Sicherheit durch Kryptographie

Sicherheit durch Kryptographie

- Vertraulichkeit
- Integrität
- Authentizität und digitale Signaturen
- Zertifikate

Sicherheit durch PKI

- Schlüsselverwaltung
- Sicherheitsaspekte
  - Woher kommt das Ausstellerzertifikat
  - Ungültige Zertifikate
  - Zertifikatsformate
- Aufgaben einer PKI

Vertraulichkeit

Ziel Nur Befugte können die übermittelten Daten lesen

Methode symmetrische Verschlüsselung

Alice und Bob haben den gleichen Schlüssel

Verfahren DES 3DES AES IDEA Blowfish ...

Problem Schlüsselverteilungsproblem

Sym. Verschlüsselung

Anforderung an Algorithmus und Schlüssel

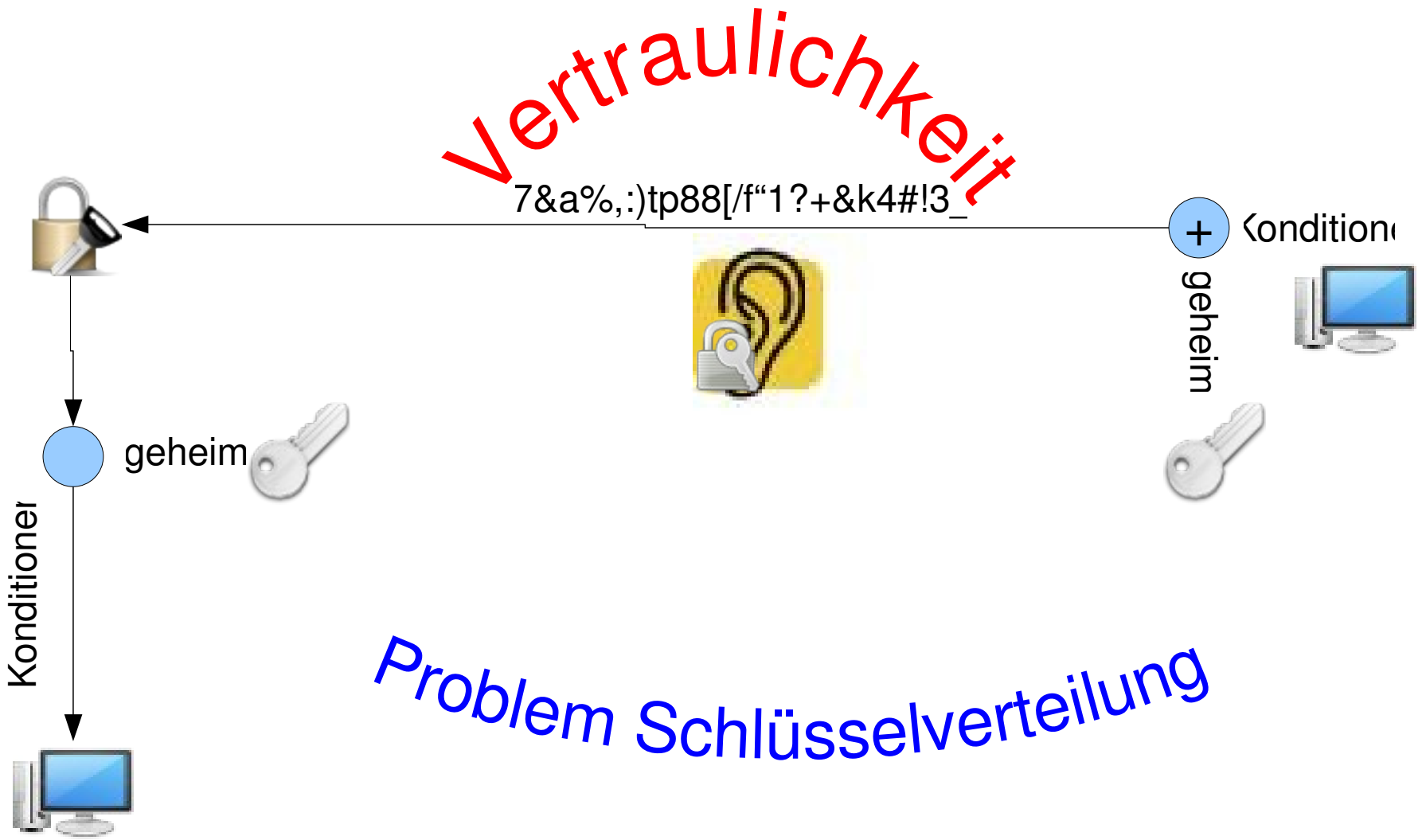
- Algorithmus kann ***nur*** mit Kenntnis des Schlüssels arbeiten
- ***nur*** das Ausprobieren aller Schlüssel führt zu seiner Kenntnis
  („Brute Force Attacke“)

==> der Algorithmus muß bekannt und prüfbar sein

==> Schlüssellänge groß (ab 128 bit, Brute Force langwierig)

Wir machen den Angriff so teuer, daß Aufwand und Nutzen eines Angriffs unverhältnismäßig sind

Alice und Bob



Integrität

Ziel	Die Daten werden bei der Übertragung nicht verändert
Methode	Hashfunktion *Aus den Daten wird eine Zahl errechnet* *(Hashwert, Digest, Fingerprint)*
Verfahren	MD5, SHA, SHA-1, RipeMD160
Problem	Kollision (Hashwert endlich, Daten unendlich)

Hashfunktionen

Anforderung an Hashfunktion und Hashwert

- Hashwert ist eindeutig (z.B. 128-bit Zahl)

Es gibt nicht zwei verschiedene Daten,
die den gleichen Hashwert erzeugen

- Hashfunktion ist unumkehrbar (Einwegfunktion)

Aus dem Hashwert kann nicht auf die Daten zurückgerechnet werden

Alice und Bob

Authentizität

Ziel	Die Daten werden nachprüfbar von einem bestimmbaren Absender gesendet
Methode	Asymmetrische Verschlüsselung *Verwendung zweier Schlüssel* *privatekey + publickey*
Verfahren	RSA, DSA, PGP, GPG
Vorteil	A) Lösung des Schlüsselverteilungsproblems B) digitale Signaturen möglich
Problem	Authentizität des public-keys

Private-Publickey Verfahren

Anforderung an das Verfahren

- Lösung des Schlüsselverteilungsproblems

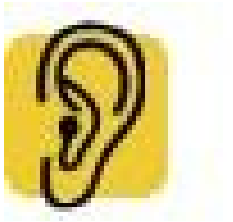
  Mit dem *privatekey* können Daten *entschlüsselt* werden,
  die mit dem *publickey verschlüsselt* wurden

- Digitale Signaturen

  Mit dem *publickey* können Daten *entschlüsselt* werden,
  die mit dem *privatekey verschlüsselt* wurden

Alice und Bob

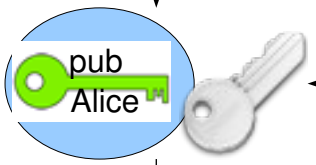
pub Alice



pub Alice

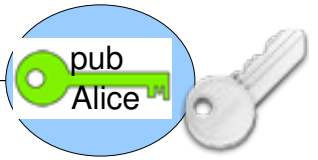
sym-key

= ”geheim“



pub Alice

m;i?e-h#e_g

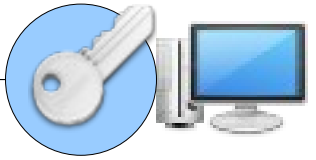


pub Alice

”geheim“

Vertraulichkeit

\7&a%,:)tp88[/f“1?+&k4#3



Konditioner

Lösung Schlüsselverteilung

Alice und Bob

Und wer signiert die public keys ?

Zertifikate

Ziel	Die Bindung eines publickeys an eine Person soll nachprüfbar sein
	Die publickeys werden von einer dritten Instanz durch digitale Signatur beglaubigt
Standards	X509
Vorteil	Lösung des Problems der Authentizität des publickeys
Problem	Schlüsselverwaltung, Zertifikatsformate

Certification Authority CA

certCA

privCA

signCA(pubS)=privCA[MD5(pubS)

pubS
signCA(pubS)
Aussteller (Issuer)
Antragsteller (Subject)
Gültigkeit
Anwendungszweck
.....

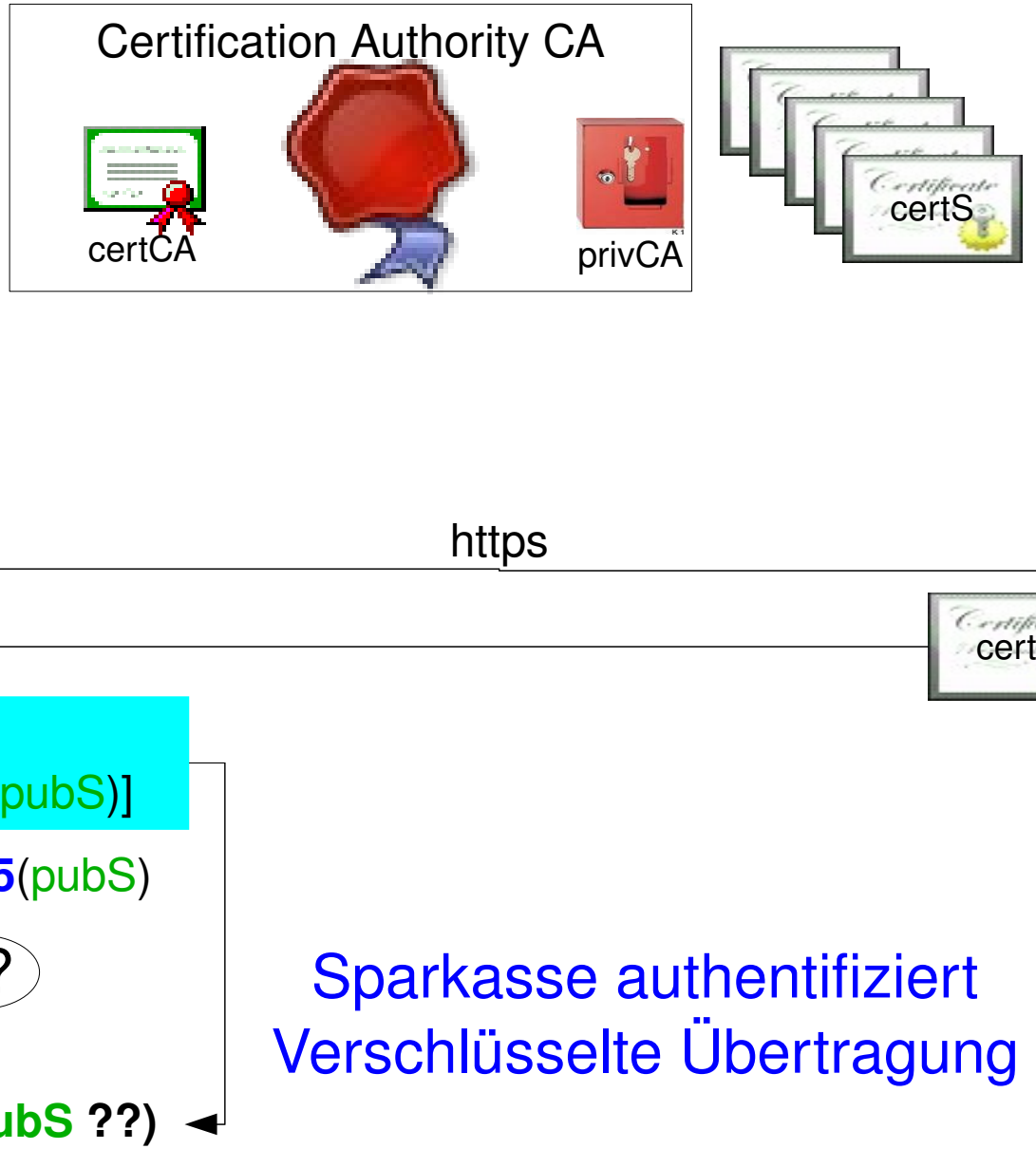
<------ Certificate Signing Request CSR <----

Kunde

Sparkasse

pubS

privS


Certification Authority CA
certCA
privCA
certS
Kunde
Sparkasse
https
certS
pubS ??
privCA[MD5(pubS)]
pubCA
certCA
==> MD5(pubS)
=?
privS
MD5(pubS ??)
Sparkasse authentifiziert
Verschlüsselte Übertragung
Und woher kommt das CA-Zertifikat ?

