

## CAcert

### Was ist das?



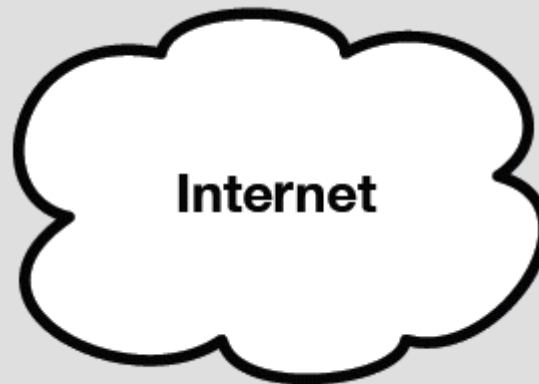
# Was ist CAcert?

Sichere Kommunikation

## Was ist CAcert?



**Bob**



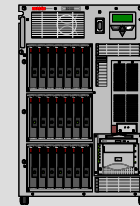
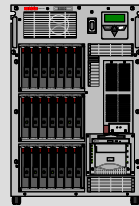
**Alice**

## Was ist CAcert?

### Unverschlüsselte Übertragung



**Bob**



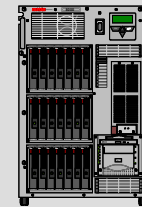
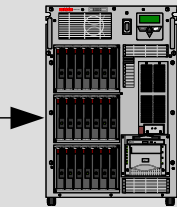
**Alice**

## Was ist CAcert?

### Unverschlüsselte Übertragung



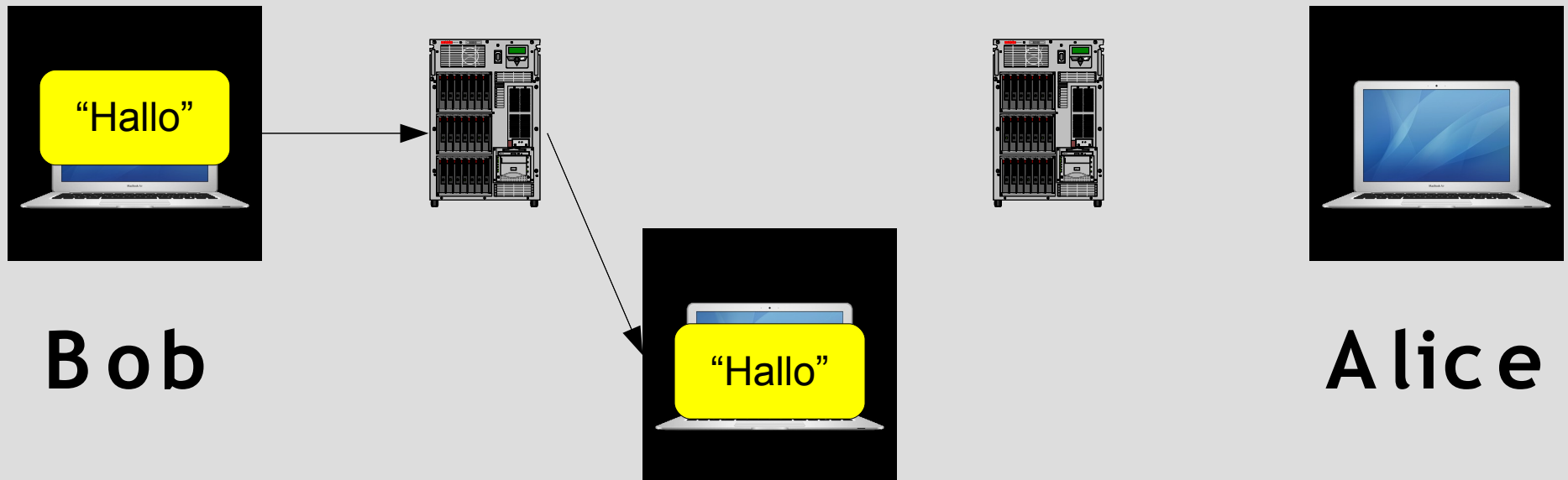
**Bob**



**Alice**

## Was ist CAcert?

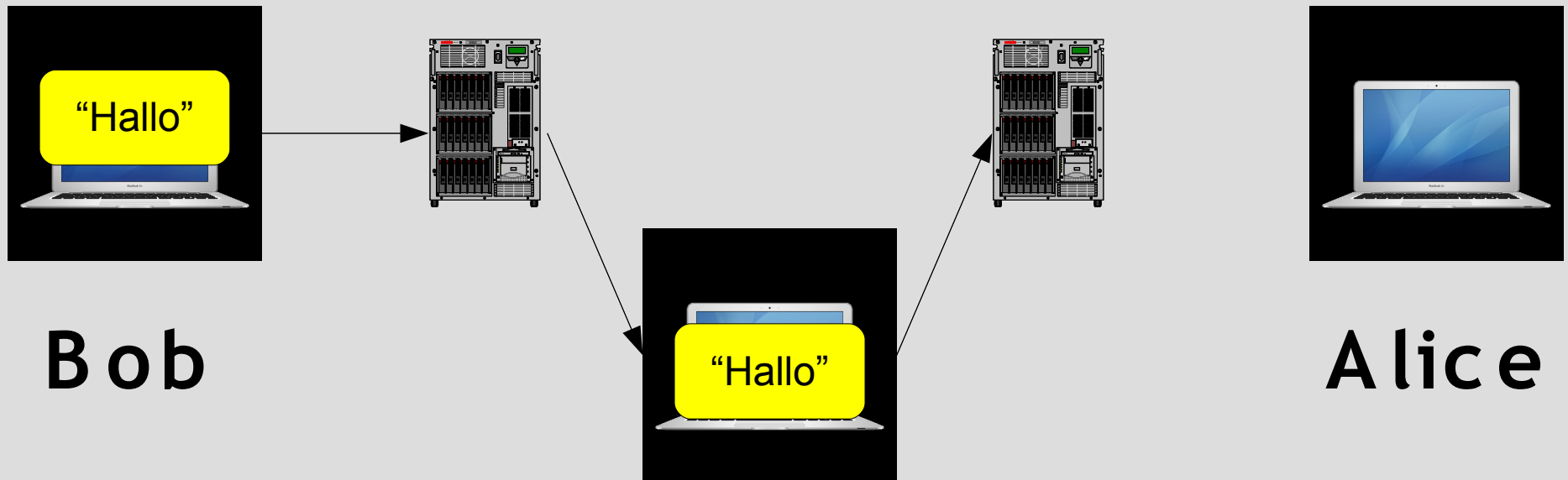
### Unverschlüsselte Übertragung



!!!!

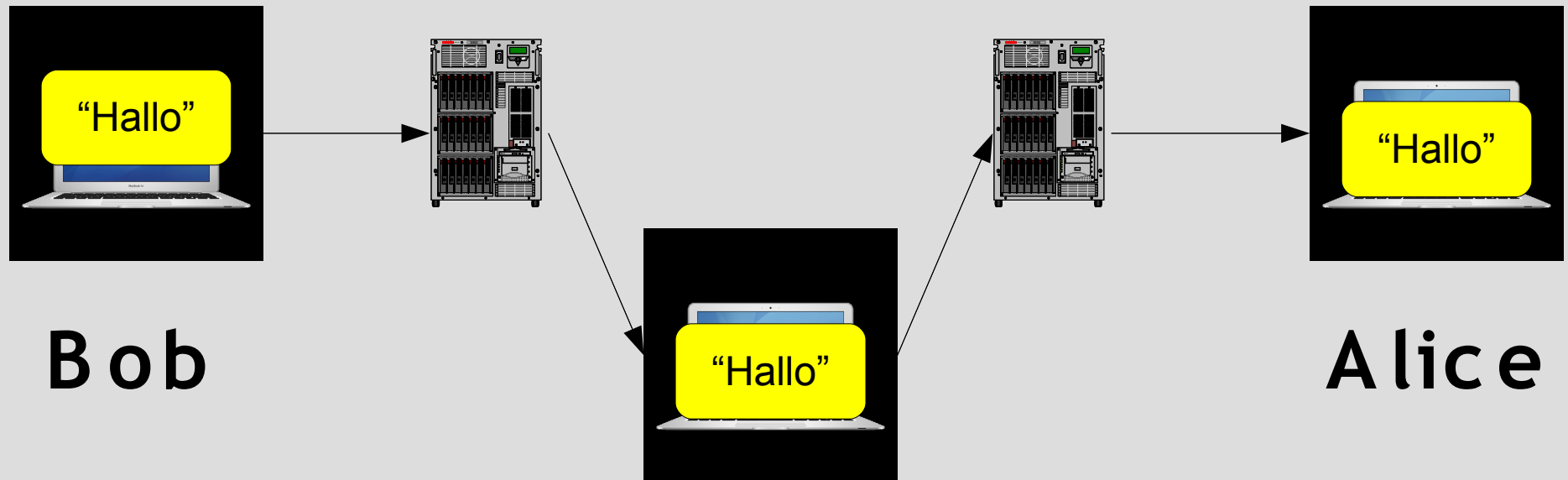
## Was ist CAcert?

