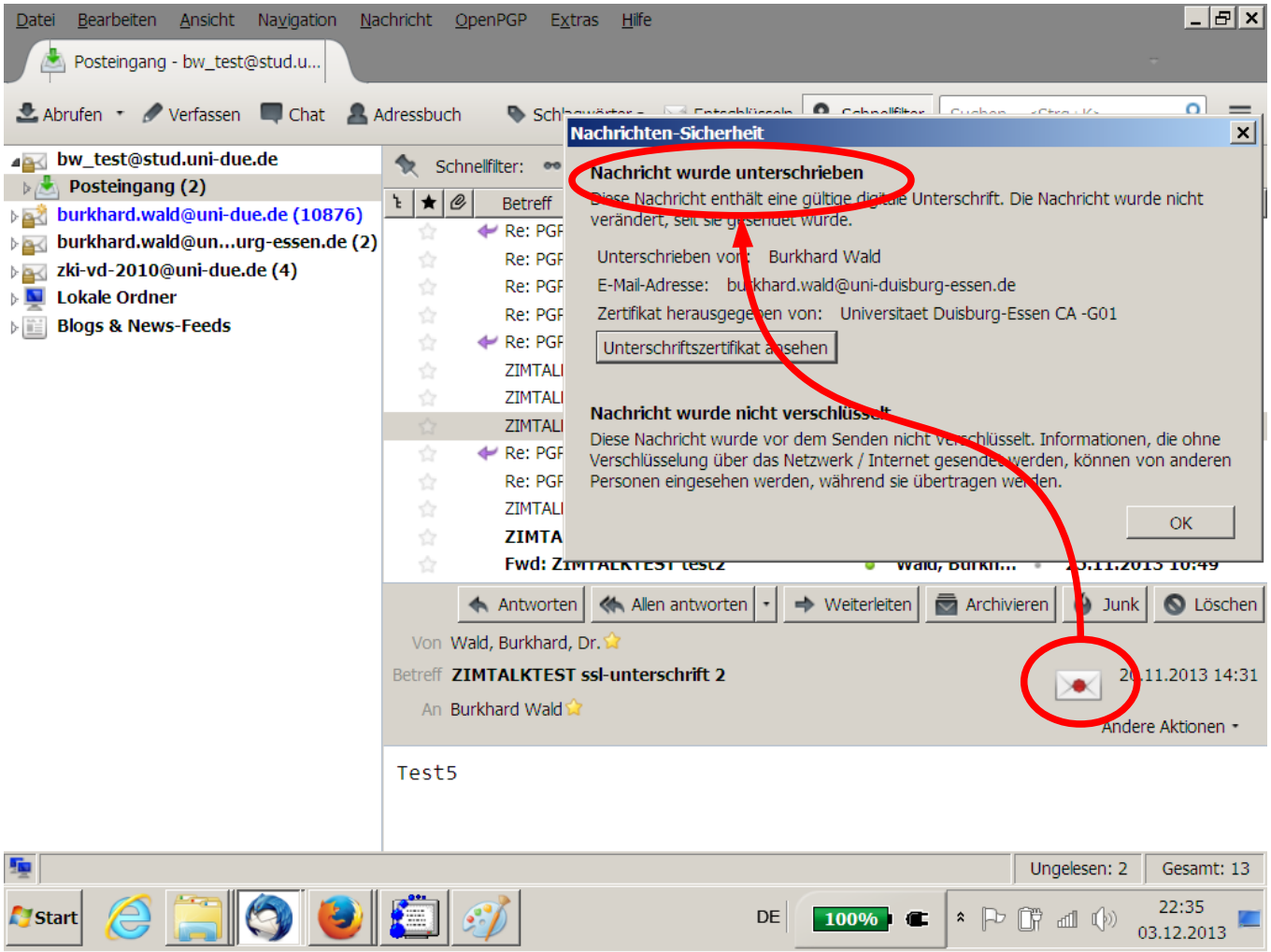
Offen im Denken



Versclüsselte Nachricht lesen



