

SSL Installation auf Lotus Domino 8.5

Willkommen zum Domino 8.5 Hands On!

Im Folgenden gibt es einen step-by step guide zur Einrichtung von HTTPS am Domino Server mit einem selbsterstellten Zertifikat.

Danach werden die Schritte gezeigt, die nötig sind, um ein Client-Zertifikat in die Notes-ID zu bringen, die es ermöglicht, verschlüsselte / signierte smtp-mails auszutauschen.

Bernhard Kolb

www.ebe-edv.com

Bernhard.Kolb@ebe-edv.com

Lab 1: SSL via Server Certificate Admin

- 1) Certserv.nsf öffnen
- 2) Create self signed certificate
- 3) Passwort vergeben *lotusnotes*

This form lets you easily create a key ring with a self-certified certificate. The resulting key ring is ready for use with SSL, but is not appropriate for production use due to the certificate being signed by yourself instead of a trusted authority.

Key Ring Information

Key Ring File Name: selfcert.kyr

Key Ring Password: *****

Password Verify: *****

Distinguished Name

Common Name: Admincamp 2010

Organization: BKH

Organizational Unit: (optional)

City or Locality: (optional)

State or Province: NRW (no abbreviations)

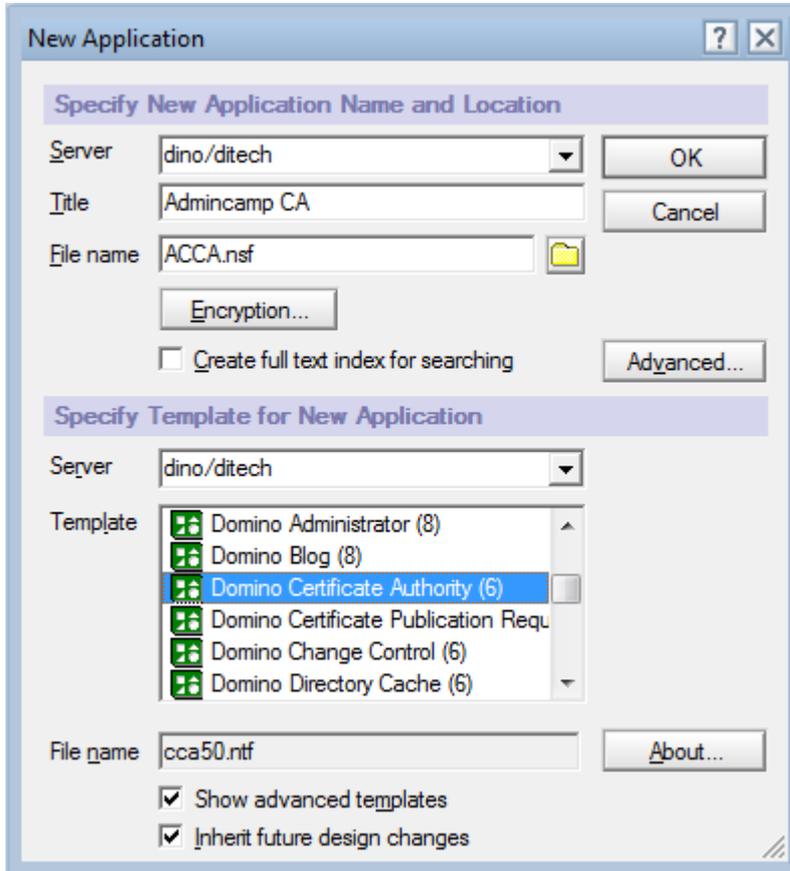
Country: DE (two character country code)

Two-character representation for the country (e.g. US)

- 4) Selfcert.kyr und .sth ins Domino Data verzeichnis kopieren
- 5) Im serverdokument unter internet-Protocols SSL Keyfile angeben selfcert.kyr
- 6) https – YES
- 7) Serverdoc speichern
- 8) Tell http restart
- 9) Zugriff auf die Webseite via https

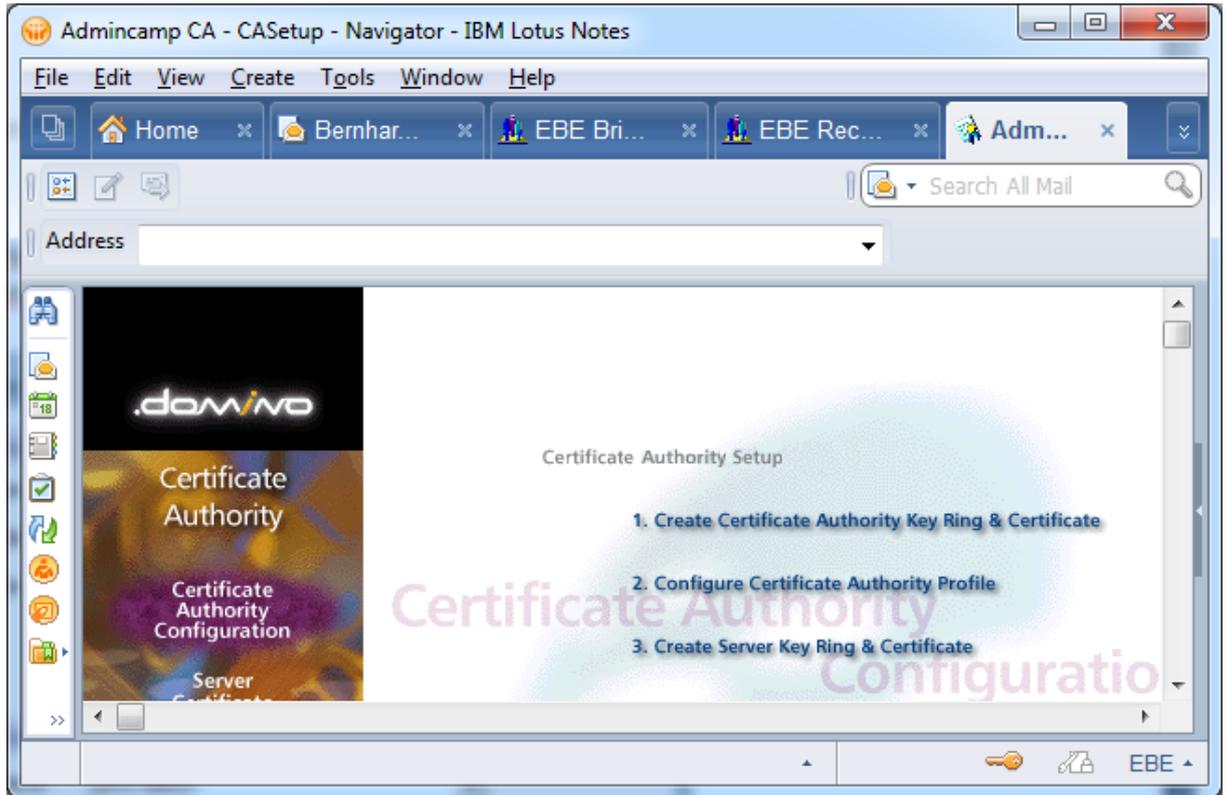
Lab 2: Zertifizierungsstelle einrichten

- 1) **Certificate Authority einrichten**
am server neue DB von der CCA50 Schablone erstellen



- 2) **DB schließen** und neu öffnen
..sonst sind nicht alle Rollen dem aktuellen User zugeordnet...

3) Create Server Certificate & Keyring



Create Certificate Authority Key Ring

This form lets you create the Certificate Authority key ring.

Key Ring Information

Key Ring File Name: CAKey.kyr

Key Ring Password: *****

Password Verify: *****

Key Size

1024

Distinguished Name

Common Name: Admincamp 2010

Organization: BKH

Organizational Unit: (optional)

City or Locality: (optional)

State or Province: NRW (no abbreviations)

Country: DE (two character country code)

Two-character representation for the country (e.g. US) (two characters)

Das Certificate Authority-Keyring-File entspricht der cert.id in der Domino-Welt und wird für die spätere Ausstellung von Zertifikaten benötigt.

Achtung: diese Datei wird lokal auf der Notes-Client Maschine erzeugt!

4) Configure Certificate Authority

Use this form to configure settings needed by the Certificate Authority application.

CA Settings	Quick Help
CA Key File C:\Program Files (x86)\IBM\Lotus\Notes\Data\ACCAKey.kyr	- The name of the CA key ring file is stored here automatically when you create it. If you move the CA key ring file, you must update the path here so the application can find it.
Certificate Server DNS Name www.admincamp.local	- The DNS for the server is needed for the automatic generation of the e-mail that is sent to users for certificate pickup.
Use SSL for certificate transactions? <input checked="" type="checkbox"/> Yes	If this is selected, the automatically generated e-mail will contain a reference to the SSL port for secure certificate pick-up
Certificate Server Port Number 80	- The port number is also needed for the automatic generation of the e-mail that is sent to users for certificate pickup. This is the TCP/IP port on which the Certificate Server will be running.
Mail confirmation of signed certificate to requestor? <input type="checkbox"/> Yes	Selecting this default option is for an e-mail confirmation of a signed certificate request
Submit signed certificates to AdminP for addition to the Directory? <input type="checkbox"/> Yes	Selecting this default option is for the signed certificate request to be submitted to the Administration Process for storage of the certificate in

Achtung: üblicherweise wird Mailconfirmation auf YES gesetzt! Nur hier im Lab wird auf Mail Benachrichtigung verzichtet.