Schlüsselverwaltung

Anforderung an die Schlüsselverwaltung

- Zertifikatsanforderung verarbeiten

  Certificate Signing Request CSR
- Zertifikate öffentlich zugänglich machen

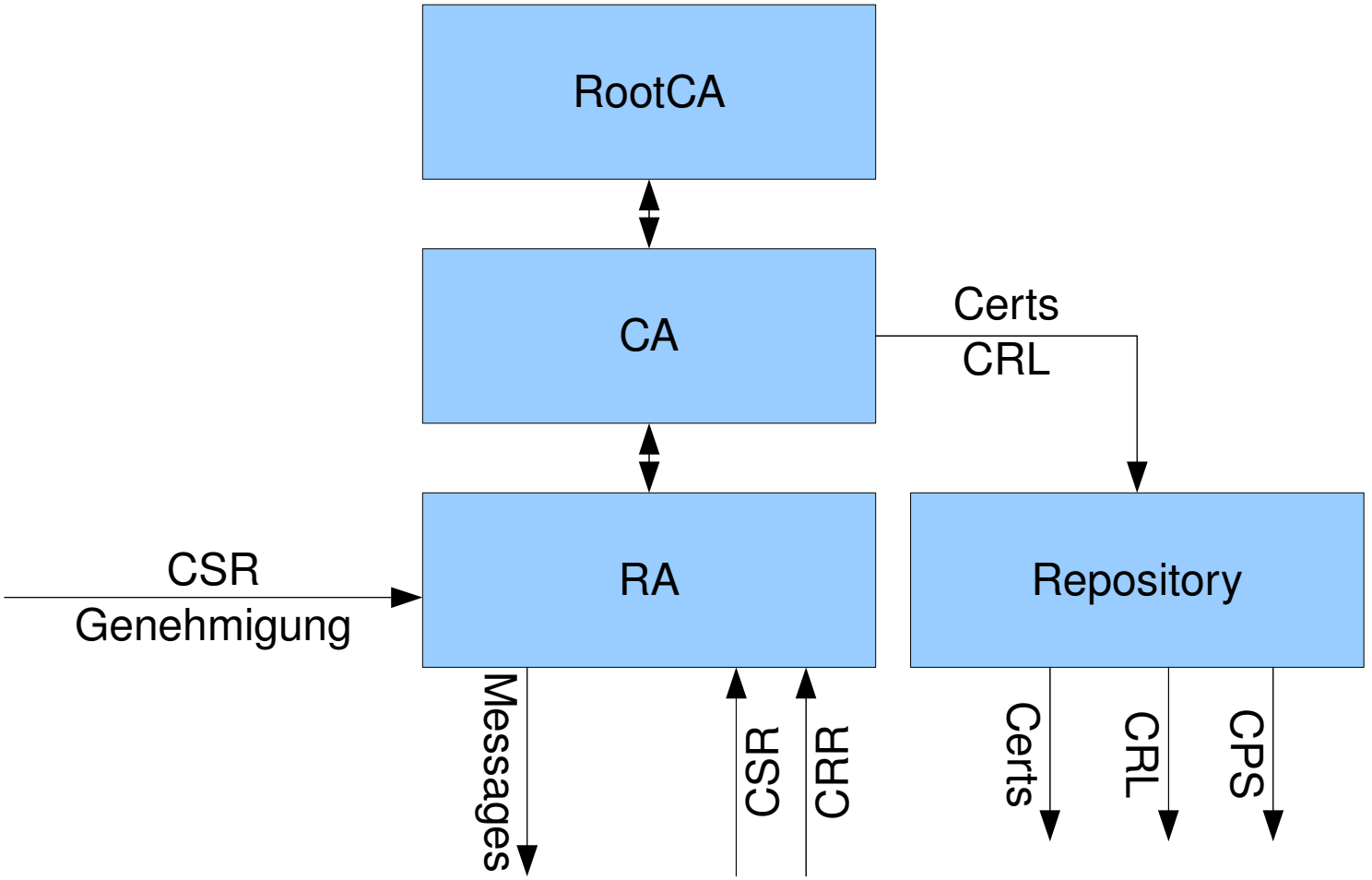
  Certificate Distribution Point CDP
- Widerrufsanträge verarbeiten

  Certificate Revocation Request CRR
- Widerrufslisten öffentlich zugänglich machen

