# CAcert

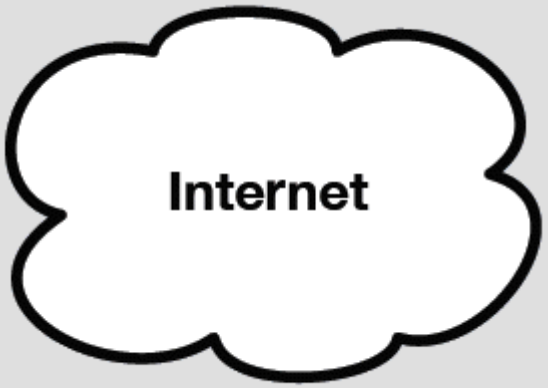
# Was ist das?

# Was ist CAcert?

## Sichere Kommunikation

# Was ist CAcert?

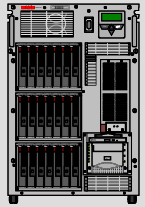
Bob

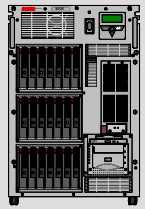


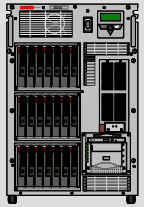

Alice

# Was ist CAcert?

## Unverschlüsselte Übertragung







Bob

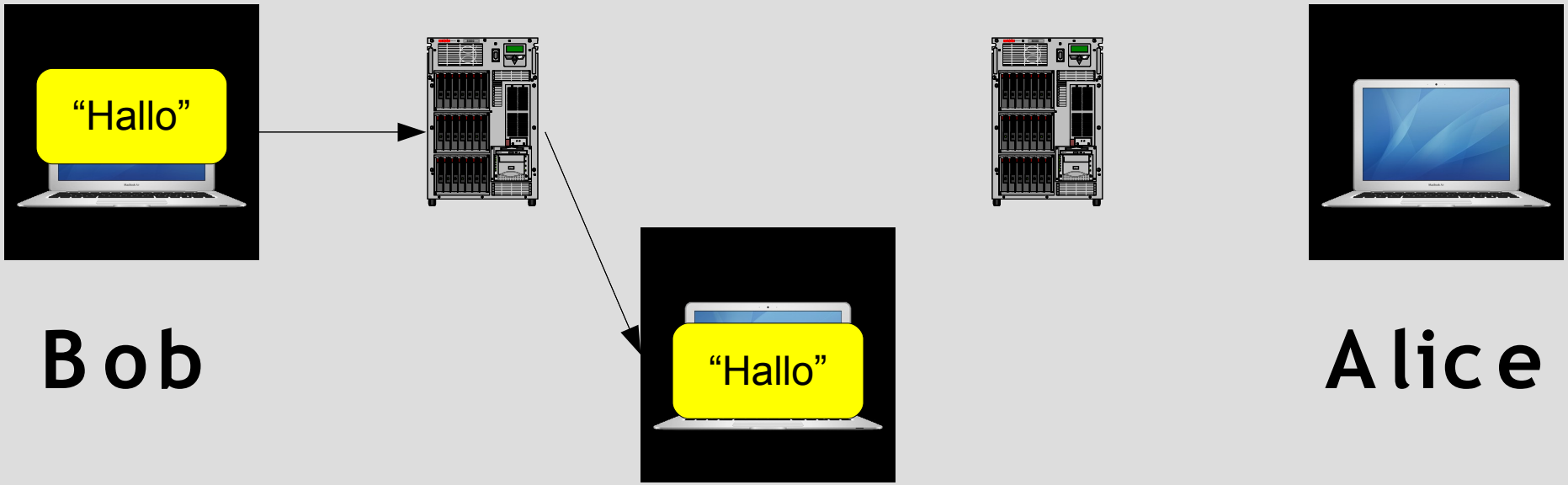
Alice

# Was ist CAcert?

## Unverschlüsselte Übertragung

# Was ist CAcert?

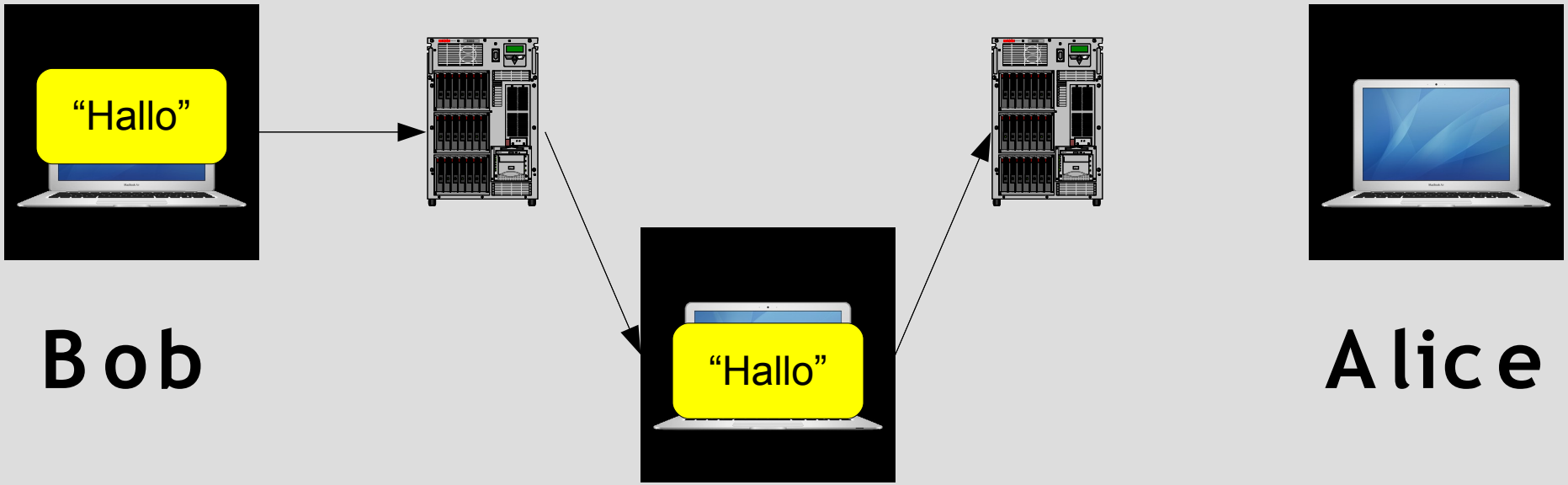
## Unverschlüsselte Übertragung




!!!!!

# Was ist CAcert?

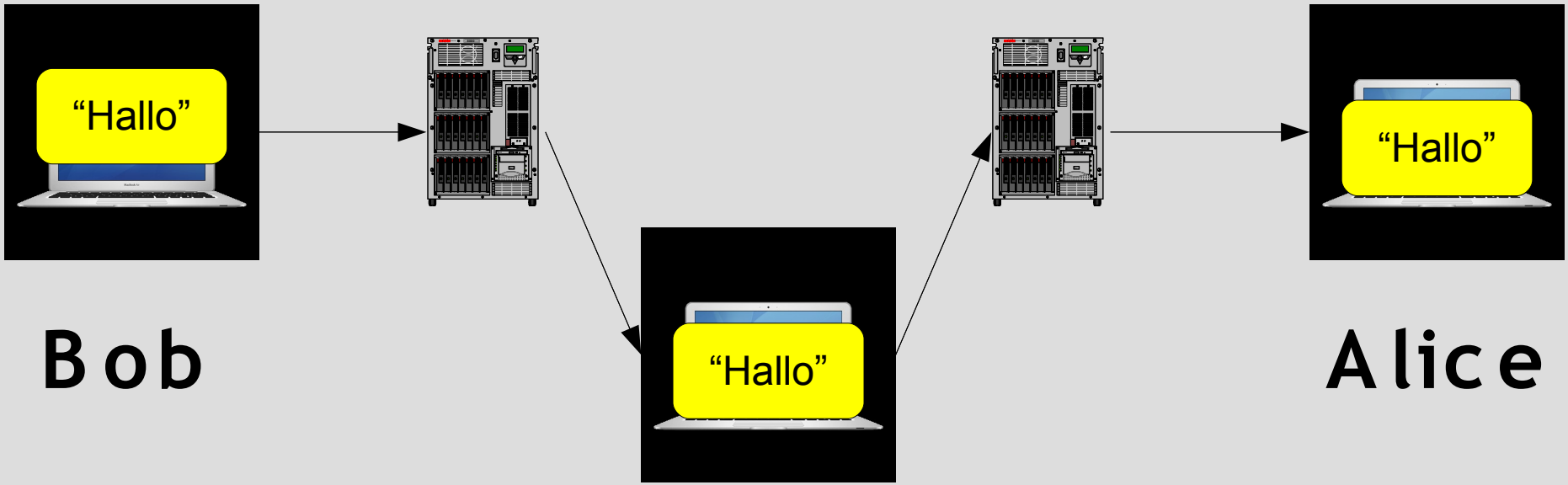
## Unverschlüsselte Übertragung




!!!!!

# Was ist CAcert?

## Unverschlüsselte Übertragung




!!!!!

# Was ist CAcert?

## Unverschlüsselte Übertragung

**5. Chemnitzer Linux-Tag**
01.-02. März 2003
Neues Hörsaal- und Seminargebäude der TU Chemnitz
Reichenhainer Str. 70

TOP SECRET !!!!

Meine neueste Idee für den Ausbau des Europäischen Geschäfts ....

Mit freundlicher Unterstützung von:

teegee
www.teegee.de

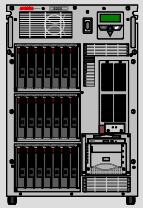
Weitere Informationen zum Linux - Tag finden Sie unter http://www.tu-chemnitz.de/linux/tag/