5) Create Server KeyRing

Create CA Server Key Ring

Use this form to create the server key ring for the CA server. When you submit the form, Domino will carry out all the internal steps of creating the server key ring, creating the server certificate request, signing it with the CA certificate, then installing the CA certificate and the signed server certificate into the server key ring.

Note: Once the server key ring has been created, you should use the Server Certificate Admin application to view and manage the server key ring contents.

Server Key Ring Information	
Key Ring File Name:	<input type="text" value="keyfile.kyr"/>
Key Ring Password:	<input type="password" value="*****"/>
Password Verify:	<input type="password" value="*****"/>
Specify the name and password for the server key ring file you are creating.	
Key Size	
Key Size:	<input type="text" value="1024"/>
Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength.	
Note: With International Editions of the Domino server, the 1024 bit key size can only be used if you qualify for and have purchased a Verisign Global Server ID	
CA Certificate Label:	<input type="text" value="Admincamp 2010"/>
This label identifies the CA Trusted Root certificate that is automatically installed in the server key ring you are creating.	

- 6) Die beiden Dateien **Keyfile.kyr** und **Keyfile.sth** aus dem lokalen Notes Data Verzeichnis ins Data Verzeichnis am Domino Server kopieren

7) Im Serverdokument des Domino Directories unter *Ports – Internet Ports* SSL aktivieren

The screenshot shows the IBM Lotus Notes Server Configuration window for 'Server: Domino/kolb'. The window is titled 'Server: Domino/kolb - IBM Lotus Notes' and has a menu bar with 'File', 'Edit', 'View', 'Create', 'Actions', 'Text', 'Tools', 'Window', and 'Help'. The main window is divided into several tabs: 'Basics', 'Security', 'Ports...', 'Server Tasks...', 'Internet Protocols...', 'MTAs...', 'Miscellaneous', and 'Transactional'. The 'Ports...' tab is active, and the 'Internet Ports...' sub-tab is selected. The 'SSL settings' section is expanded, showing the following options:

- SSL key file name:
- SSL protocol version (for use with all protocols except HTTP):
- Accept SSL site certificates: Yes No
- Accept expired SSL certificates: Yes No
- SSL ciphers:
 - RC4 encryption with 128-bit key and MD5 MAC
 - RC4 encryption with 128-bit key and SHA-1 MAC
 - Triple DES encryption with 168-bit key and SHA-1 MAC
 - DES encryption with 56-bit key and SHA-1 MAC
 - RC4 encryption with 40-bit key and MD5 MAC
- Enable SSL V2: (SSL V3 is always enabled) Yes

Below the 'SSL settings' section, there are tabs for 'Web', 'Directory', 'Mail', 'DIIOP', 'Remote Debug Manager', and 'Server Controller'. The 'Web' tab is selected, showing the following options:

- TCP/IP port number:
- TCP/IP port status:
- Enforce server access settings:
- Authentication options:
 - Name & password:
 - Anonymous:
- SSL port number:
- SSL port status:
- Authentication options:
 - Client certificate:
 - Name & password:
 - Anonymous:

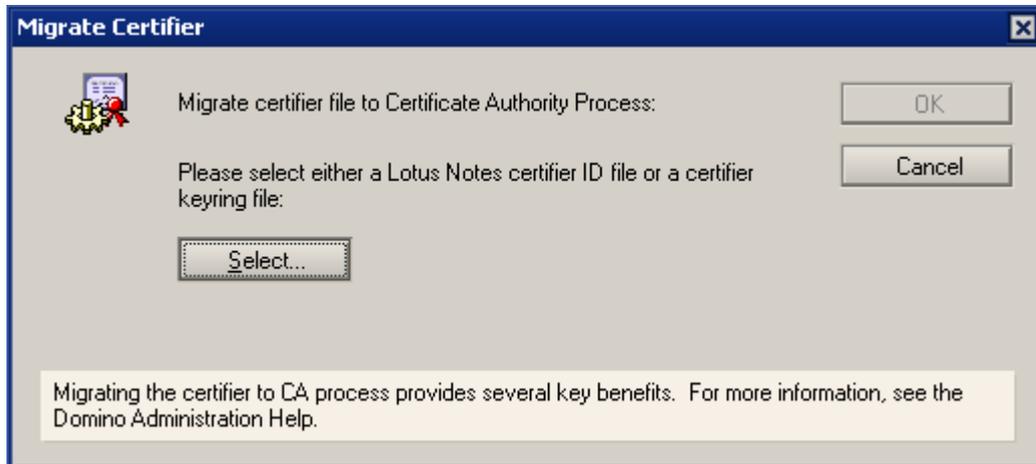
At the bottom of the window, there is a text field with the placeholder text: 'Enter the name of the SSL key ring the Domino Web server uses for encryption activities.'

auf der Serverconsole mit **tell http restart** den http Task neu starten bzw mit load http starten falls er noch nicht läuft

