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.

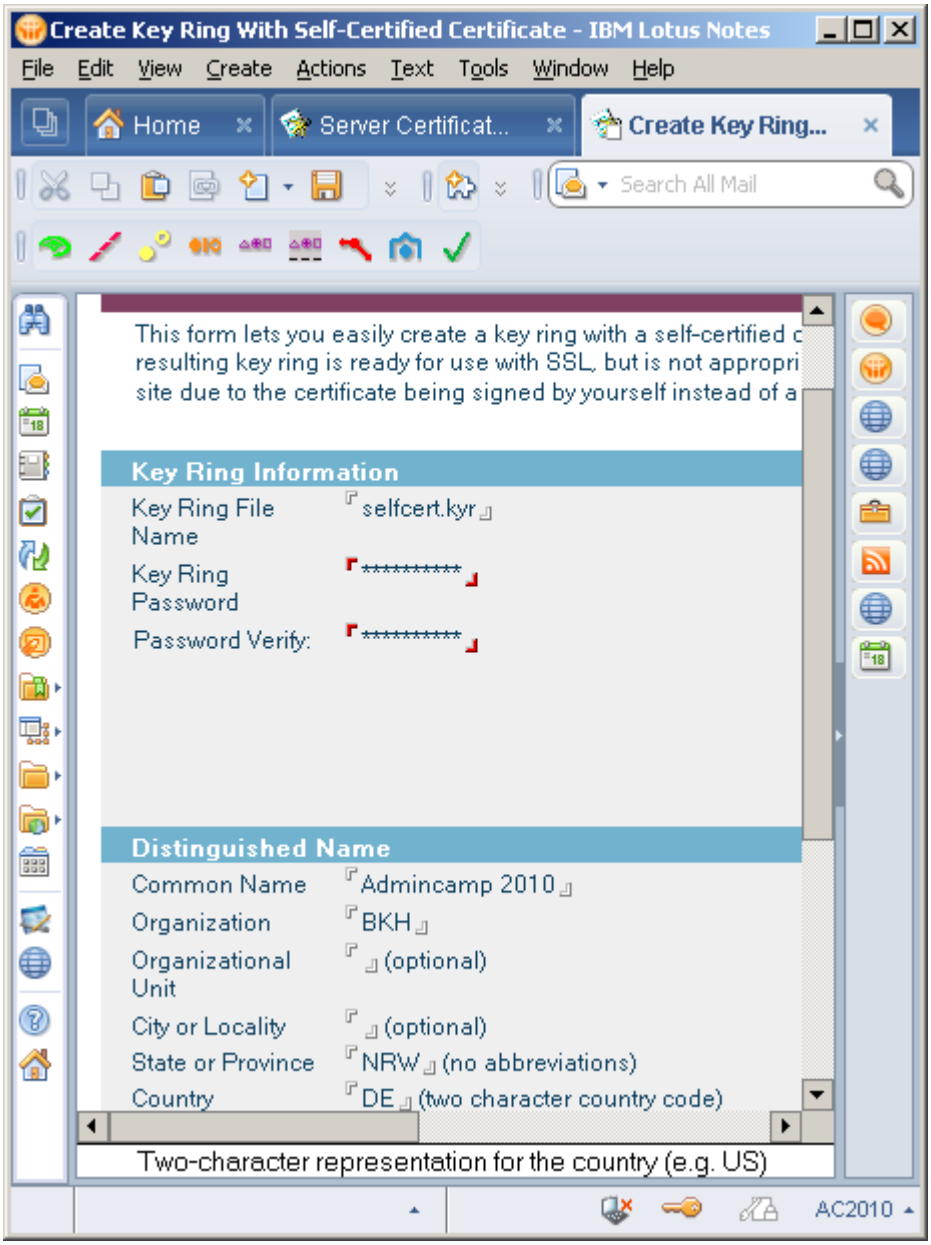
Bernhard Kolb

www.ebe-edv.com

Bernhard.Kolb@ebe-edv.com

Lab 1: SSL via Server Certificate Admin

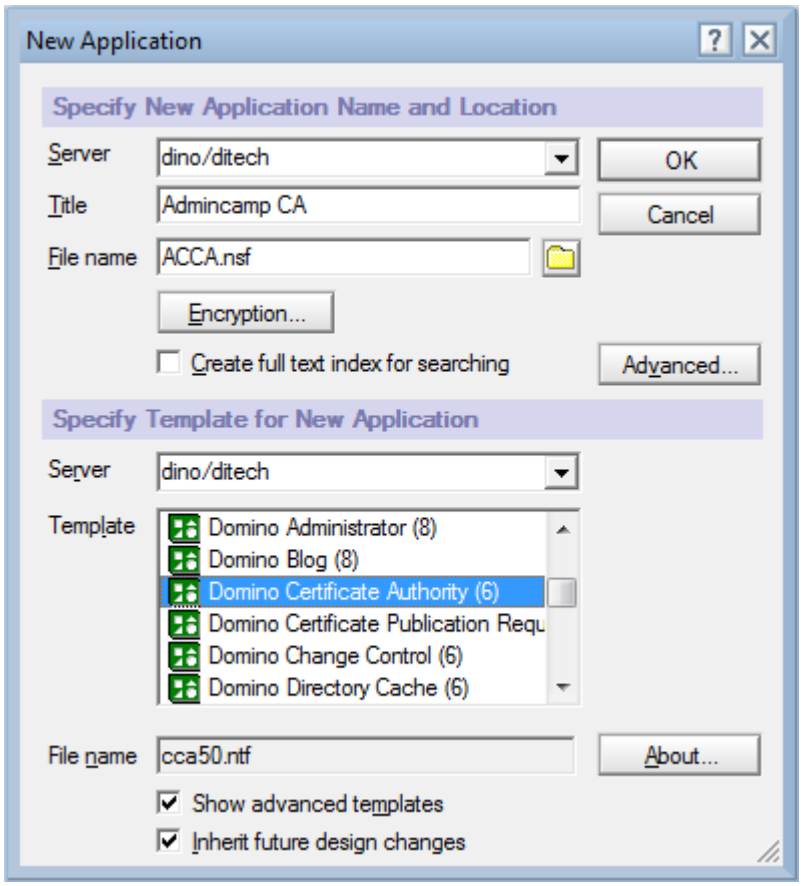
1) Certserv.nsf öffnen
2) Create self signed certificate
3) Passwort vergeben *lotusnotes*



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

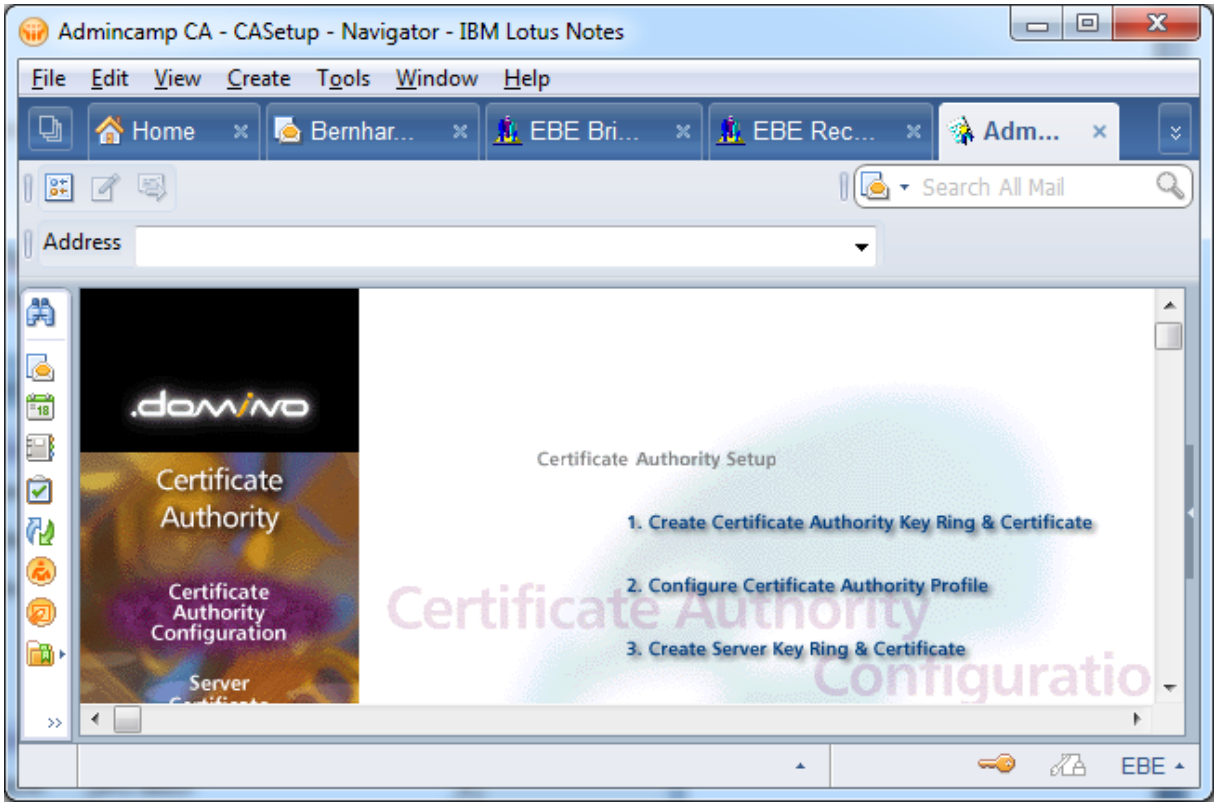
Lab 2: Zertifizierungsstelle einrichten

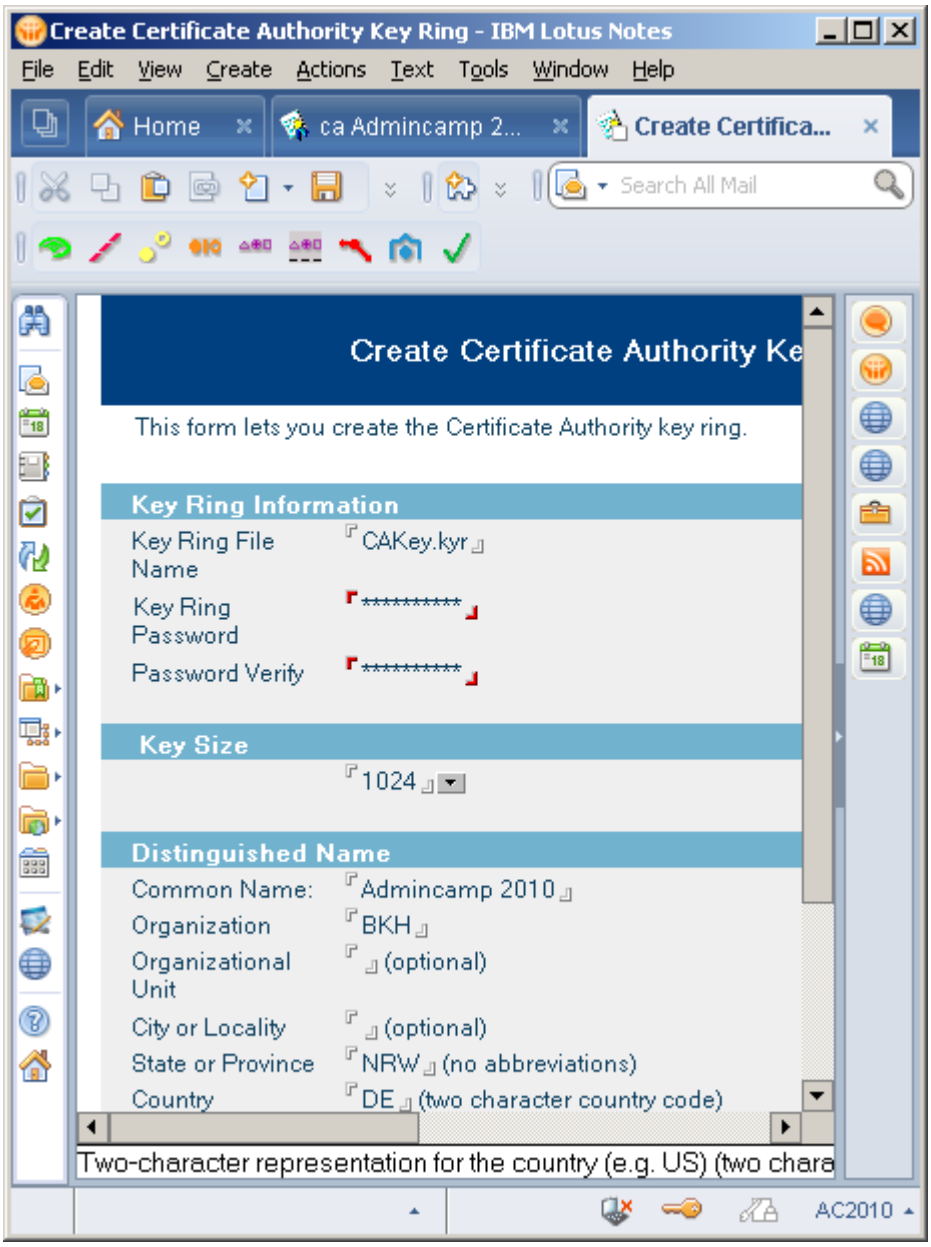
1) **Certificate Authority einrichten**
   am server neue DB von der CCA50 Schablone erstellen