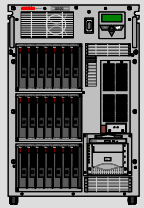
Alice

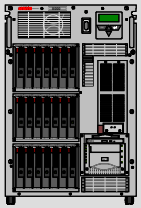
(c) by pebd

# Was ist CAcert?

## Verschlüsselte Übertragung





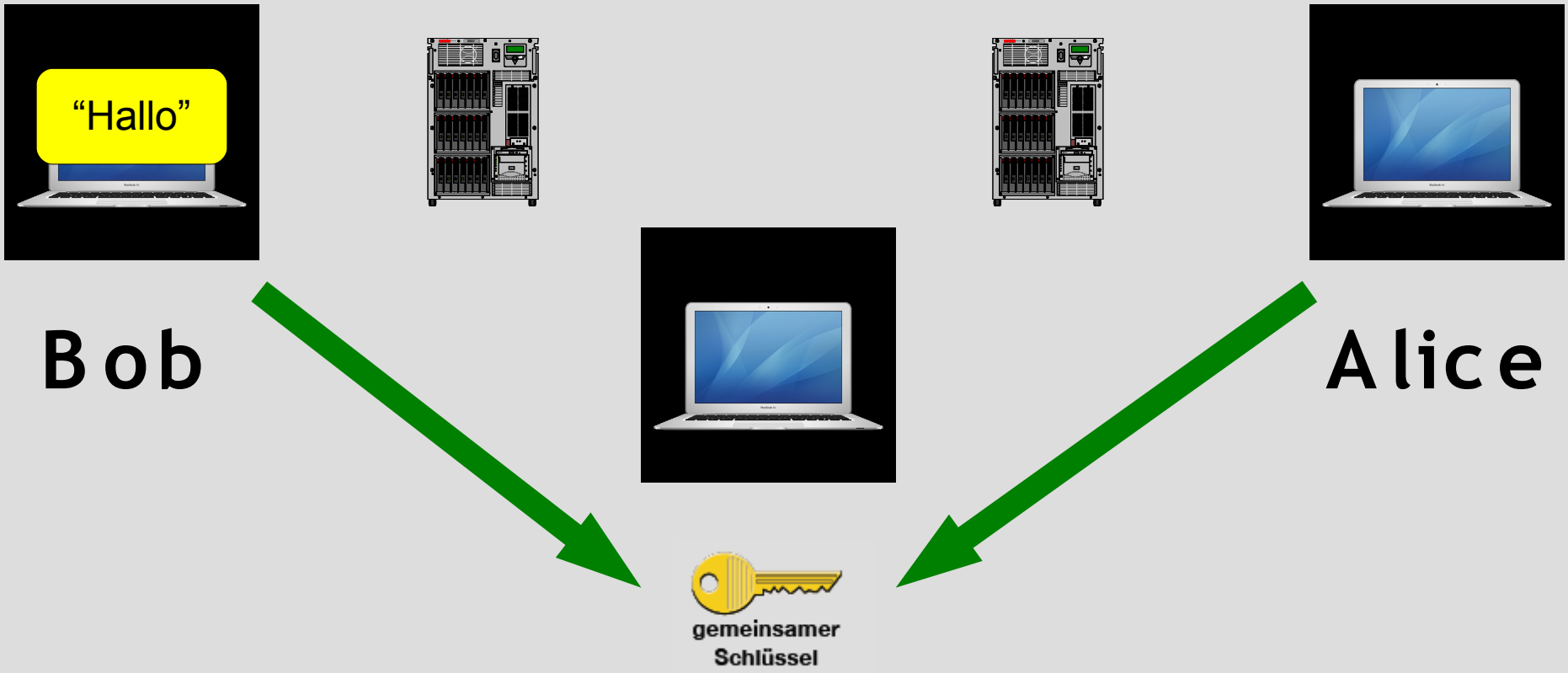


Bob

Alice

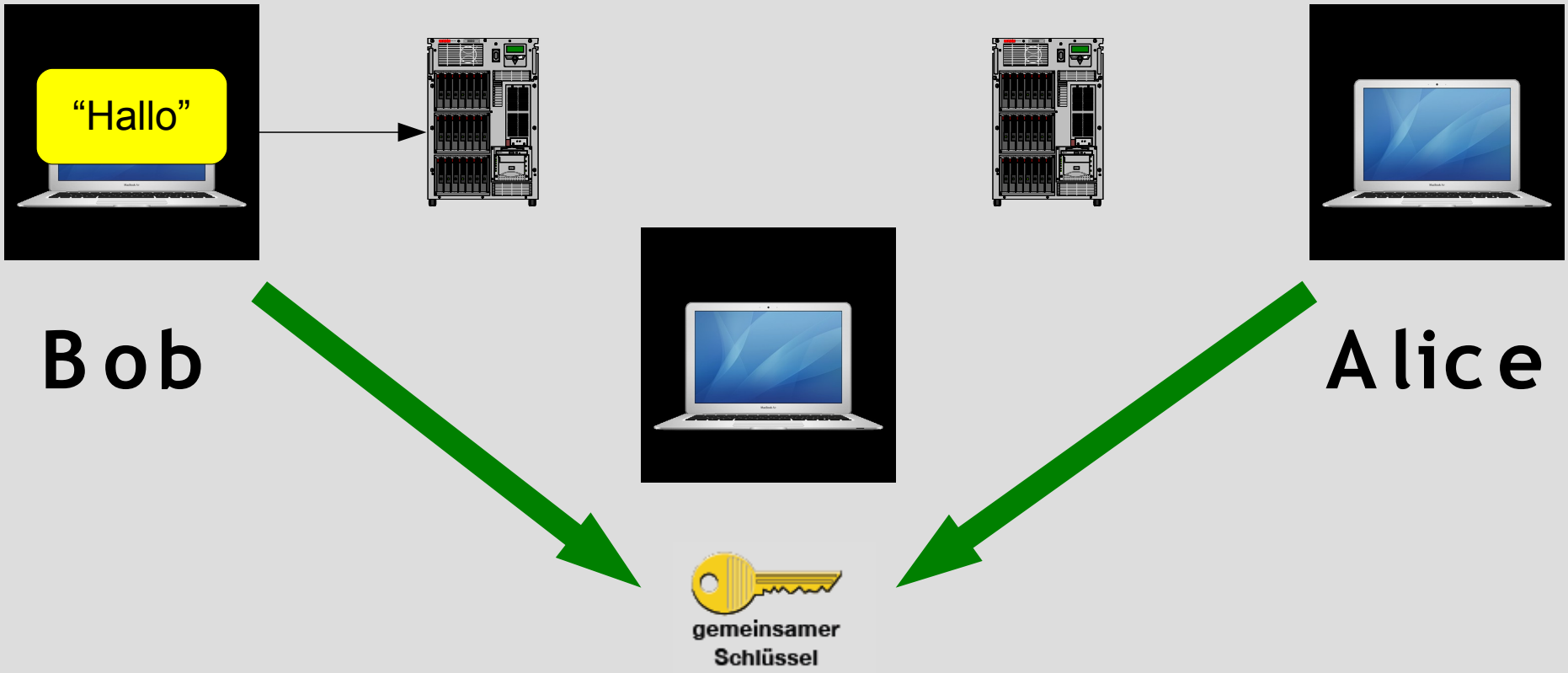
# Was ist CAcert?

## Verschlüsselte Übertragung



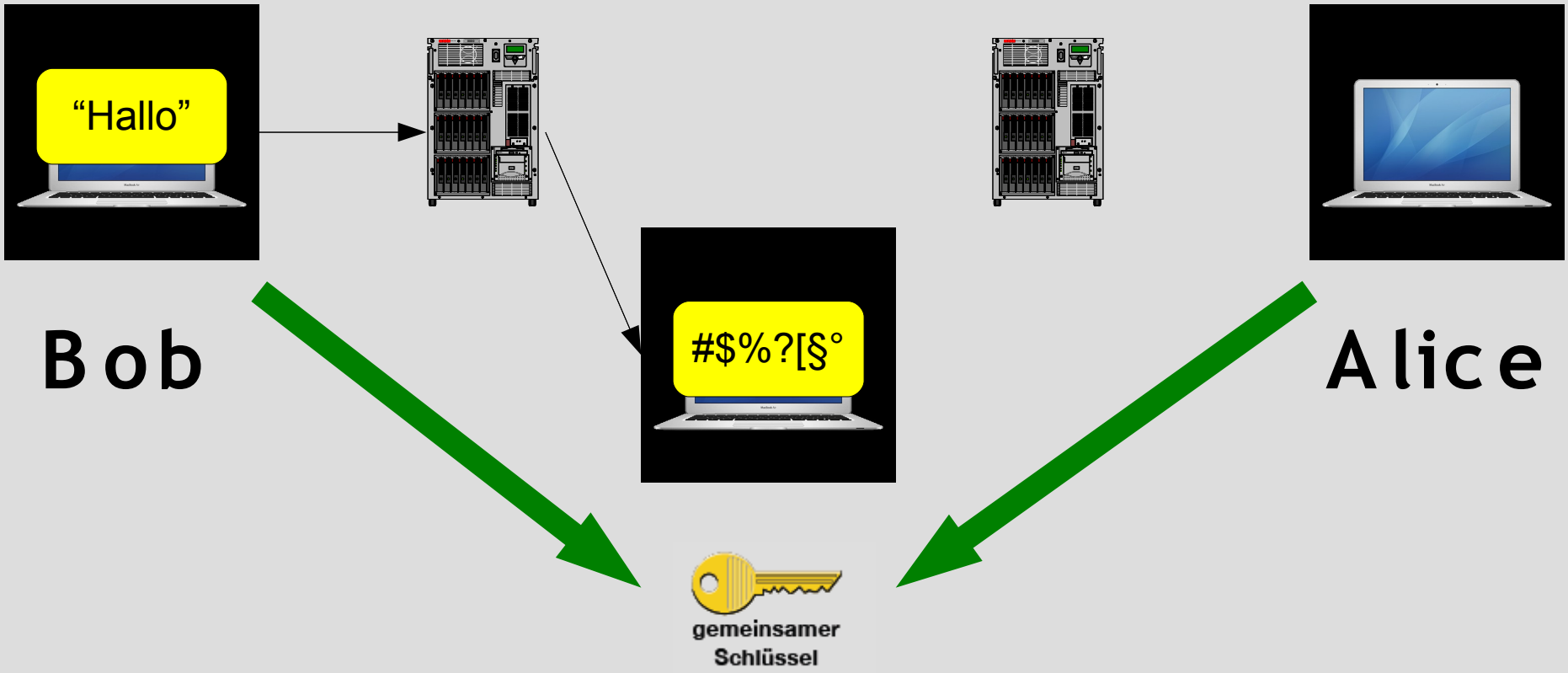
# Was ist CAcert?

## Verschlüsselte Übertragung



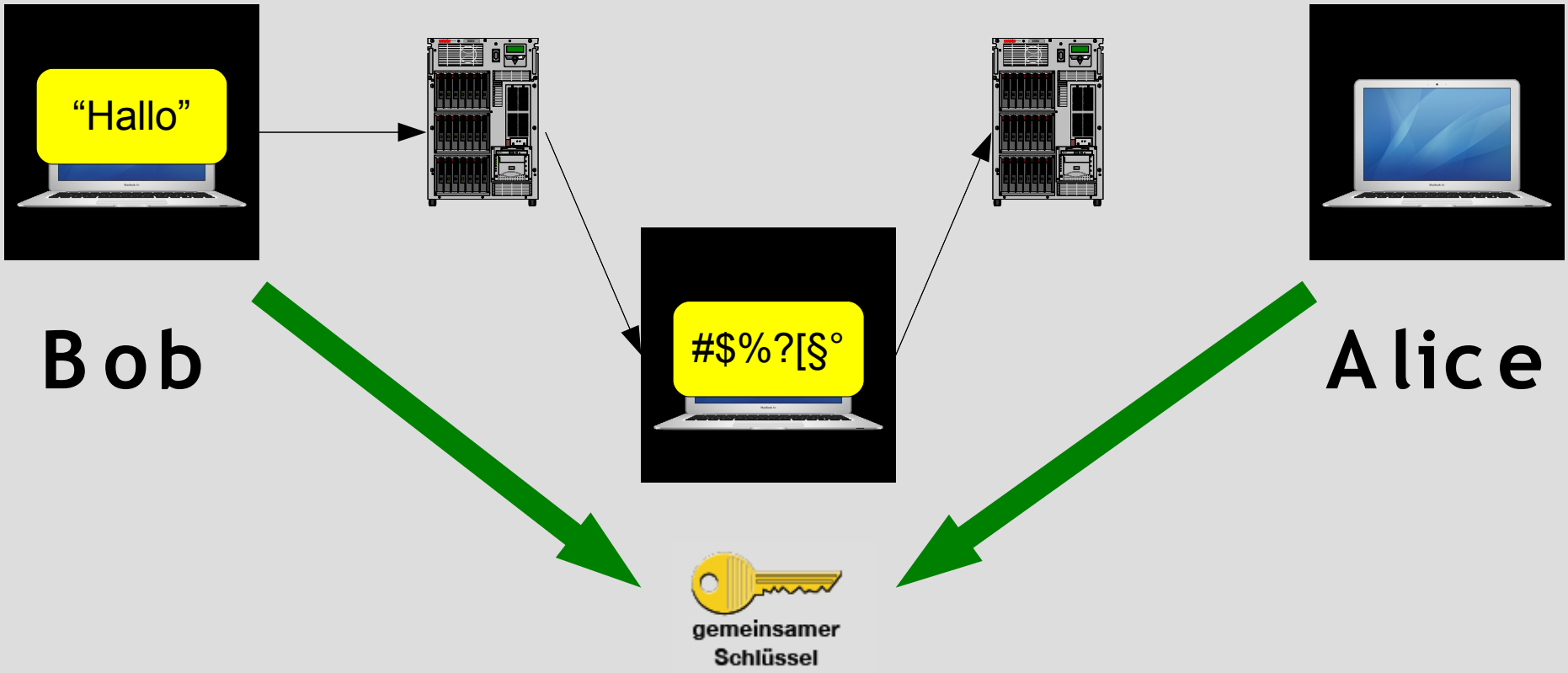
# Was ist CAcert?