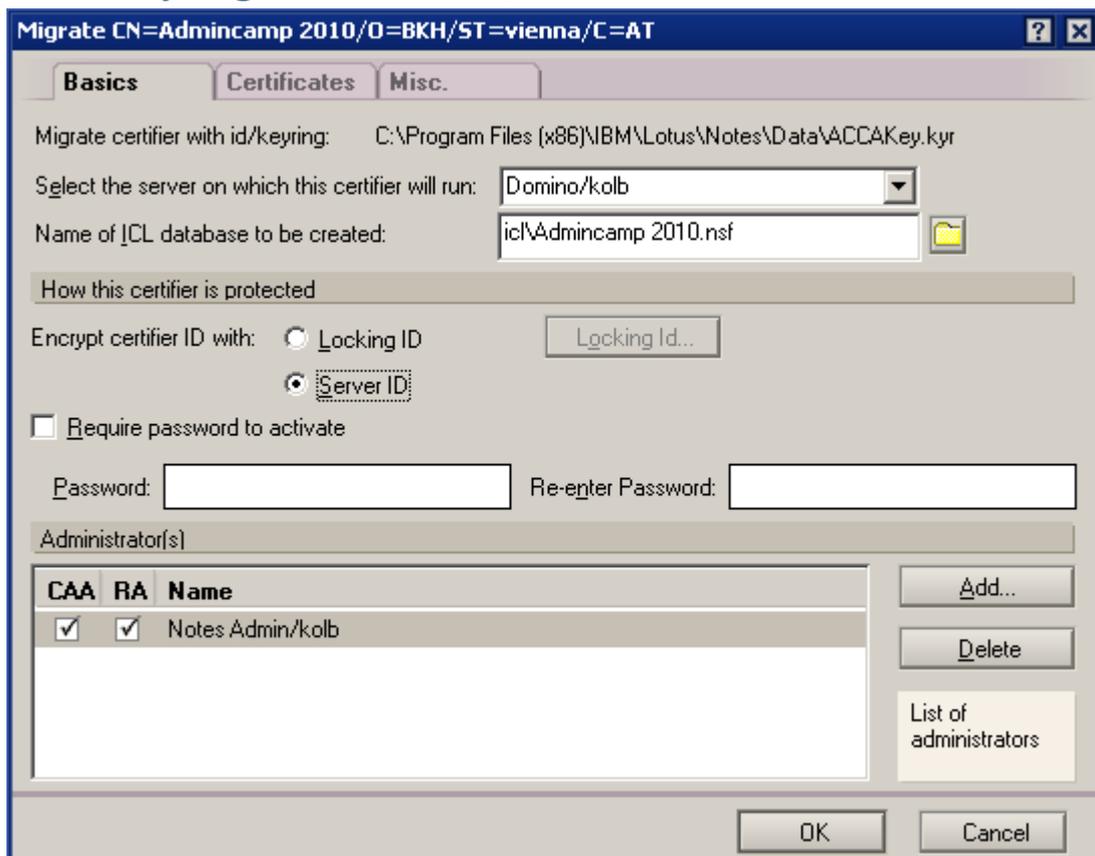
Lab 3: Cerifier migrieren

1) Migrate certifier

Admin Client – configuration – Migrate Certifier

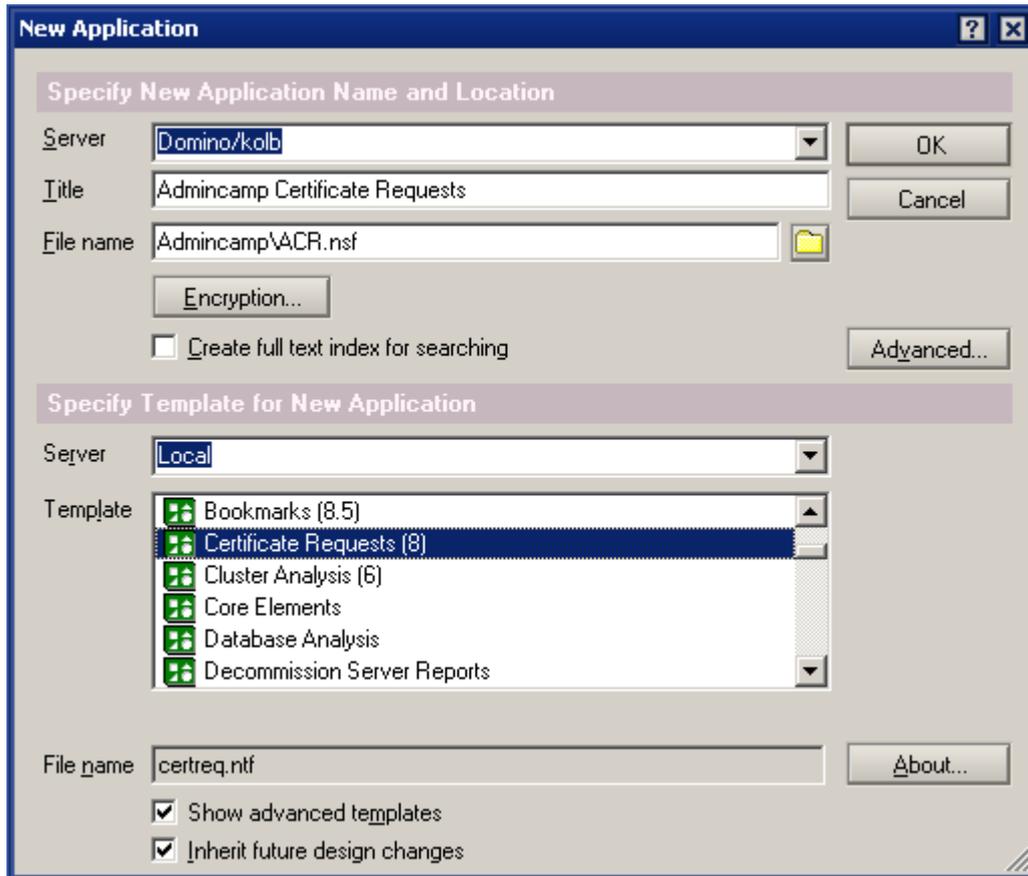


2) Select Keyring File -> ICL DB anlegen



3) Certreq.nsf anlegen

File – Application new (certreq.ntf)



4) Konfiguration

Database Administration:	
Supported CA:	Server: <input type="text" value="Domino/kolb"/> <input type="button" value="v"/> Certifier: <input type="text" value="CN=Admincamp 2010/O=BKH/ST=vi"/>
Supported Certificate Types:	<input type="radio"/> Client Certificates Only <input type="radio"/> Server Certificates Only <input checked="" type="radio"/> Both Client and Server Certificates
Client Request Customization:	
Validity Period:	<input type="text" value="2"/> years
Key Usages:	<input type="text" value="Digital Signature, Key Encipherment"/> <input type="button" value="v"/>
Extended Key Usages:	<input type="text" value="Client Authentication, EMail Protection"/> <input type="button" value="v"/>
Server Request Customization:	
Validity Period:	<input type="text" value="1"/> years
Key Usages:	<input type="text" value="Digital Signature, Key Encipherment"/> <input type="button" value="v"/>
Extended Key Usages:	<input type="text" value="Server Authentication"/> <input type="button" value="v"/>
Request Processing:	
Processing Method:	<input type="text" value="Manual"/> <input type="button" value="v"/>
Mail Notification:	
Mail confirmation of handled request to requestor?	<input type="radio"/> Yes <input checked="" type="radio"/> <input type="text" value="No"/>

Achtung: auch hier normalerweise Mail confirmation -> YES. Nur hier im Lab werden keine Mails versendet

5) CA Servertask starten

Auf der Serverconsole: **load ca**

6) Im Browser einen Request erstellen

Mit dem Firefox auf <http://127.0.0.1/Admincamp/ACR.nsf>

Request a Client Certificate for Netscape Navigator or Compatible

Use this form to enter the information required for your client certificate request.

Certificate Info:
The following information will be included in your client certificate.

Your Full Name: e.g. John Doe
 Organizational Unit(s):

 Organization:
 City/Locality:
 State/Province: No abbreviations
 Country: 2 letter country code, e.g. us
 E-Mail Address:
 Your e-mail address is required if you will be using this certificate for S/MIME e-mail.

Contact Information:
Provide the following information in case the Certificate Authority needs to contact you.

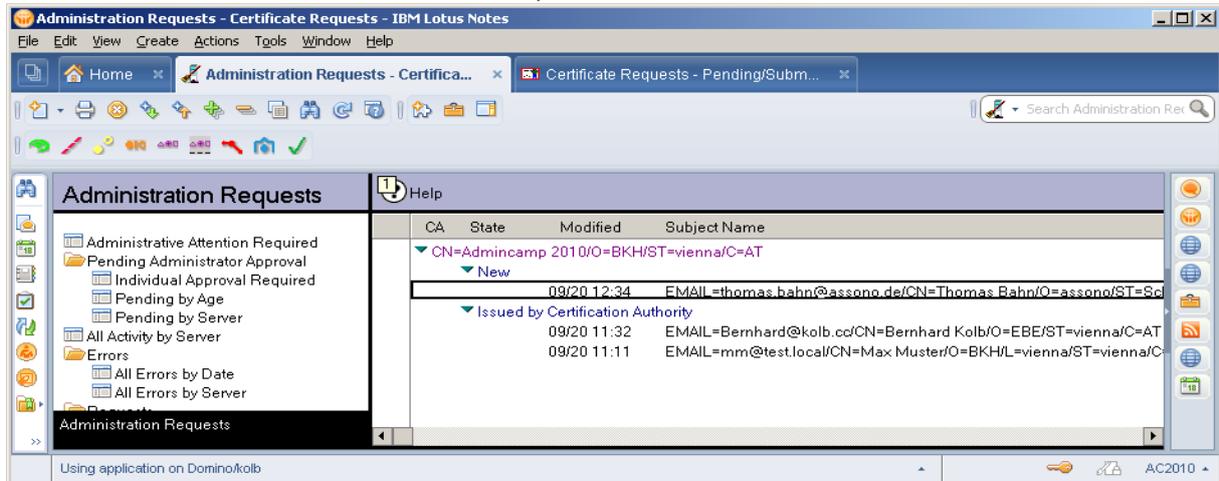
Return E-Mail:
 Directions for picking up your certificate will be sent to this email address.

Damit ist der Request in der certreq.nsf

Dort selektieren und -> Submit to adminP

7) Im Administrationsprozeß freigeben

in der Admin4.nsf in der view Certificate Requests

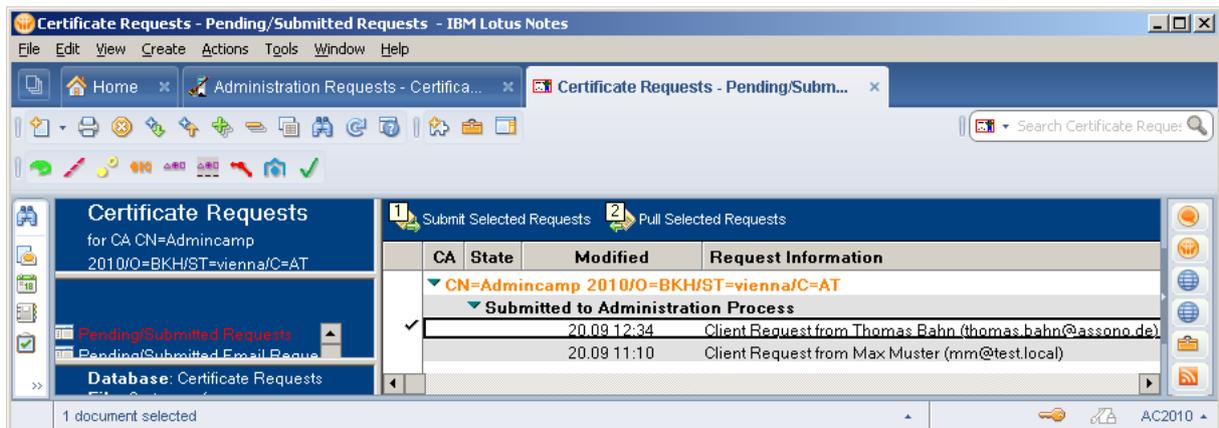


Eintrag editieren

optional: Zuordnung zu einem Personendokument (oder Not Published auswählen)