### 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 Ge-  
schäfts ....

Mit freundlicher Unterstützung von:



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



# Alice

---

---

---

---

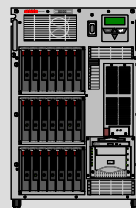
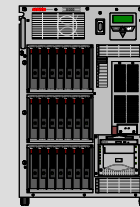
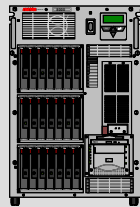
(c) by pebd

## Was ist CAcert?

### Verschlüsselte Übertragung



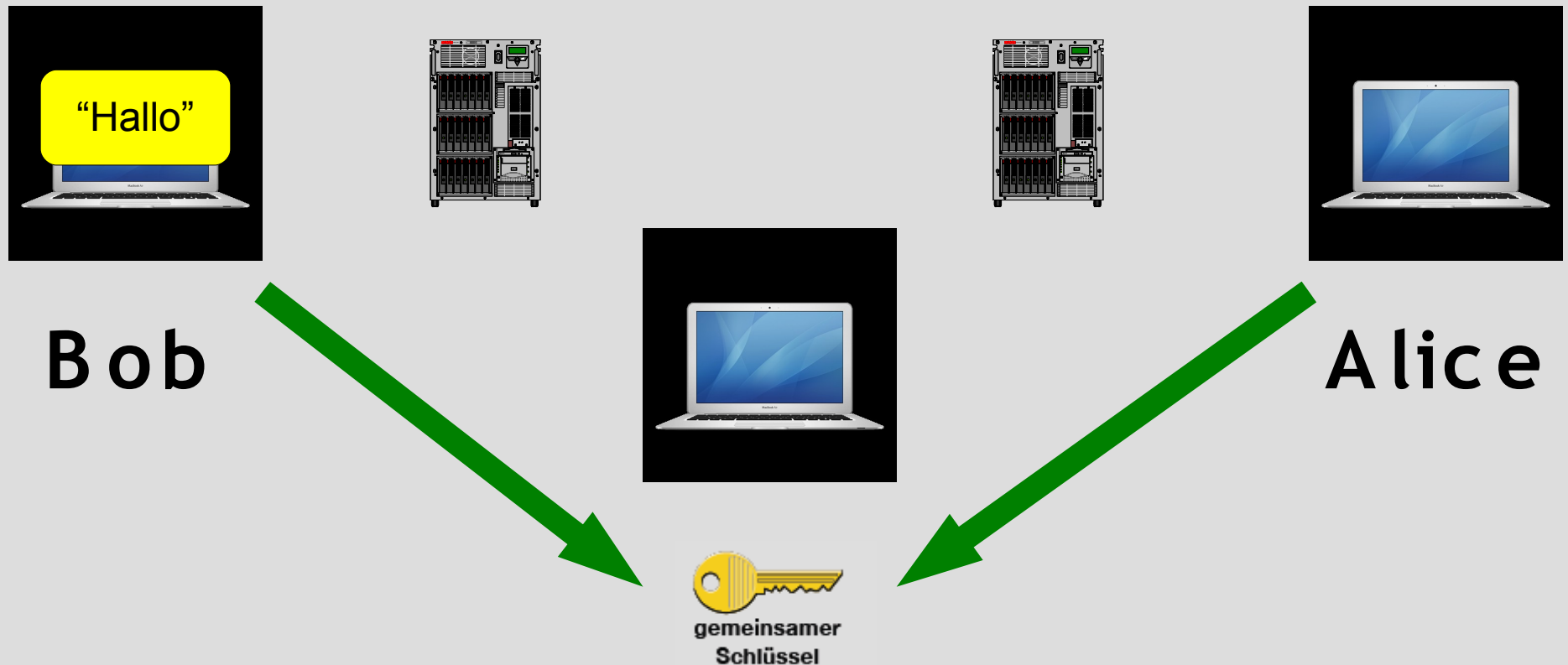
**Bob**



**Alice**

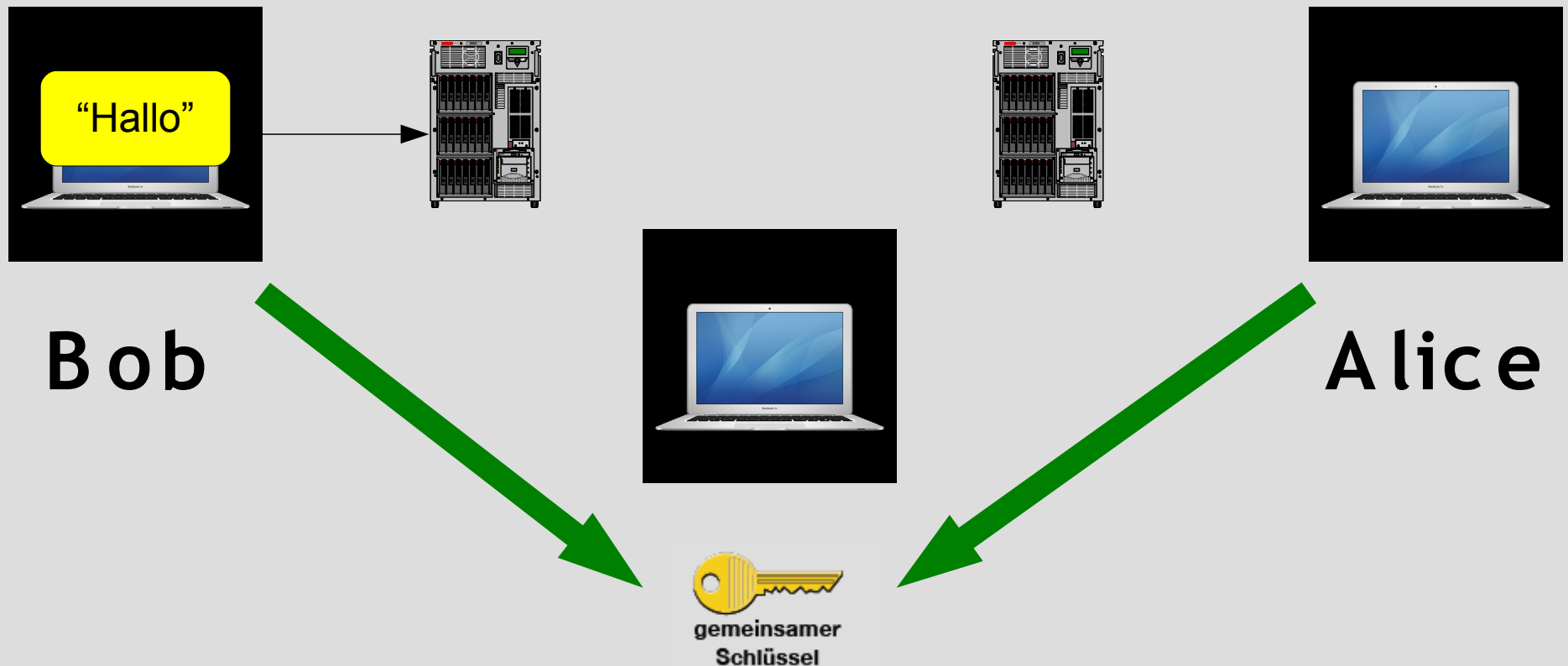
## Was ist CAcert?

### Verschlüsselte Übertragung



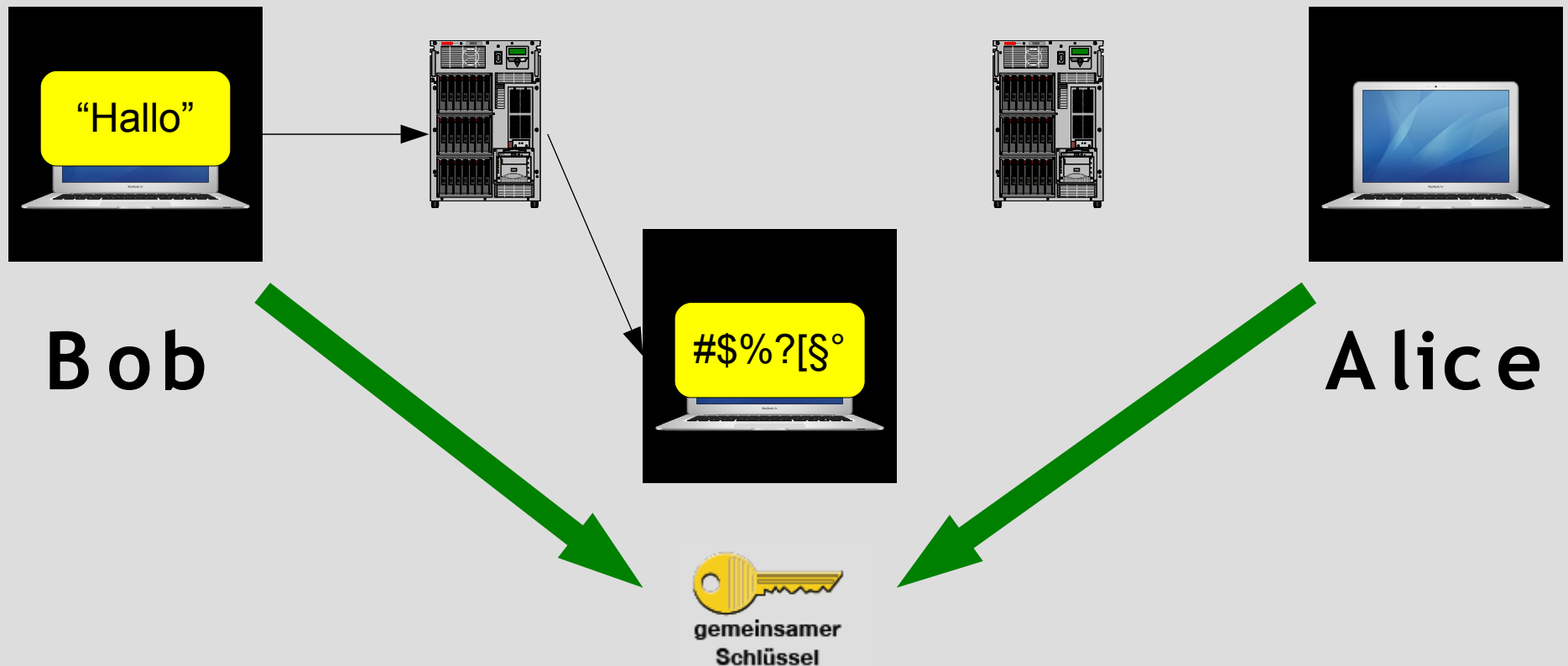
## Was ist CAcert?