  Certificate Revokation List CRL

- ... Private-Publickey Infrastructure PKI

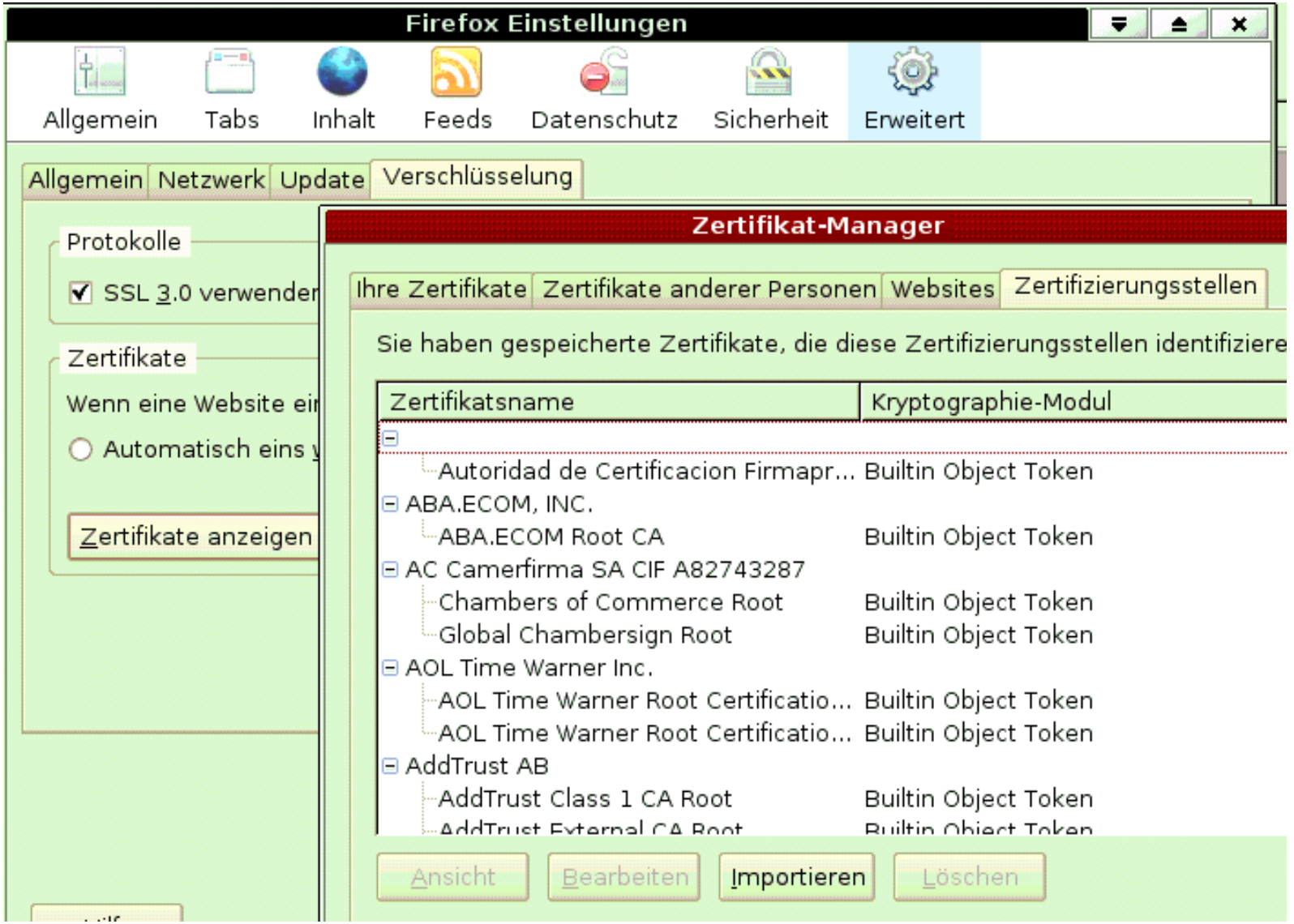
PKI

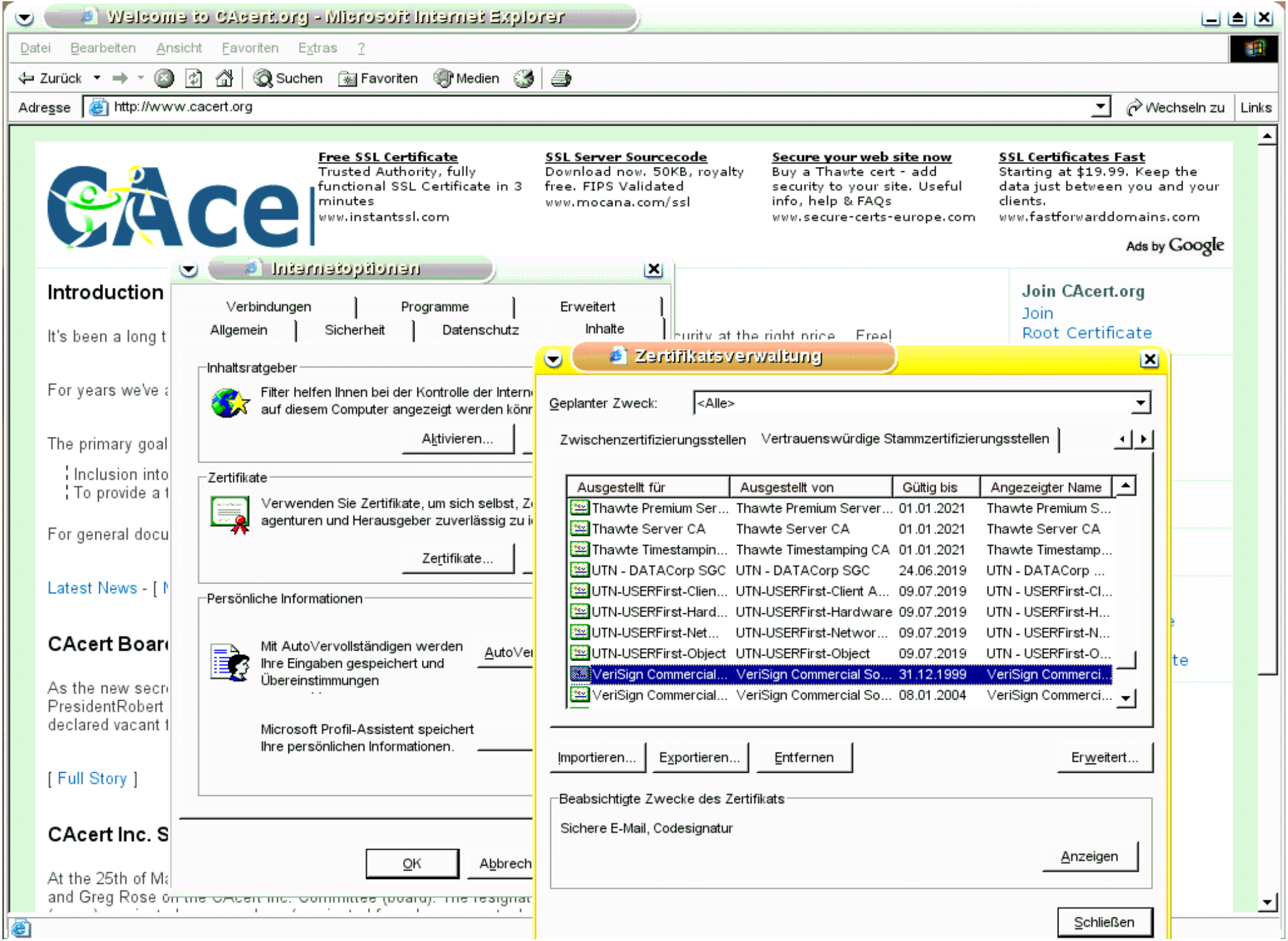


Sicherheitsaspekte

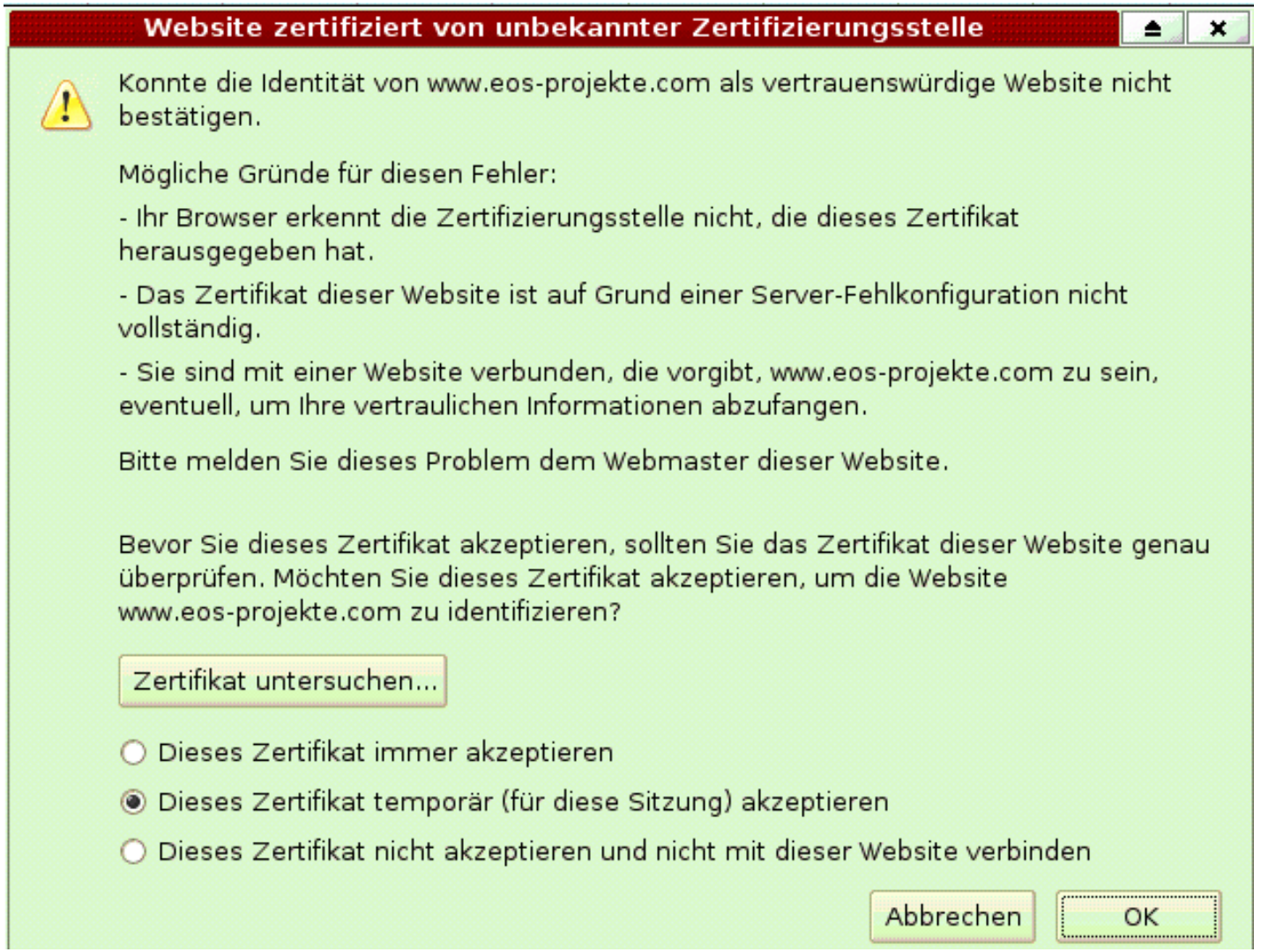
- Woher kommt das Ausstellerzertifikat ?
- Ungültige Zertifikate
  - Ungültige Attribute
  - Zertifikatswiderruf
- Zertifikatsformate

Firefox : Zertifikatsspeicher

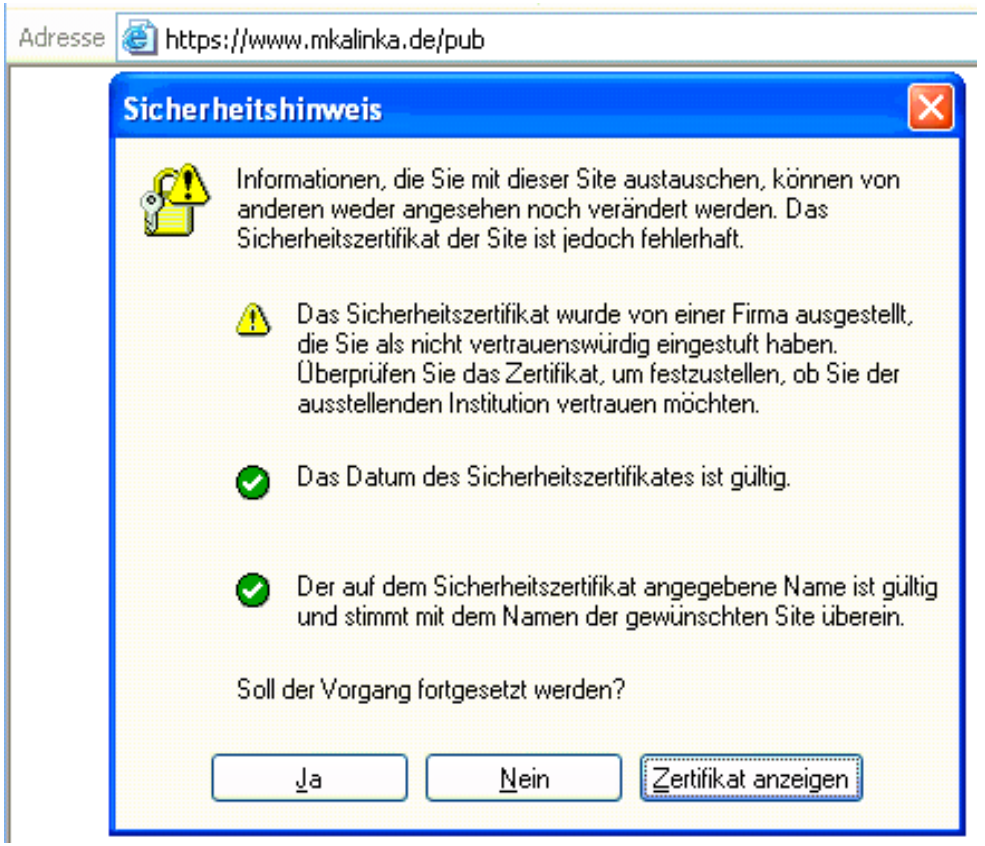



Welcome to CAcert.org - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Medien
Adresse http://www.cacert.org
Wechseln zu Links
Free SSL Certificate
Trusted Authority, fully functional SSL Certificate in 3 minutes
www.instantssl.com
SSL Server Sourcecode
Download now. 50KB, royalty free. FIPS Validated
www.mocana.com/ssl
Secure your web site now
Buy a Thawte cert - add security to your site. Useful info, help & FAQs
www.secure-certs-europe.com
SSL Certificates Fast
Starting at $19.99. Keep the data just between you and your clients.
www.fastforwarddomains.com
Ads by Google
Introduction
Join CAcert.org
Join
Root Certificate
Internetoptionen
Verbindungen
Programme
Erweitert
Allgemein
Sicherheit
Datenschutz
Inhalte
Inhaltsratgeber
Aktivieren...
Zertifikate
Zertifikate...
Persönliche Informationen
Mit AutoVervollständigen werden Ihre Eingaben gespeichert und Übereinstimmungen
Microsoft Profil-Assistent speichert Ihre persönlichen Informationen.
OK
Abbrech
Zertifikatsverwaltung
Geplanter Zweck:
<Alle>
Zwischenzertifizierungsstellen
Vertrauenswürdige Stammzertifizierungsstellen
Ausgestellt für
Ausgestellt von
Gültig bis
Angezeigter Name
Thawte Premium Ser... Thawte Premium Server... 01.01.2021 Thawte Premium S...
Thawte Server CA Thawte Server CA 01.01.2021 Thawte Server CA
Thawte Timestampin... Thawte Timestamping CA 01.01.2021 Thawte Timestamp...
UTN - DATACorp SGC UTN - DATACorp SGC 24.06.2019 UTN - DATACorp ...
UTN-USERFirst-Clien... UTN-USERFirst-Client A... 09.07.2019 UTN - USERFirst-Cl...
UTN-USERFirst-Hard... UTN-USERFirst-Hardware 09.07.2019 UTN - USERFirst-H...
UTN-USERFirst-Net... UTN-USERFirst-Networ... 09.07.2019 UTN - USERFirst-N...
UTN-USERFirst-Object UTN-USERFirst-Object 09.07.2019 UTN - USERFirst-O...
VeriSign Commercial... VeriSign Commercial So... 31.12.1999 VeriSign Commerci...
VeriSign Commercial... VeriSign Commercial So... 08.01.2004 VeriSign Commerci...
Importieren...
Exportieren...
Entfernen
Erweitert...
Beabsichtigte Zwecke des Zertifikats
Sichere E-Mail, Codesignatur
Anzeigen
Schließen
Latest News - [M
CAcert Boar
As the new secr
PresidentRobert
declared vacant t
[Full Story]
CAcert Inc. S
At the 25th of Ma
and Greg Rose

Kein CA-Zertifikat : Firefox



IE6 : kein CA-Zert.



Zertifikatsinhalte

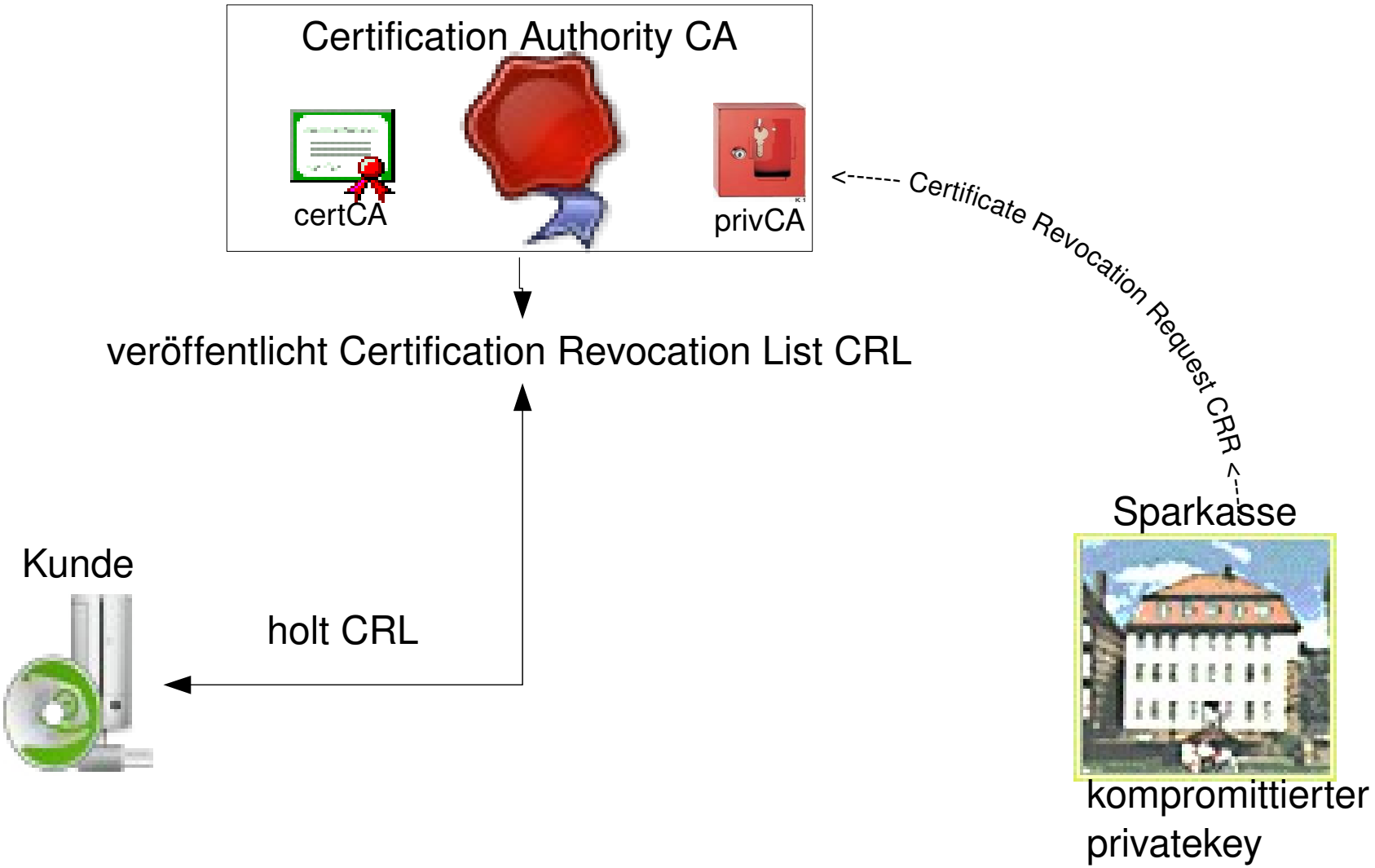
Certificate:
Data:
Version: 3 (0x2)
Serial Number: f5:17:fd:42:cd:d4:7d:ea
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=DE, O=MKalinka ITB, OU=MKalinka ITB CA,
CN=Michael Kalinka/emailAddress=camanager@mkalinka.de
Validity Not Before: Apr 15 17:38:00 2007 GMT
Not After : Apr 12 17:38:00 2017 GMT
Subject: C=DE, O=MKalinka ITB, OU=MKalinka ITB CA,
CN=Michael Kalinka/emailAddress=camanager@mkalinka.de
Subject Public Key Info: Public Key Algorithm: rsaEncryption
RSA Public Key: (4096 bit)
Modulus (4096 bit): 00:c3:a3:44:ce:bf:be:b7:1e:d9: [...] a3:7c:c9
Exponent: 65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption
2a:3d:79:8d:90:a4:77:b7:0d:3e:61:ab:88:cd:36:db:0f:b8:
[...]
42:86:2d:2c:f2:61:bf:7b