8) Zertifikat zum download bereitstellen

In der certreq.nsf den Eintrag selektieren – Pull request

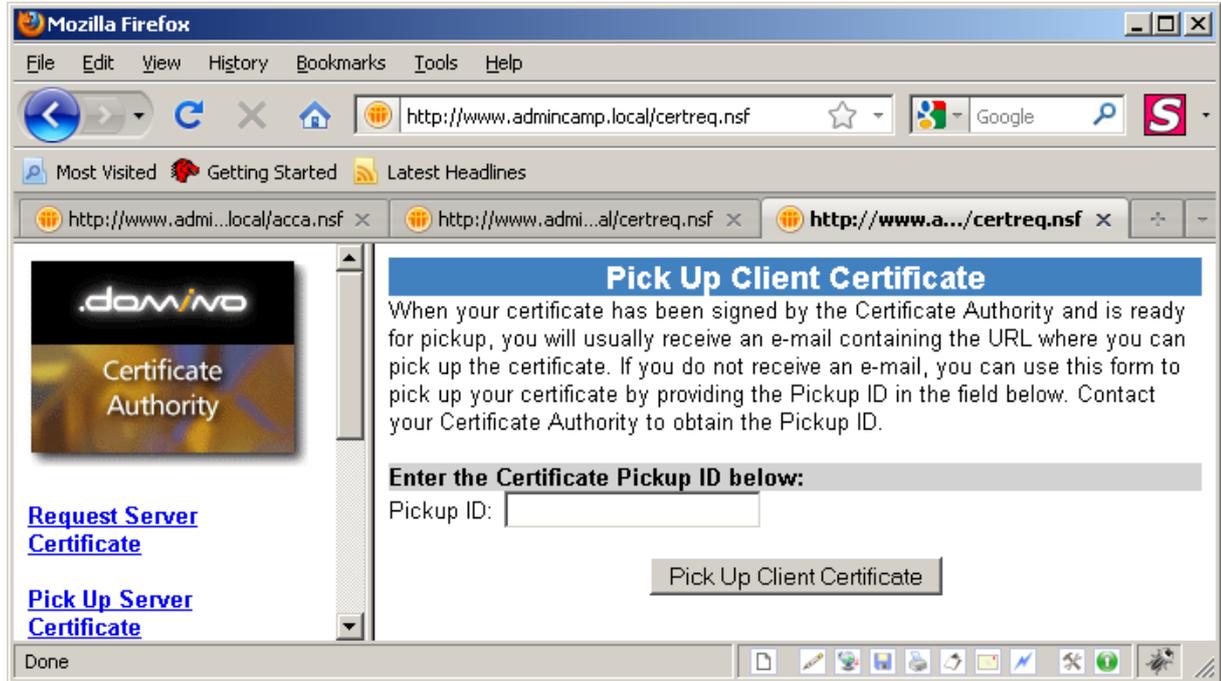


Der Request liegt nun in der View Issued Certificate Requests

Dort den Eintrag öffnen und die Pickup ID kopieren

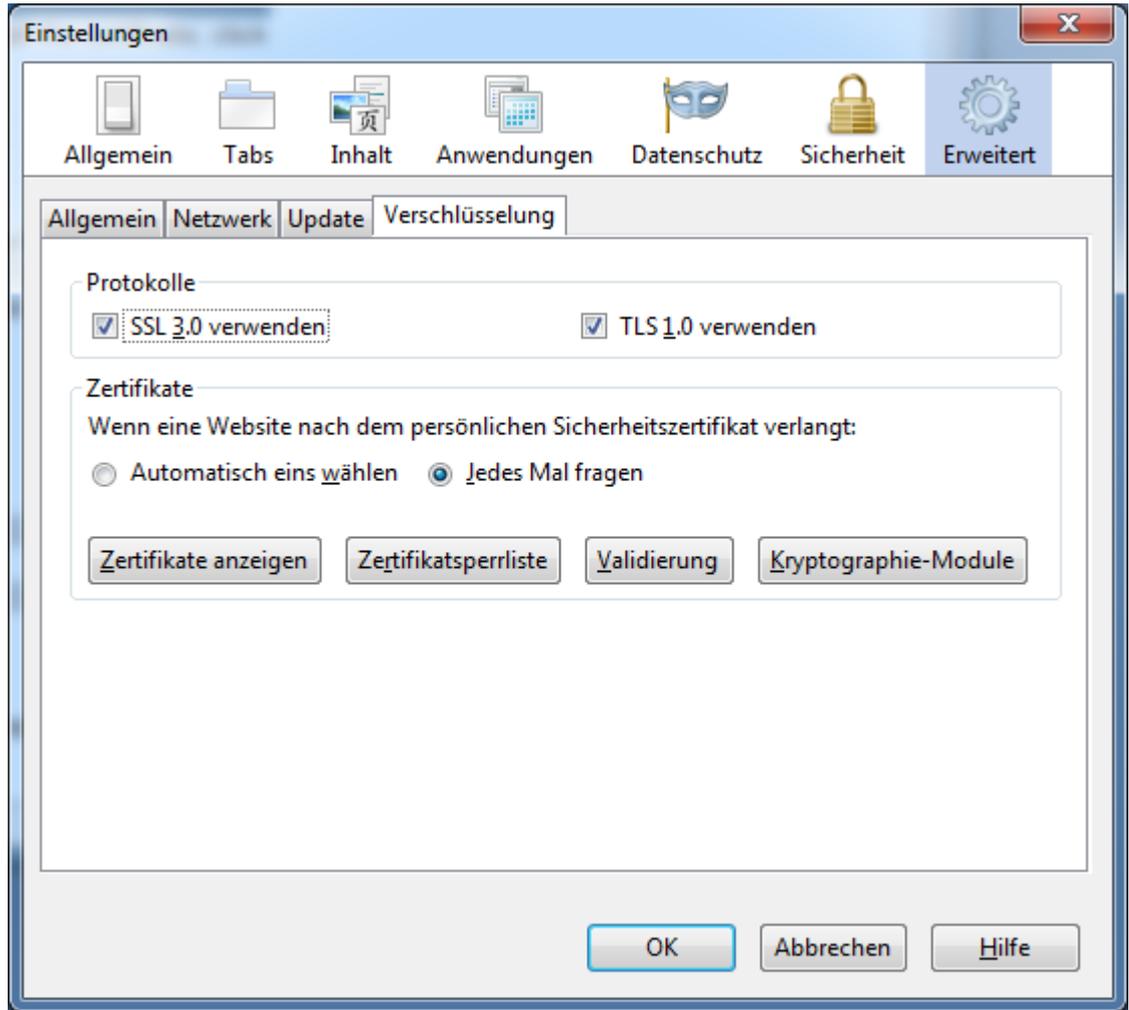