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

3) **Create Server Certificate & Keyring**

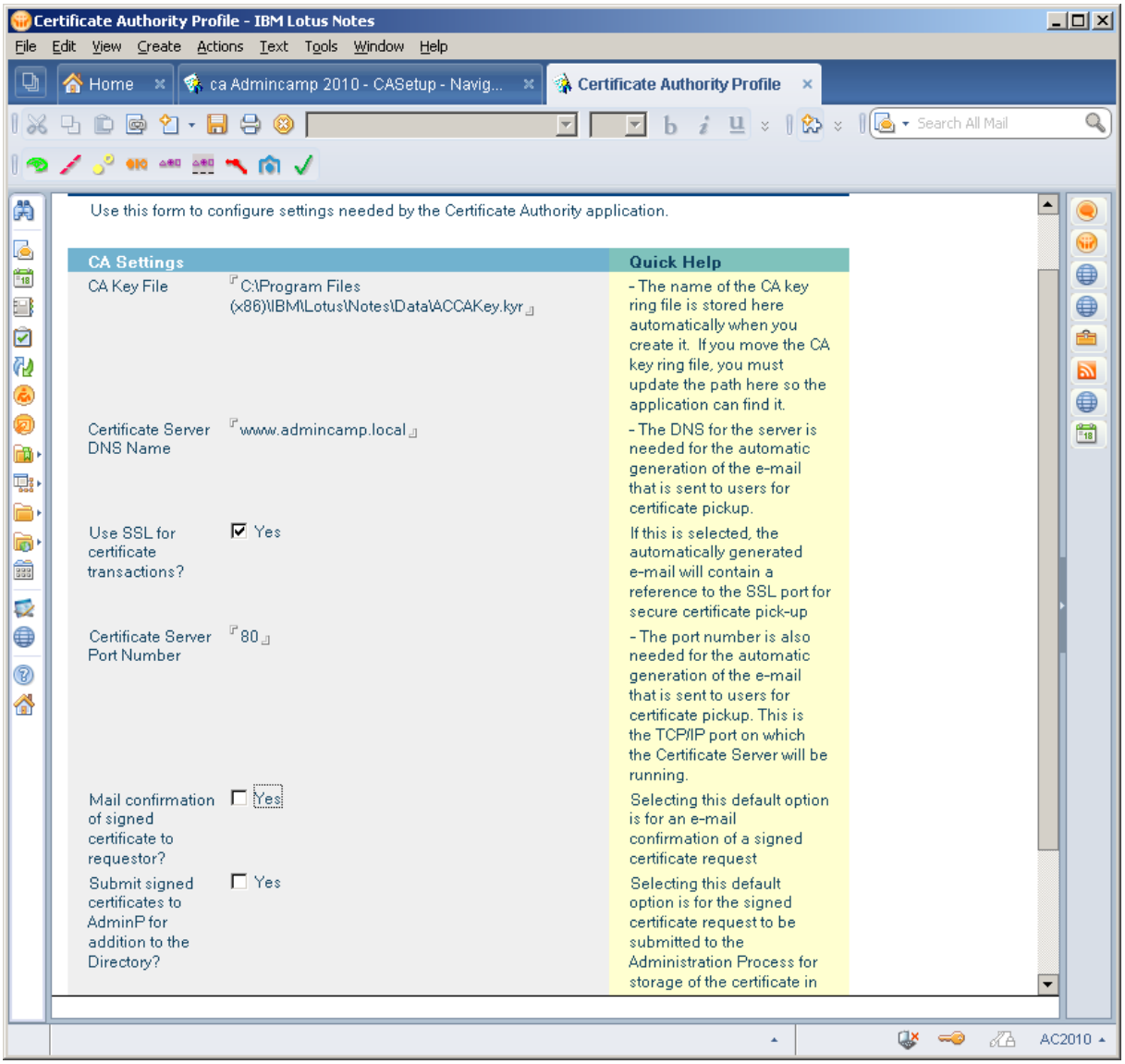




Das Certificate Authority-Keyring-File entspricht der cert.id in der Domino-Welt und wird für die spätere Ausstellung von Zertifikaten benötigt.

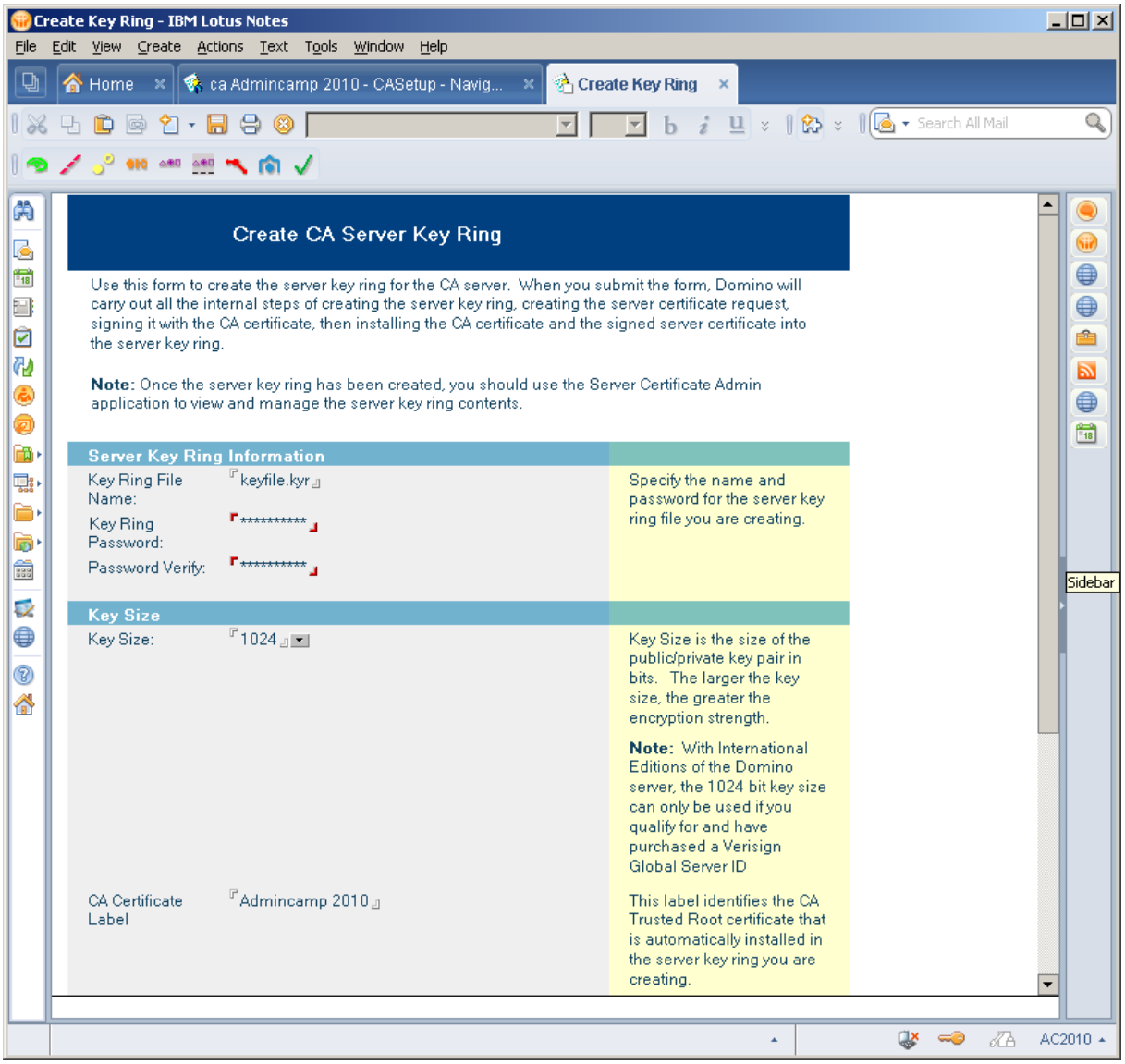
Achtung: diese Datei wird lokal auf der Notes-Client Maschine erzeugt!