Zertifikatsinhalte (v3-Extensions)

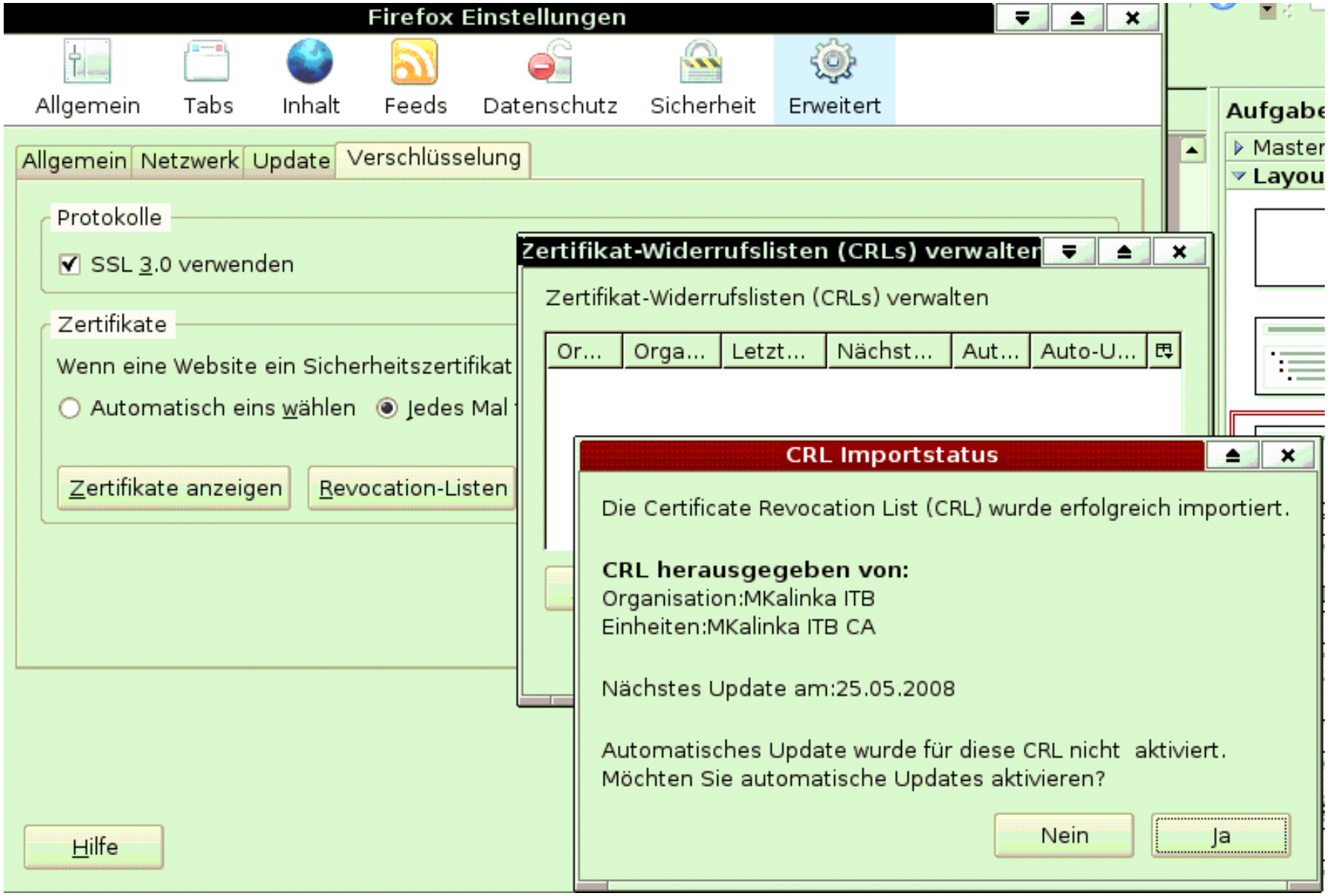
X509v3 extensions:

X509v3 Basic Constraints: critical	CA:TRUE
X509v3 Subject Key Identifier:	26:AD:52:[...]:F5:5B:33:EE:4B:24:57:7C
X509v3 Authority Key Identifier:	[...]
X509v3 Key Usage:	Certificate Sign, CRL Sign
X509v3 Subject Alternative Name:	email:camanager@mkalinka.de
X509v3 Issuer Alternative Name:	email:camanager@mkalinka.de
Netscape Cert Type:	SSL CA, S/MIME CA, Object Signing CA
Netscape Comment:	Certification Authority Certificate
X509v3 CRL Distribution Points:	URI:http://www.mkalinka.de/pub/crl/cacrl.crl
Netscape CA Revocation Url:	http://www.mkalinka.de/pub/crl/cacrl.crl
Netscape Revocation Url:	http://www.mkalinka.de/pub/crl/cacrl.crl

Zertifikatswiderruf



Firefox : CRL manuell



Firefox : CRL automatisch

Sinn : im Moment der Zertifikatsverifikation wird beim Aussteller
die aktuelle Gültigkeit des Zertifikats nachgefragt
O nline **C** ertificate **S** tatus **P** rotokoll

Zertifikatsformate

- PEM (Privacy Enhancement for El. Mail)
  - ASCII-Format, base64-codiert.
  - .pem-Datei enthält meist nur Zertifikat
- p12
  - Binärformat mit priv.+publickey, verschlüsselt
  - Standardaustauschformat (M$: pfx)
- DER (Distinguished Encoding Rules)
  - Binärformat, meist für CRLs

Konvertierung

- PEM to p12
  - `openssl pkcs12 -export -in cert.pem -inkey key.pem -out cert_key.p12`
- p12 to PEM
  - `openssl pkcs12 -in cert_key.p12 -out cert_key.pem`
- PEM to DER
  - `openssl x509 -in cert.pem -outform der -out cert.der`
- PFX to p12 (Microsoft-proprietär)
  - `cp cert_key.pfx cert_key.p12`

Literatur

Bücher	Author	Verlag	Jahr	Bezug
Kryptographie Verfahren, Protokolle, Infrastrukturen	Klaus Schmeh	dpunkt	2007 3. Auflage	ISBN 3-89864-435-9
Kryptographie RSA Security's Official Guide	Steve Burnett Stephen Paine	RSA Press	2001	ISBN 3-8266-0780-5
Angewandte Kryptographie Applied Cryptography	Bruce Schneier	Addison Wesley	2006	ISBN 3-8273-7228-3

Tutorials

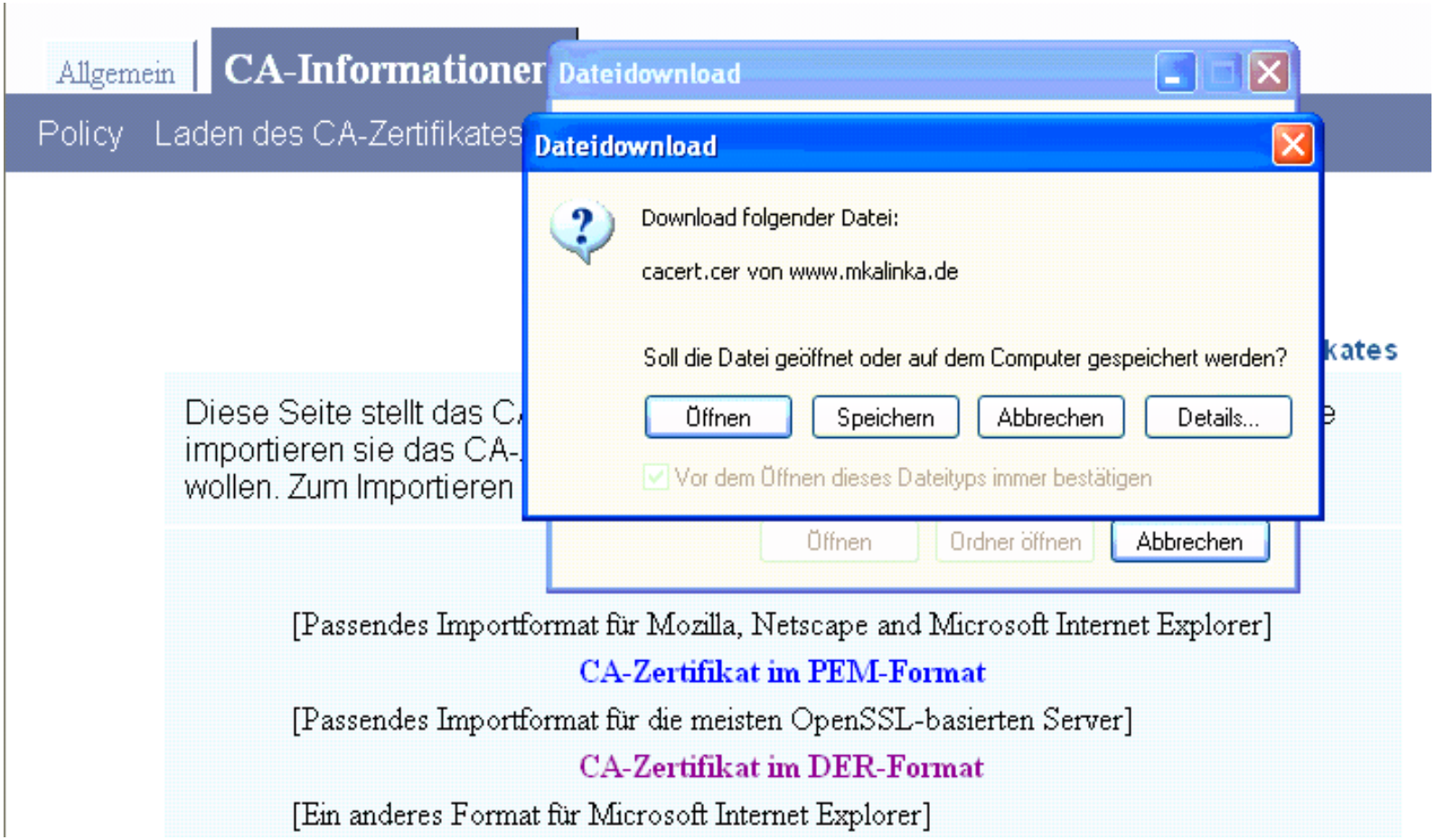
Cryptolounge	Christian Thöing	- online -	http://cryptolounge.de.vu
CA-Handbuch DFN-CERT	http://www.dfn-cert.de/informationen/themen/verschluesselung_und_pki/ca-handbuch.pdf		
OpenCA-Guide	https://www.openca.org/projects/openca/docs/openca-guide.pdf		
BSI Kurzinfo	http://www.bsi.bund.de/literat/faltbl/F10ElektronischeSignatur.htm#2		