Lab 4: Client Zertifikat installieren

- 1) Im Firefox das Zertifikat abholen und akzeptieren

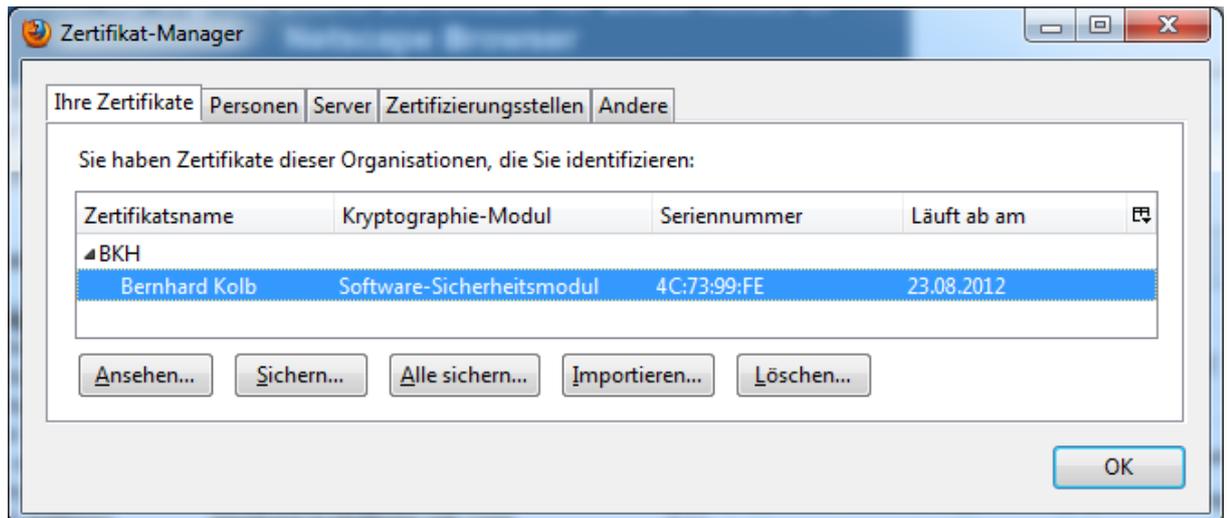


Damit ist das Zertifikat dann im Firefox

2) Exportieren via: Extras – Einstellungen

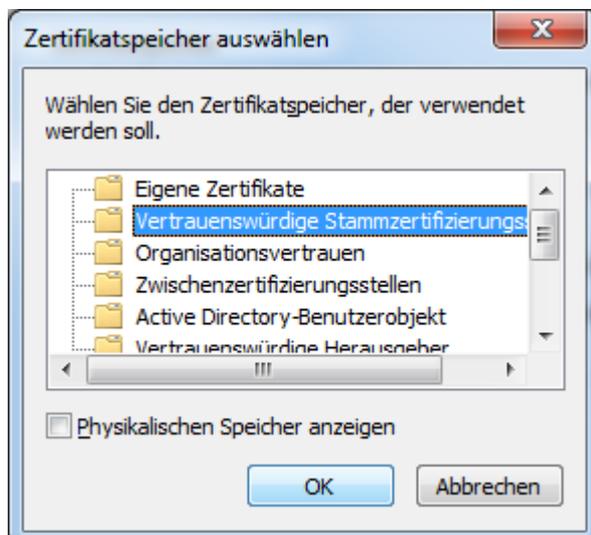
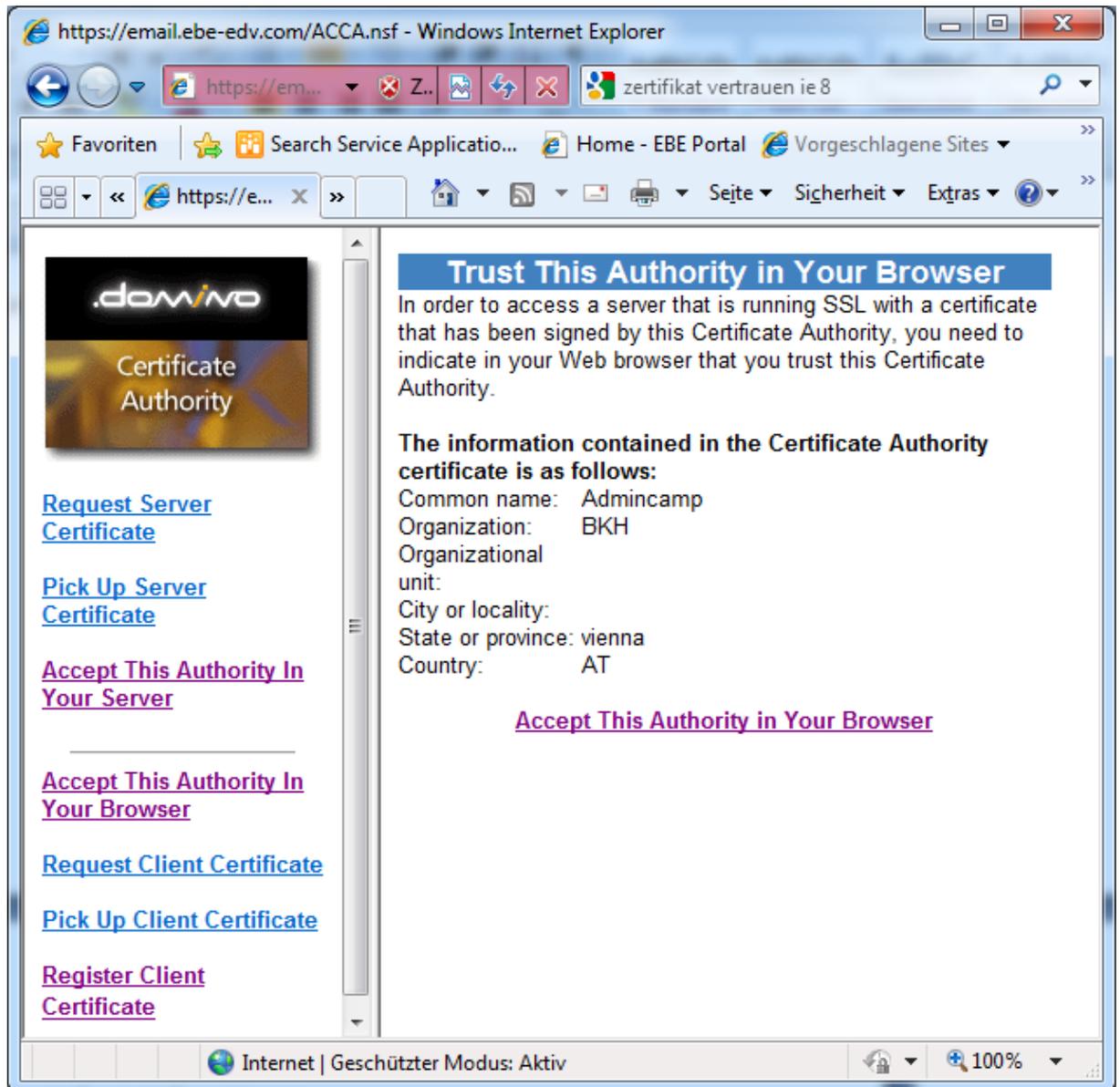