4) **Configure Certificate Authority**



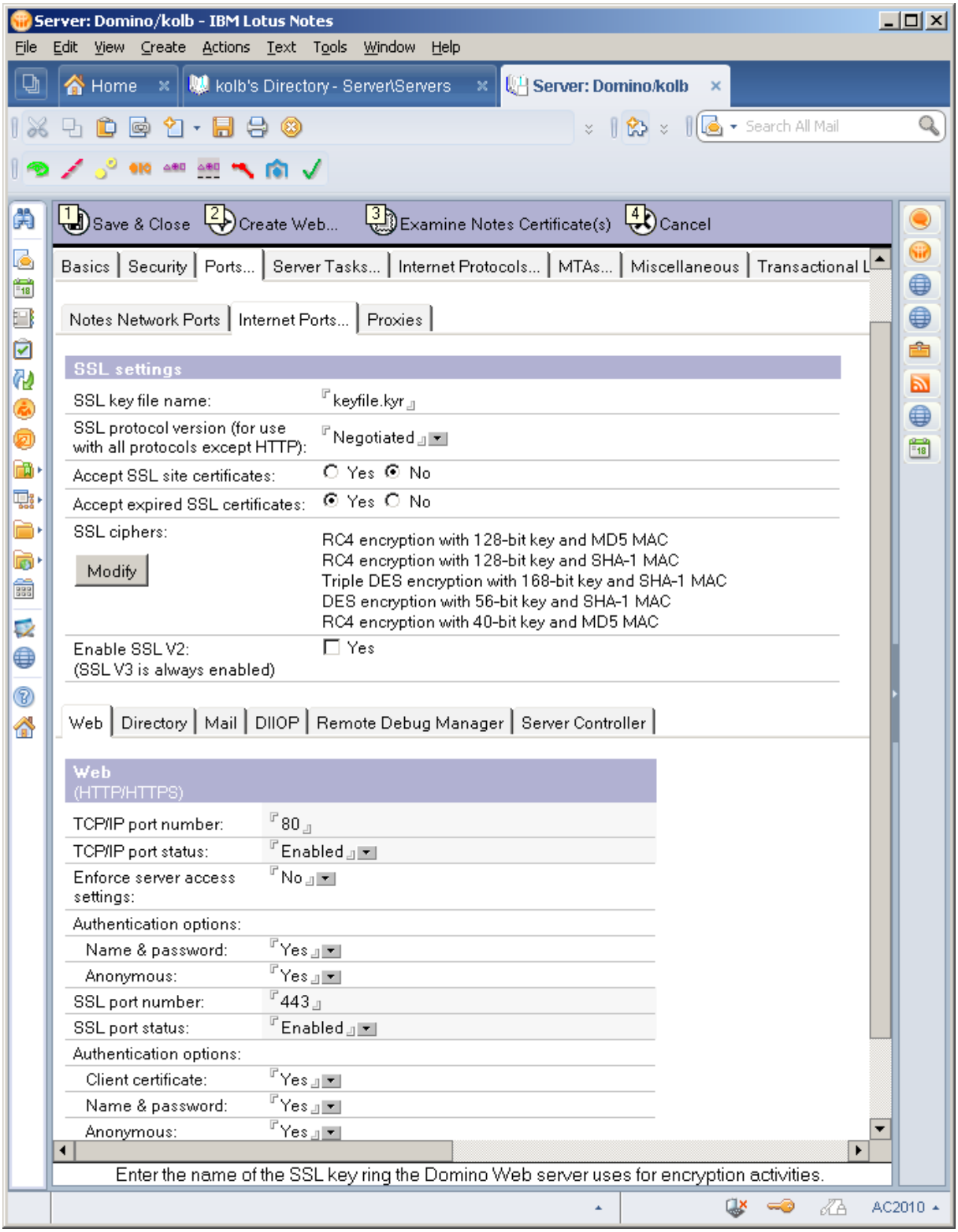
Achtung: üblicherweise wird Mailconfirmation auf YES gesetzt! Nur hier im Lab wird auf Mail Benachrichtigung verzichtet.

5) **Create Server KeyRing**



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

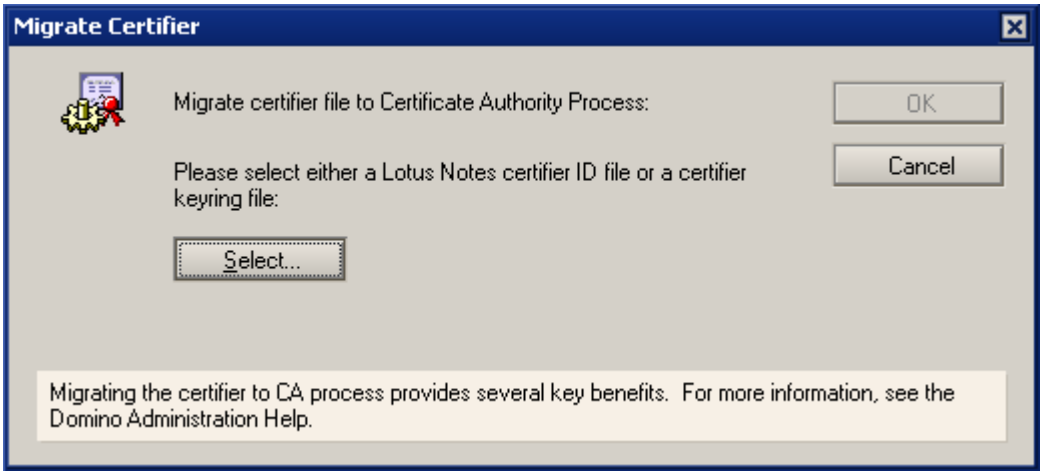


auf der Serverconsole mit **tell http restart** den http Task neu starten bzw mit load http starten falls er noch nicht läuft