## Verschlüsselte Übertragung



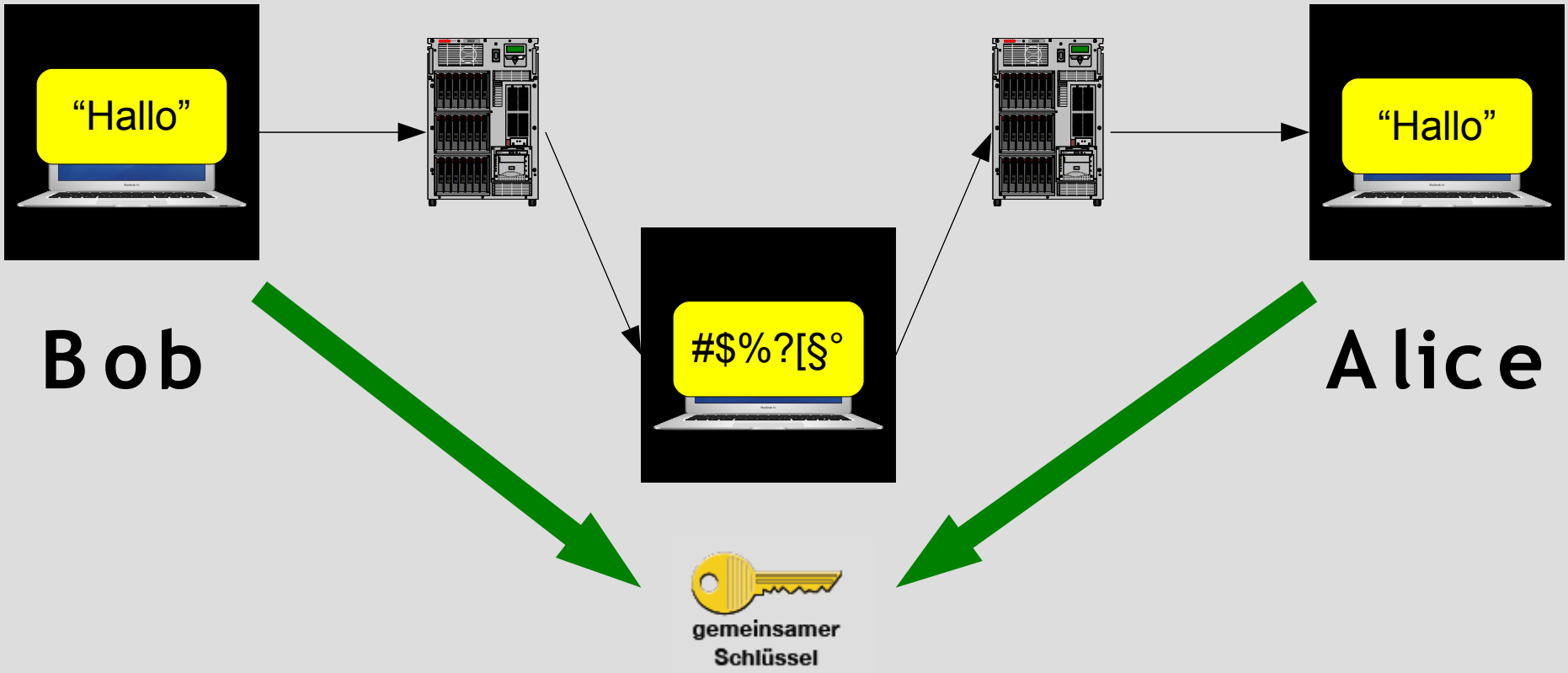
# Was ist CAcert?

## Verschlüsselte Übertragung



# Was ist CAcert?

## Verschlüsselte Übertragung



# Was ist CAcert?

## Verschlüsselte Übertragung


Problem:

Transfer des

gemeinsamen Schlüssels


Bob

Alice

gemeinsamer Schlüssel

# Was ist CAcert?

## Asymetrische Verschlüsselung

Bob

Alice

privater Schlüssel
Bob

öffentl. Schlüssel
Bob

# Was ist CAcert?

## Asymetrische Verschlüsselung

Bob

Alice

privater Schlüssel
Bob

öffentl. Schlüssel
Bob

öffentl. Schlüssel
Alice

privater Schlüssel
Alice

# Was ist CAcert?

## Asymetrische Verschlüsselung

Bob

Alice

privater Schlüssel
Bob

öffentl. Schlüssel
Bob

öffentl. Schlüssel
Alice

privater Schlüssel
Alice

# Was ist CAcert?

## Asymetrische Verschlüsselung

Bob

Alice

privater Schlüssel
Bob

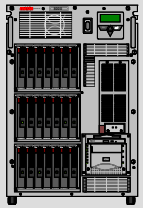
öffentl. Schlüssel
Bob

öffentl. Schlüssel
Alice

privater Schlüssel
Alice

# Was ist CAcert?

## Asymetrische Verschlüsselung



Bob

Alice

privater Schlüssel
Bob

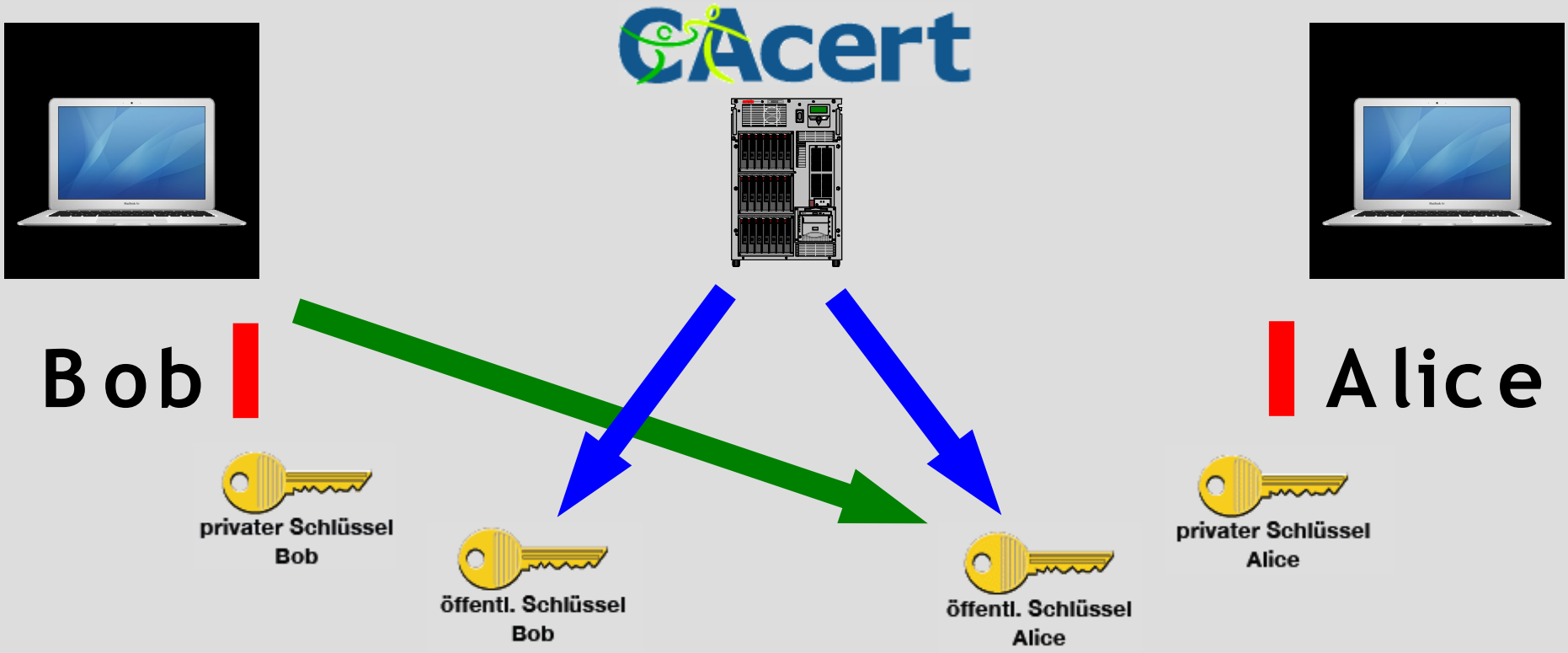
öffentl. Schlüssel
Bob

öffentl. Schlüssel
Alice

privater Schlüssel
Alice

# Was ist CAcert?

## Asymetrische Verschlüsselung



# Was ist CAcert?

## Asymetrische Verschlüsselung

Schlüssel Transfer unproblematisch:

- Sichere Verbindung zu HTTPS://www.CAcert.org für Privaten Schlüssel
- Transfer öffentlicher Schlüssel zum E-Mail Partner via Signatur