### Verschlüsselte Übertragung



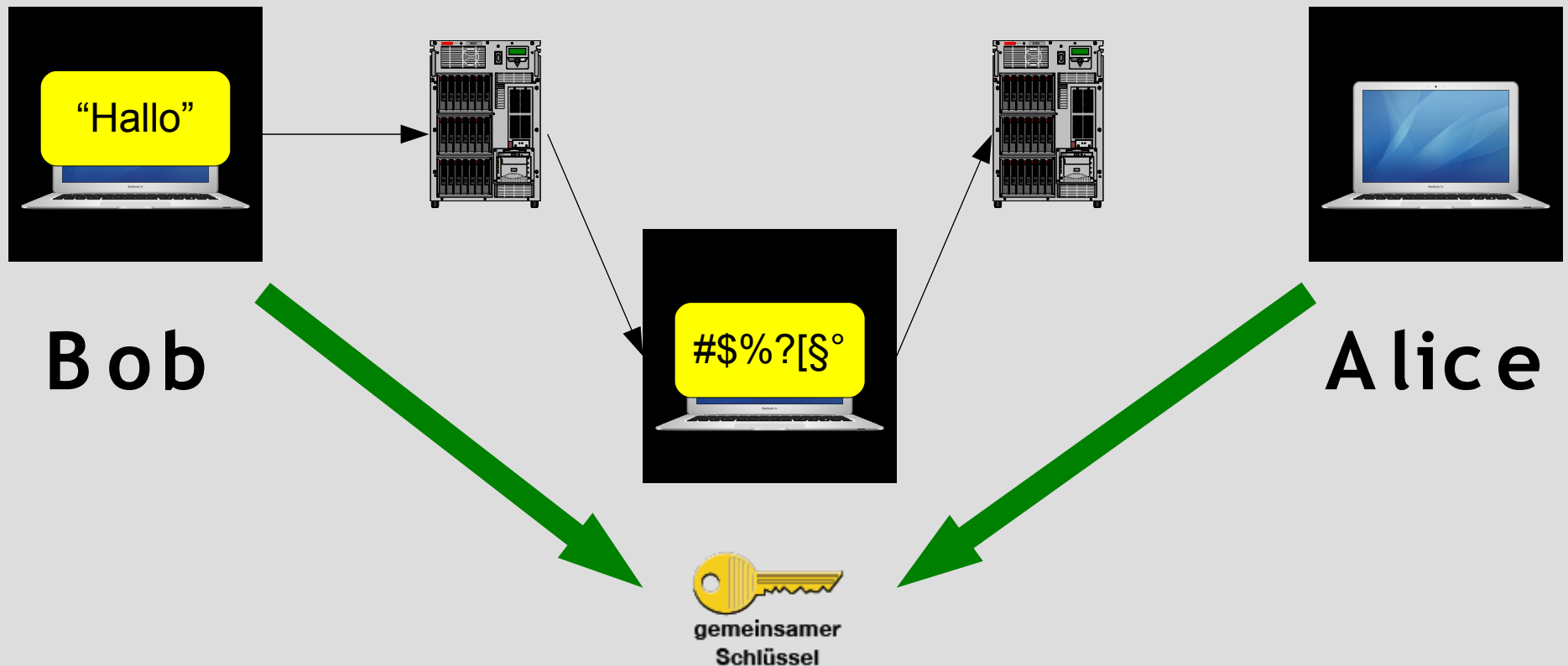
## Was ist CAcert?

### Verschlüsselte Übertragung



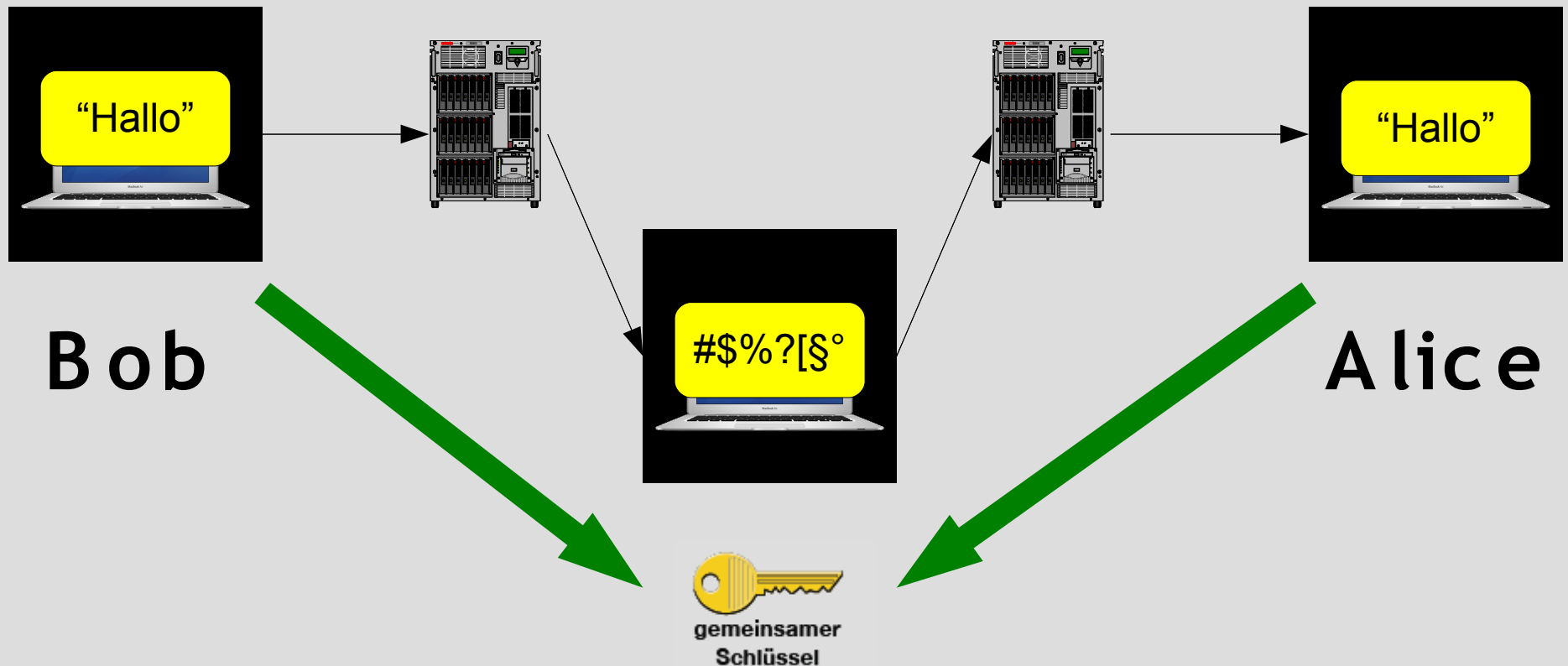
## Was ist CAcert?