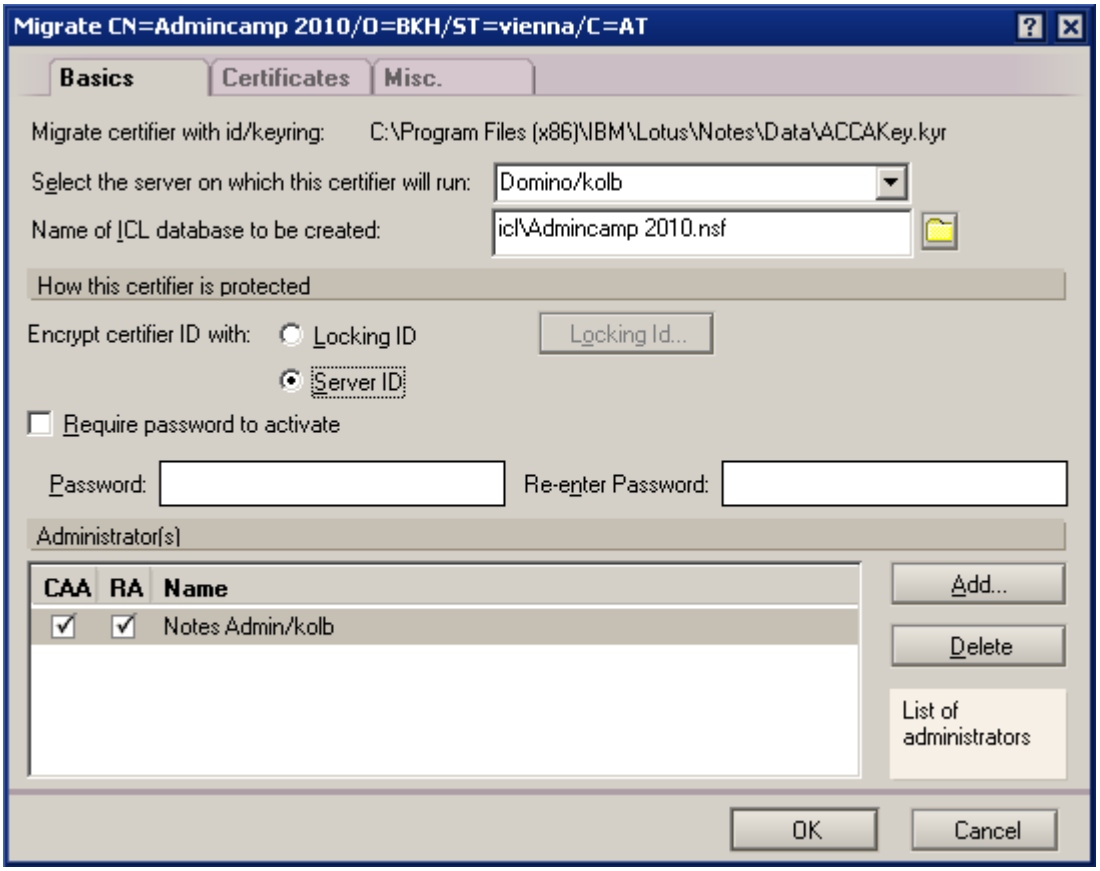
Lab 3: Cerifier migrieren

1) Migrate certifier

Admin Client – configuration – Migrate Certifier

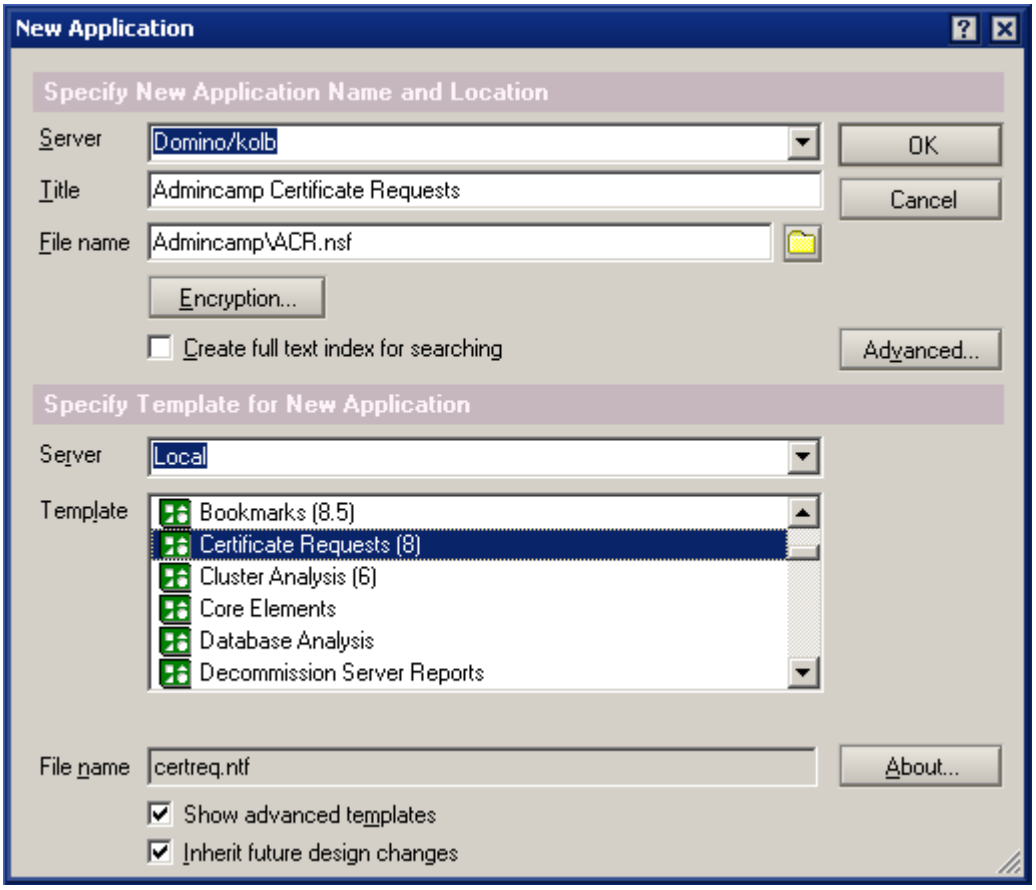


2) Select Keyring File -> ICL DB anlegen

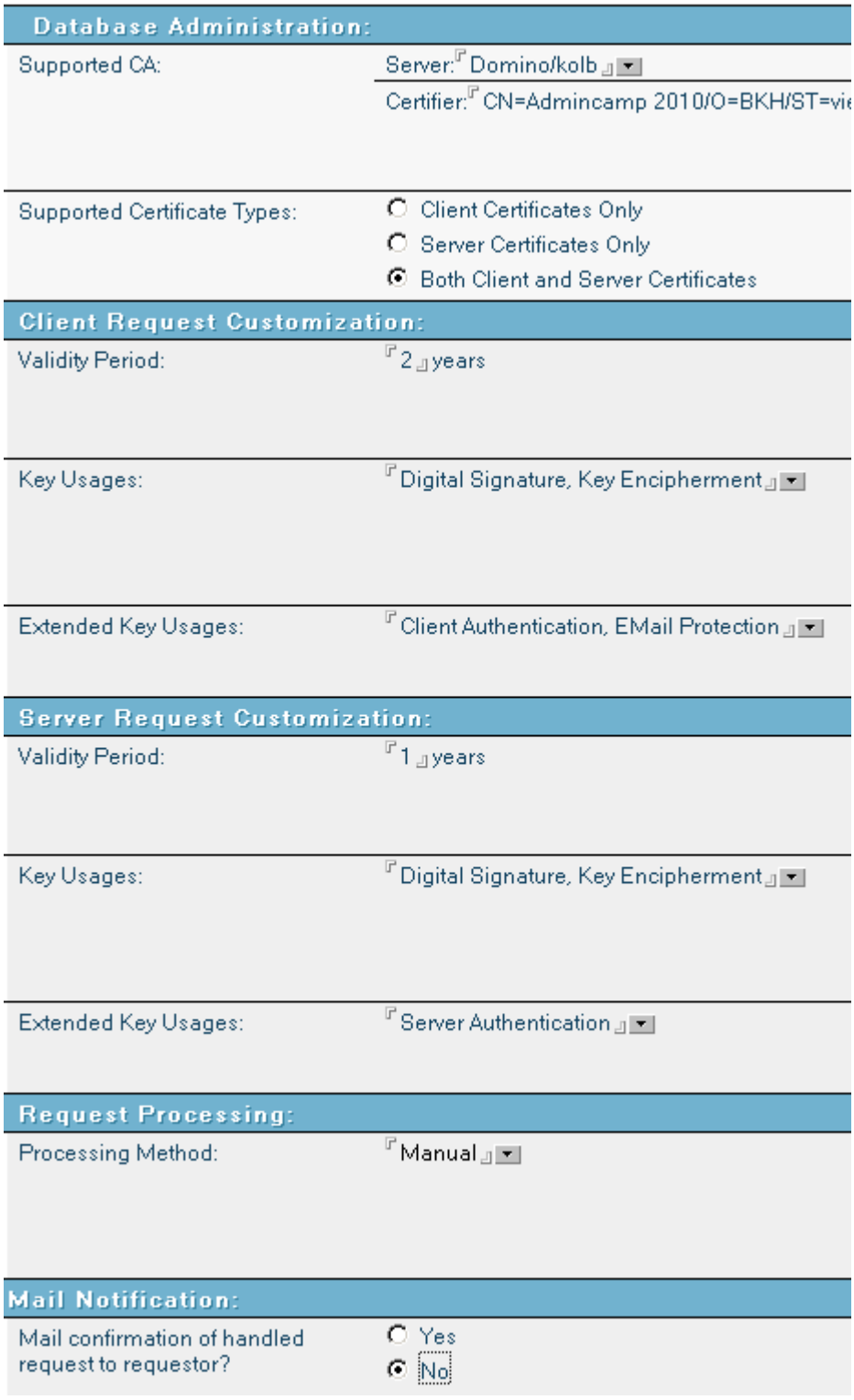


3) Certreq.nsf anlegen

File – Application new (certreq.ntf)



4) Konfiguration



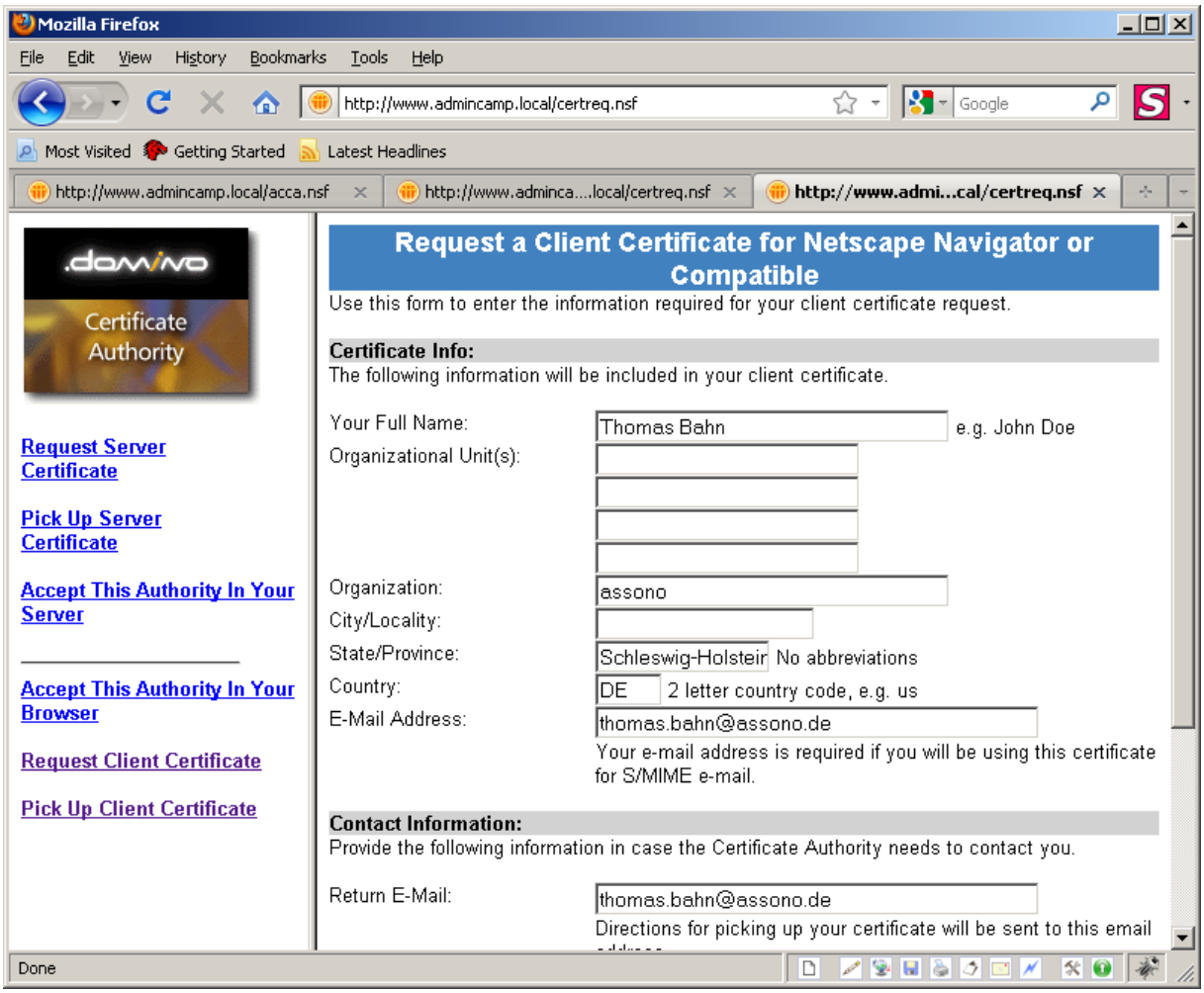
Achtung: auch hier normalerweise Mail confirmation -> YES. Nur hier im Lab werden keine Mails versendet