Gesetze/Standards

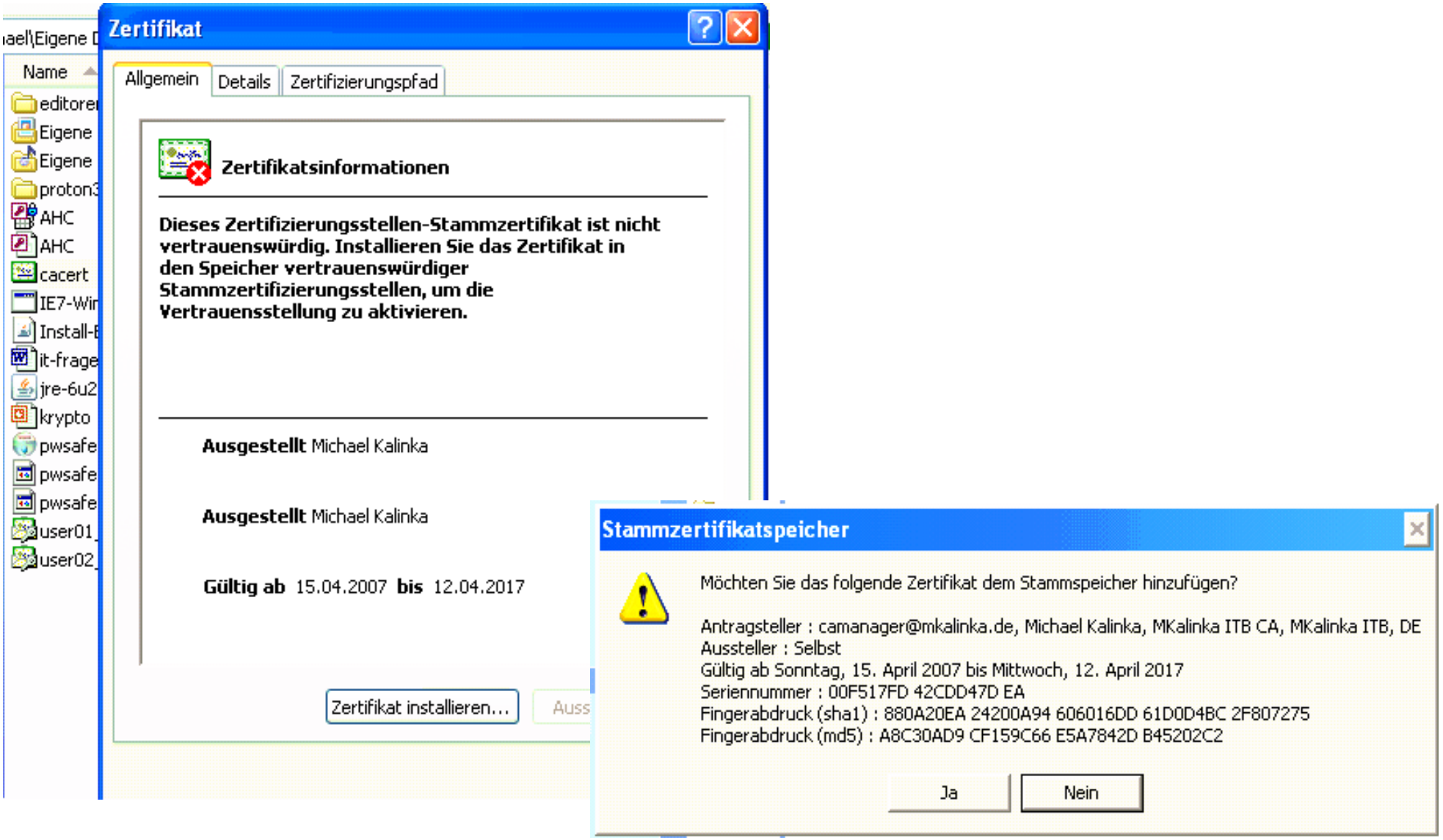
Signaturgesetz SigG (IUKDG)	http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf		
Signaturverordnung SigV	http://www.gesetze-im-internet.de/bundesrecht/sigv_2001/gesamt.pdf		
EU-Richtlinie 1999/93/EG – el. Signaturen	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:013:0012:0020:DE:PDF		
EU-Bericht	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0120:FIN:DE:PDF		
RFC 5280 X.509 PKI Cert+CRL Profile	Cooper et.al.		2008	http://www.rfc-editor.org

Michael Kalinka	http://www.mkalinka.de	Kurse -> Kursmaterial Kurse -> Kryptographie

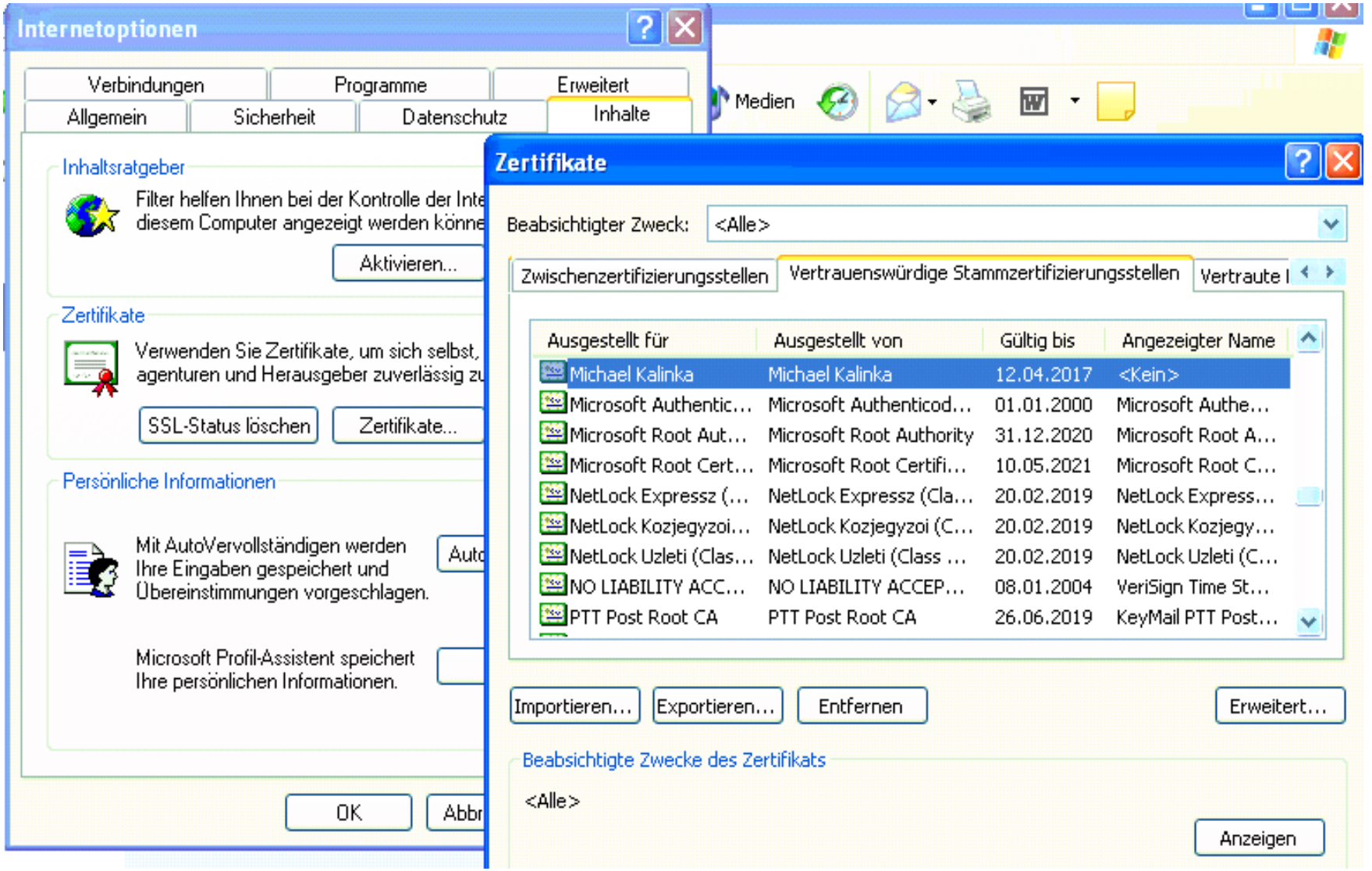
CA-Zert download



CA-Zert installieren



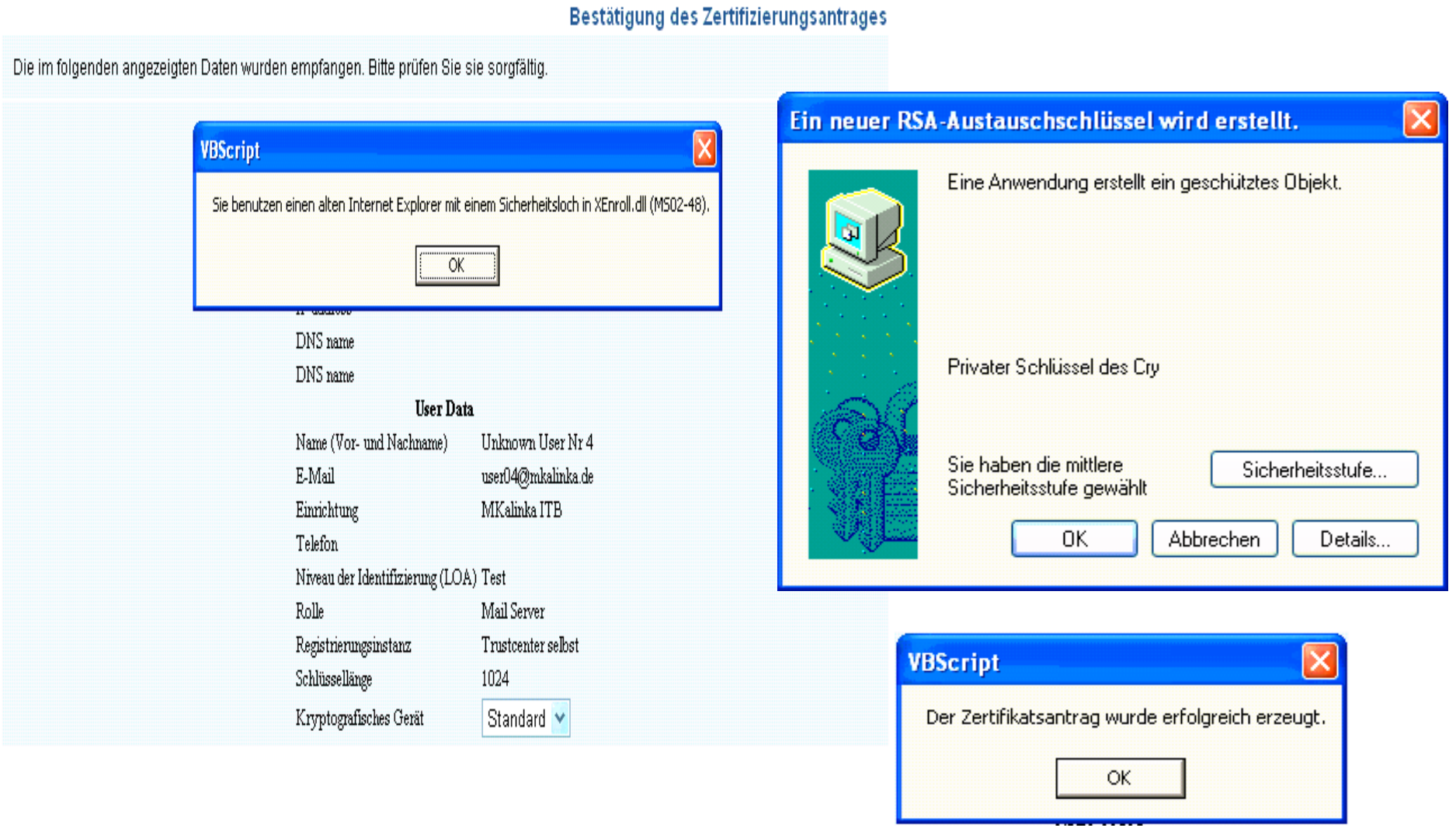
Wo ist das CA-Zert ?