Zertifikate anzeigen -> Sichern

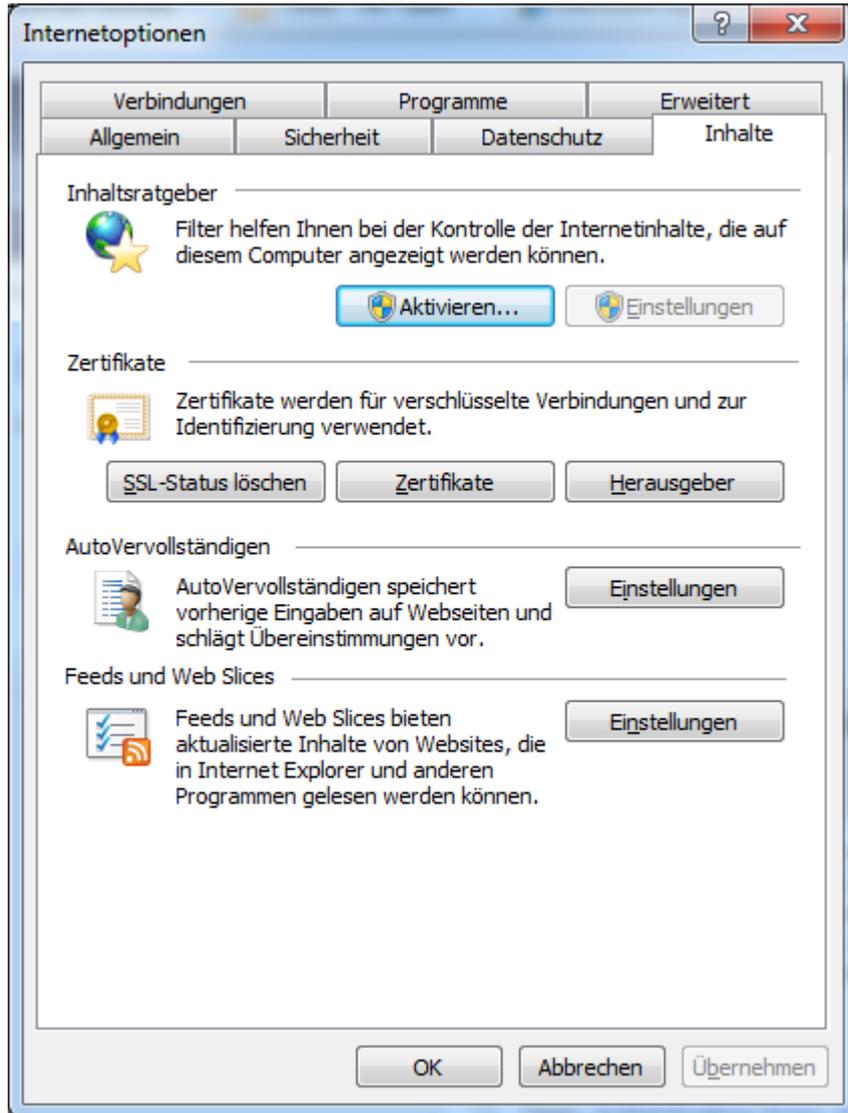


damit wird das Zertifikat (public und Private Key) in eine Datei exportiert

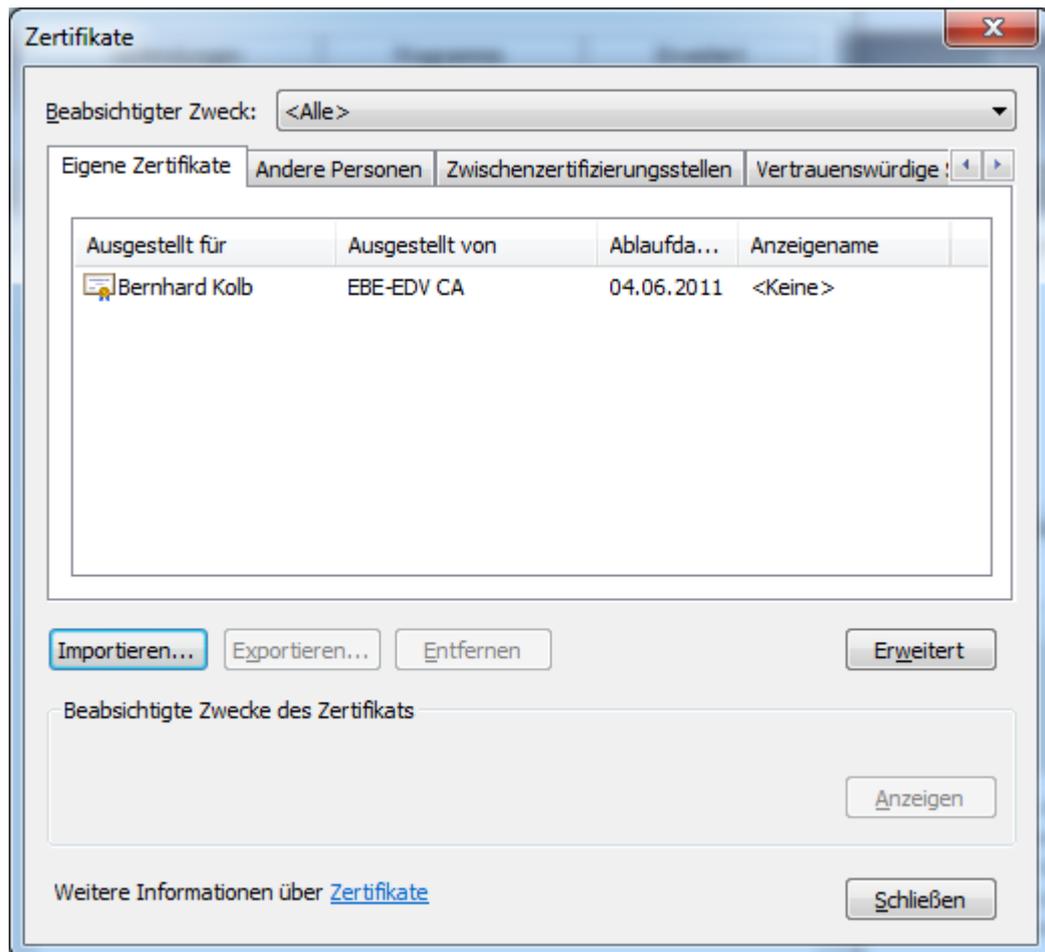
- 3) Im Internet Explorer **der Ausstellungsstelle vertrauen**
mit dem IE die ACCA.nsf öffnen und „Accept This Authority in your Browser“



4) In den Internet Explorer importieren

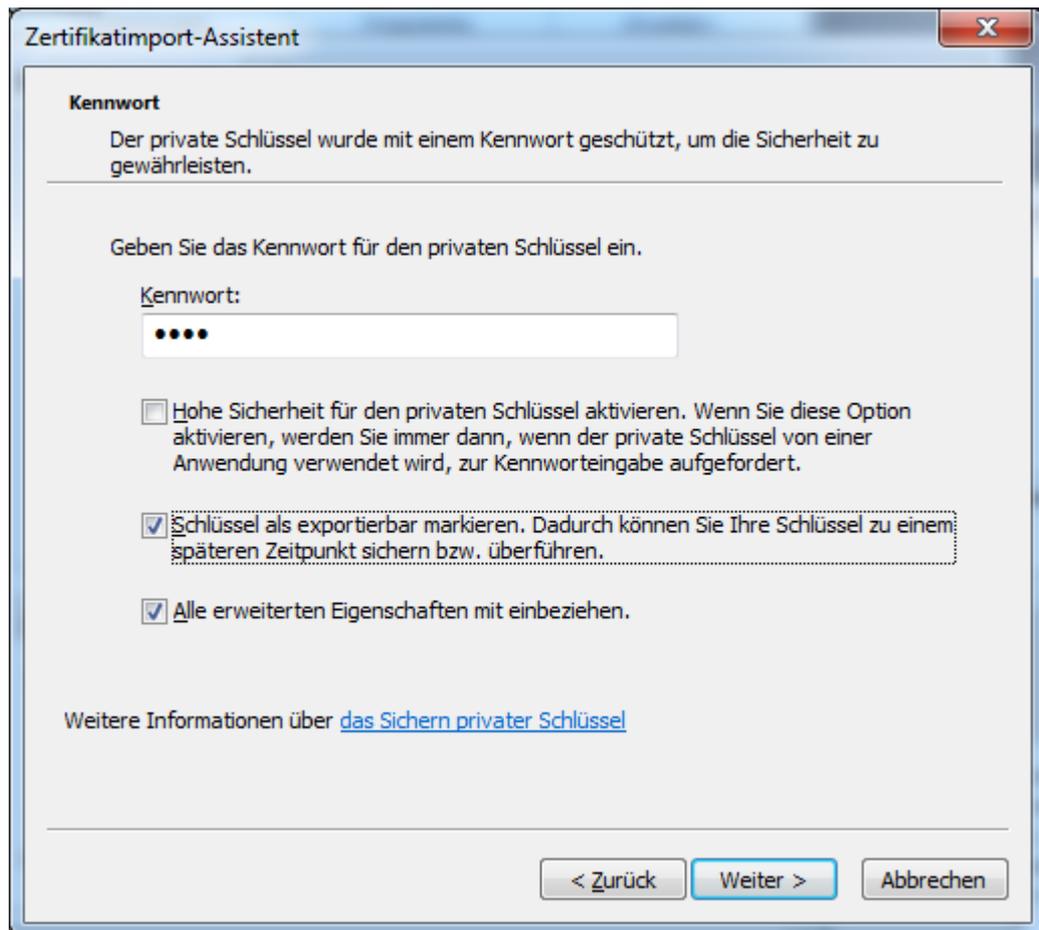


Es müssen die Attribute gesetzt werden – das geht im IE...

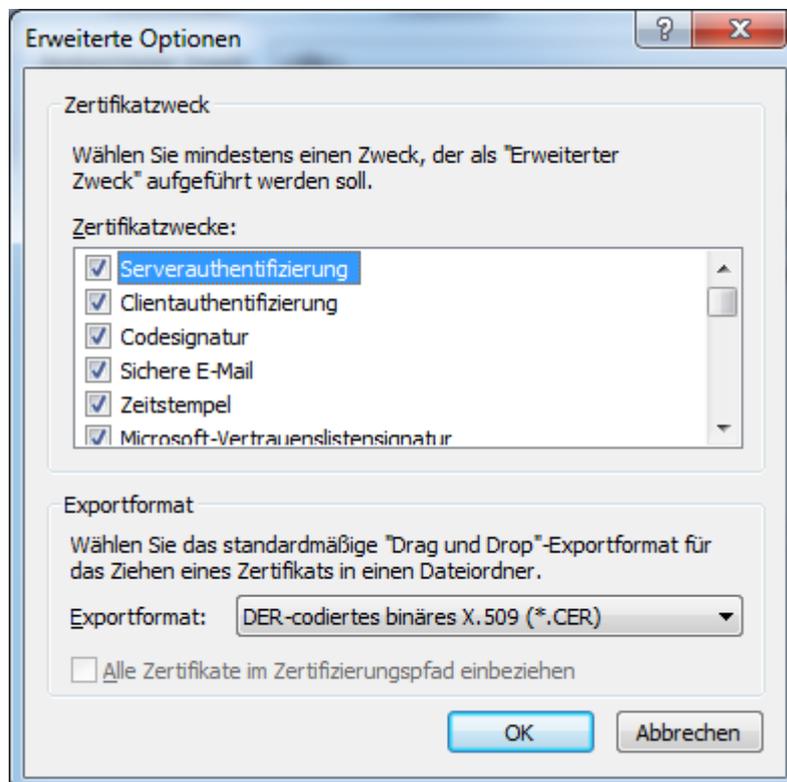


importieren...

wichtig: Schlüssel als exportierbar markieren!