### Verschlüsselte Übertragung



## Was ist CAcert?

### Verschlüsselte Übertragung



## Was ist CAcert?

### Verschlüsselte Übertragung



**Bob**

**Problem:**

**Transfer des**

**gemeinsamen Schlüssels**



**Alice**



**gemeinsamer  
Schlüssel**



# Was ist CAcert?

## Asymetrische Verschlüsselung



**Bob**



**Alice**



# Was ist CAcert?

## Asymmetrische Verschlüsselung



**Bob**



**Alice**



## Was ist CAcert?

### Asymmetrische Verschlüsselung



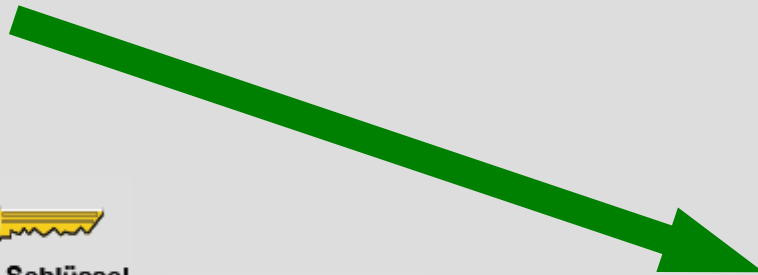
**Bob**



privater Schlüssel  
Bob



öffentl. Schlüssel  
Bob



**Alice**



privater Schlüssel  
Alice



öffentl. Schlüssel  
Alice

## Was ist CAcert?

### Asymmetrische Verschlüsselung



**Bob**



privater Schlüssel  
Bob



öffentl. Schlüssel  
Bob



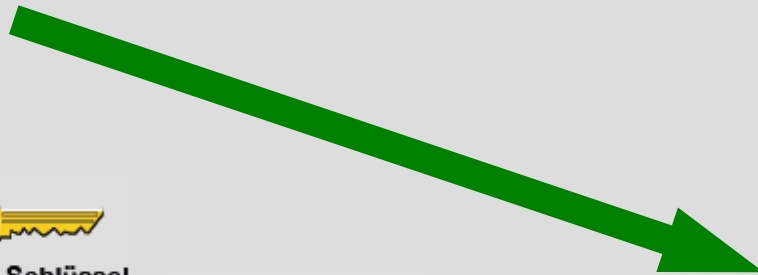
**Alice**



privater Schlüssel  
Alice

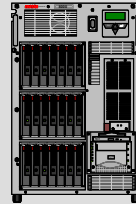


öffentl. Schlüssel  
Alice



## Was ist CAcert?

### Asymmetrische Verschlüsselung



**Bob**



privater Schlüssel  
Bob



öffentl. Schlüssel  
Bob

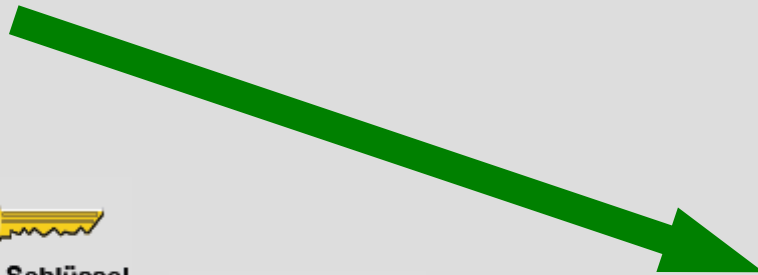
**Alice**



privater Schlüssel  
Alice

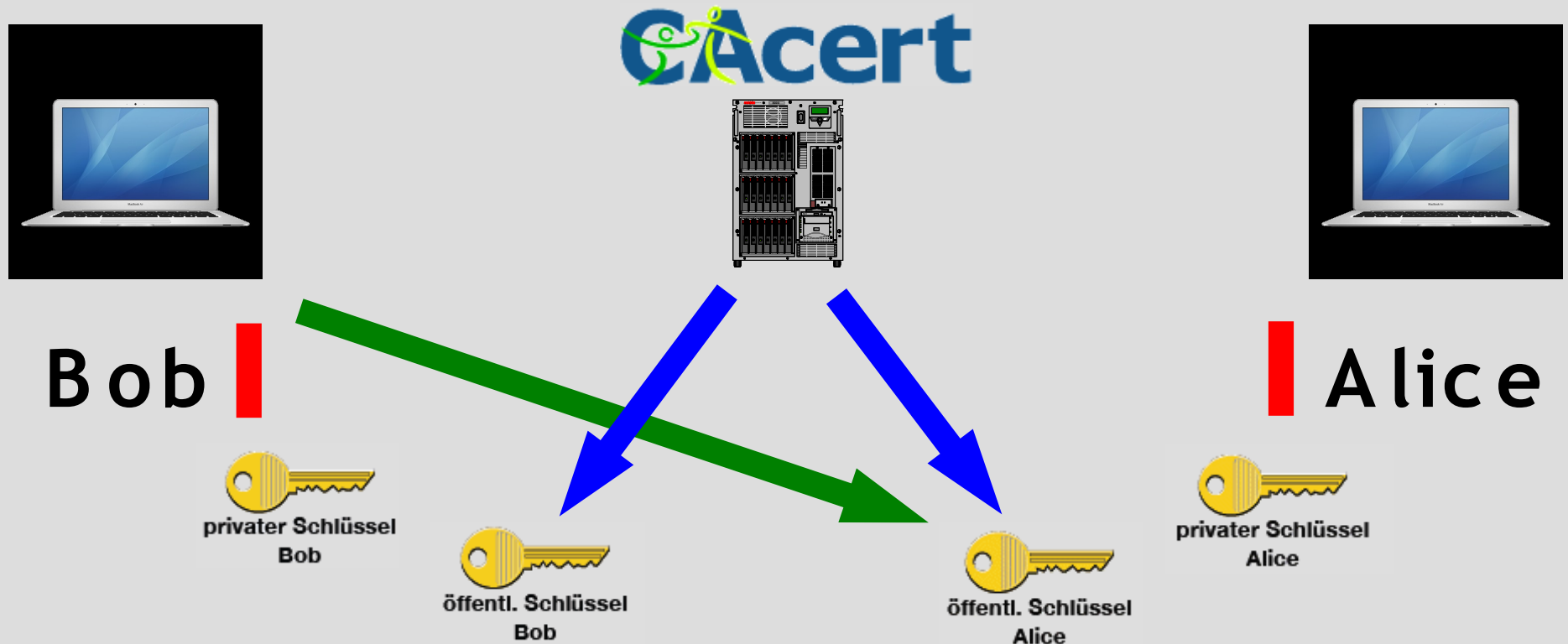


öffentl. Schlüssel  
Alice



## Was ist CAcert?

### Asymmetrische Verschlüsselung



## Was ist CAcert?

### Asymmetrische Verschlüsselung



**Bob**



**Alice**

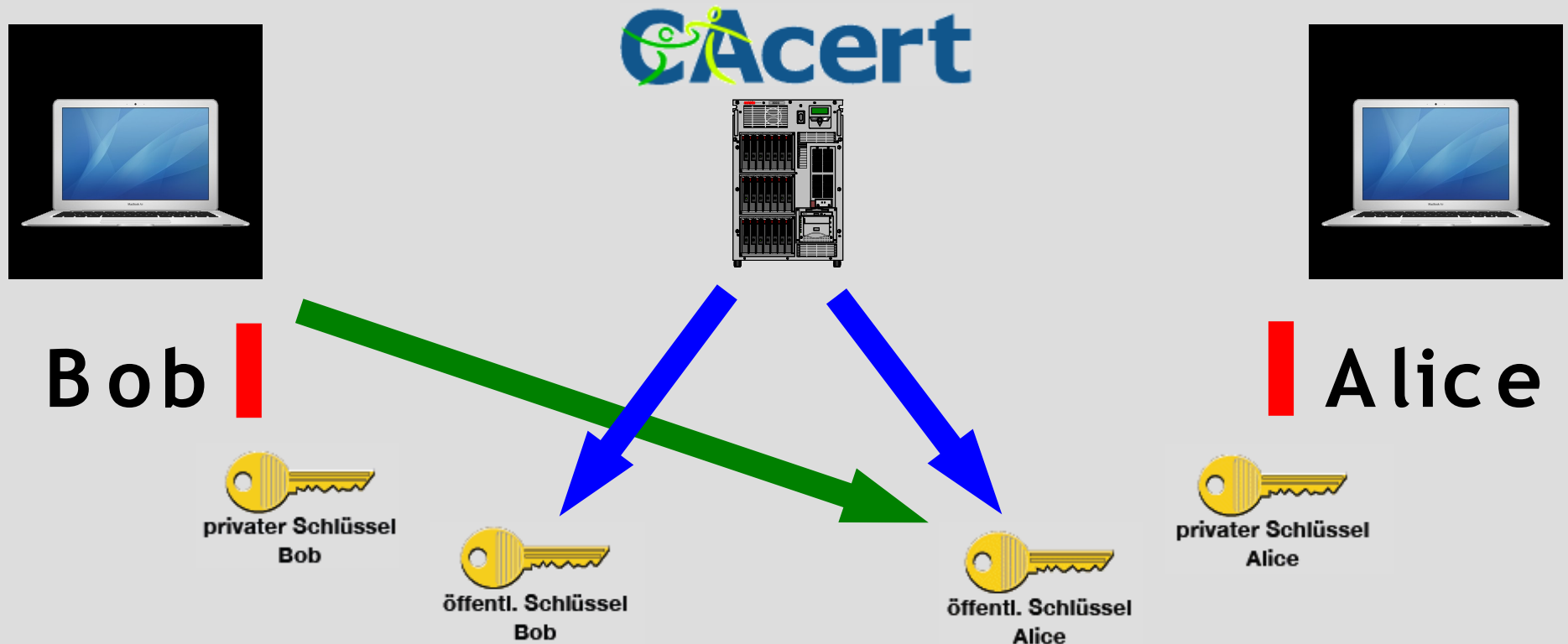


Schlüssel Transfer unproblematisch:

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

## Was ist CAcert?

### Zertifizieren von Schlüsseln





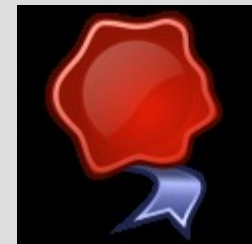
## Was ist CAcert?

- 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?

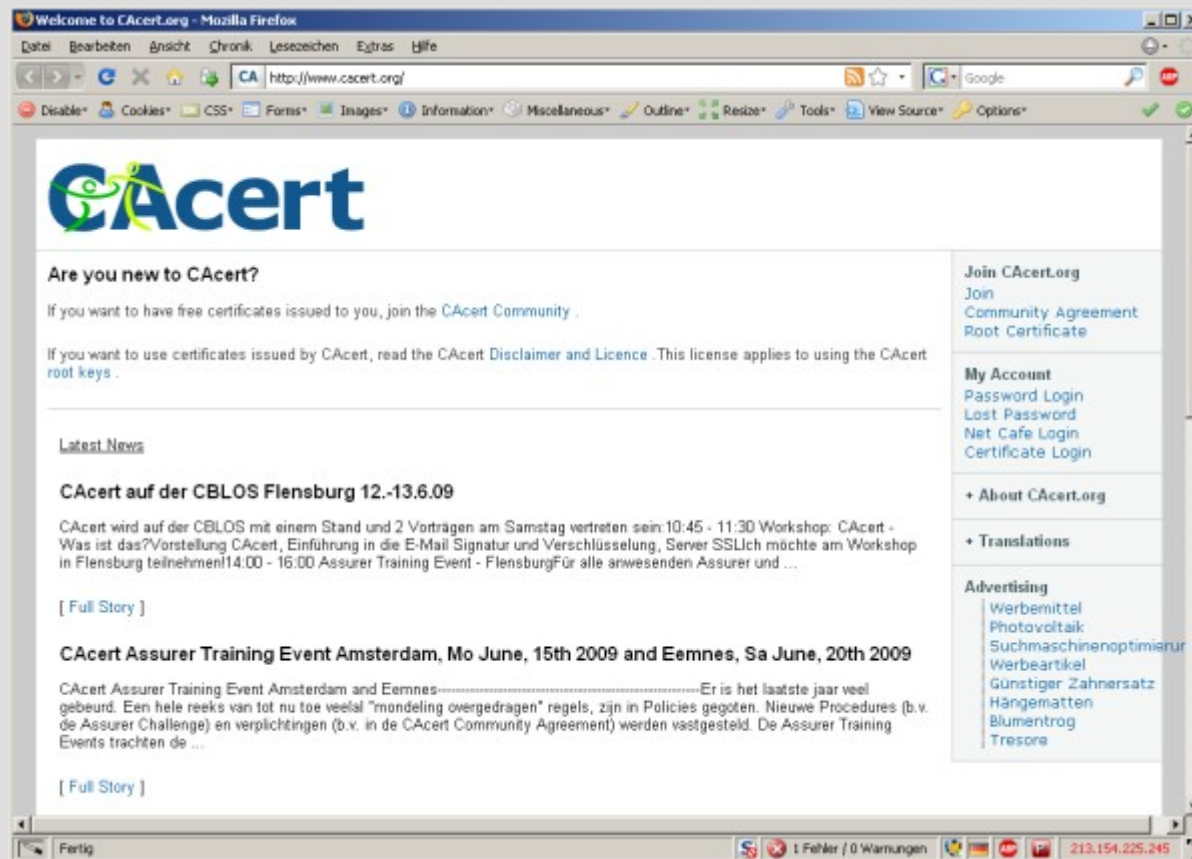
- Security und Privatsphäre darf nichts kosten
- CAcert bietet kostenlos ...
  - ✓ Zertifikate für E-Mail Signatur
  - ✓ Zertifikate für E-Mail Verschlüsselung
  - ✓ SSL Server Zertifikate
  - ✓ Code Signing
  - ✓ Dokument Signing