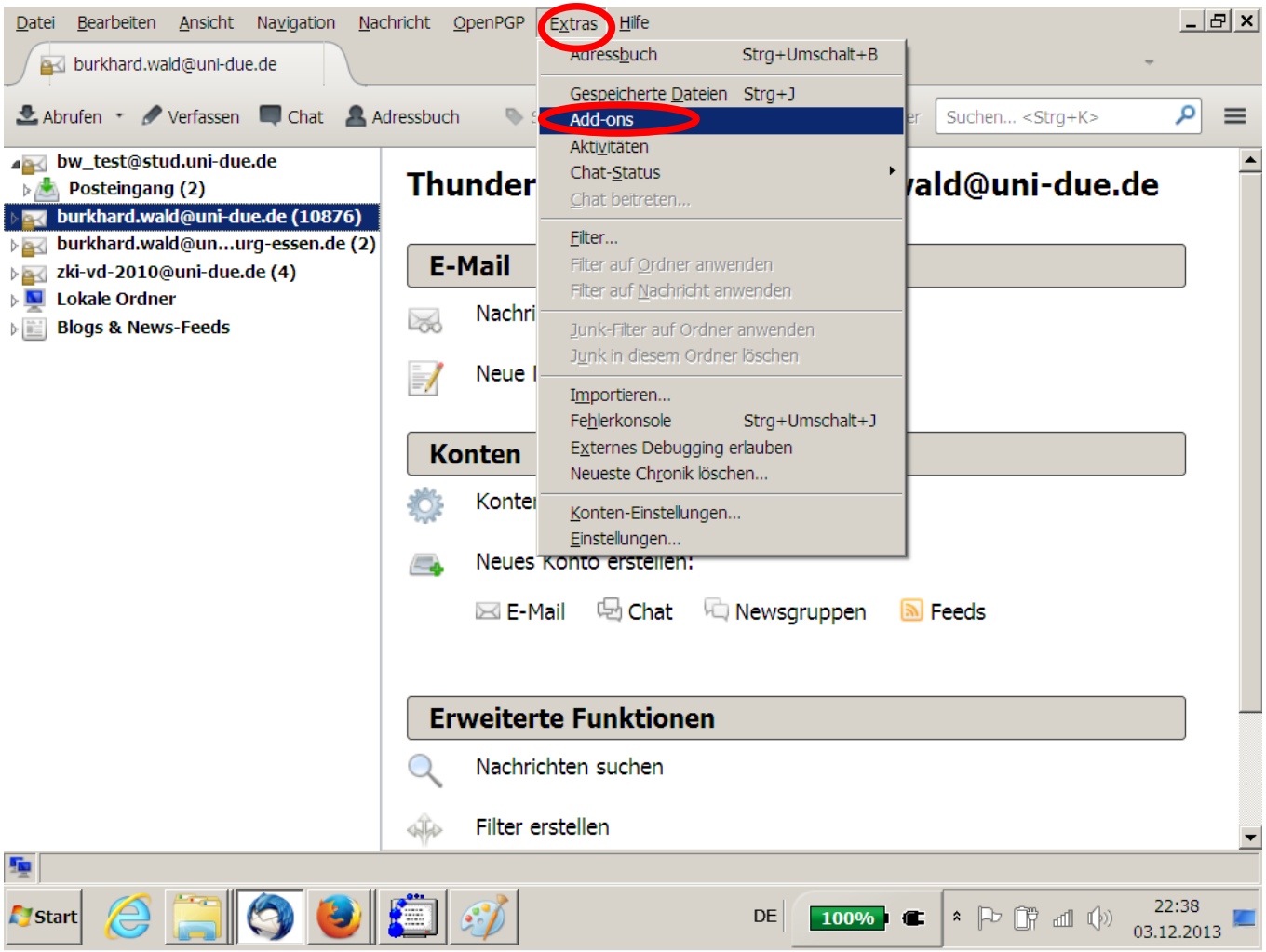
Unterschrift prüfen