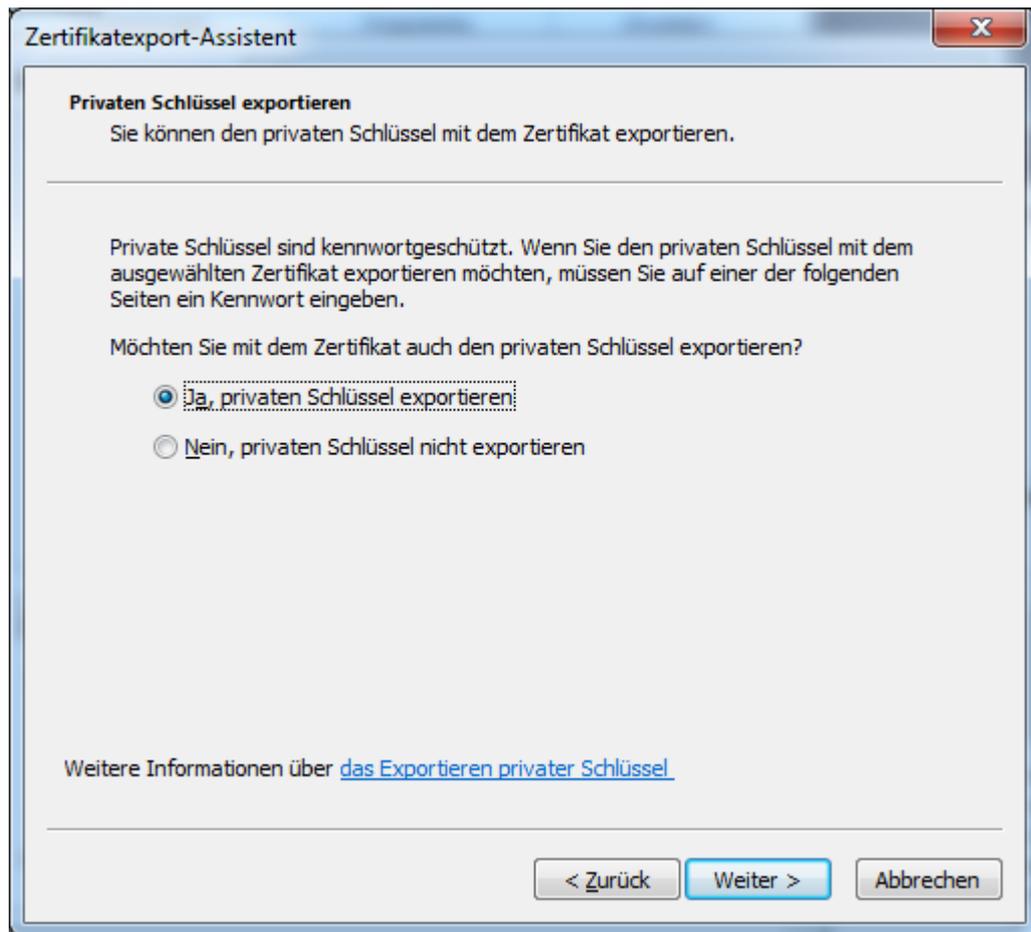


Dann das Zertifikat auswählen – erweitert

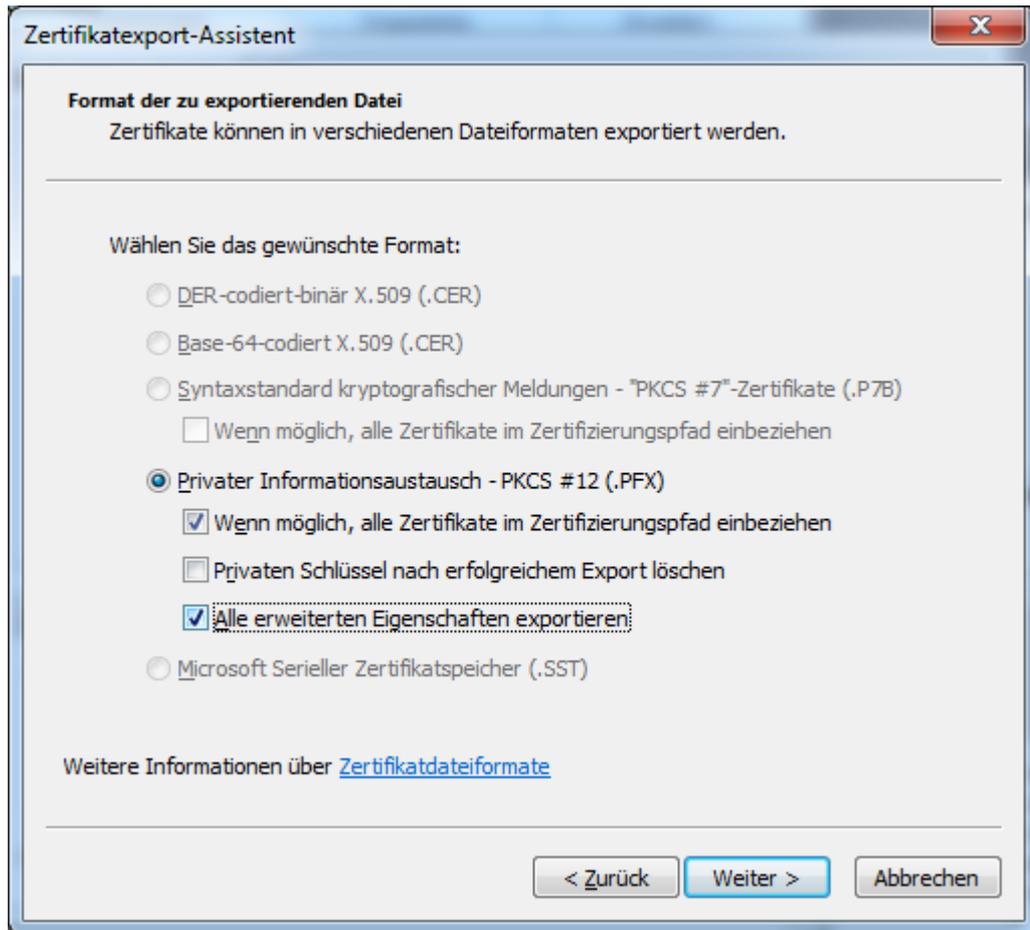


Clientauthentifizierung auswählen und **Sichere-email**

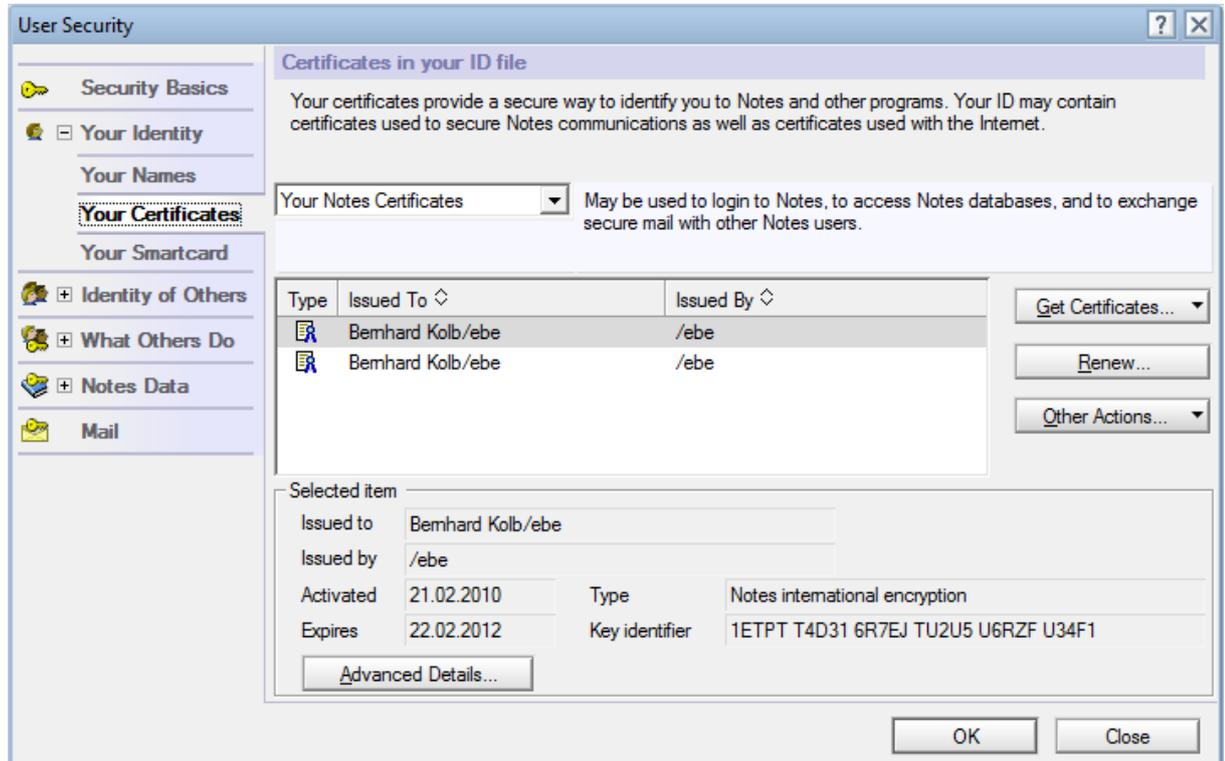
Dann wieder **exportieren**.