Bob

Alice

privater Schlüssel Bob

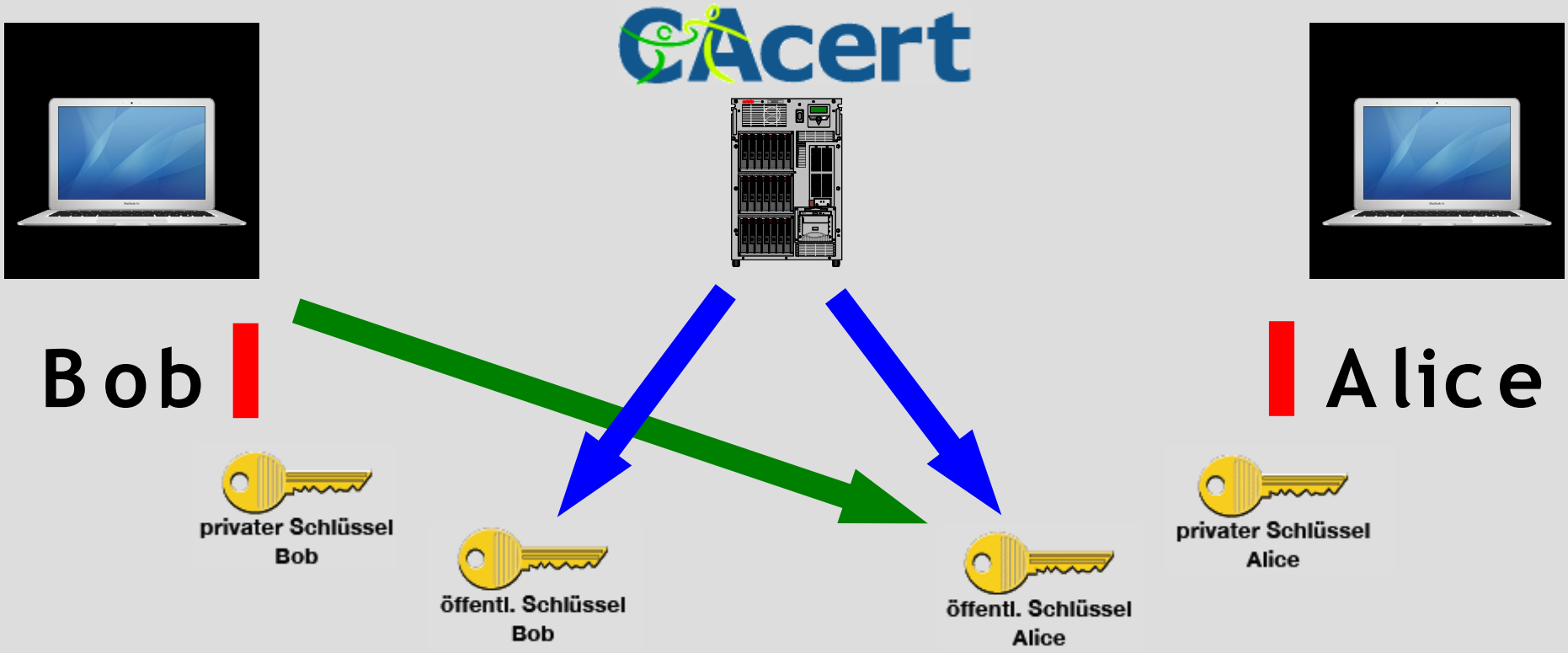
öffentl. Schlüssel Bob

öffentl. Schlüssel Alice

privater Schlüssel Alice

# Was ist CAcert?

## Zertifizieren von Schlüsseln



# Was ist CAcert?

- 2002 startete CAcert Org → CAcert Community
- 2003 startete CAcert Inc. → ein Non-Profit Verein mit Sitz in NSW Australien
- CAcert Inc. betreibt eine PKI Infrastruktur für die Community Member
- Basierend auf dem Open Source Gedanken

# Was ist CAcert?

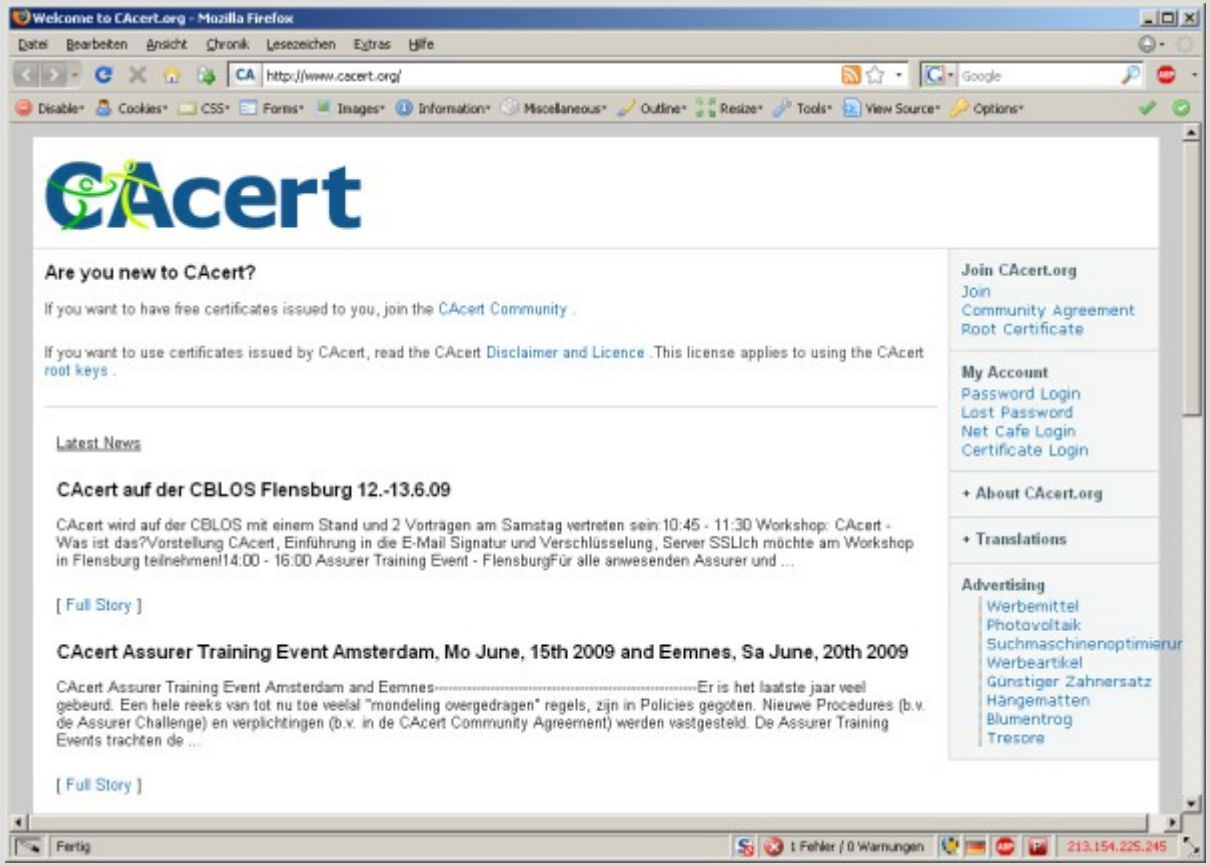
- Security und Privatsphäre darf nichts kosten

- CAcert bietet kostenlos …
  - ✔ Zertifikate für E-Mail Signatur
  - ✔ Zertifikate für E-Mail Verschlüsselung
  - ✔ SSL Server Zertifikate
  - ✔ Code Signing
  - ✔ Dokument Signing