# Was ist CAcert?

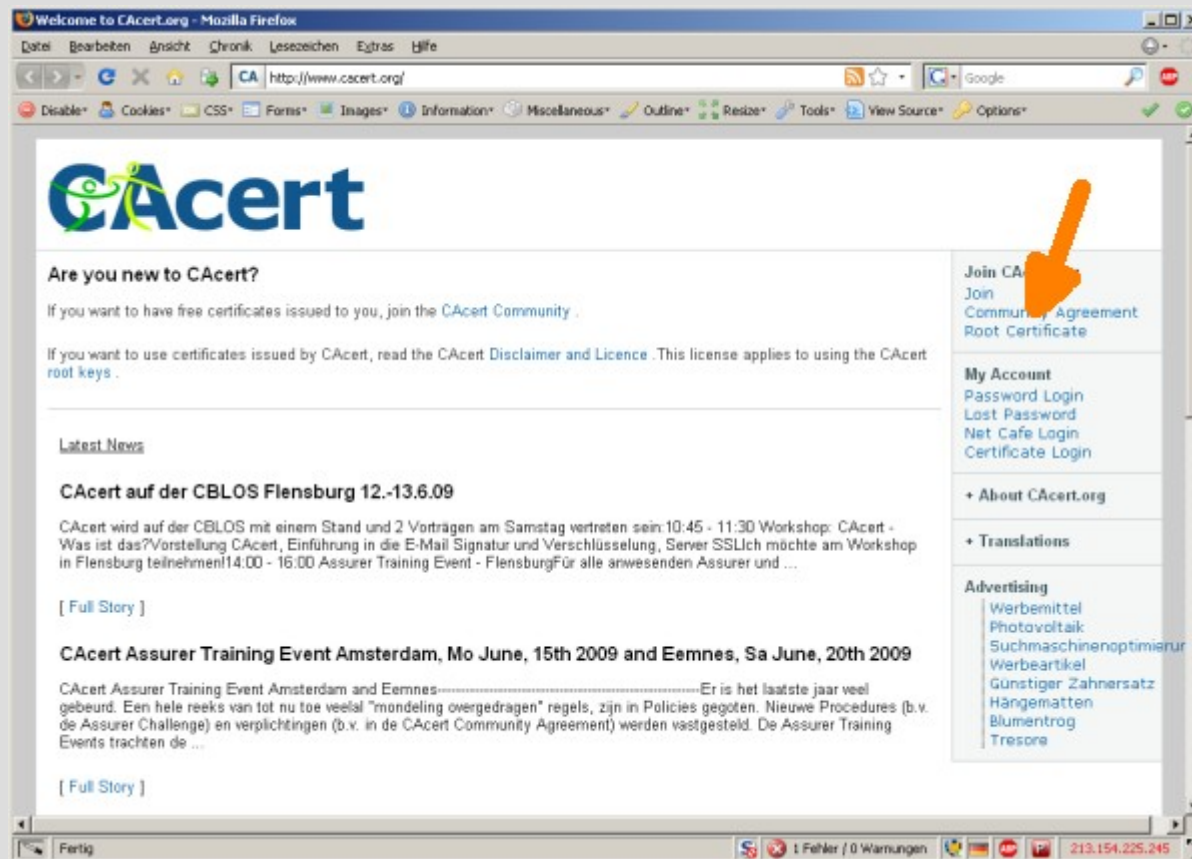
- Root Zertifikate  
Firefox

## Was ist CAcert?



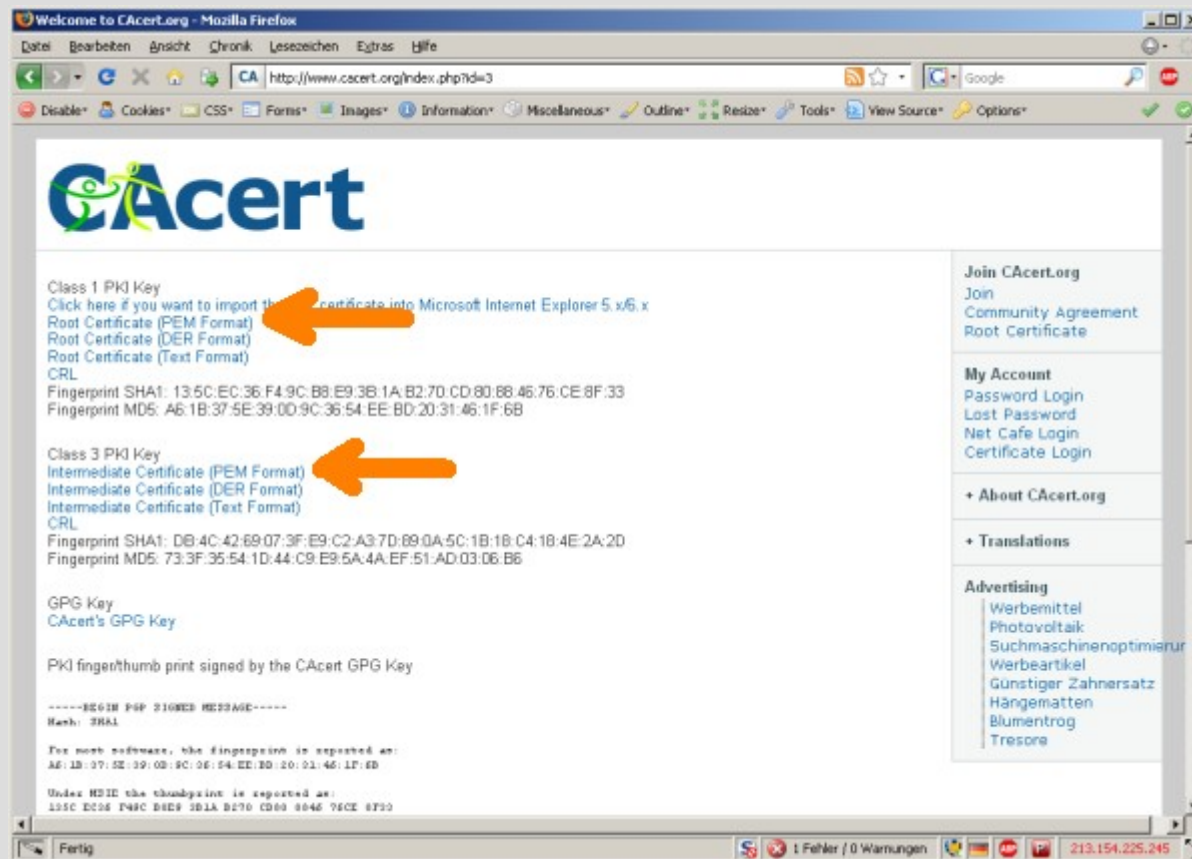
<http://www.CAcert.org>

## Was ist CAcert?



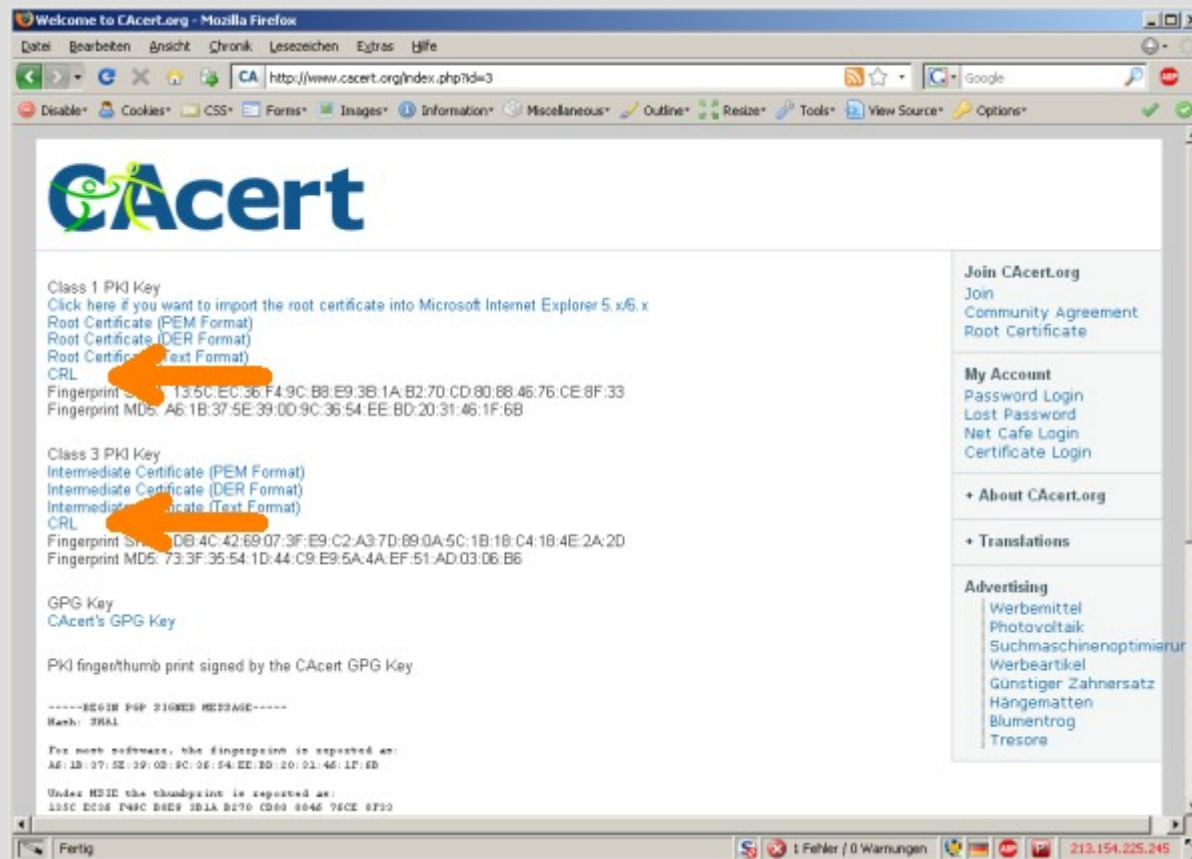
<http://www.CAcert.org>

## Was ist CAcert?



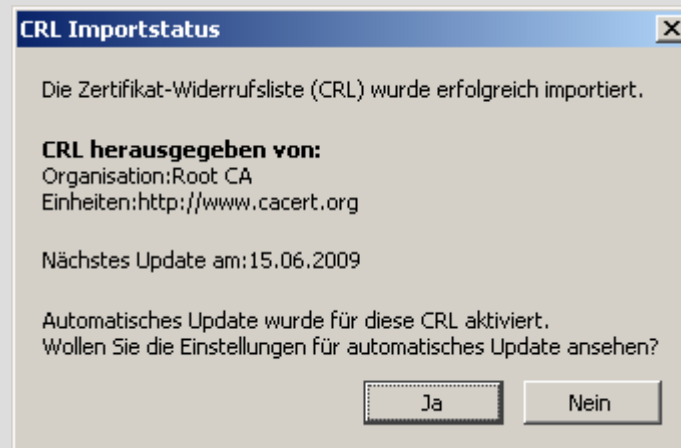
CAcert: Class1 + Class3 Root Zertifikate