5) CA Servertask starten

Auf der Sevrerconsole: **load ca**

6) Im Browser einen Request erstellen

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

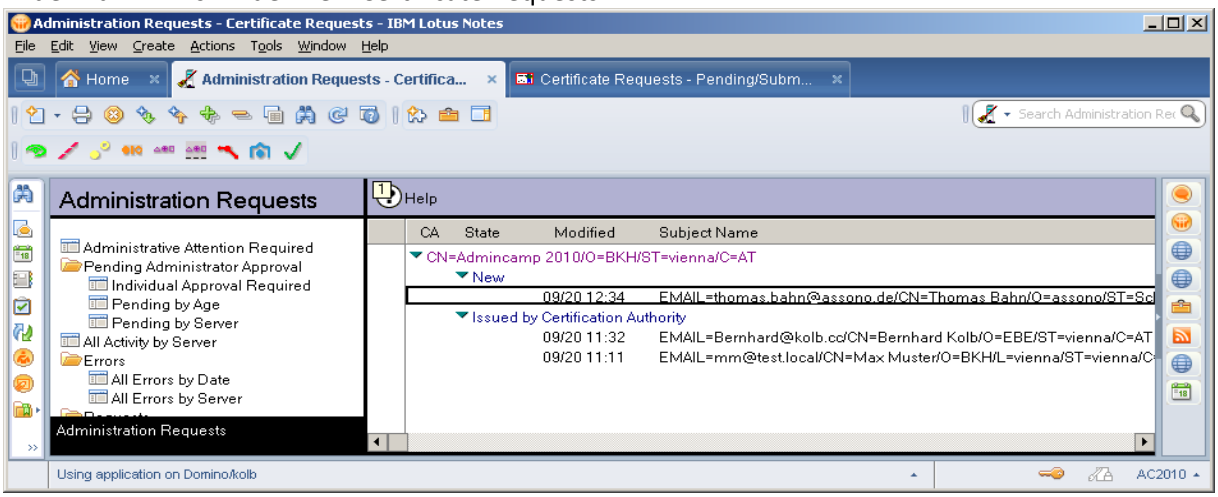


Damit ist der Request in der certreq.nsf

Dort selektieren und -> Submit to adminP

7) Im Administrationsprozeß freigeben

in der Admin4.nsf in der view Certificate Requests

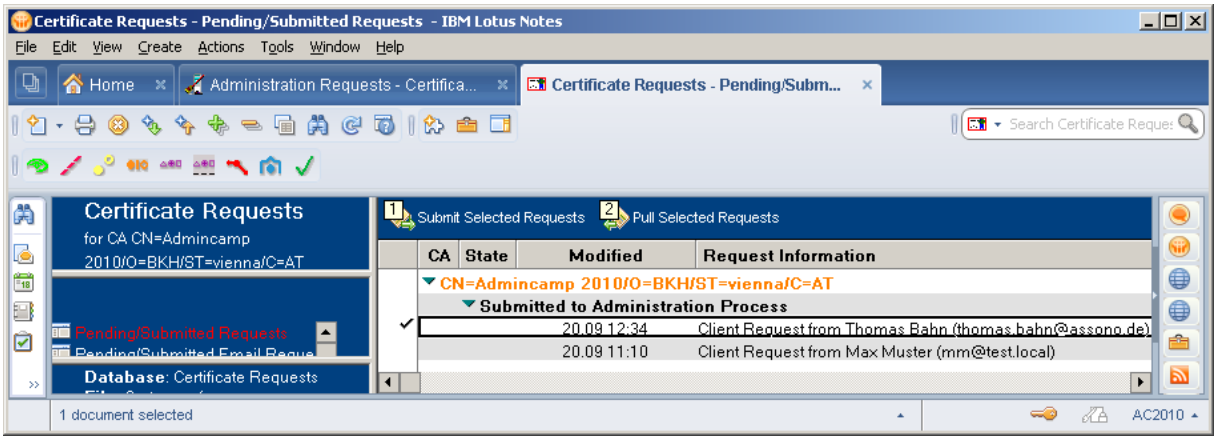


Eintrag editieren

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

8) Zertifikat zum download bereitstellen

In der certreq.nsf den Eintrag selektieren – Pull request

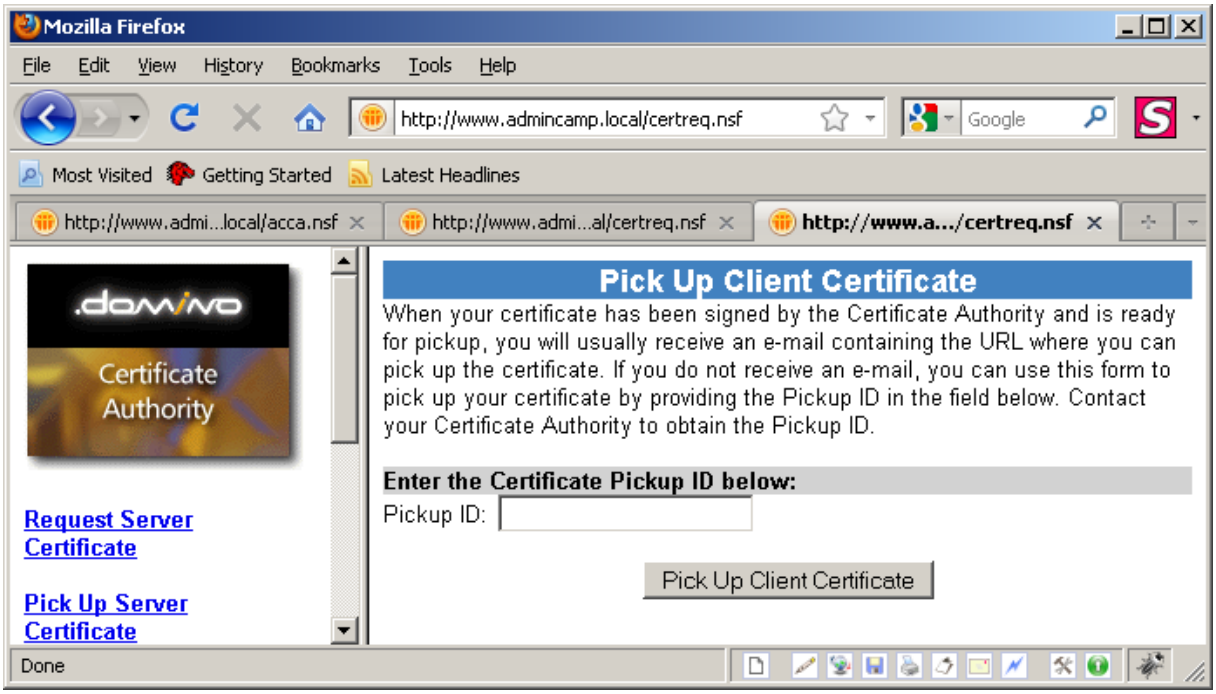


Der Request liegt nun in der View Issued Certificate Requests

Dort den Eintrag öffnen ind die Pickup ID kopieren

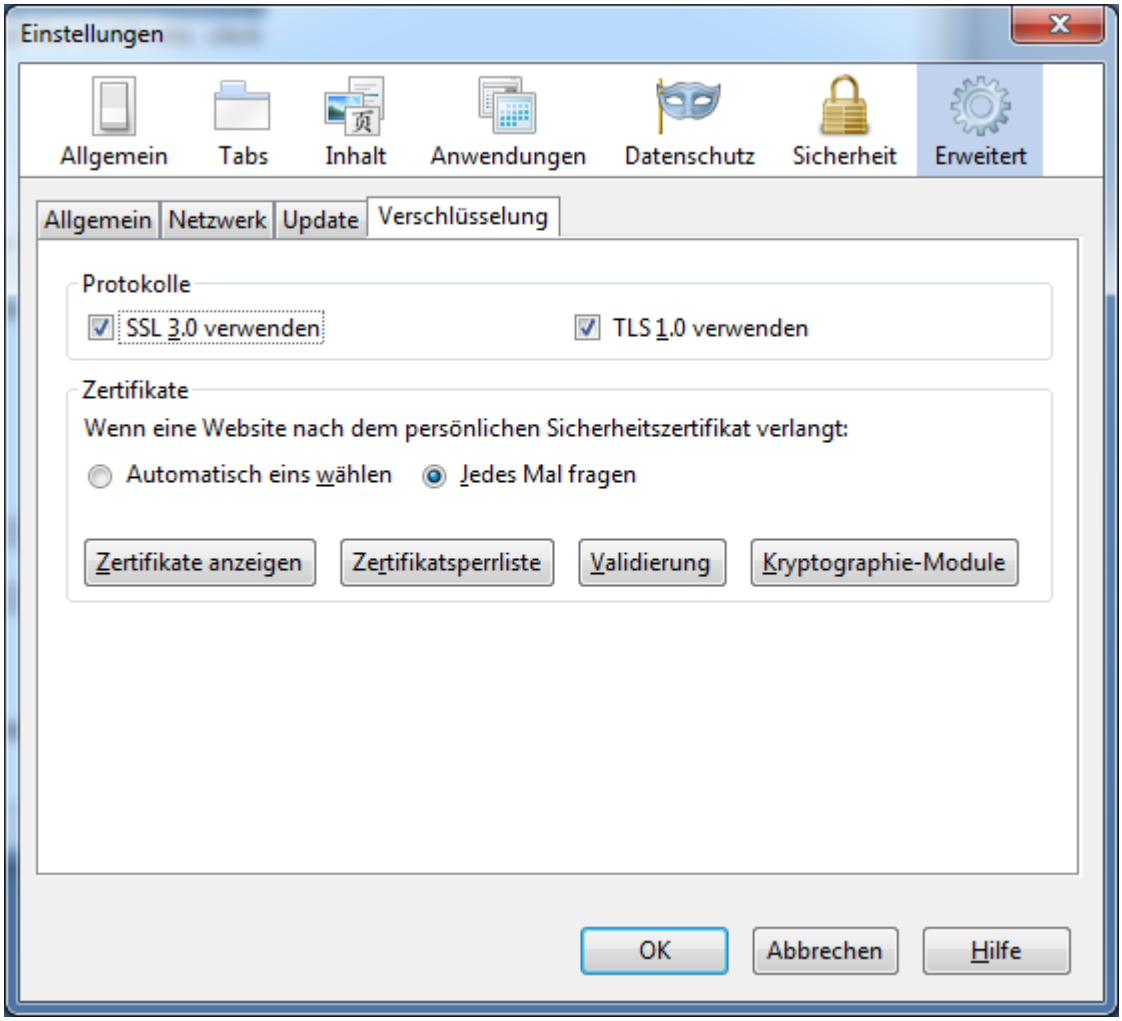