# Was ist CAcert?

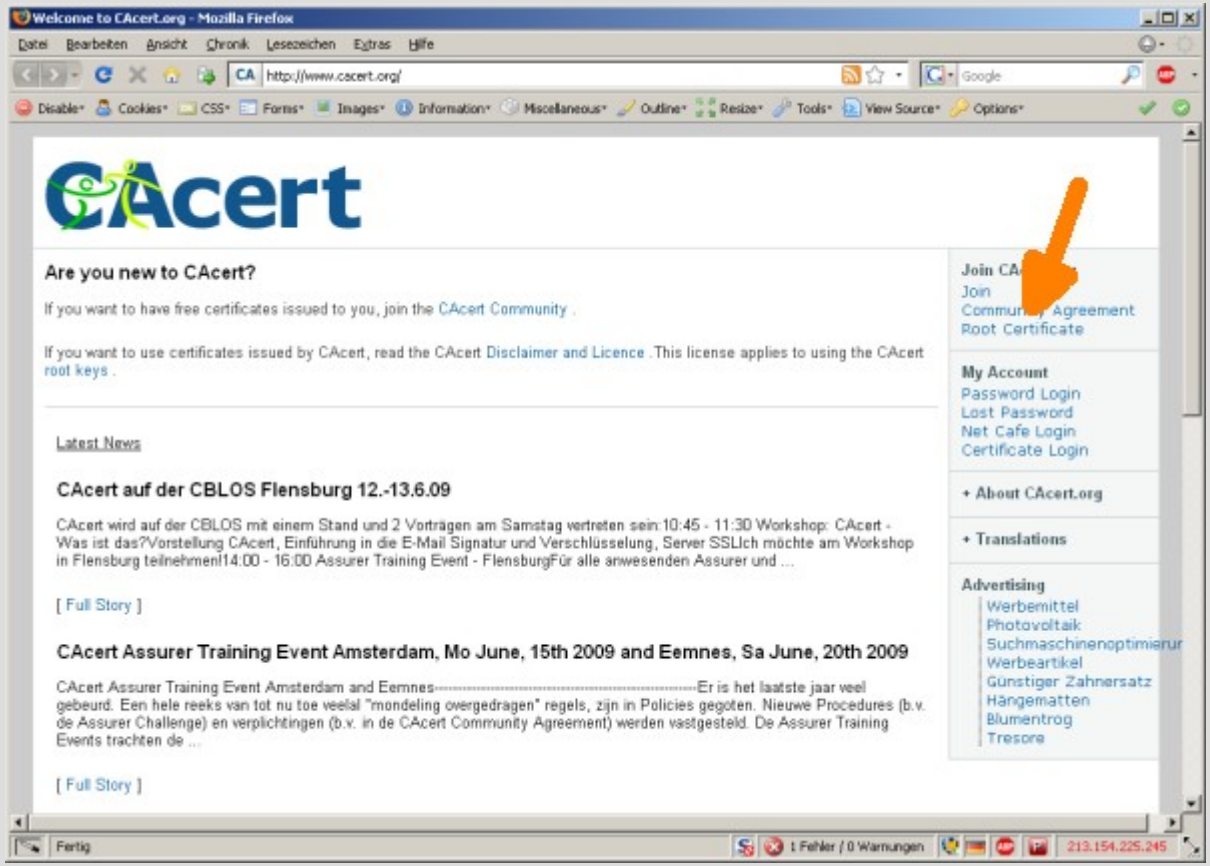
- Root Zertifikate Firefox

# Was ist CAcert?



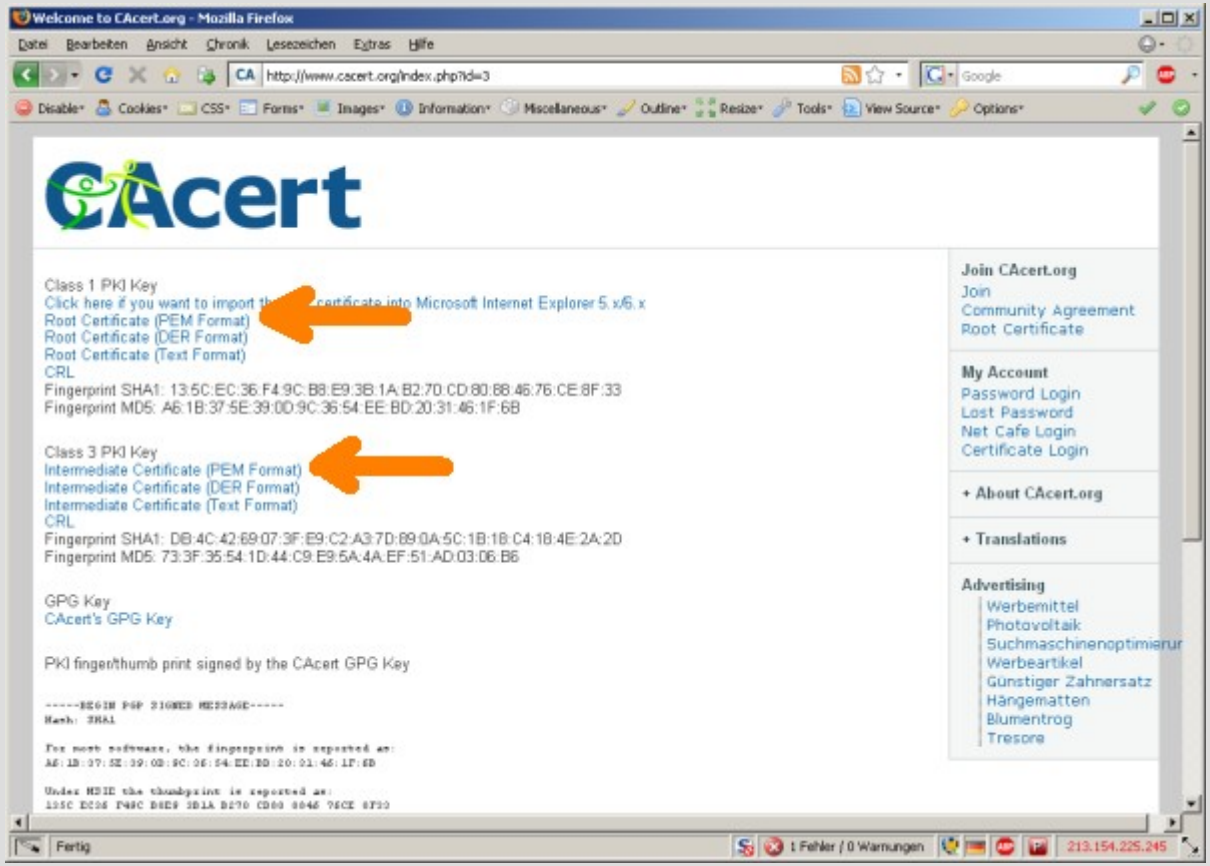

http://www.CAcert.org

# Was ist CAcert?



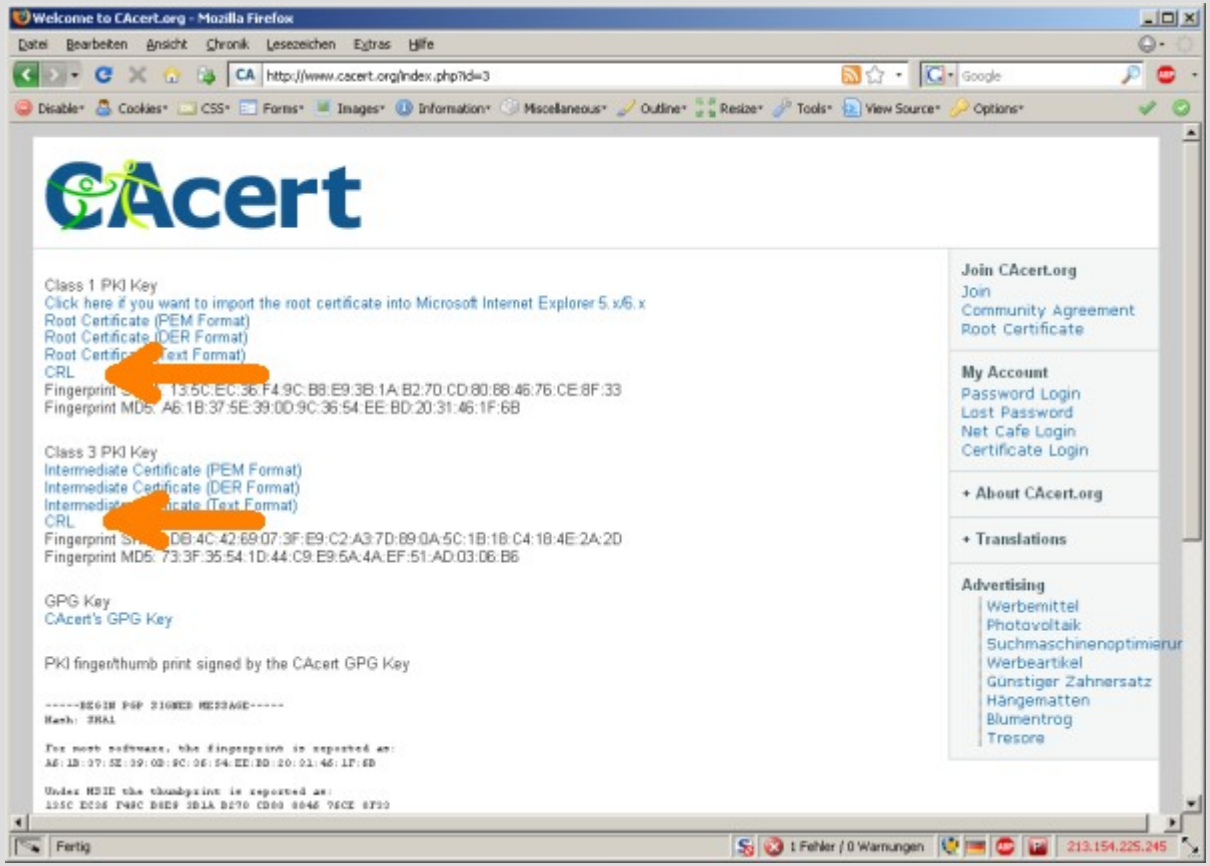

http://www.CAcert.org

# Was ist CAcert?



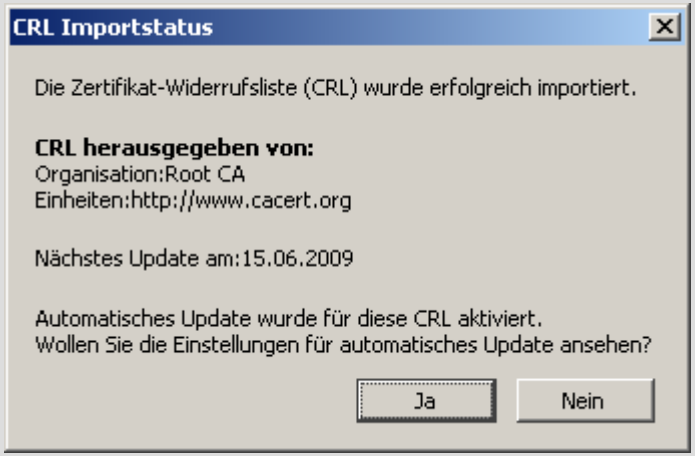

CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?




CAcert: Class1 + Class3 Root CRL's

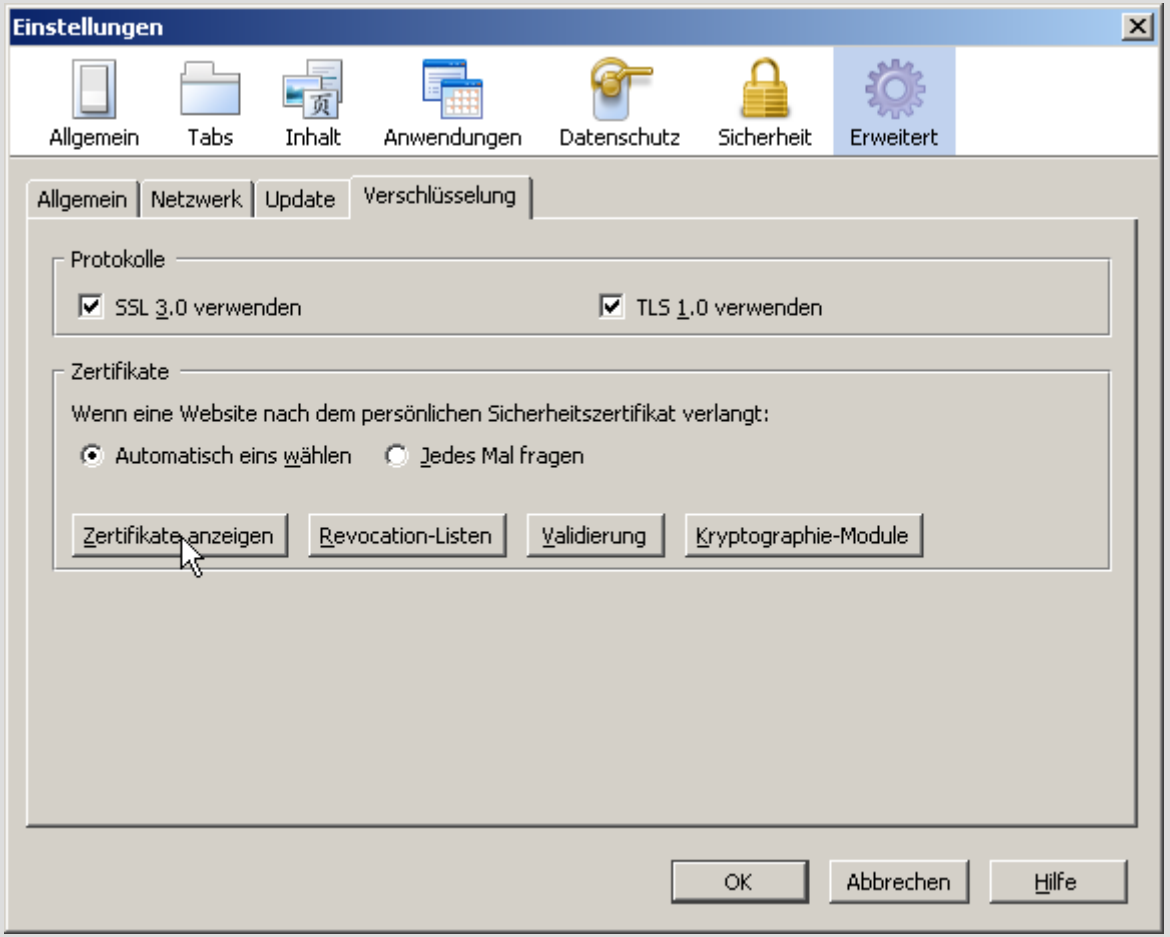
# Was ist CAcert?