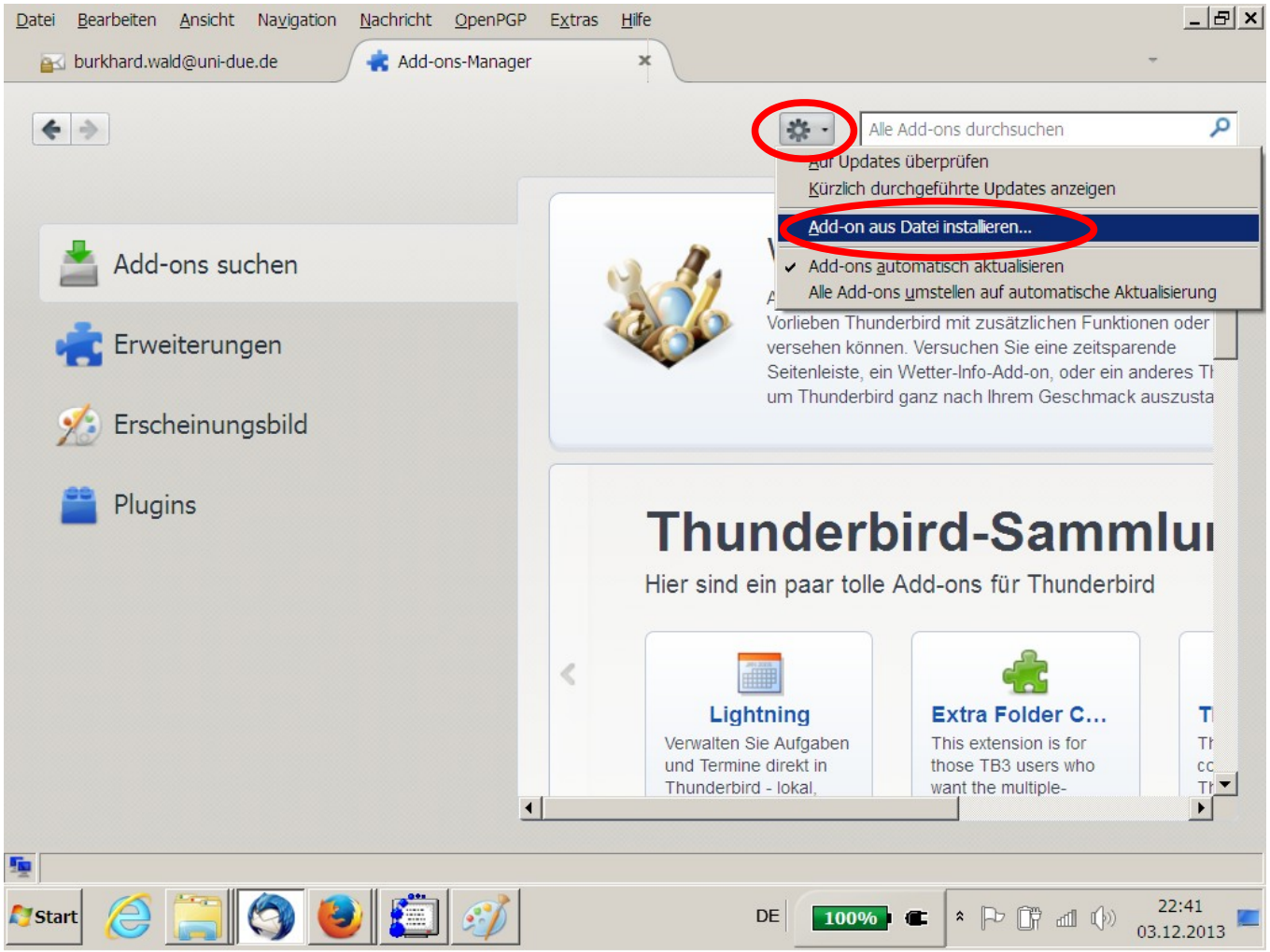
PGP

- 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)