IE6 : CSR erstellen

IE6 CSR Daten

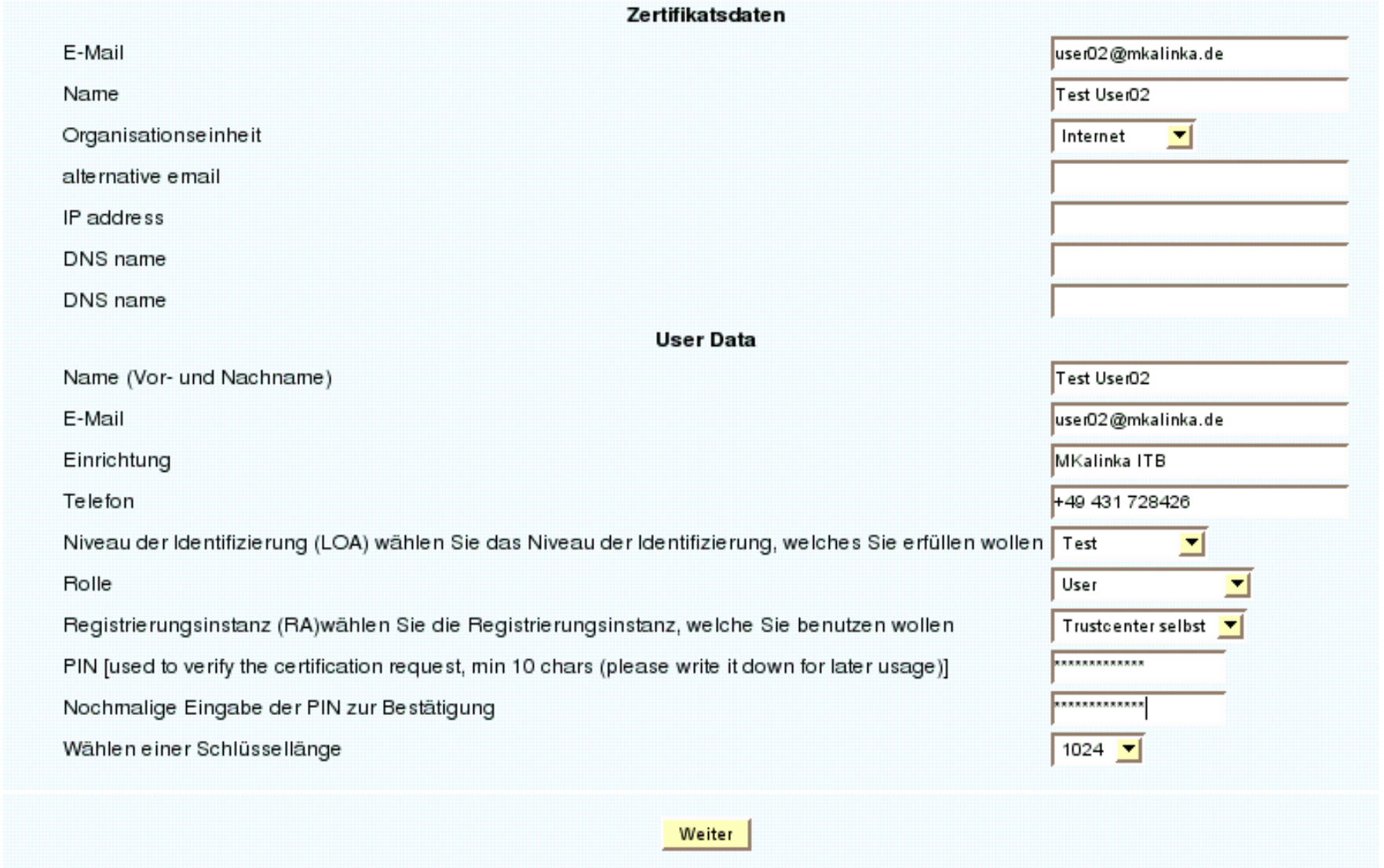
IE6 CSR privatekey



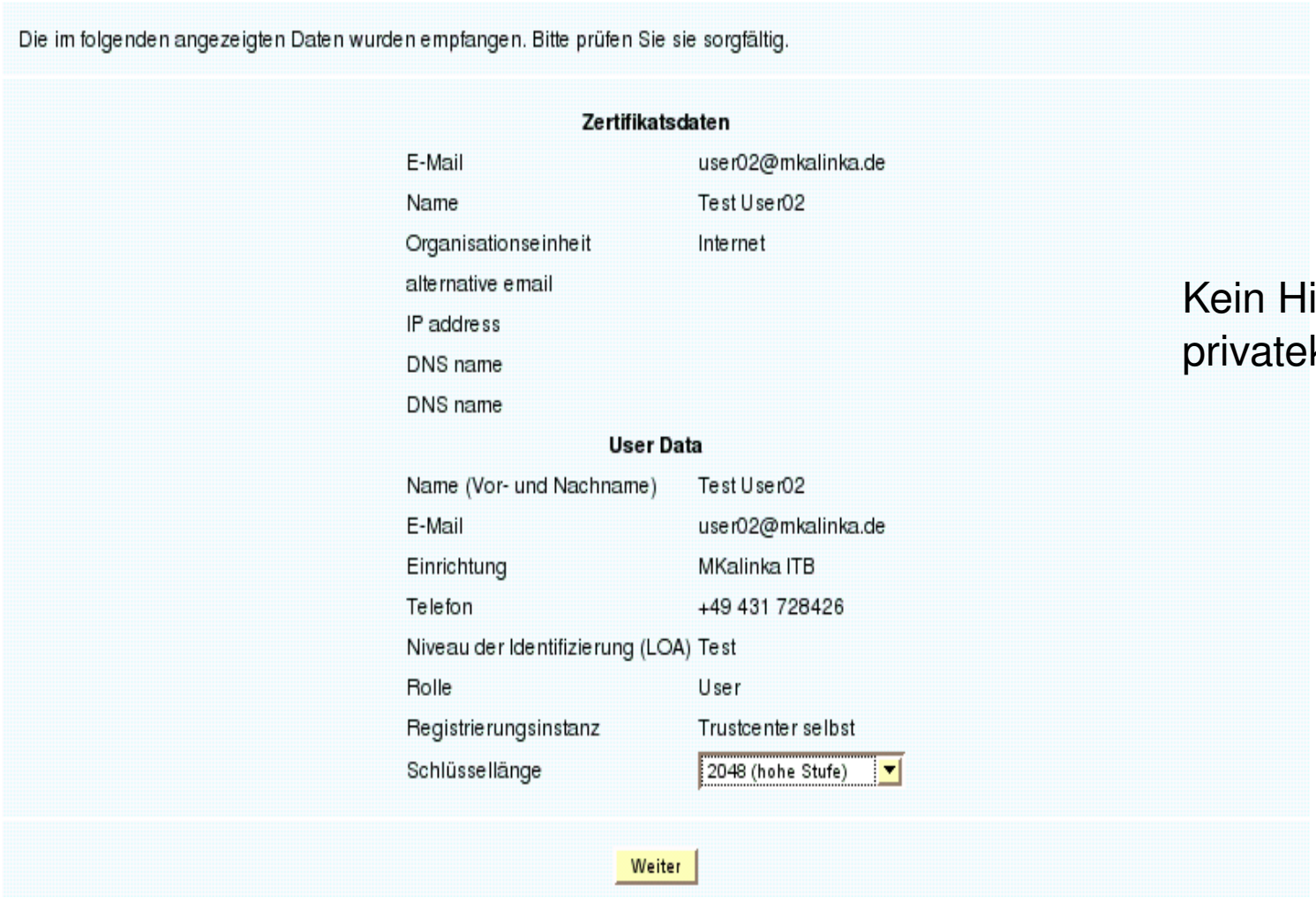
Firefox CSR


OpenCA - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe
https://www.mkalinka.de/cgi-bin/pub/pki?cmd=getSt
Google
Allgemein
CA-Informationen
Nutzer
Zertifikate
Anträge
Language
Beantragen eines Zertifikates
Laden des beantragten Zertifikates
Test Certificate
Zertifikat zurückrufen
Beantragen eines Zertifikates
Zum Erstellen eines Zertifzierungsantrages benutzen Sie einen der folgenden Links. Sie werden aufgefordert ein Formluar auszufüllen und die eingegebenen Daten zu bestätigen Wenn Sie den Antrag vervollständigt und abgesendet haben, müssen Sie zu einer RA Ihrer Wahl gehen, um die Zertifizierung abzuschließen.
Beantragen eines Zertifikates mit automatischer Browsererkennung
[Benutzen Sie diesen Link, wenn Sie nicht wissen, was Sie tun sollen]
Allgemeiner Zertifzierungsantrag
[Serverseitige Schlüssel- und Antragserstellung]
Antrag für einen Hardwaretoken
[Beantragen eines Hardwaretokens von der Registrierungsinstanz]
Netscape-Zertifizierungsantrag
[Zertifizierungsantrag für Browser - SPKAC]
Zertifizierungsantrag für Internet Explorer
[Zertifizierungsantrag für Browser - Microsoft]
Zertifzierungsantrag für Server
[PEM-formatierter PKCS#10-Antrag]
Fertig
www.mkalinka.de

Firefox CSR Daten



Firefox CSR absenden


Die im folgenden angezeigten Daten wurden empfangen. Bitte prüfen Sie sie sorgfältig.

Zertifikatsdaten

E-Mail	user02@mkalinka.de
Name	Test User02
Organisationseinheit	Internet
alternative email	
IP address	
DNS name	
DNS name	

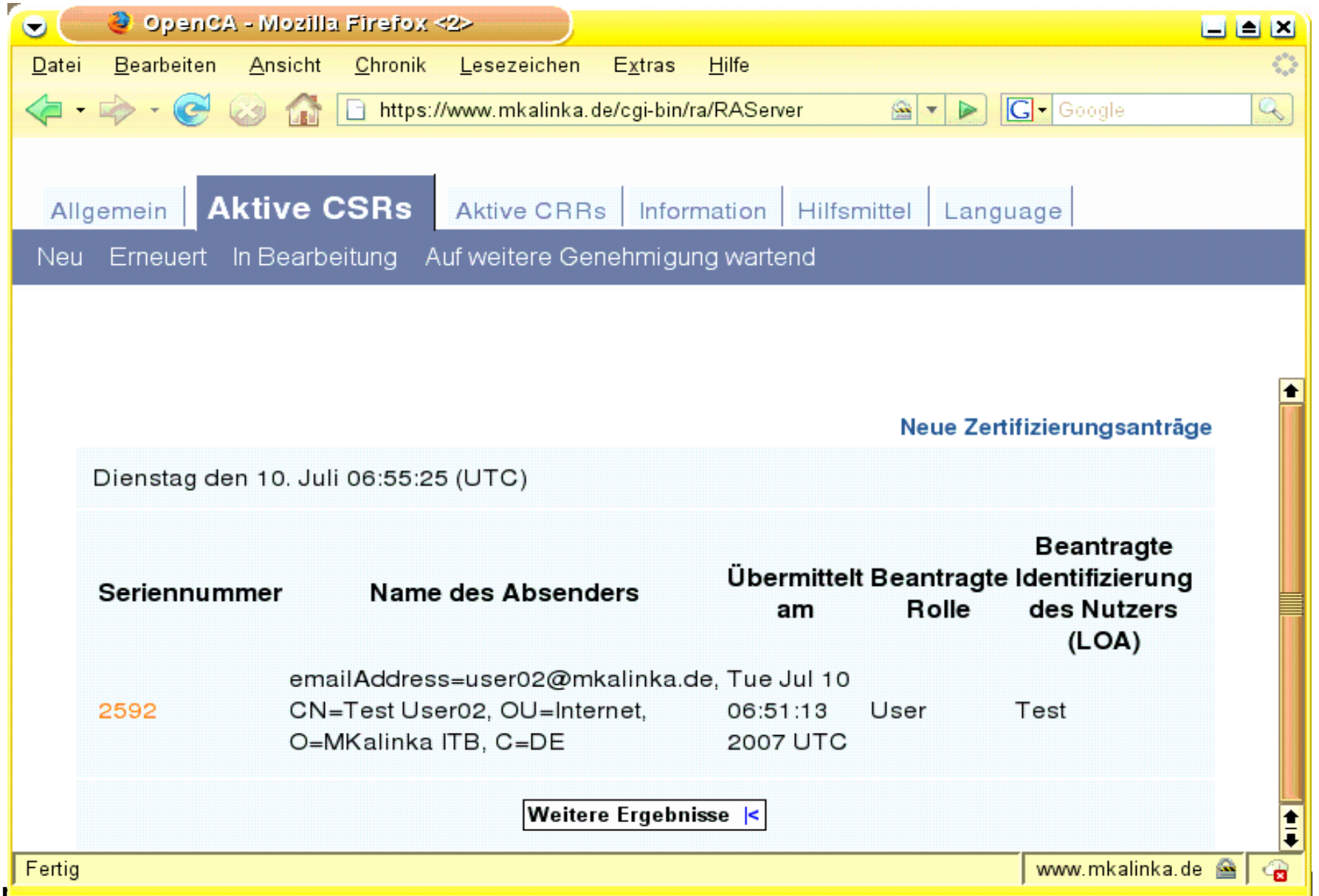
User Data

Name (Vor- und Nachname)	Test User02
E-Mail	user02@mkalinka.de
Einrichtung	MKalinka ITB
Telefon	+49 431 728426
Niveau der Identifizierung (LOA)	Test
Rolle	User
Registrierungsinstanz	Trustcenter selbst
Schlüssellänge	2048 (hohe Stufe)