CAcert: Class1 + Class3 Root CRL's

# Was ist CAcert?

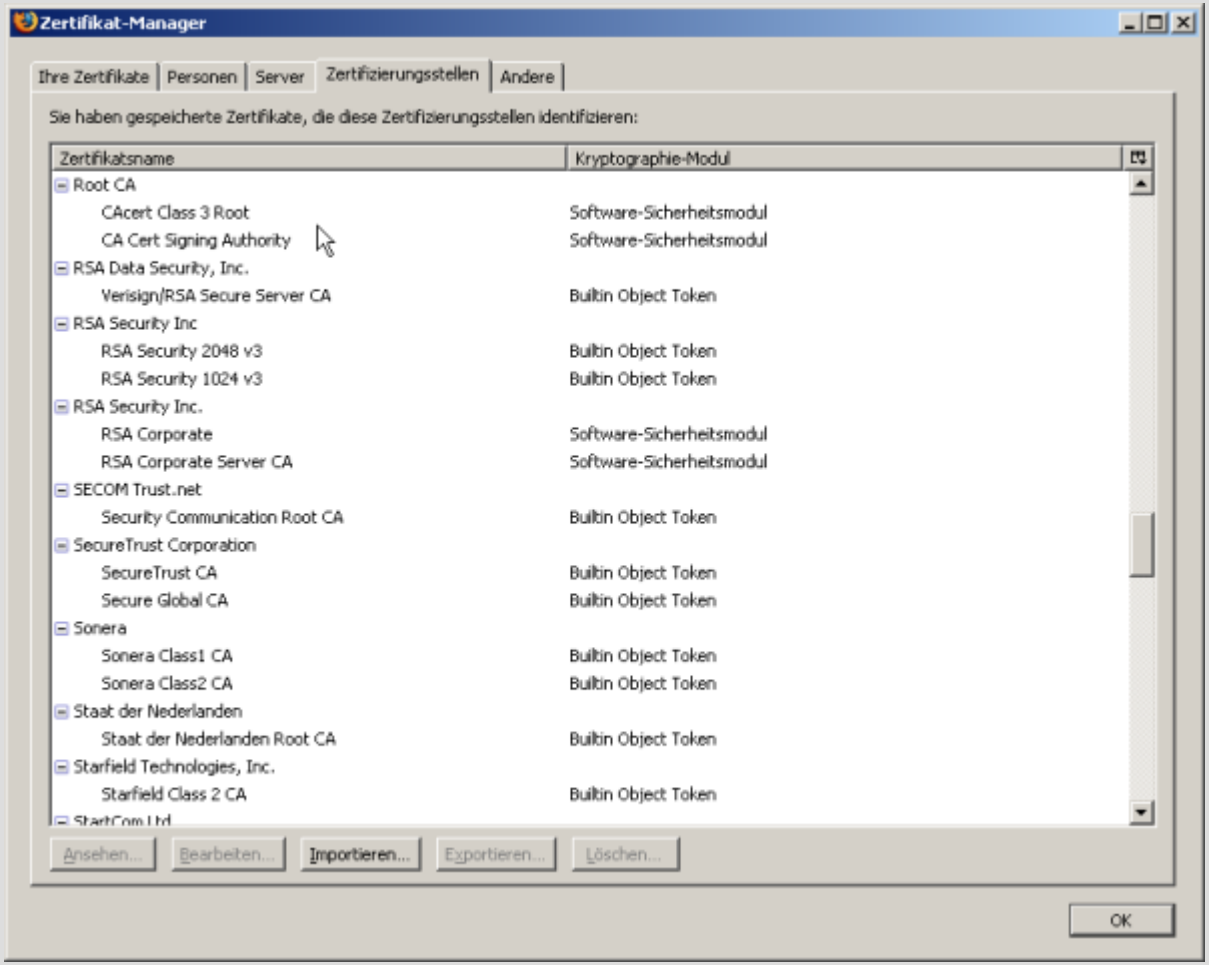
Menü:
- Extras
- Einstellungen
- Erweitert
- Tab Verschlüsselung
- Zertifikate anzeigen




CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?

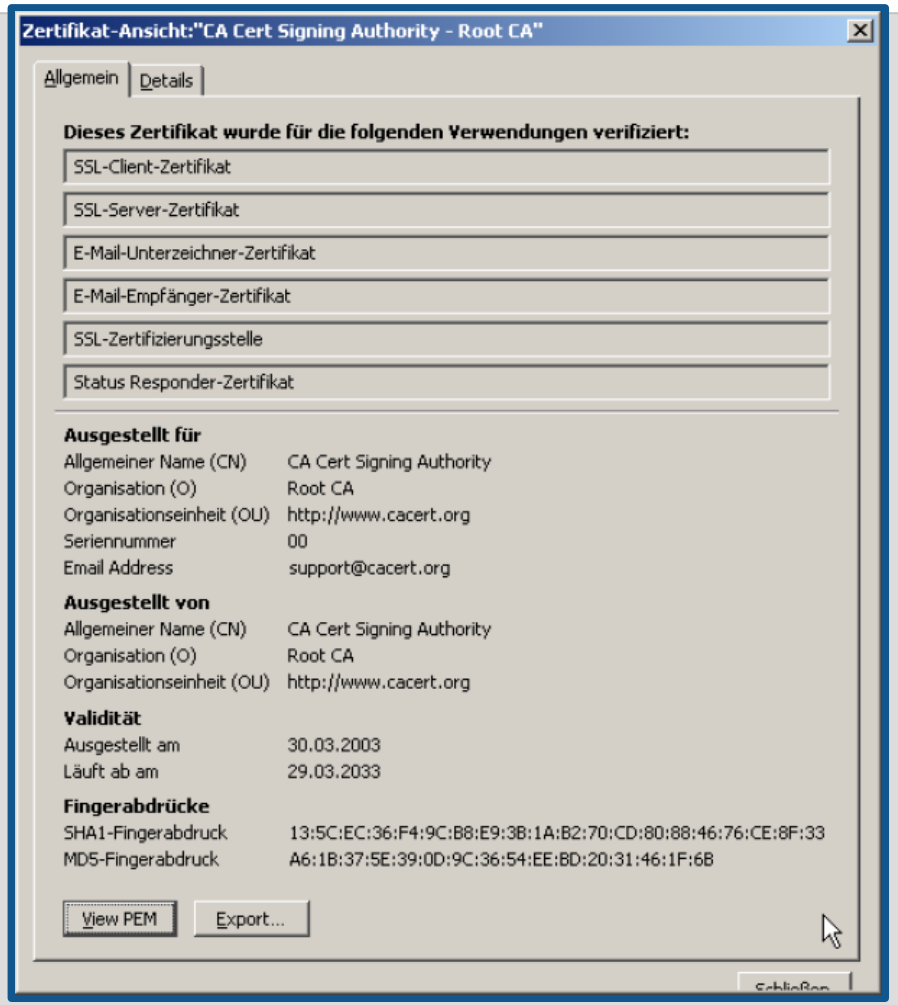
Tab Zertifizierungsstellen




CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?

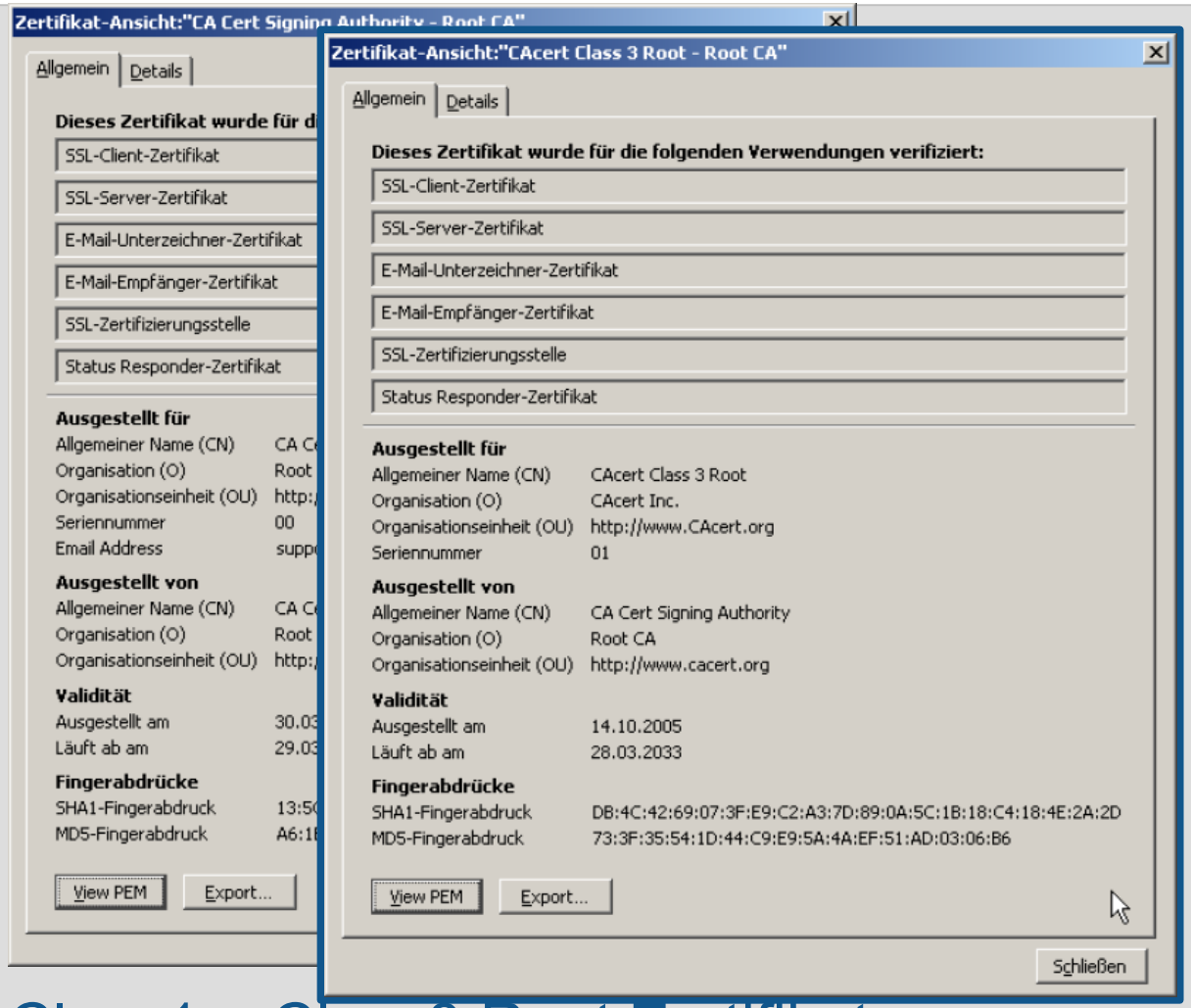
CAcert Signing Authority
Root CA




CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?

CAcert Class 3 Root
Root CA

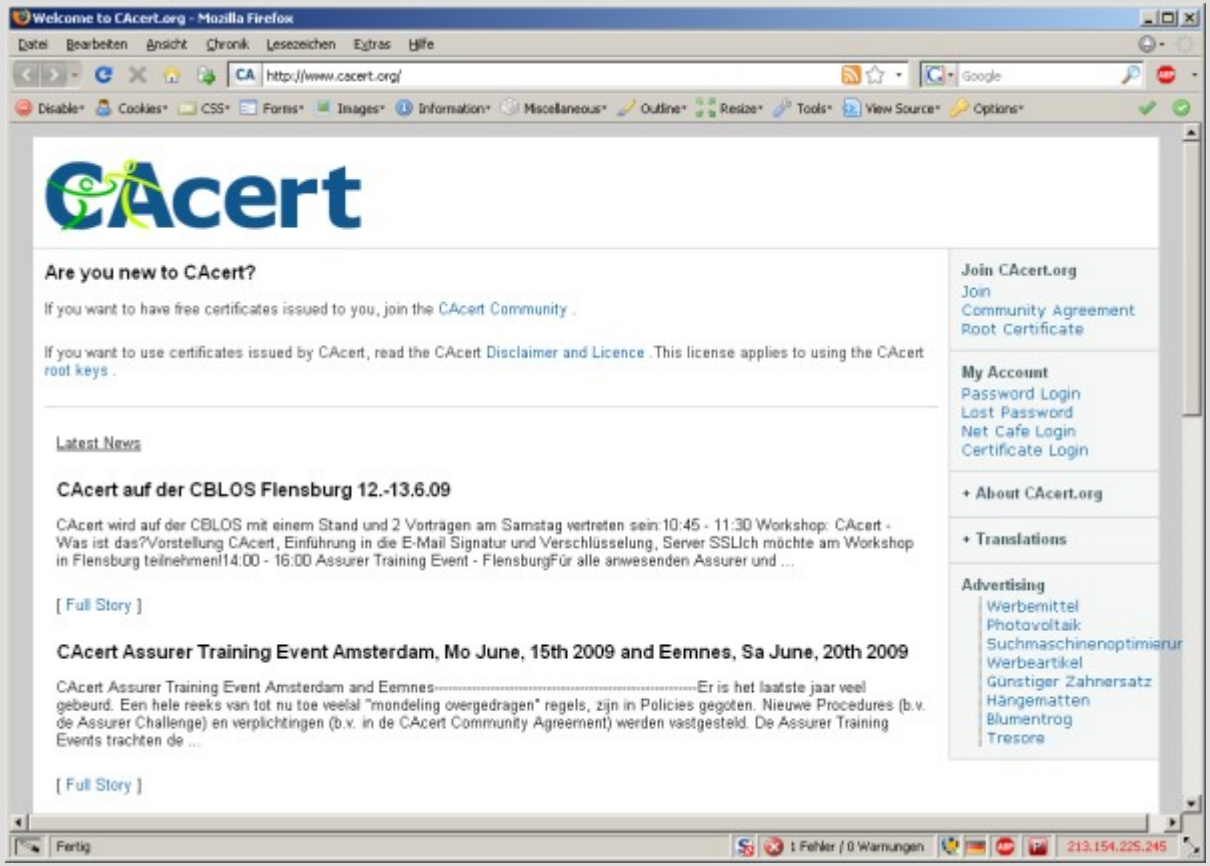



CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?