Thunderbird: Add-Ons verwalten



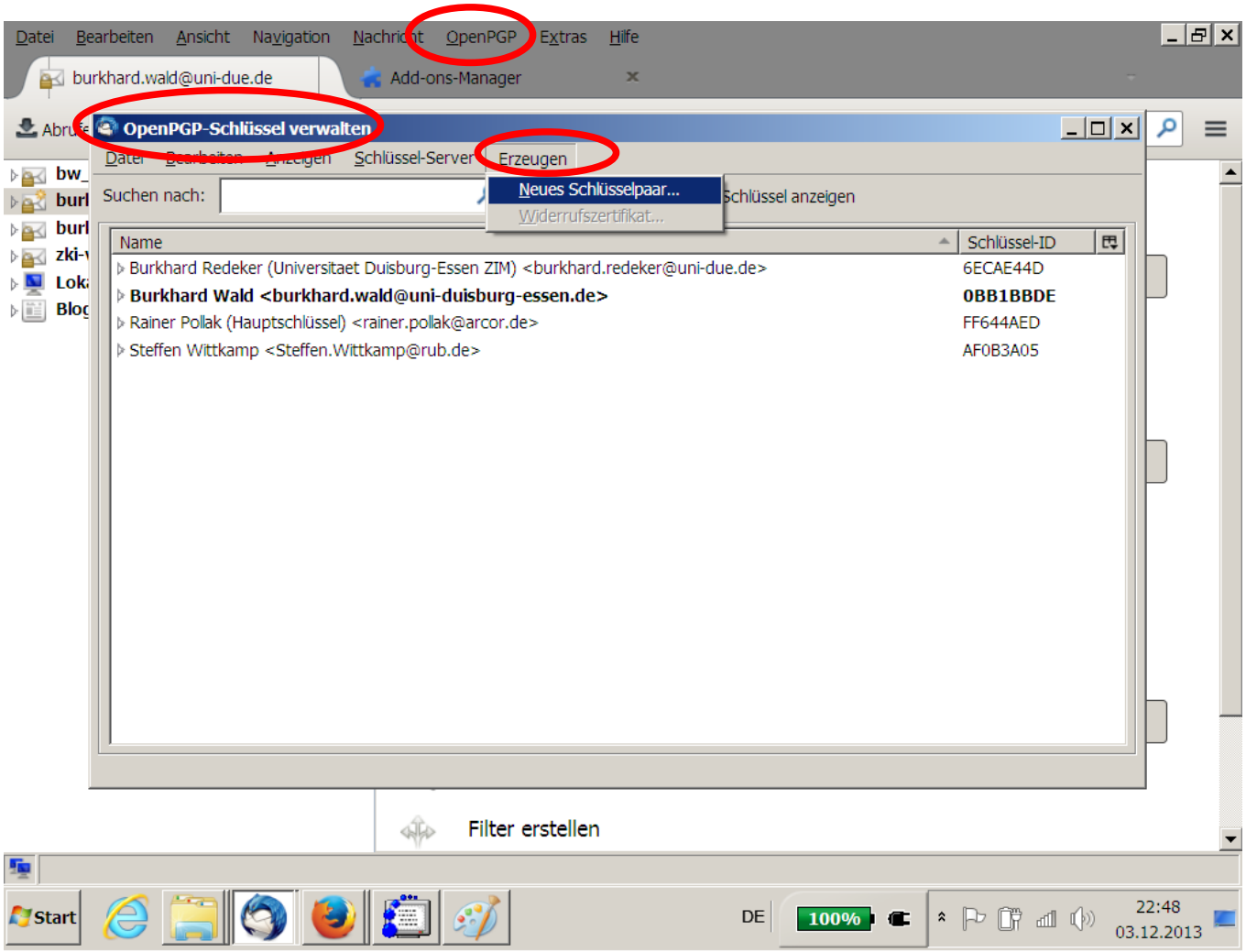
Enigmail-Add-On aus Datei installieren



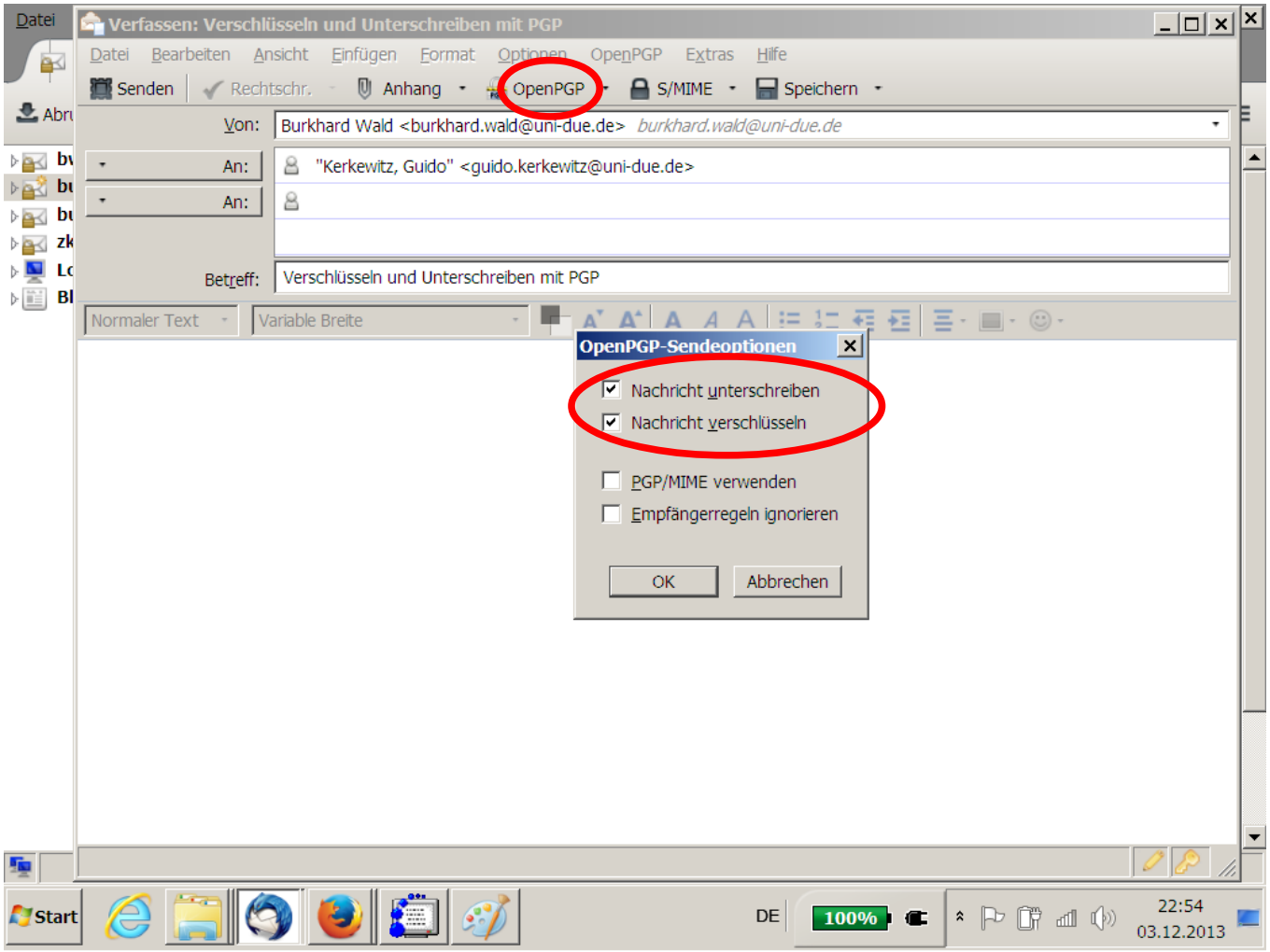
PGP-Schlüssel erzeugen und verwalten