Lab 4: Client Zertifikat installieren

1) Im Firefox das Zertifikat abholen und akzeptieren

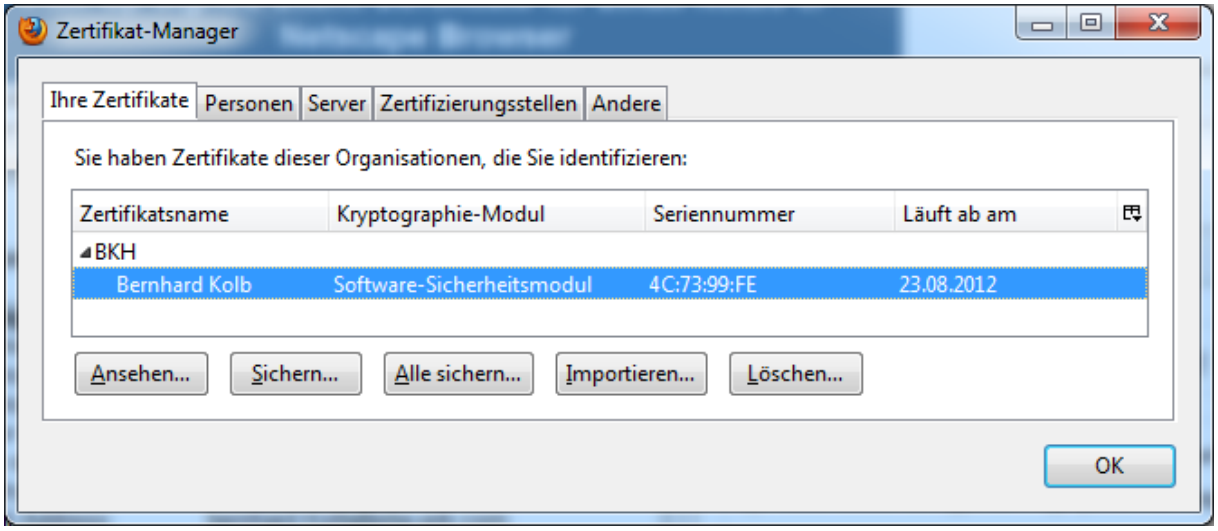


Damit ist das Zertifikat dann im Firefox

2) Exportieren via: Extras – Einstellungen

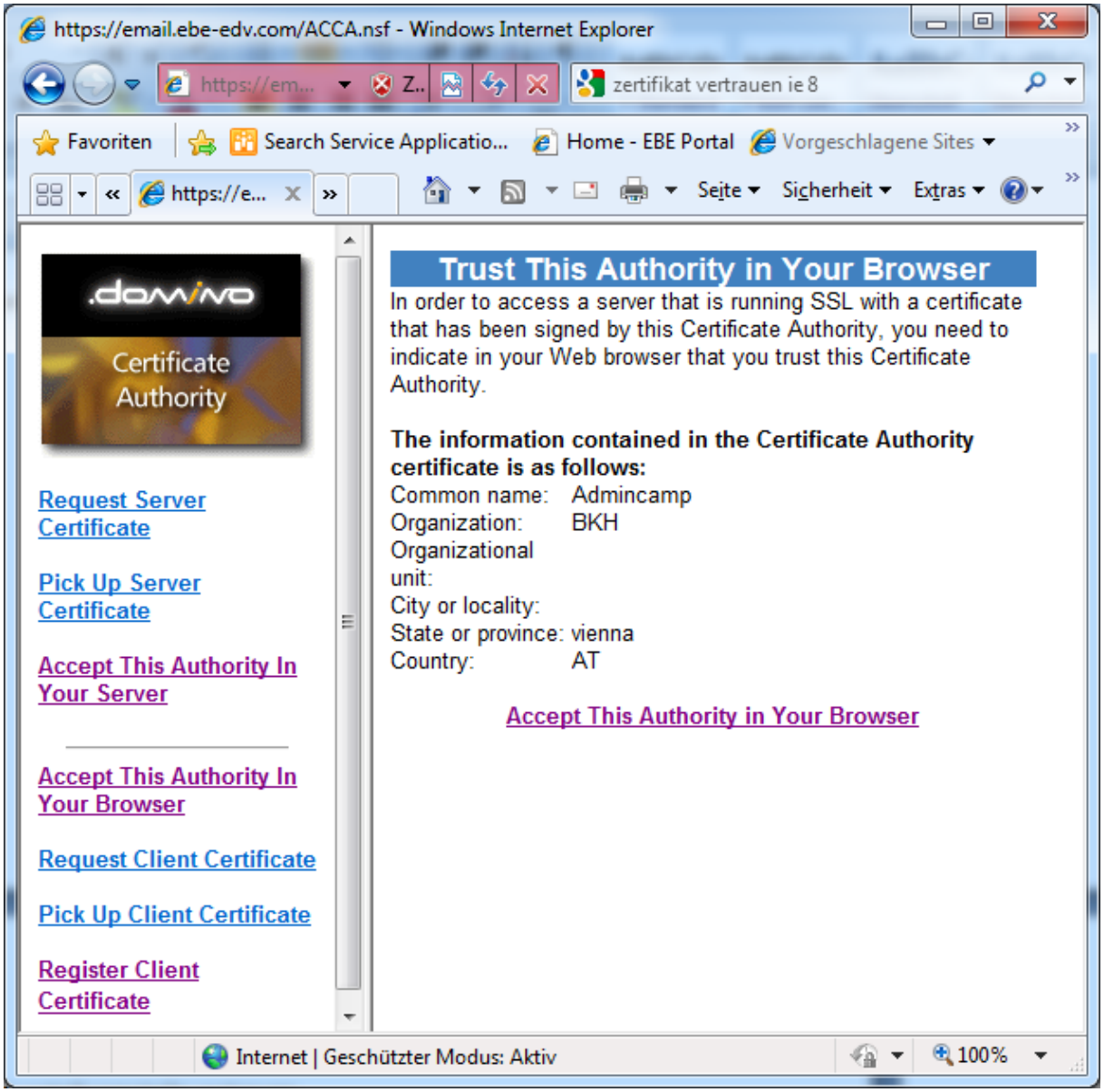


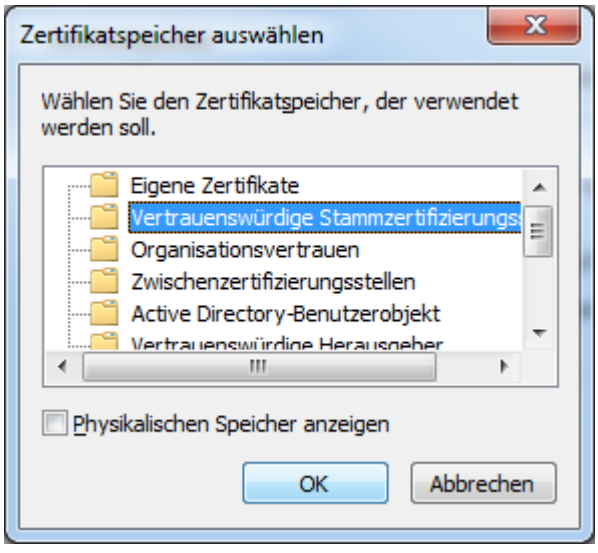
Zertifikate anzeigen -> Sichern



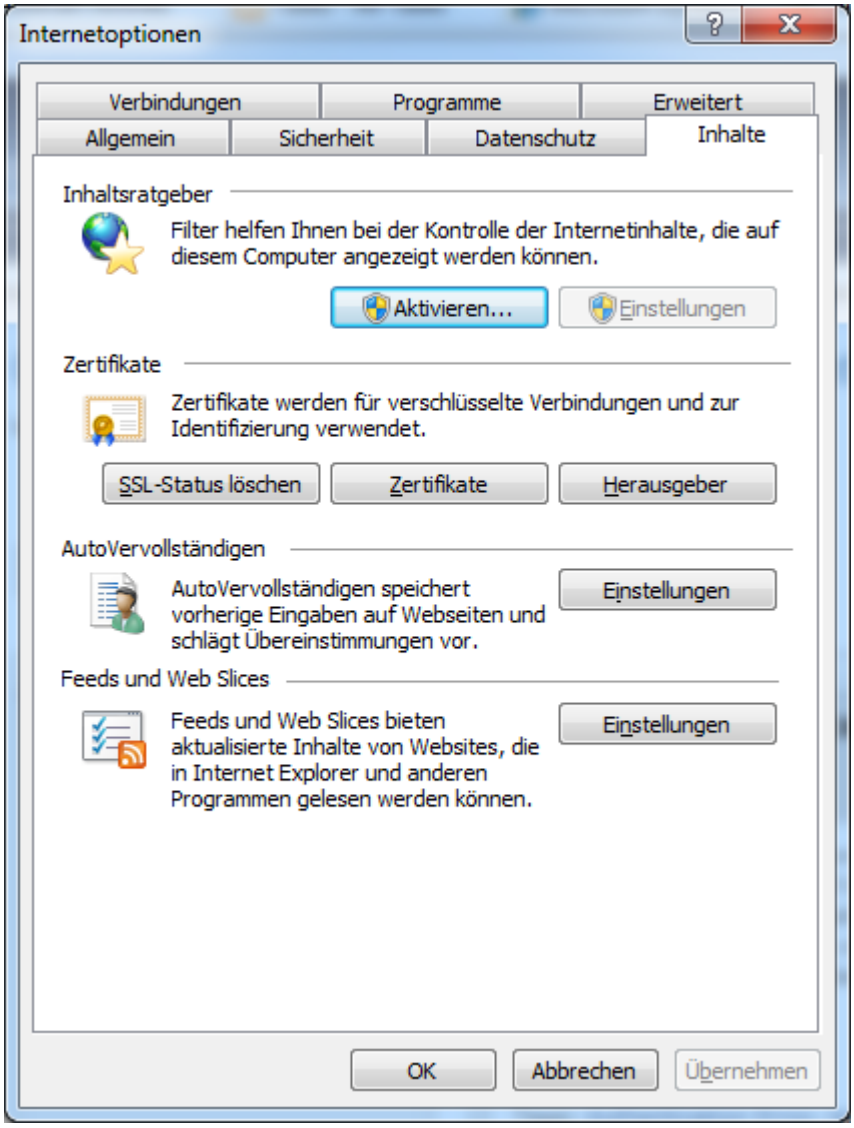
damit wird das Zertifikat (public und Private Key) in eine Datei exportiert

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

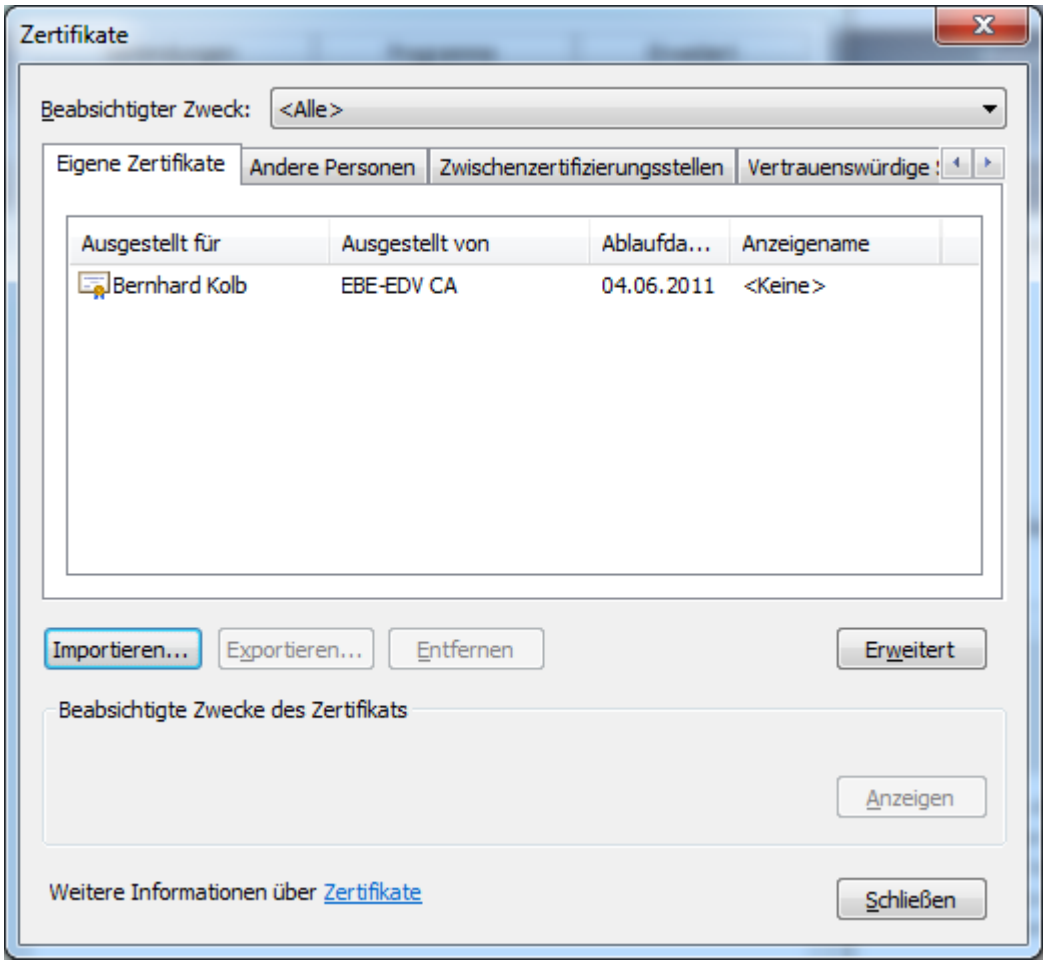




4) In den Internet Explorer importieren

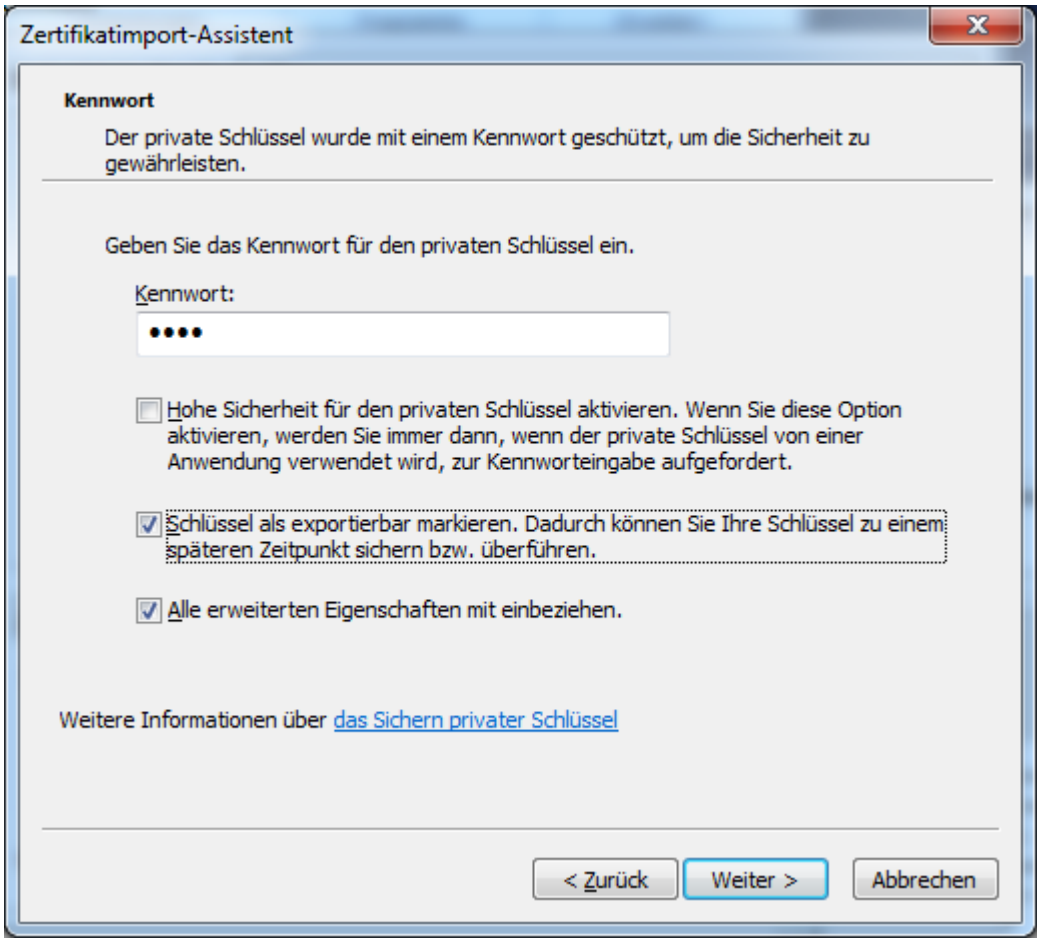


Es müssen die Attribute gesetzt werden – das geht im IE…

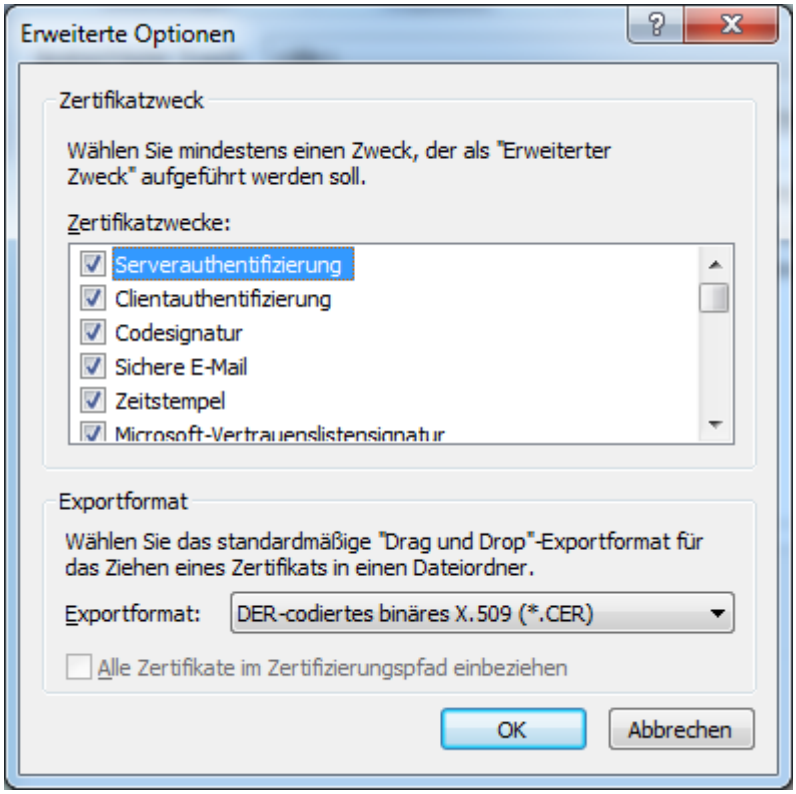


importieren…

wichtig: Schlüssel als exportierbar markieren!