## Was ist CAcert?



CAcert: Class1 + Class3 Root CRL's

# Was ist CAcert?



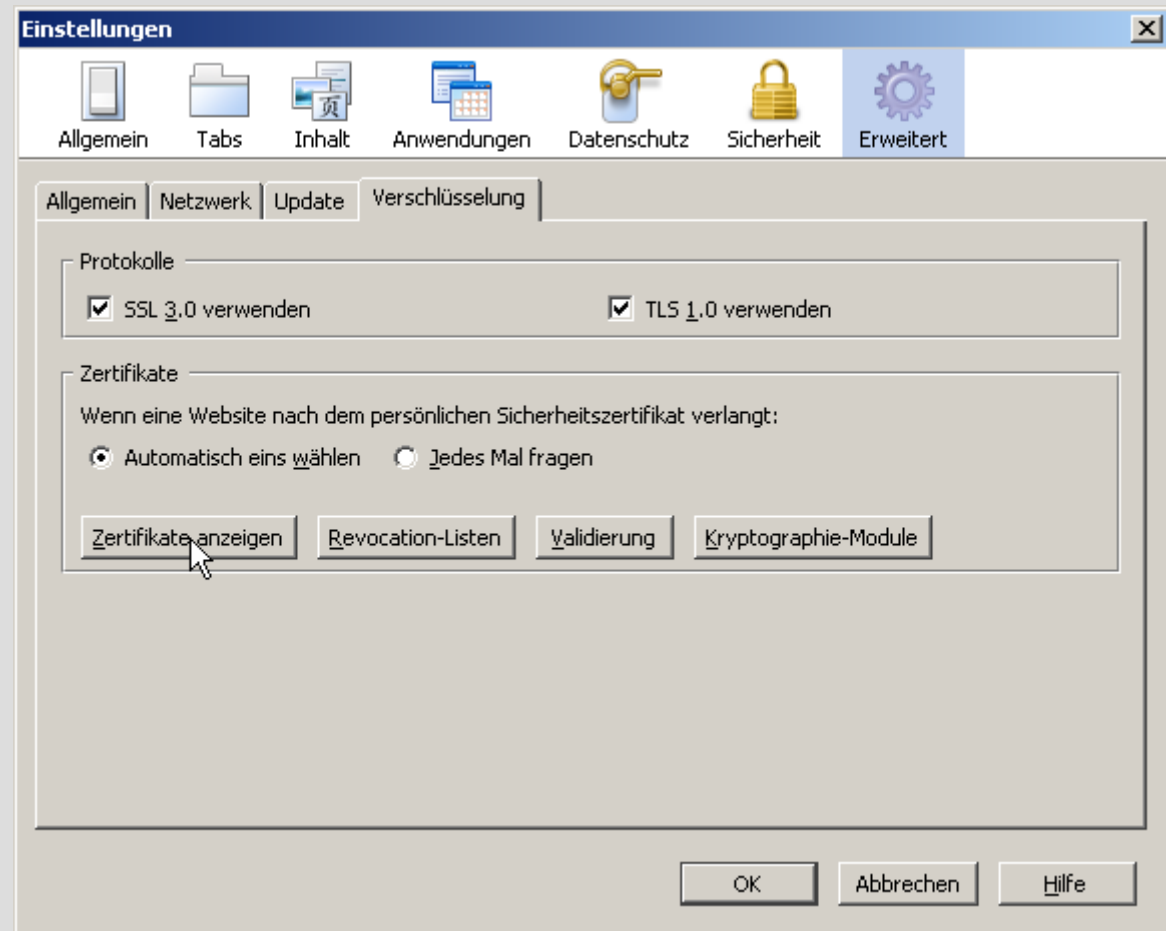
CAcert: Class1 + Class3 Root CRL's



## Was ist CAcert?

Menü:

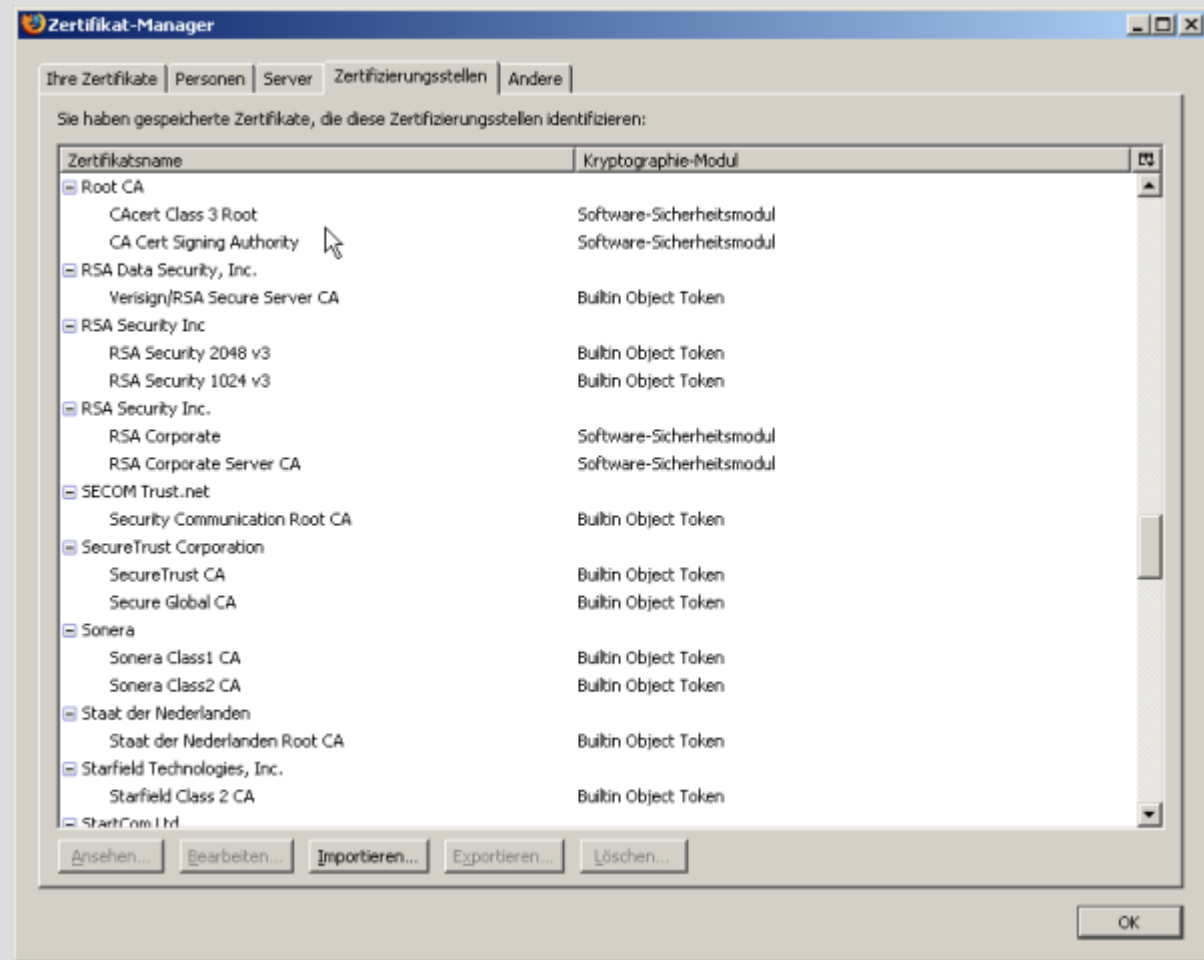
- Extras
- Einstellungen
- Erweitert
- Tab Verschlüsselung
- Zertifikate anzeigen