Weiter

Kein Hinweis auf den privatekey

RA : CSR bearbeiten

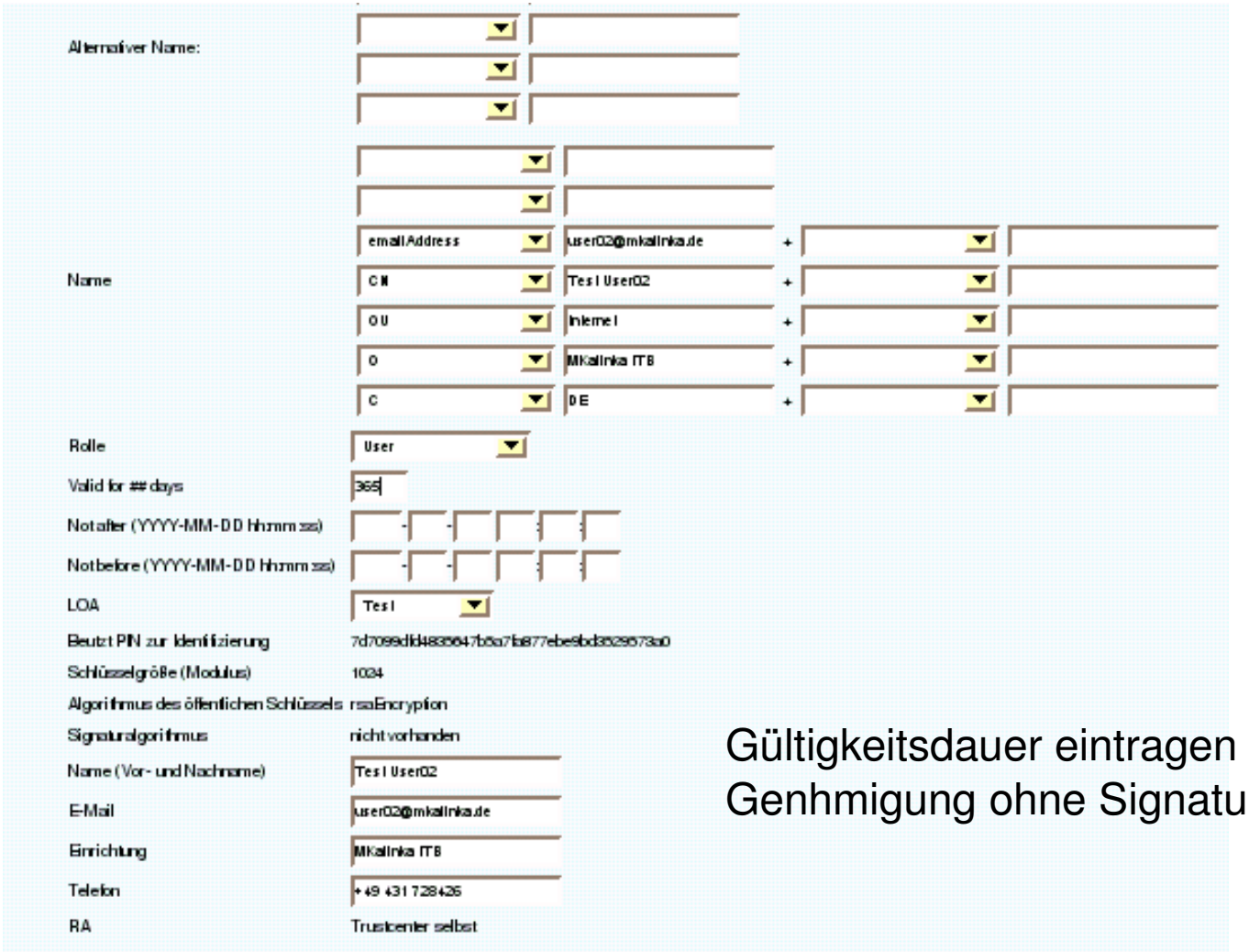


RA : CSR bearbeiten

Variable	Wert
Antragsversion	1
Seriennummer	2592
Name	Test User02
E-Mail	user02@mkalinka.de
Alternativer Name des Zertifikates	email.0=user02@mkalinka.de
Rolle	User
Lifetime (days)	n/a
Not before (YYMMDDhhmmss)	n/a
Not after (YYMMDDhhmmss)	n/a
Lifetime check	Lifetime would be ok.
LOA	Test
Eindeutiger Name	serialNumber=0, CN=Test User02, OU=Internet, O=MKalinka ITB, C=DE
Übermittelt am	Tue Jul 10 06:51:13 2007 UTC
Genehmigt am	nicht vorhanden
Beutzt PIN zur Identifizierung	7d7099dfd4835647b5a7fa877ebe9bd3529573a0
Schlüsselgröße (Modulus)	1024
Algorithmus des öffentlichen Schlüssels	rsaEncryption
Öffentlicher Schlüssel	Modulus (1024 bit): 00:bb:e5:e5:97:b9:3d:93:16:d2:07:6d:7e:d7:53: a2:ae:22:6e:67:22:fb:6c:e5:51:17:6c:96:99:1f: 74:b3:24:e5:0e:cd:b9:4f:f 16:fb:8a:73:7d:78:a5:a0:8 be:d6:ff:d9:7c:96:20:e0:8 d7:4d:8a:a5:de:3b:ac:af:b a8:d4:ea:d8:95:89:d9:6d:c 88:67:77:1f:0c:87:05:5f:4 28:d5:7d:ca:01:ec:f4:66:0 Exponent: 65537 (0x10001)
Signaturalgorithmus	nicht vorhanden
Name (Vor- und Nachname)	Test User02
E-Mail	user02@mkalinka.de
Einrichtung	MKalinka ITB
Telefon	+49 431 728426

Operationen	
Bearbeiten des Antrages	Bearbeiten des Antrages
Verify PIN	Verify PIN
Antrag genehmigen und digital signieren	Antrag genehmigen
Antrag genehmigen ohne ihn digital zu signieren	Antrag genehmigen ohne ihn digital zu signieren
Delete request	Delete request