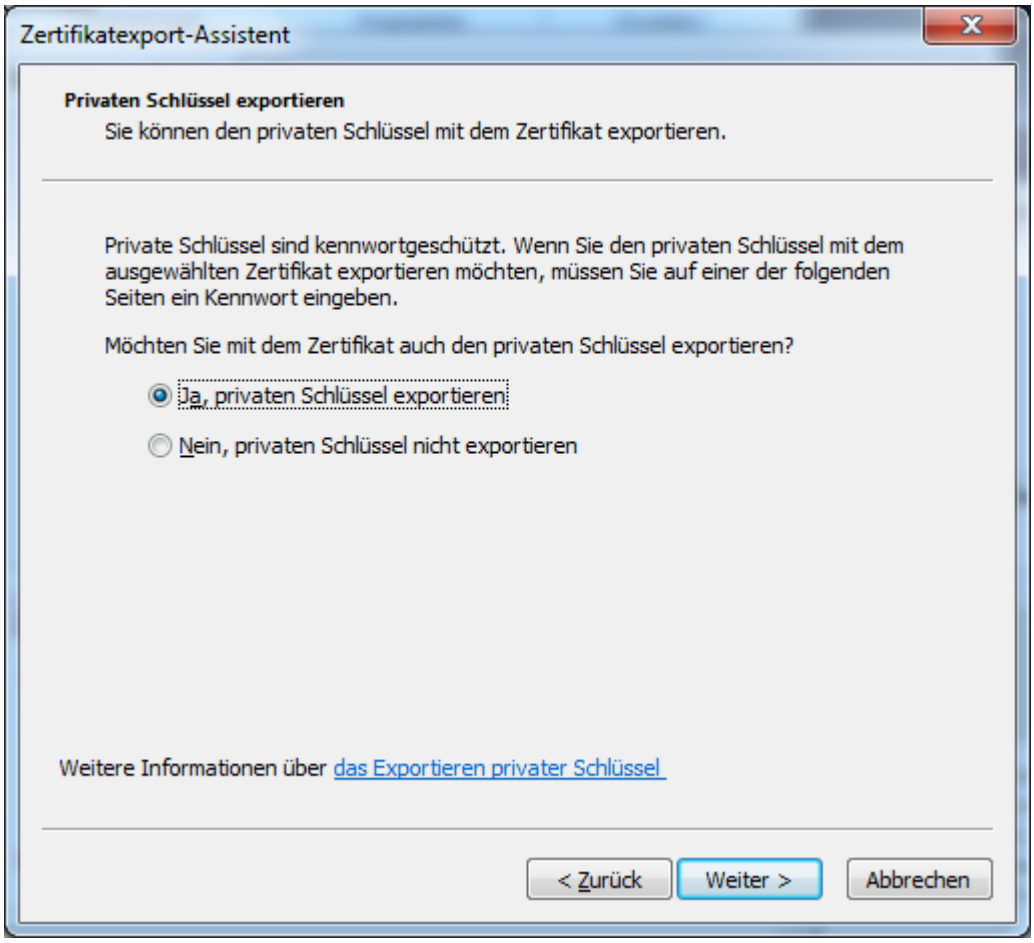


Dann das Zertifikat auswählen – erweitert

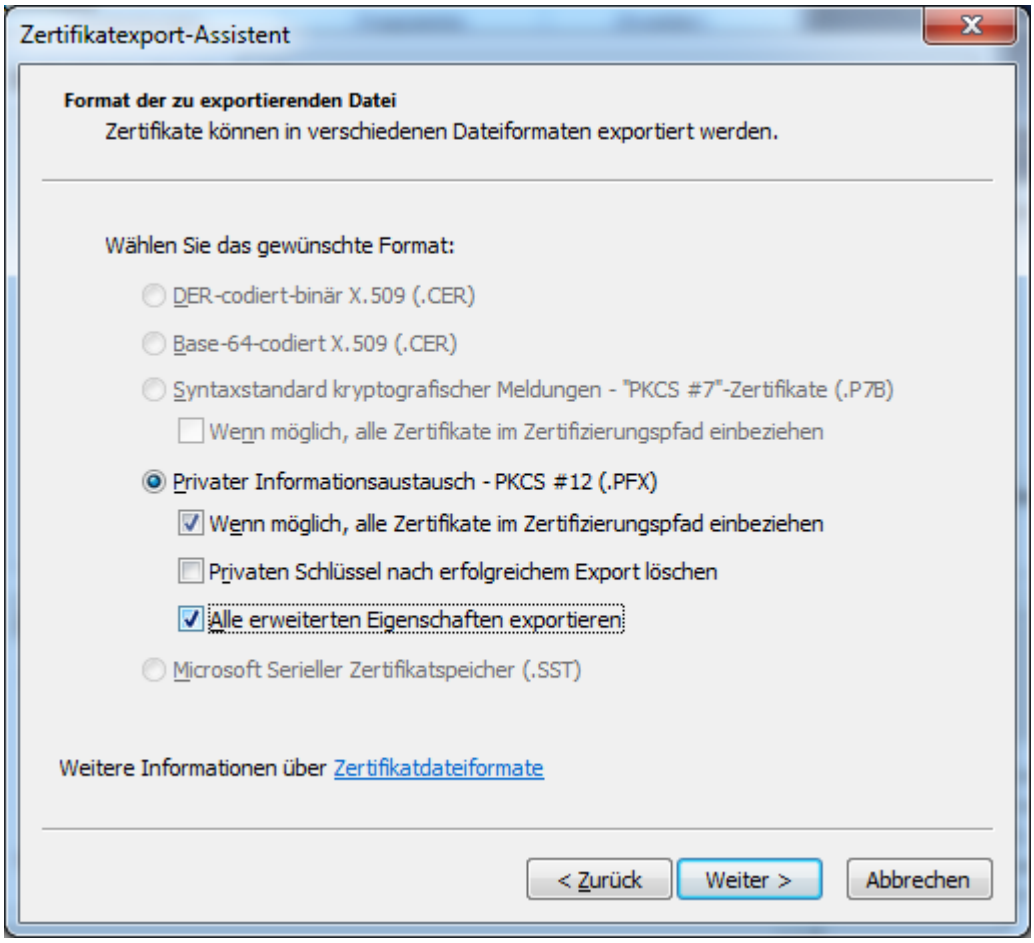


Clientauthentifizierung auswählen und **Sichere-email**

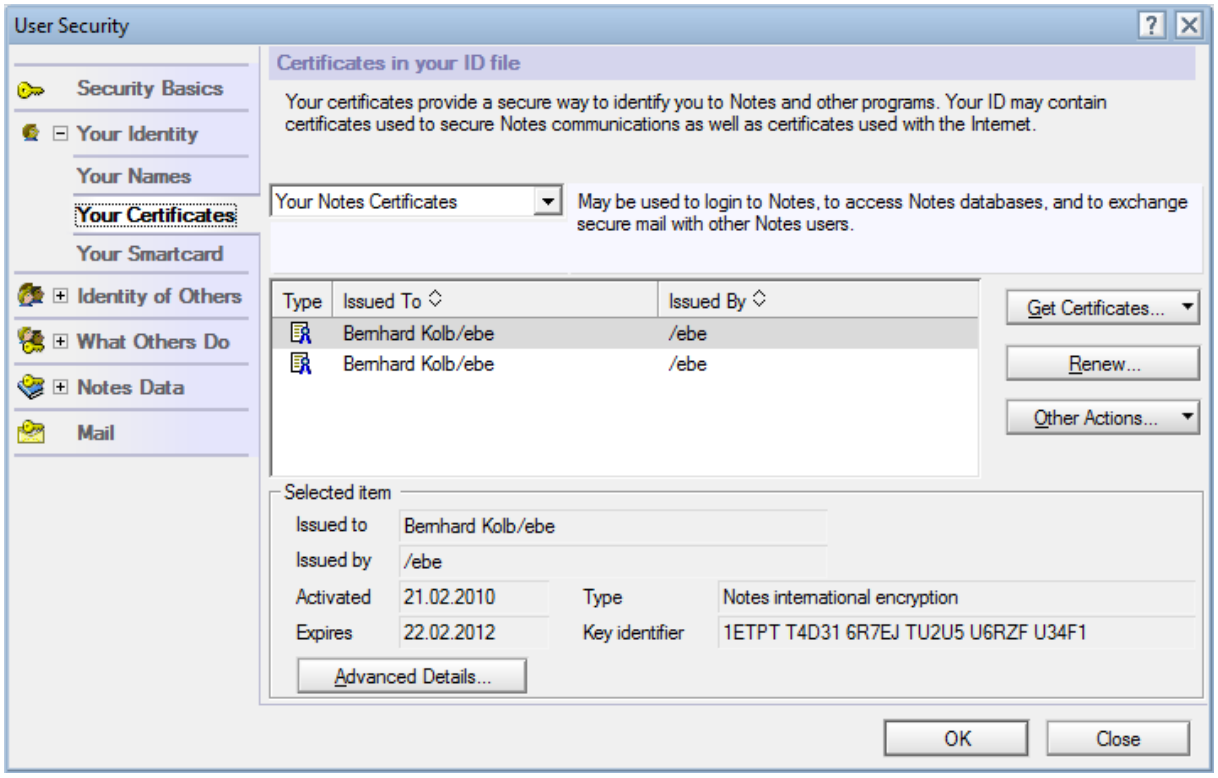
Dann wieder **exportieren.**



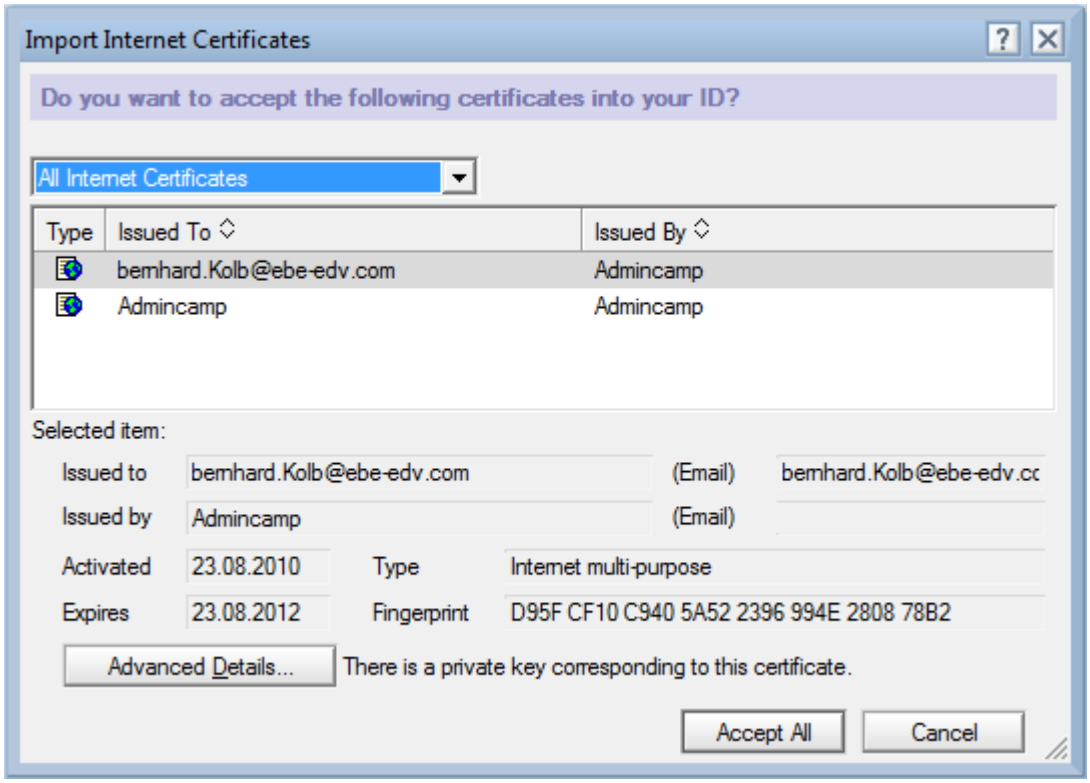
Wichtig: privaten Schlüssel exportieren!



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