CAcert: Class1 + Class3 Root Zertifikate

## Was ist CAcert?

Tab Zertifizierungsstellen



CAcert: Class1 + Class3 Root Zertifikate

## Was ist CAcert?

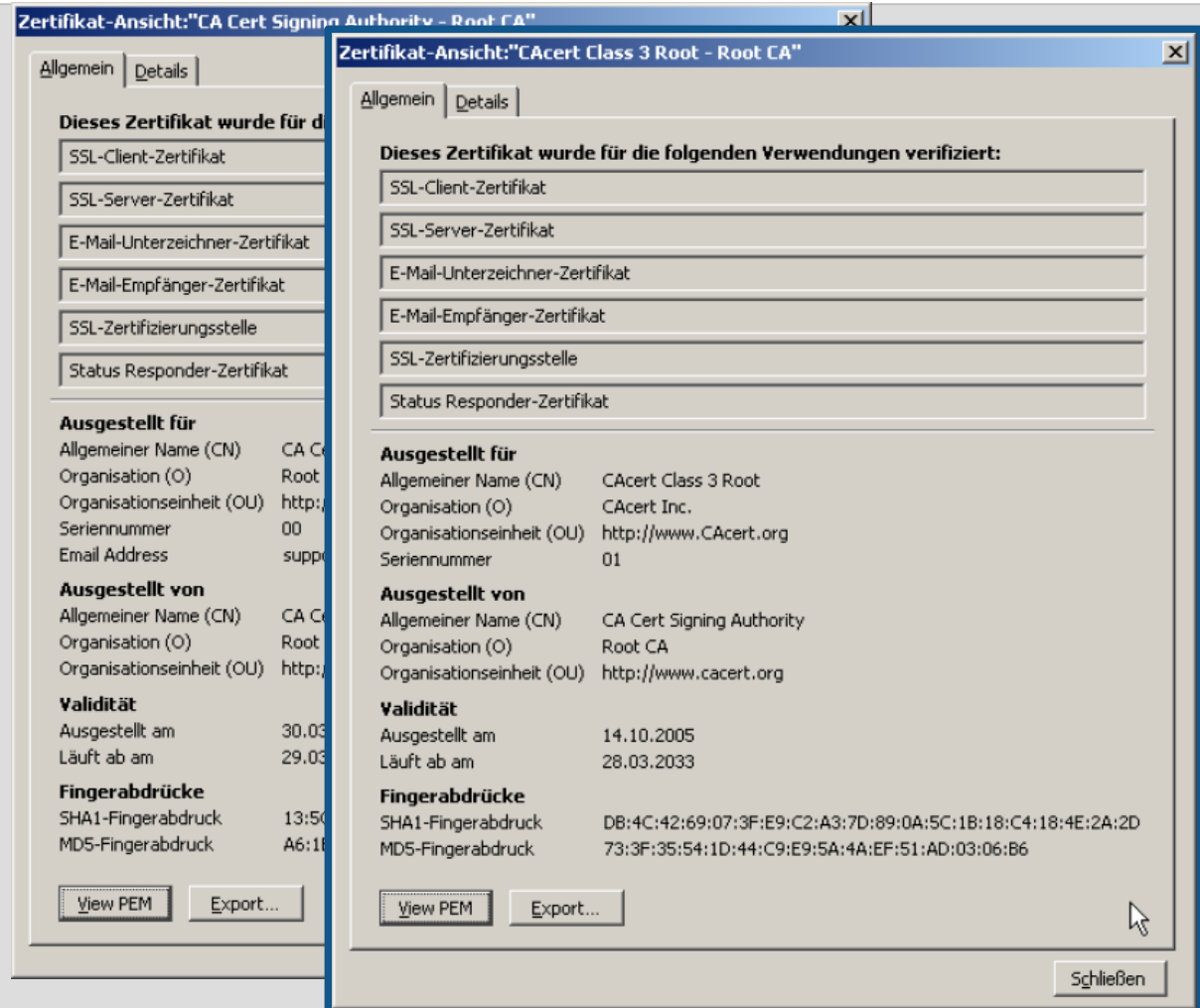
CAcert Signing Authority  
Root CA



CAcert: Class1 + Class3 Root Zertifikate

## Was ist CAcert?

CAcert Class 3 Root  
Root CA

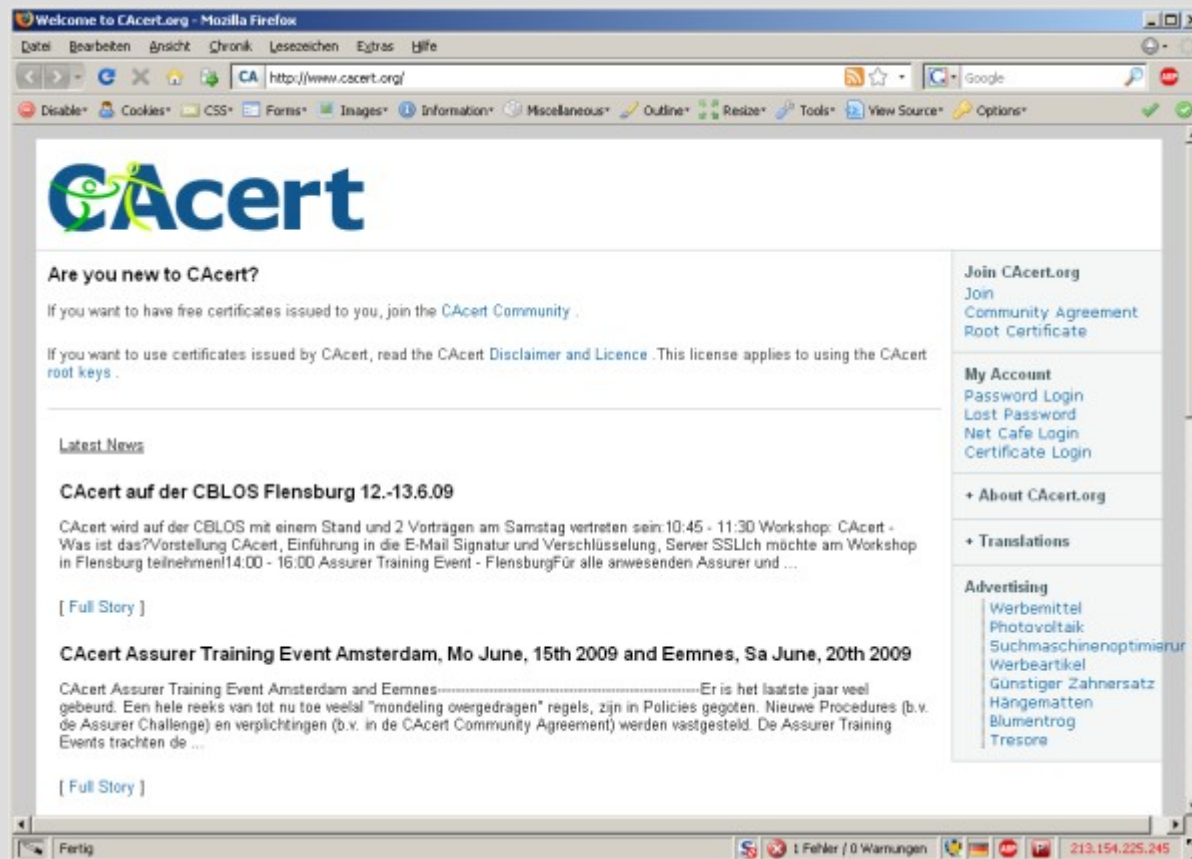


CAcert: Class1 + Class3 Root Zertifikate

# Was ist CAcert?

- Wie kann ich mitmachen?

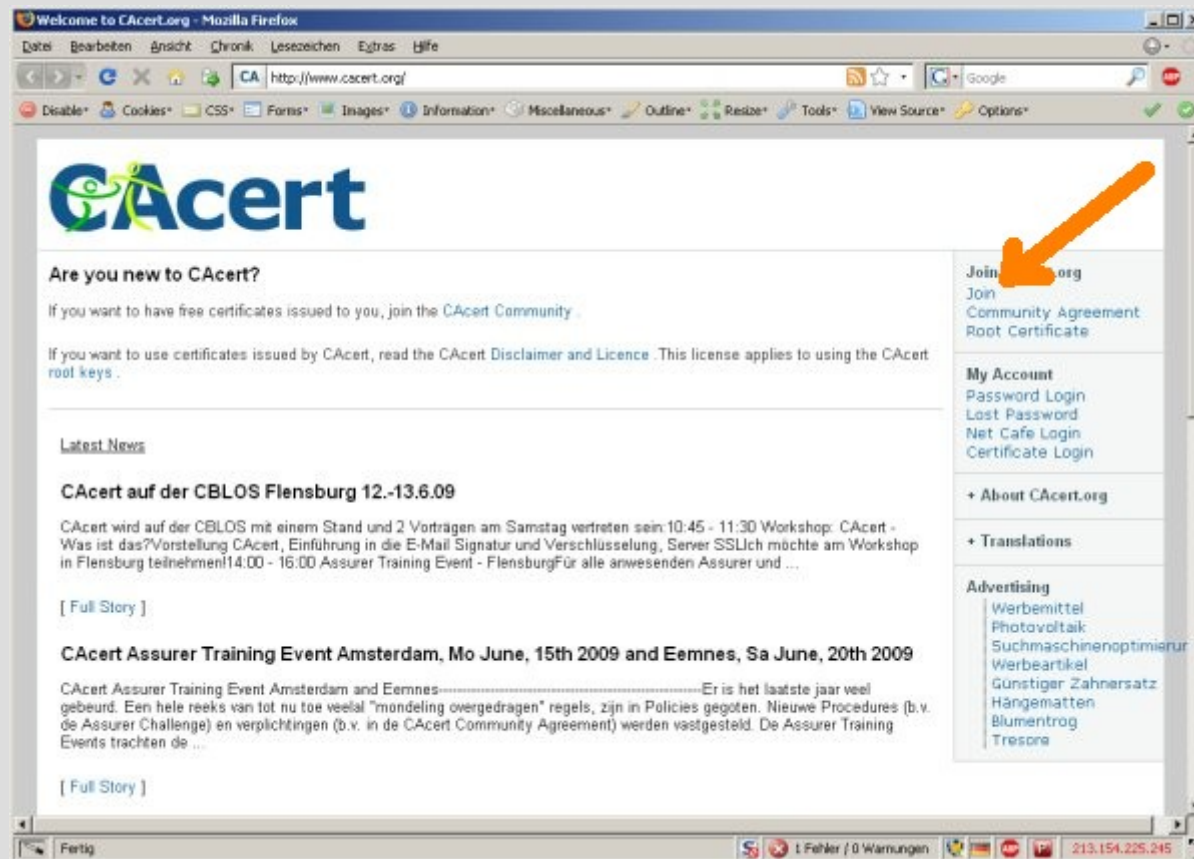
## Was ist CAcert?



<http://www.CAcert.org>

## Was ist CAcert?

Join !



<http://www.CAcert.org>

# Was ist CAcert?

My Details	
First Name:	<input type="text"/>
Middle Name(s) (optional)	<input type="text"/>
Last Name:	<input type="text"/>
Suffix (optional)	<input type="text"/>
Date of Birth (dd/mm/yyyy)	<input type="text" value="1"/> <input type="text" value="January (1)"/> <input type="text" value="19XX"/>
Email Address:	<input type="text"/> <small>I own or am authorised to control this email address</small>
Pass Phrase*:	<input type="text"/>
Pass Phrase Again*:	<input type="text"/>
<small>*Please note, in the interests of good security, the pass phrase must be made up of an upper case letter, lower case letter, number and symbol.</small>	
<small>Lost Pass Phrase Questions - Please enter five questions and your responses</small>	

of an upper case letter, lower case letter, number and symbol.

Lost Pass Phrase Questions - Please enter five questions and your responses to be used for security verification.

1)	<input type="text"/>	<input type="text"/>
2)	<input type="text"/>	<input type="text"/>
3)	<input type="text"/>	<input type="text"/>
4)	<input type="text"/>	<input type="text"/>
5)	<input type="text"/>	<input type="text"/>

It's possible to get notifications of up and coming events and even just general announcements, untick any notifications you don't wish to receive. For country, regional and radius notifications to work you must choose your location once you've verified your account and logged in.

Alert me if:

- General Announcements
- Country Announcements
- Regional Announcements
- Within 200km Announcements

When you click on next, we will send a confirmation email to the email address you have entered above.