UNIVERSITÄT DUISBURG ESSEN

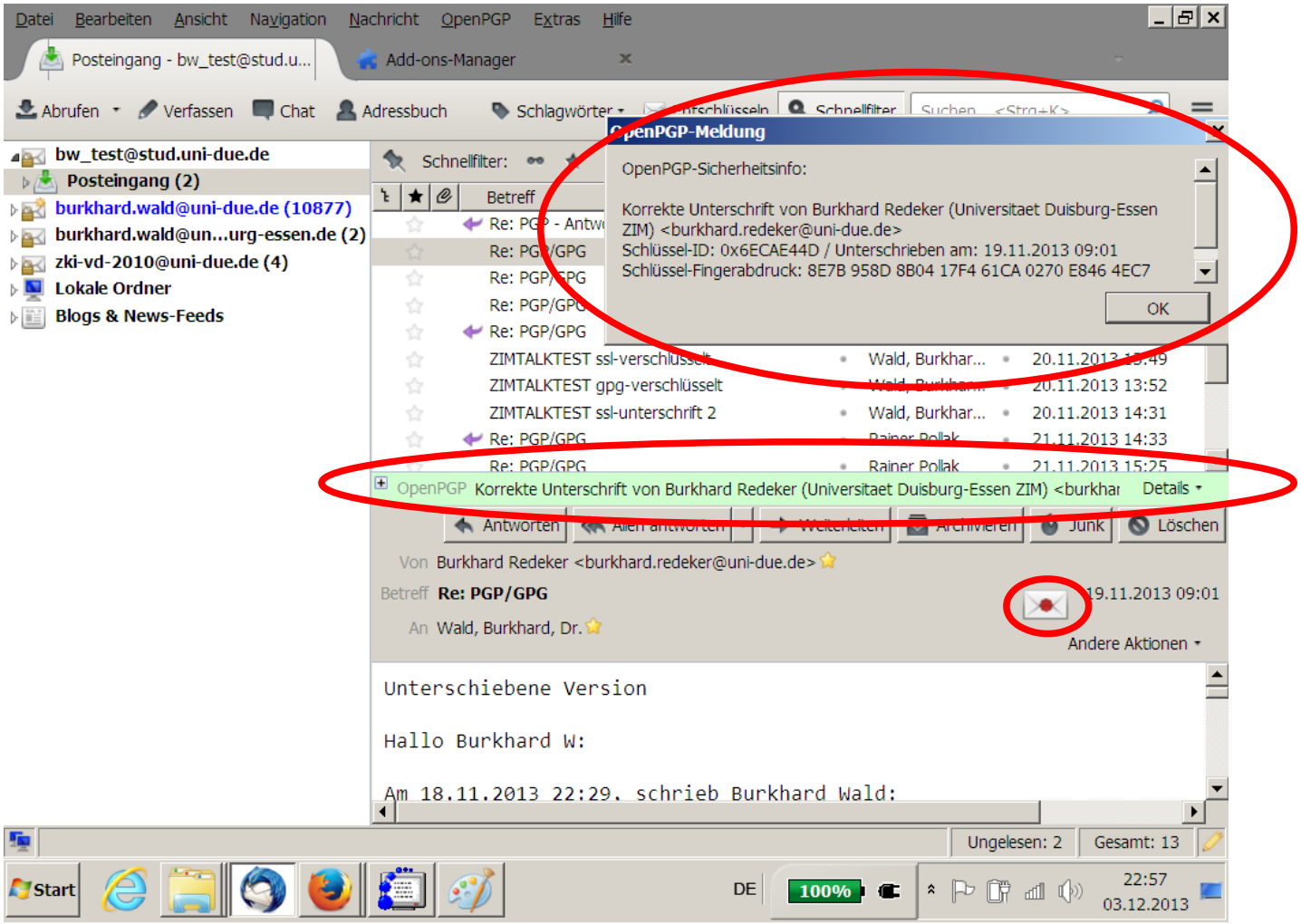
Offen im Denken



Nachricht versschlüssel und/oder unterschreiben



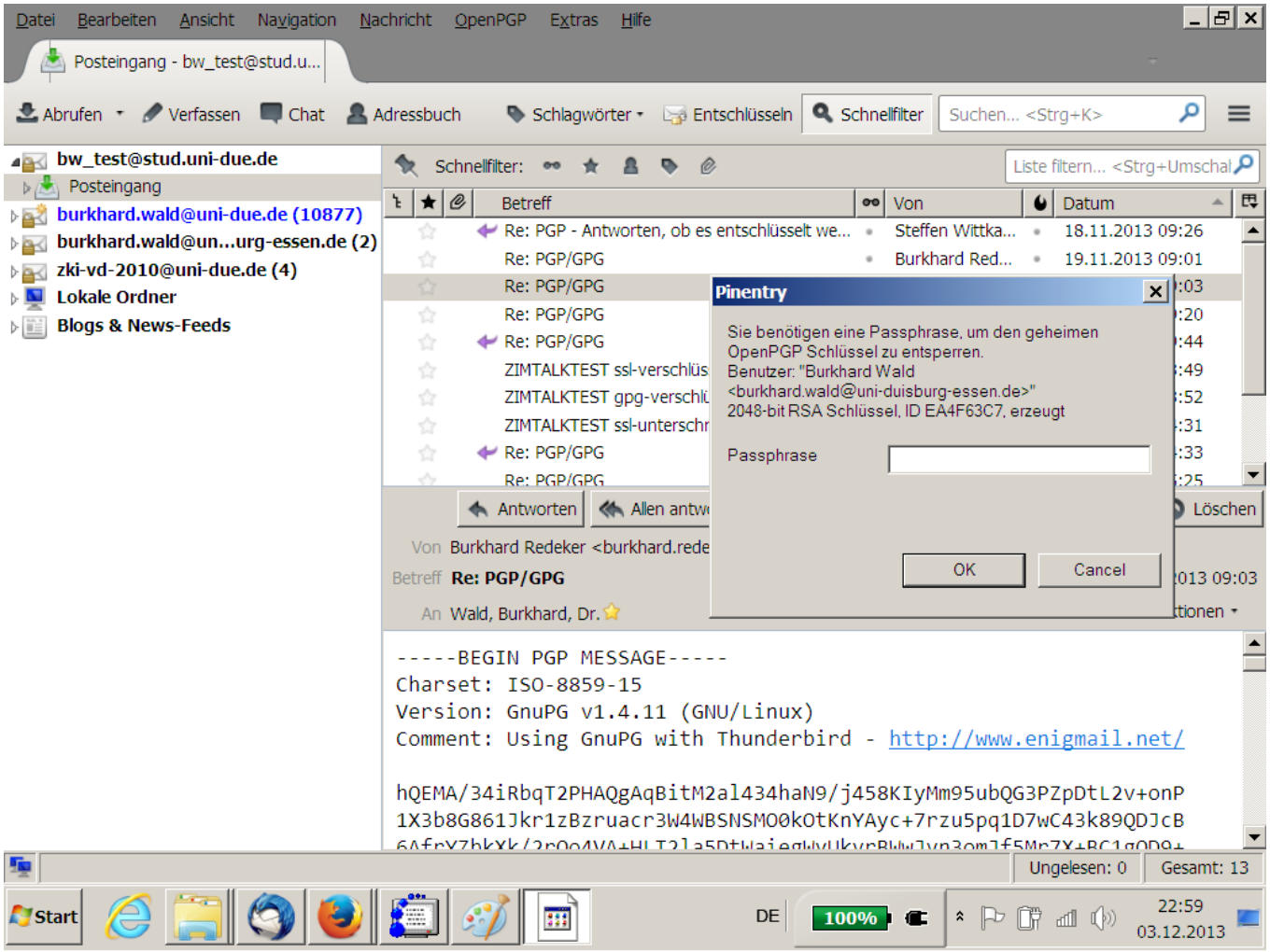
Unterschriebene Nachricht



Verschlüsselte Mail

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken



Am Anfang steht eine Entscheidung

- **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!

ZIM-Talk – http://www.uni-due.de/zim/zim-talk

UNIVERSITÄT DUISBURG ESSEN

Offen im Denken

- 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

ZIM
Zentrum für Informations- und Mediendienste