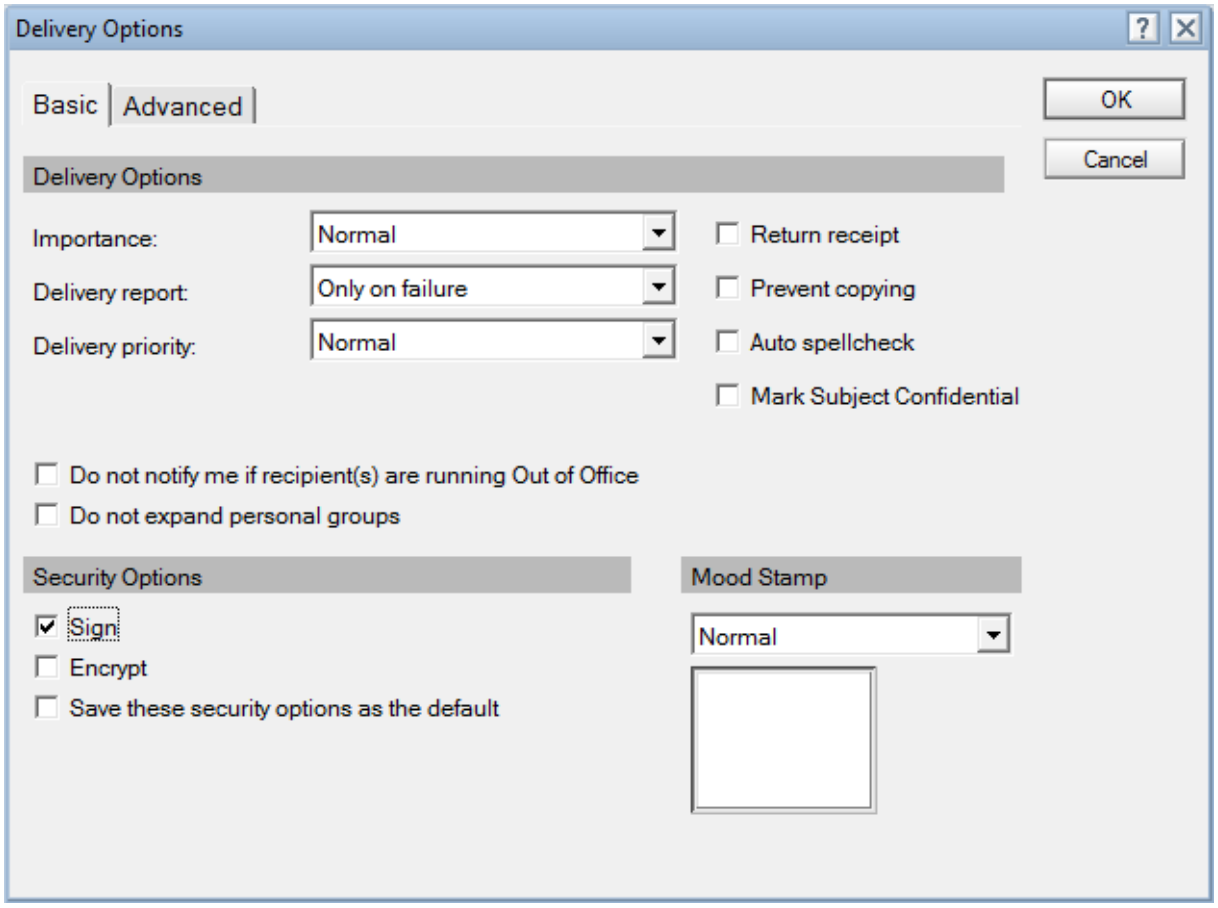


Get Certificates…Import Internet Certificate



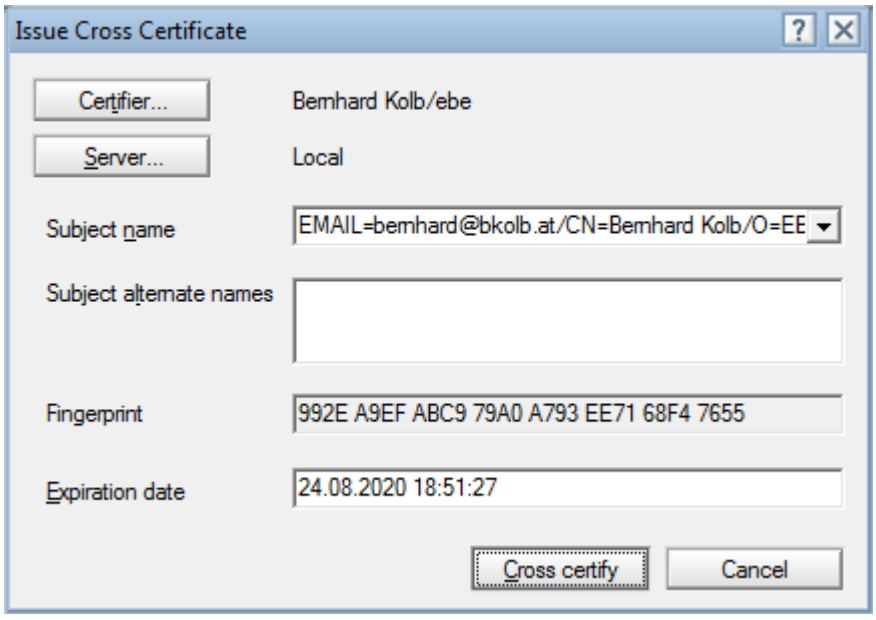
Accept all -> übernimmt das Zertifikat in die Notes ID

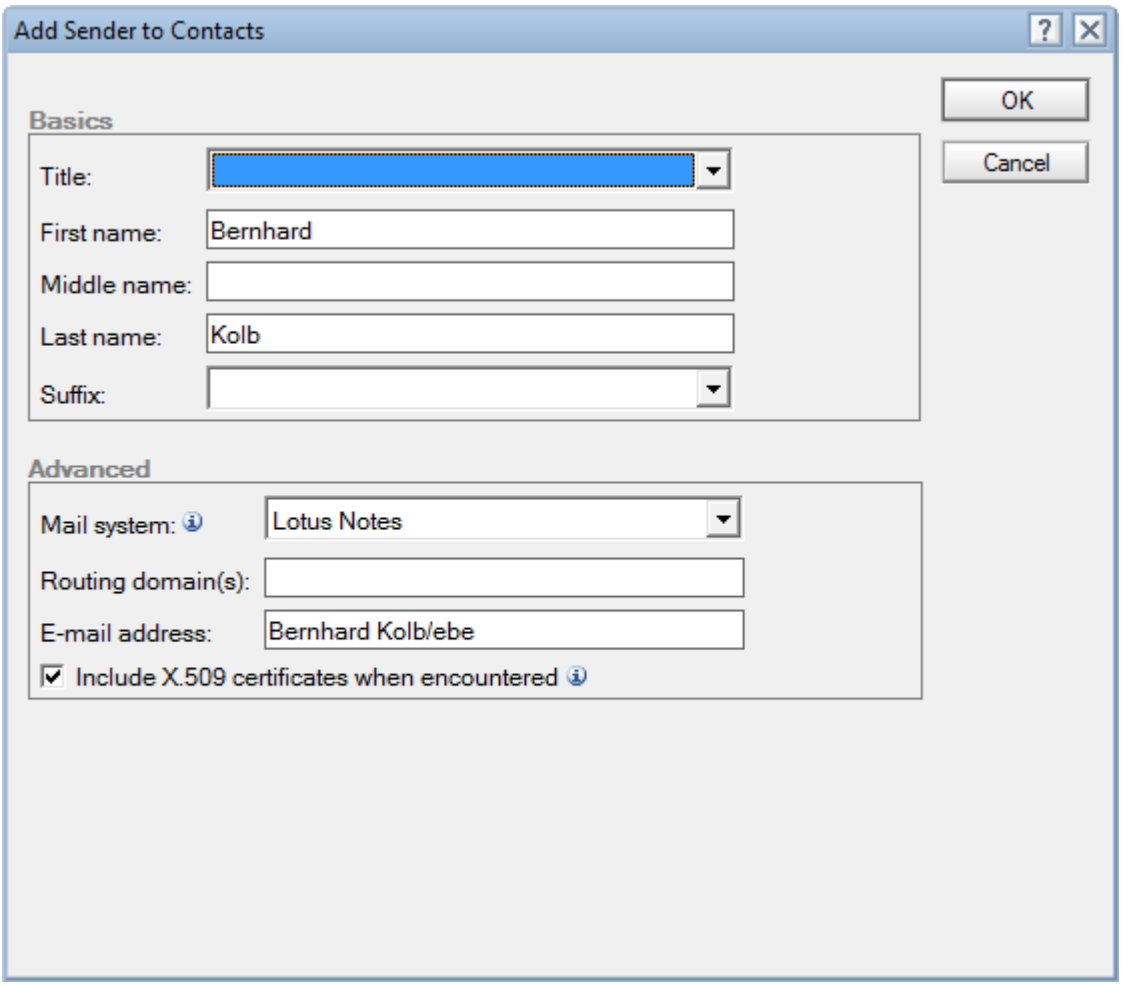
6) Tadaa – fertig! Nun kann man **Mails an Internetuser signieren**



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!





Wichtig: include X.509 certificates!