I agree to the terms and conditions of the CAcert Community Agreement:  
<http://www.cacert.org/policy/CAcertCommunityAgreement.php>

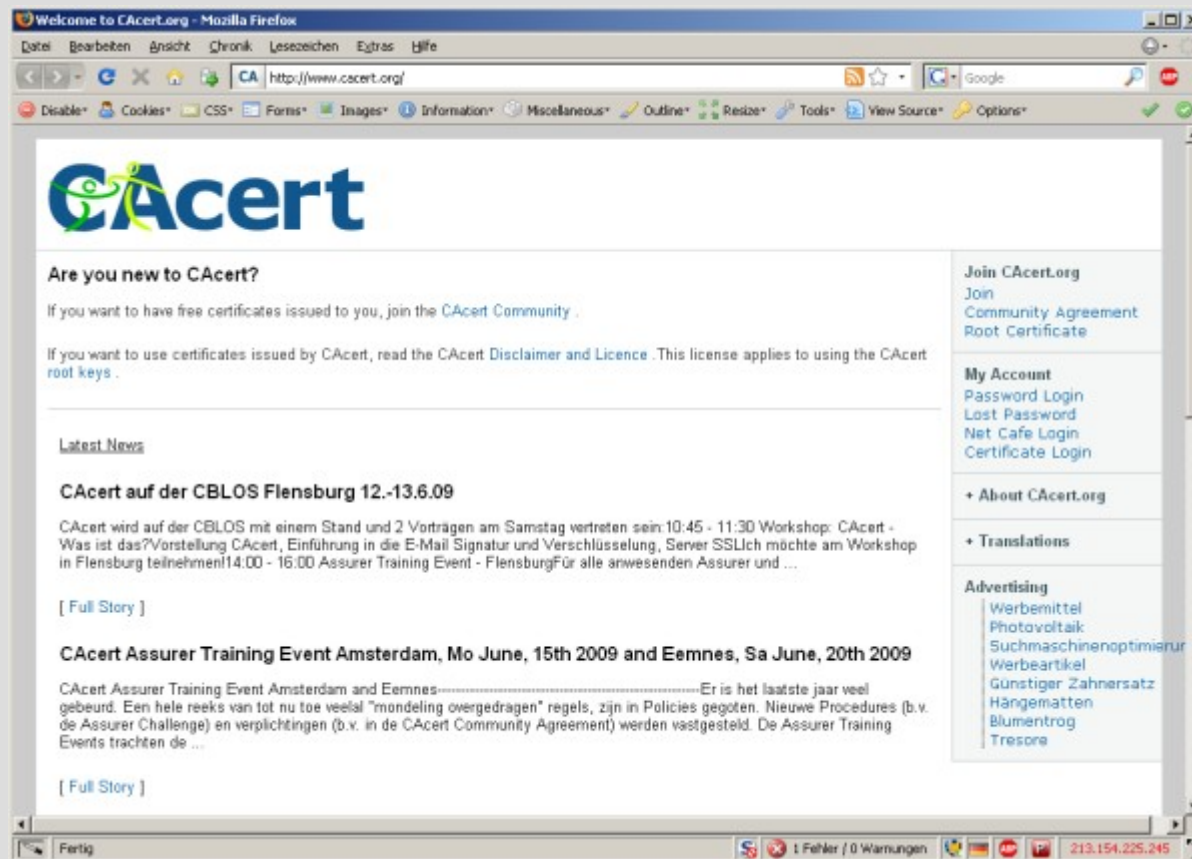
## Registrierungs Formular



# Was ist CAcert?

- Identifikationsprozess

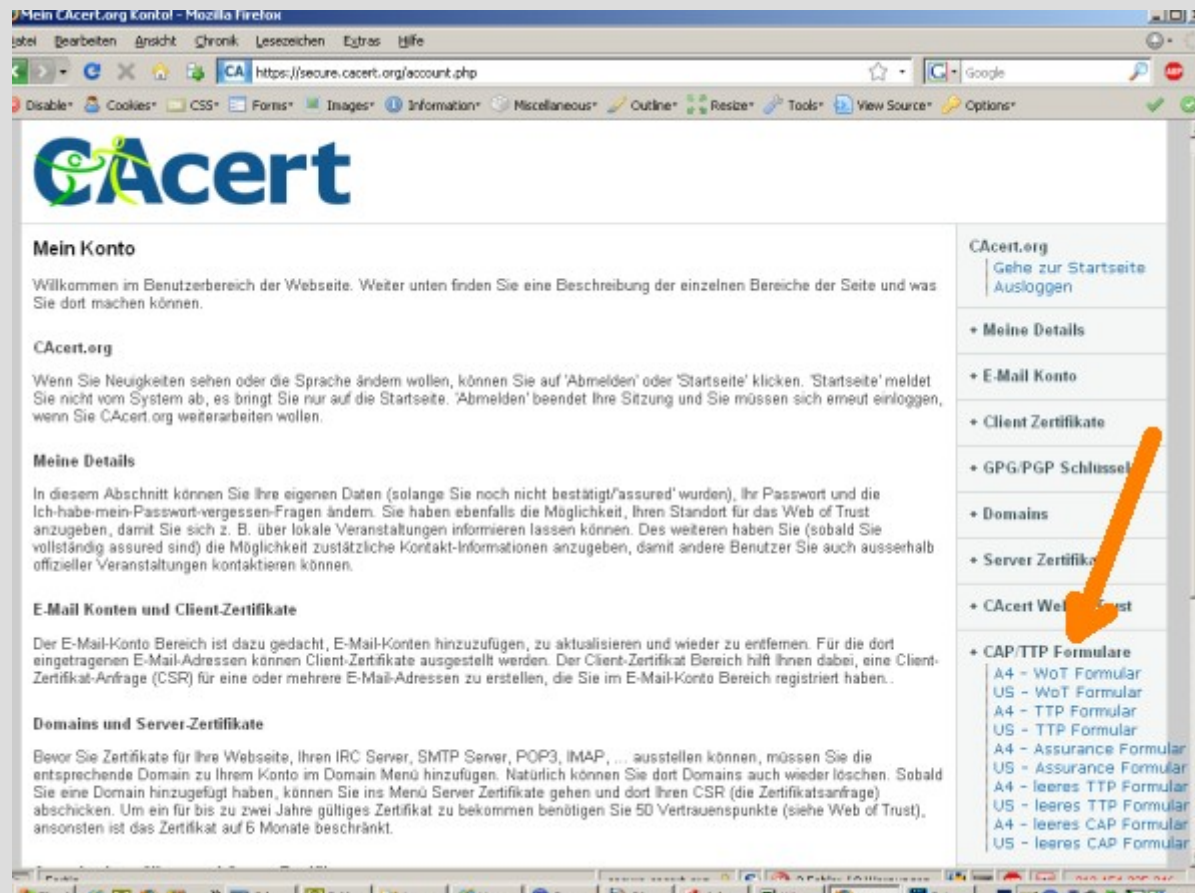
## Was ist CAcert?



<http://www.CAcert.org>

## Was ist CAcert?

### CAP Formulare



<http://www.CAcert.org>

# Was ist CAcert?

## CAP Formular

### Antragsteller

<b>Namen:</b>	
<b>Geburtsdatum:</b> (JJJJ-MM-TT)	
<b>E-Mail Adresse:</b>	

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	-
<b>Assurer Challenge</b>	<b>bestanden</b>	
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?

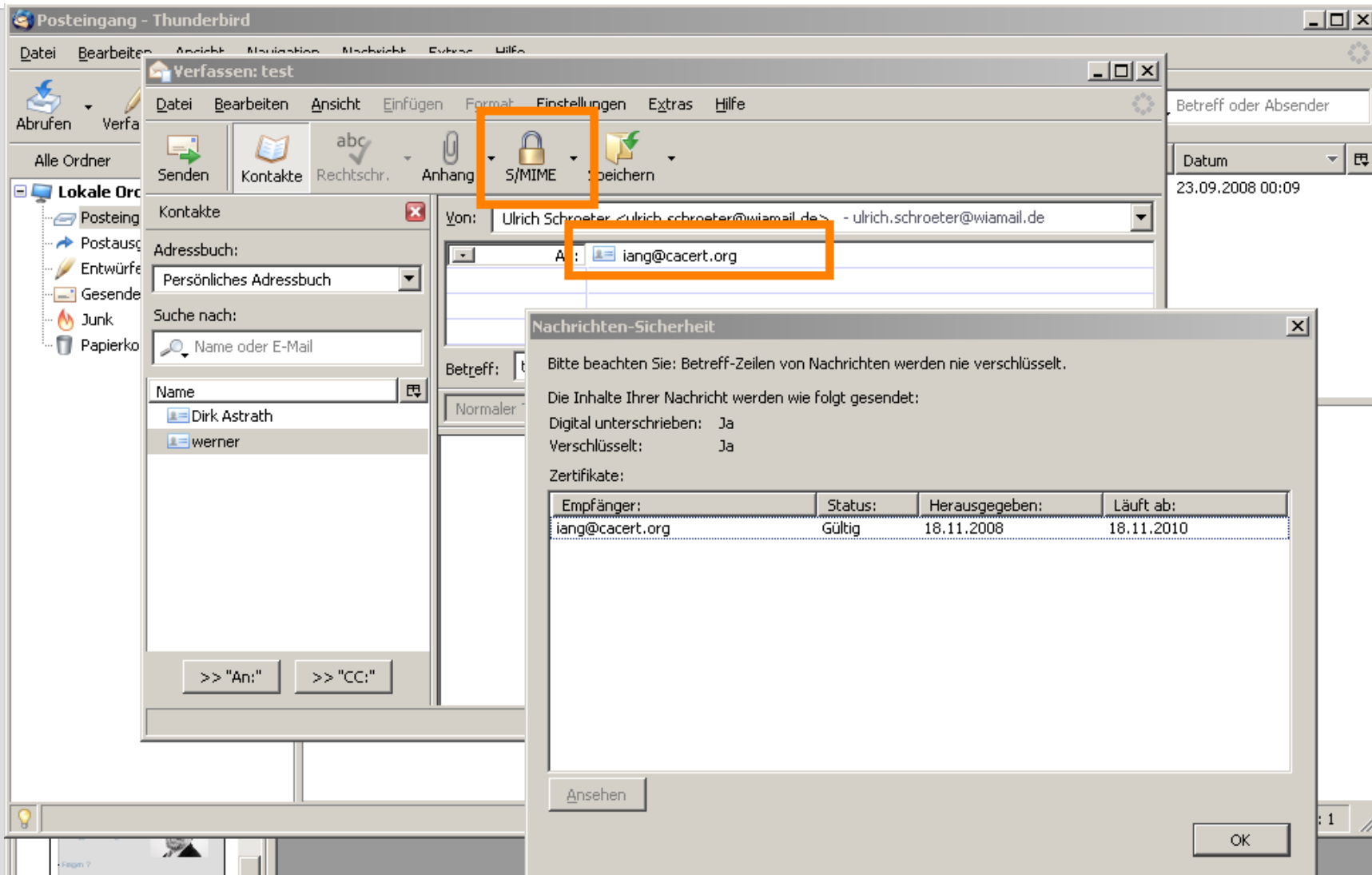
- Client Zertifikat (öffentlicher Schlüssel)  
von Kommunikationspartnern
- Importieren in Thunderbird

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](mailto:ulrich@CAcert.org)
- Fragen ?