- Wie kann ich mitmachen?

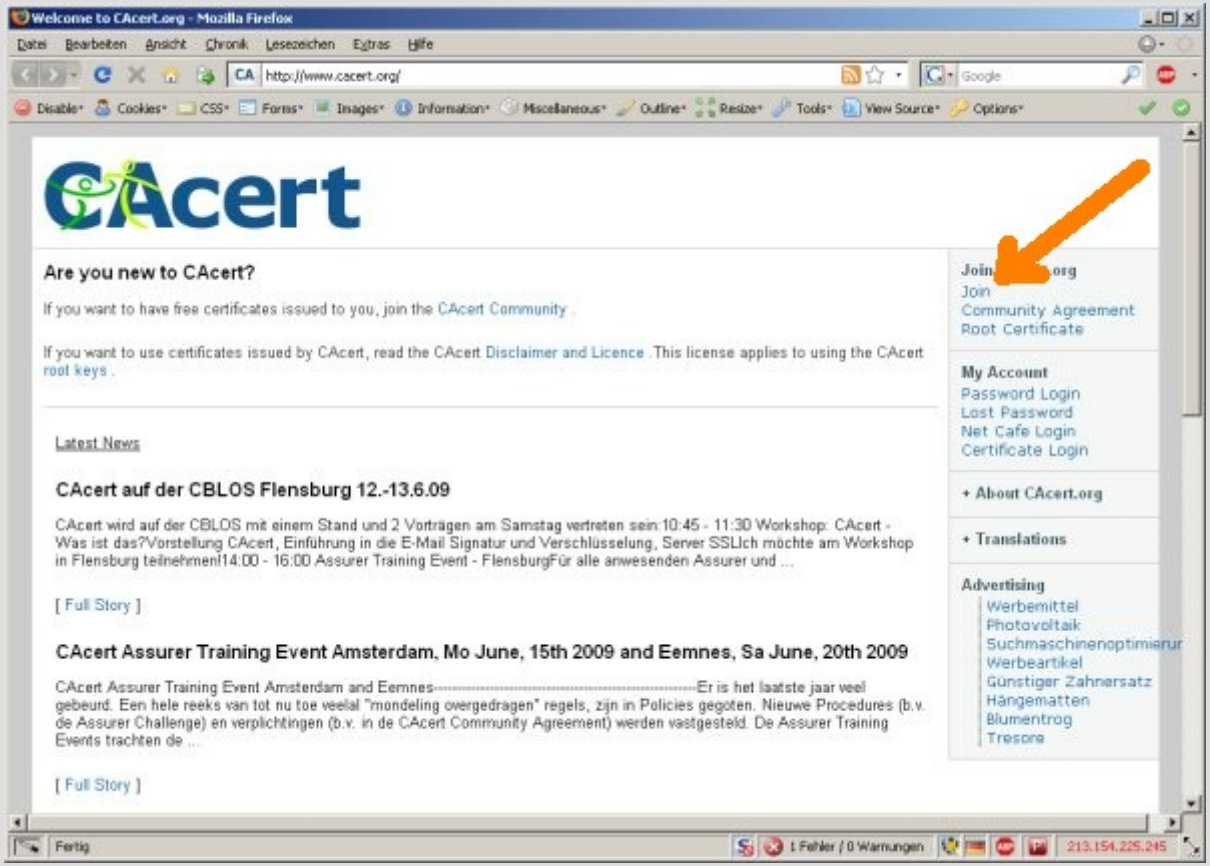
# Was ist CAcert?




http://www.CAcert.org

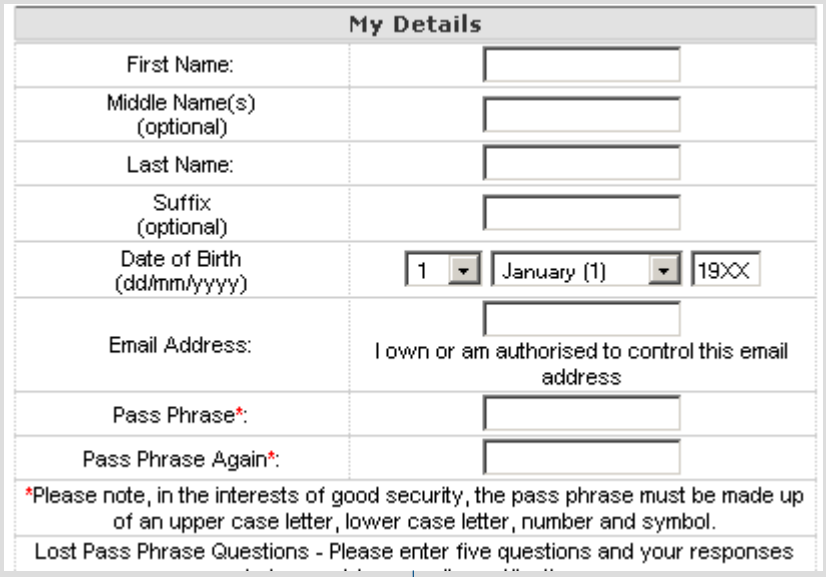
# Was ist CAcert?

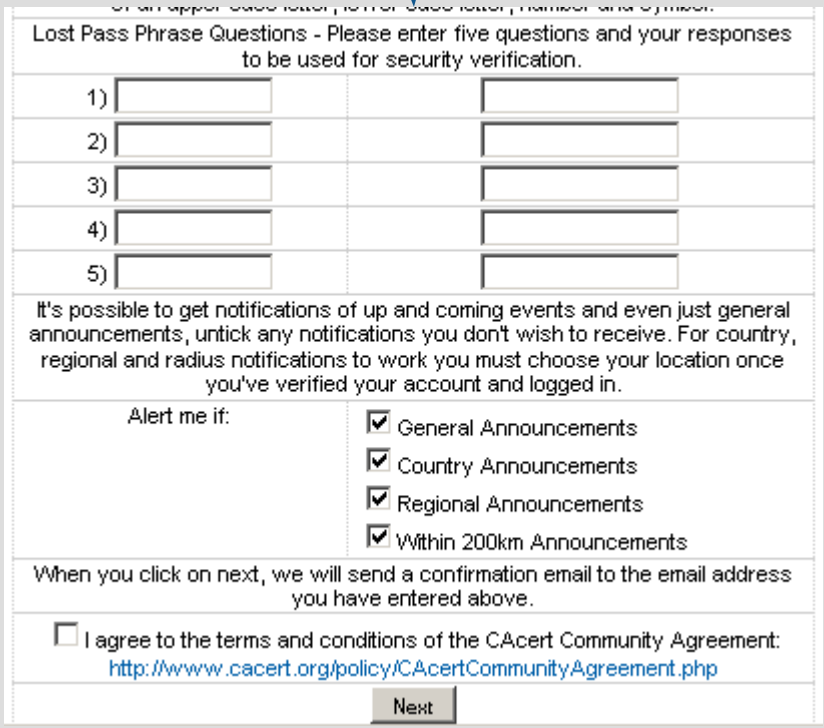
Join !