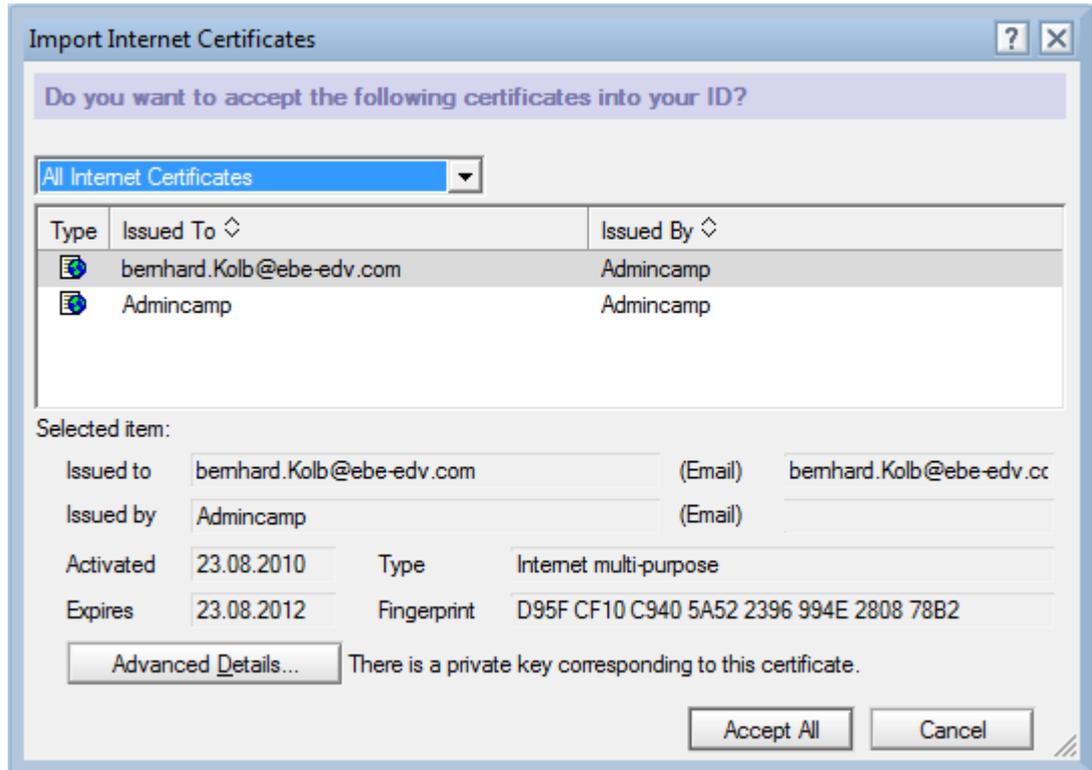
Wichtig: privaten Schlüssel exportieren!



- 5) Optional: Nun kann der **Key in den Notes Client importiert** werden
 File – Security – User Security

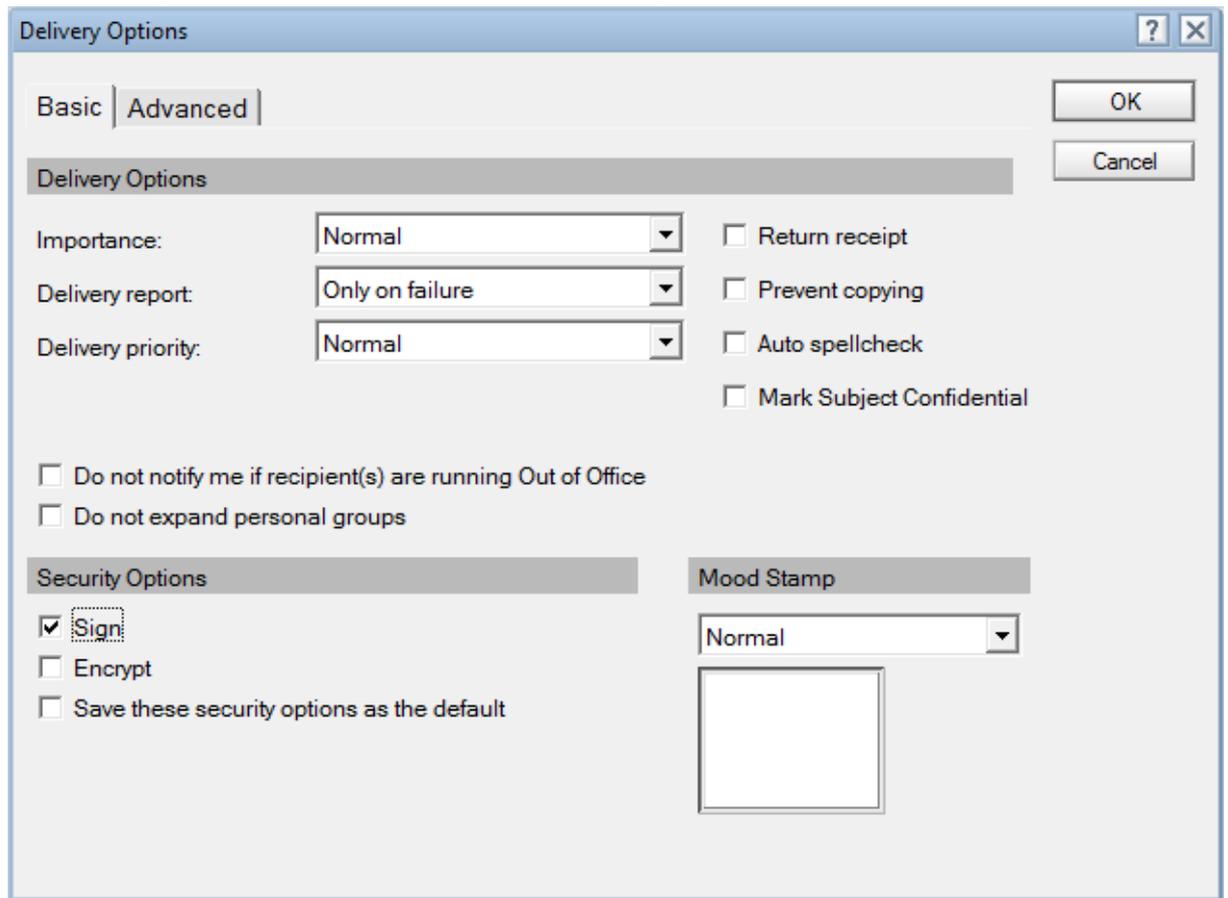


Get Certificates...Import Internet Certificate



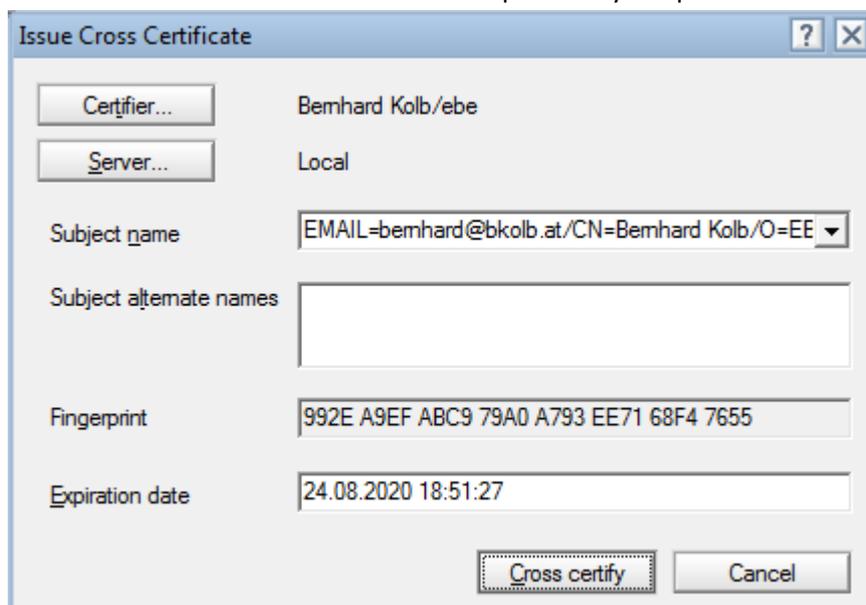
Accept all -> übernimmt das Zertifikat in die Notes ID

6) Tadaa – fertig! Nun kann man **Mails an Internetuser signieren**



Dadurch wird der eigene public Key mitgesendet – der Empfänger muß das Zertifikat akzeptieren und den Absender ins Adreßbuch aufnehmen. Damit können dann verschlüsselte Nachrichten über SMTP ausgetauscht werden!

7) Umgekehrt muß man im Notes Client den **Absender** einer unterzeichneten email ins **lokale Adreßbuch** aufnehmen um seinen public Key zu speichern!



Add Sender to Contacts [?] [X]

Basics

Title: []

First name: Bernhard

Middle name: []

Last name: Kolb

Suffix: []

Advanced

Mail system: [Lotus Notes]

Routing domain(s): []

E-mail address: Bernhard.Kolb@ebe

Include X.509 certificates when encountered [i]

OK

Cancel

Wichtig: include X.509 certificates!