http://www.CAcert.org

# Was ist CAcert?



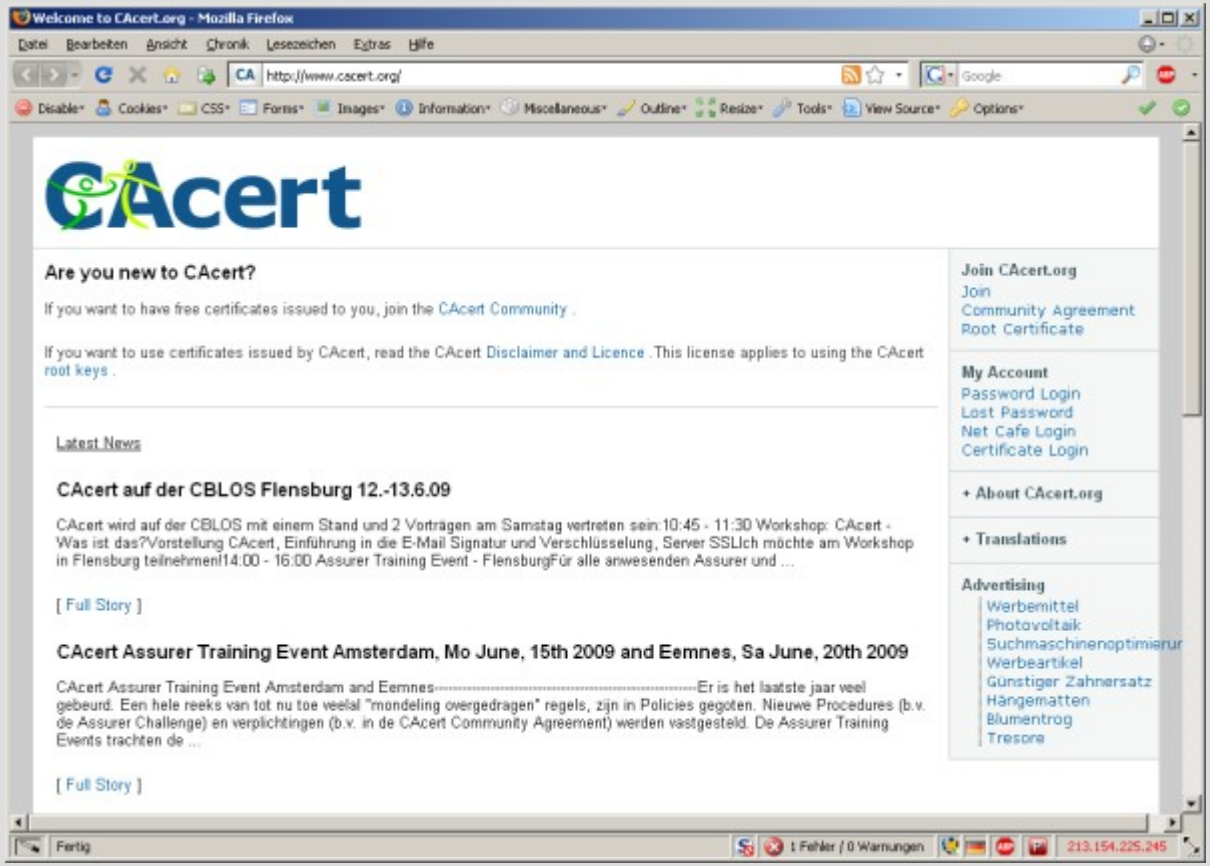




Registrierungs Formular

# Was ist CAcert?

- Identifikationsprozess

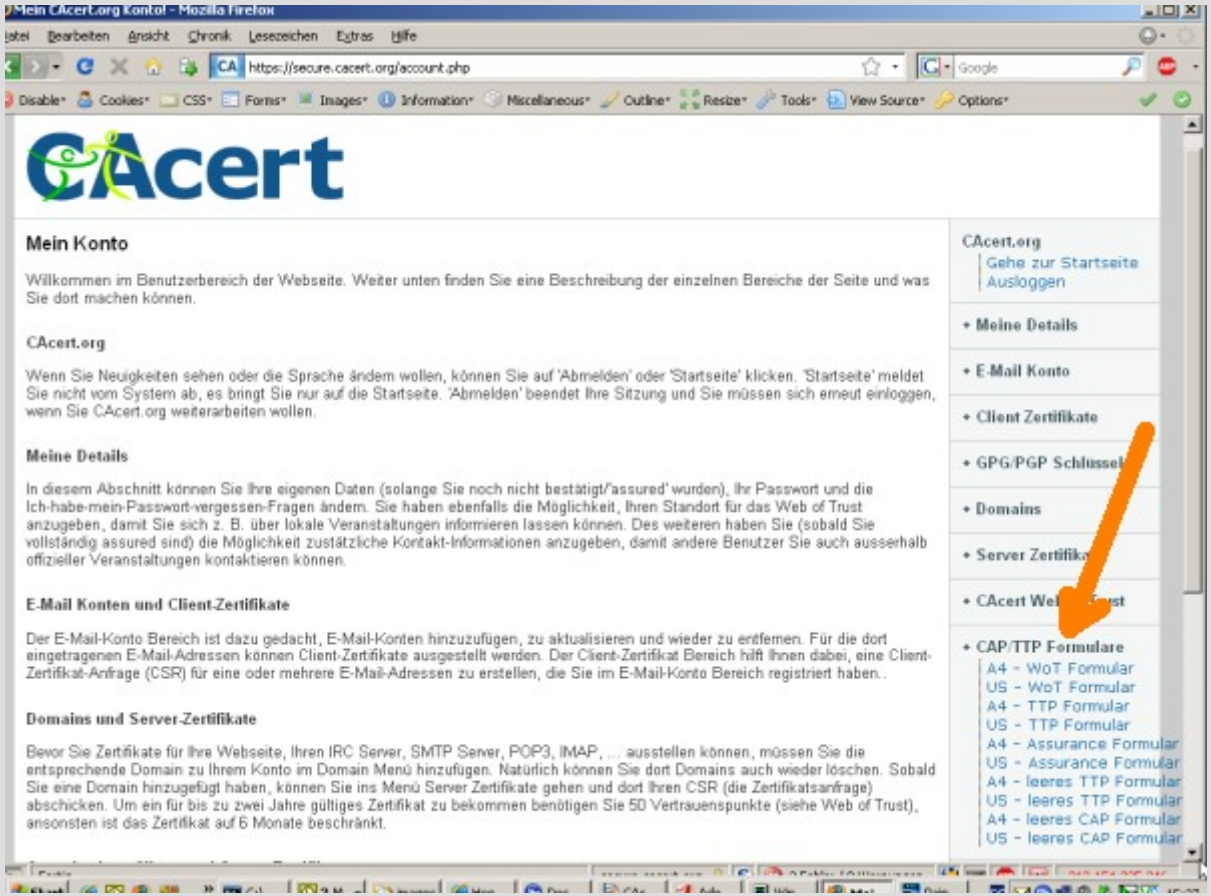
# Was ist CAcert?




http://www.CAcert.org

# Was ist CAcert?

CAP
Formulare




http://www.CAcert.org

# Was ist CAcert?

CAP Formular

## *Antragsteller*

| | |
|---|---|
| **Namen:** | |
| **Geburtsdatum:** (JJJJ-MM-TT) | |
| **E-Mail Adresse:** | |

Hiermit bestätige ich, daß meine obigen Informationen zu meiner Identität korrekt und wahrheitsgemäss sind und bitte den CAcert Assurer (siehe unten) mich entsprechend der CAcert Assurance Policy zu überprüfen.

Hiermit stimme ich den CAcert Community Bedingungen zu. ( http://www.cacert.org/policy/CAcertCommunityAgreement.php )

Unterschrift des Antragstellers: _____ Datum (JJJJ-MM-TT): 20___-___-___

## *CAcert Assurer*

Name des Assurers: _____

Foto-Ausweis vorgelegt: (Ausweistyp, keine Ausweisnummern - z. B. Führerschein, Personalausweis)

1. _____
2. _____

Ort des persönlichen Treffens: _____

Vergebene Punkte: _____

Hiermit bestätige ich als Assurer, daß ich das Mitglied entsprechend der CAcert Assurance Policy überprüft habe.
Hiermit bestätige ich, daß ich ein Mitglied der CAcert-Gemeinschaft bin, die Assurer Prüfung erfolgreich bestanden habe und mit mindestens 100 Assurance-Punkten überprüft wurde.

Unterschrift des Assurers: _____ Datum (JJJJ-MM-TT): 20___-___-___

# Was ist CAcert?

Punkteschema

| Punkte | Status | Punktevergabe (max.) |
|---|---|---|
| 0 - 49 | unassured | - |
| 50 - 100 | assured | - |
| Assurer Challenge | bestanden | |
| 100 - 109 | assurer | 10 |
| 110 - 119 | assurer | 15 |
| 120 - 129 | assurer | 20 |
| 130 - 139 | assurer | 25 |
| 140 - 149 | assurer | 30 |
| 150 | fully assured | 35 |

# Was ist CAcert?

- Root Zertifikate Thunderbird

# Was ist CAcert?

- CAcert: Class1 + Class3 Root Zertifikate
  Mit Webbrowser Downloaden
- Eigenes Client Zertifikat (Privater Schlüssel)
- Importieren in Thunderbird

Menü:
- Extras
- Einstellungen
- Erweitert
- Tab Zertifikate
- Zertifikate
- Tab Zertifizierungsstellen
- Importieren

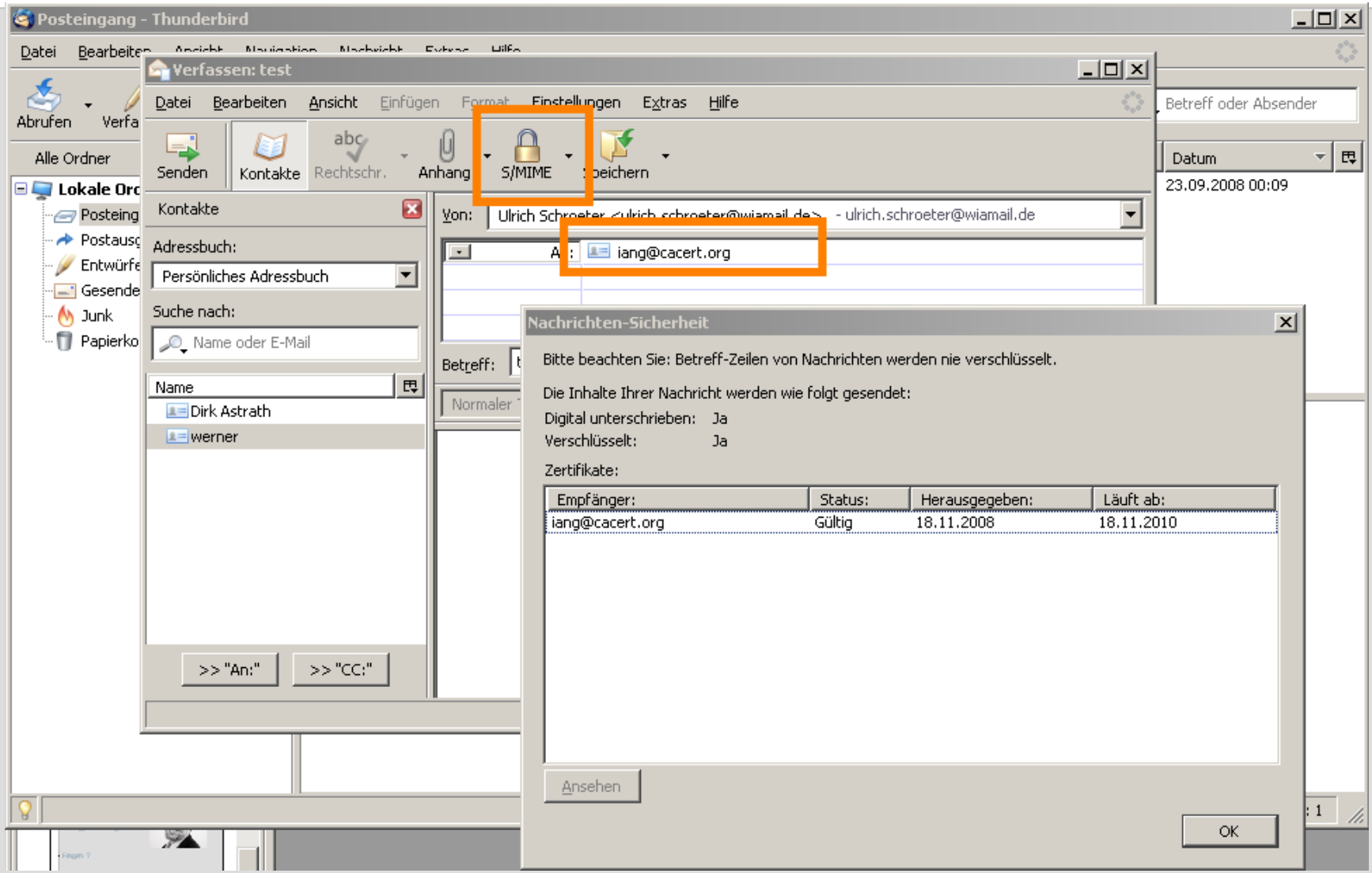
Menü:
- Extras
- Einstellungen
- Erweitert
- Tab Zertifikate
- Zertifikate
- Tab Ihre Zertifikate
- Importieren

# Was ist CAcert?

- Client Zertifikat (öffentlicher Schlüssel) von Kommunikationspartnern
- Importieren in Thunderbird

Menü:
- Extras
- Einstellungen
- Erweitert
- Tab Zertifikate
- Zertifikate
- Tab Zertifikate anderer Personen
- Importieren

# Was ist CAcert?



# Danke, Fragen & Antworten

- http://www.CAcert.org
- Ulrich Schroeter
  ulrich@CAcert.org

- Fragen ?