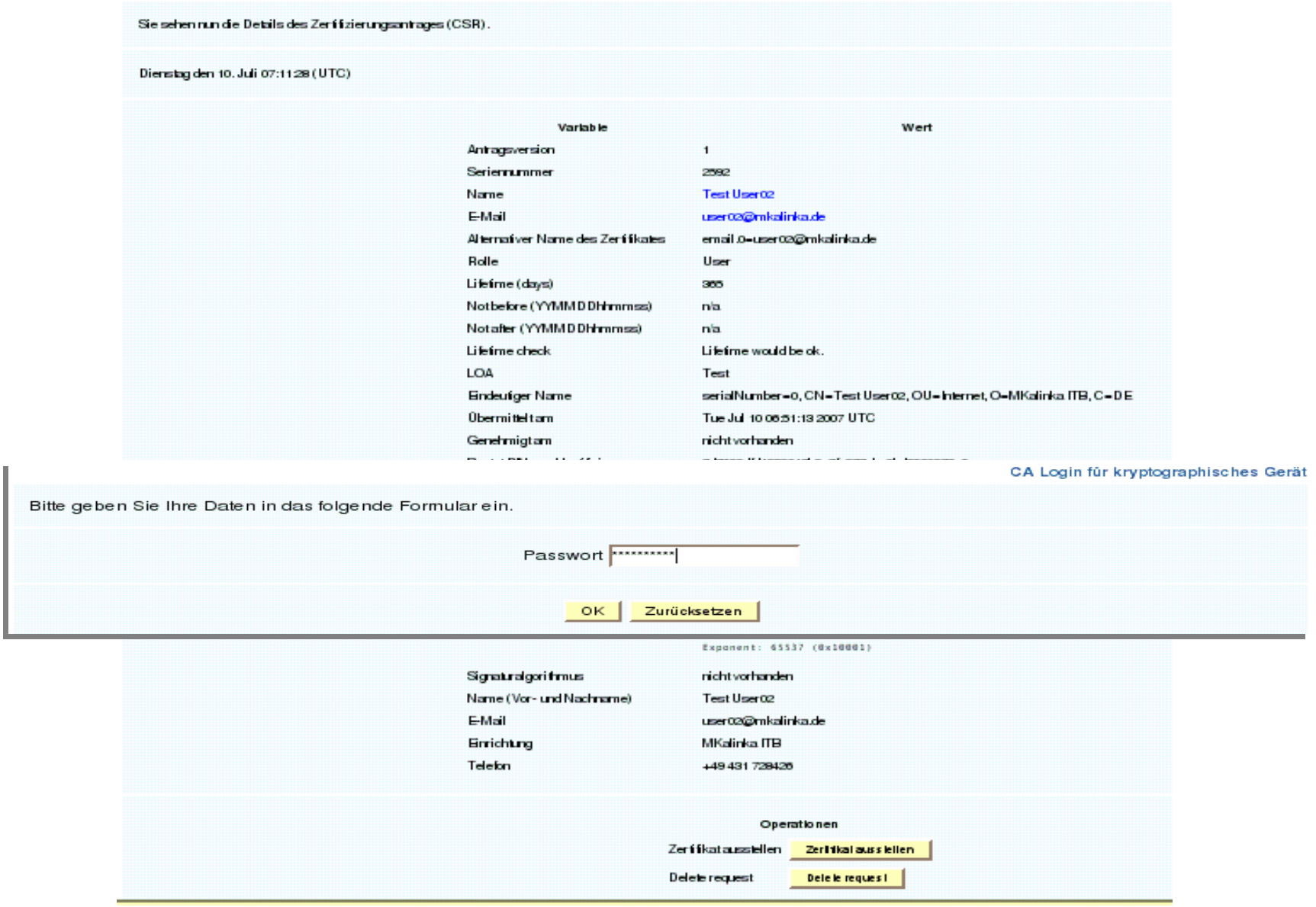
RA : CSR bearbeiten



Gültigkeitsdauer eintragen
Genhmigung ohne Signatur

CA : CSR finden

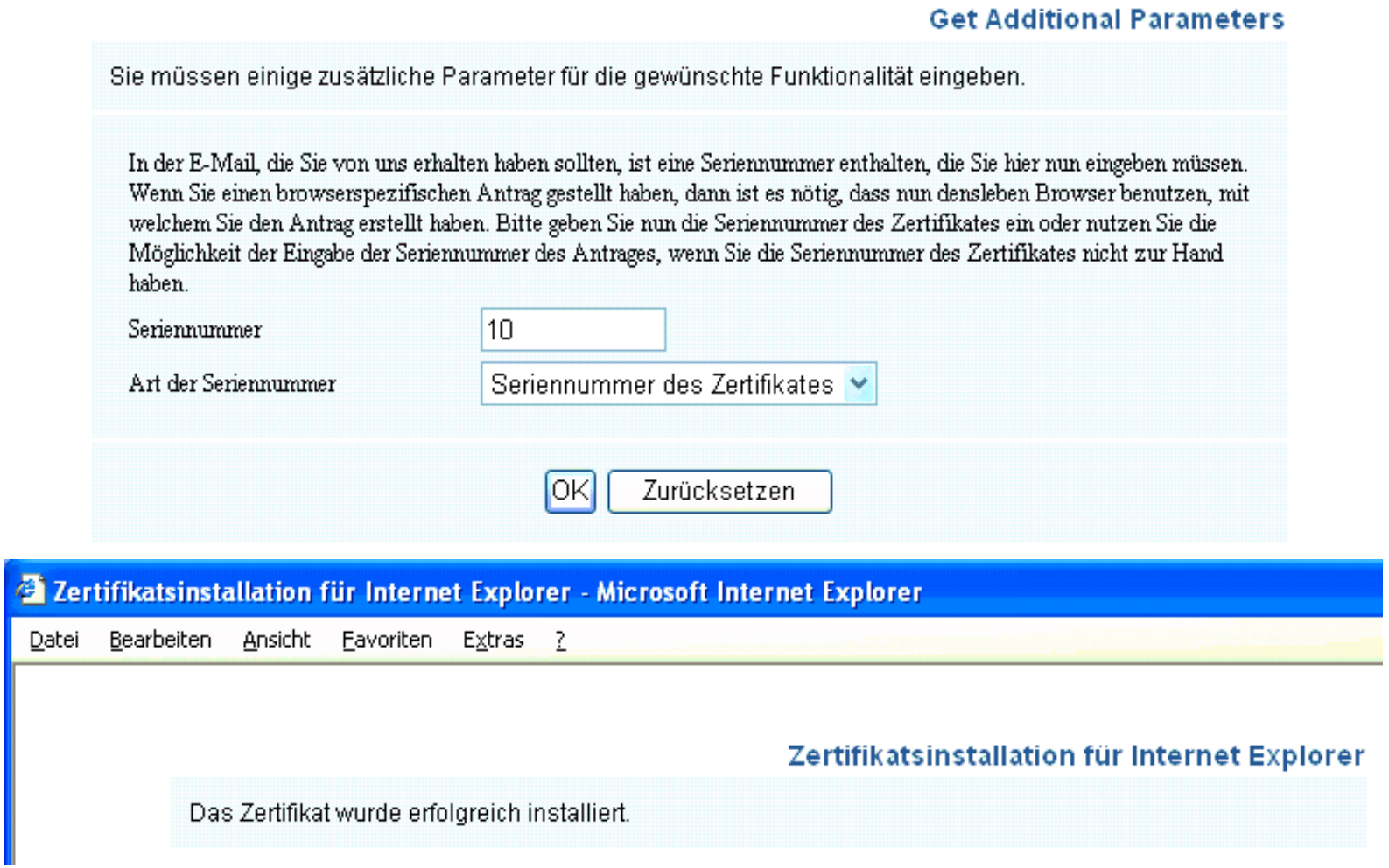
CA : CSR signieren



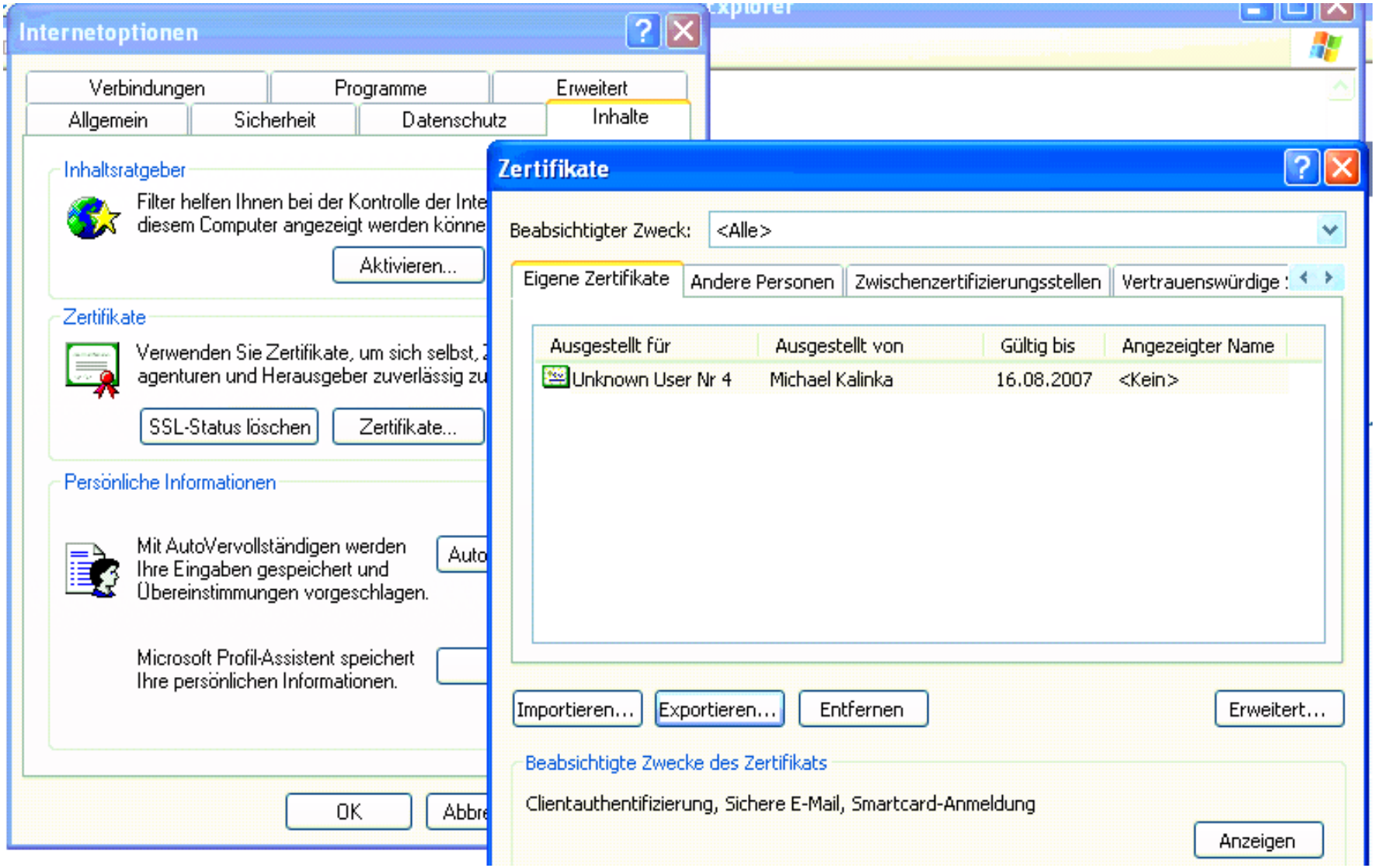
Zertifikatsinhalte

Netscape Cert Type	SSL Client, S/MIME
Netscape Comment	User Certificate of MKalinka ITB
Netscape Revocation Url	http://www.mkalinka.de/pub/crl/cacrl.crl
X509v3 Authority Key Identifier	keyid:26:AD:52:64:4E:E8:A8:50:9C:F5:F8:EE:F5:5B:33:EE:4B:24:57:7C DirName:/C=DE/O=MKalinka ITB/OU=MKalinka ITB CA/CN=Michael Kalinka/emailAddress=camanager@mkalinka.de serial:F5:17:FD:42:CD:D4:7D:EA
X509 Version 3 Basic Constraints	CA:FALSE
X509v3 CRL Distribution Points	URI:http://www.mkalinka.de/pub/crl/cacrl.crl
X509v3 Certificate Policies	Policy: 1.2.3.3.4 CPS: http://www.mkalinka.de/cps
X509v3 Extended Key Usage	TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
X509v3 Issuer Alternative Name	email:camanager@mkalinka.de
X509v3 Key Usage	Digital Signature, Non Repudiation, Key Encipherment
Alternativer Name des Zertifikates	email:user02@mkalinka.de
X509v3 Subject Key Identifier	FB:45:E8:27:A7:CC:49:E2:BC:4C:5A:54:BE:A4:54:98:D3:65:21:A3

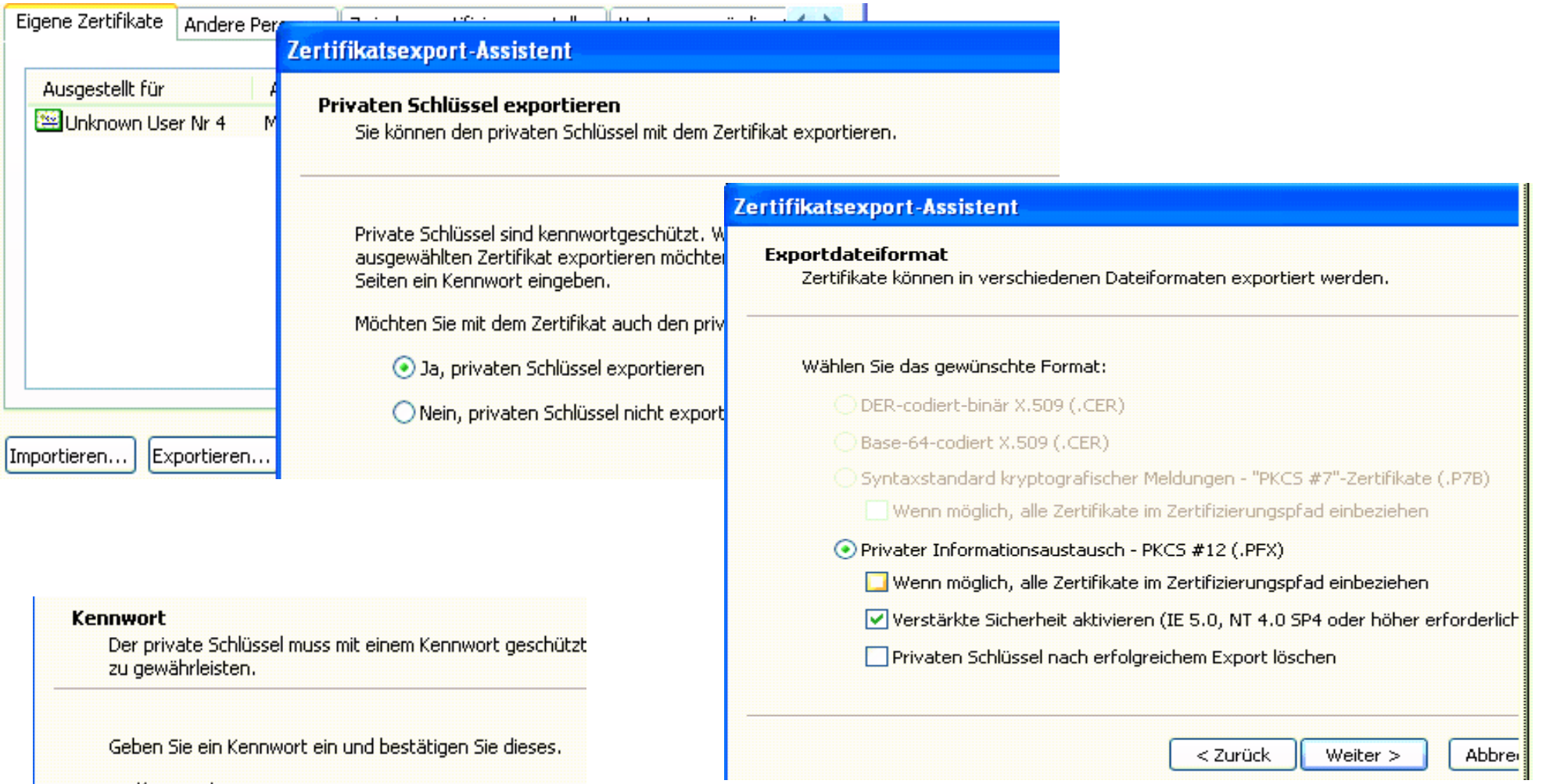
IE6 Zert. laden



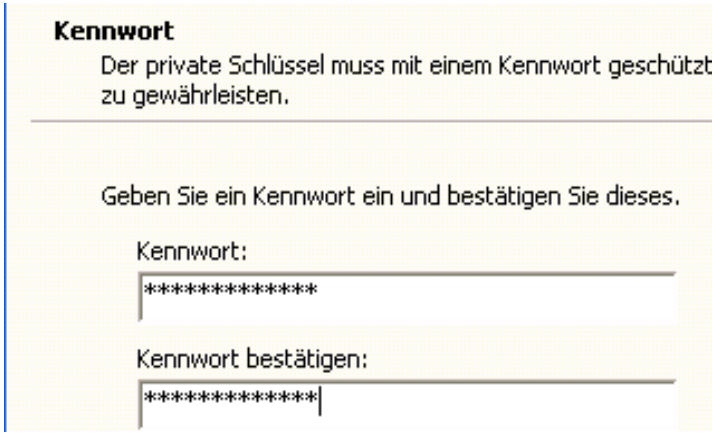
IE6 wo ist das Zert ?

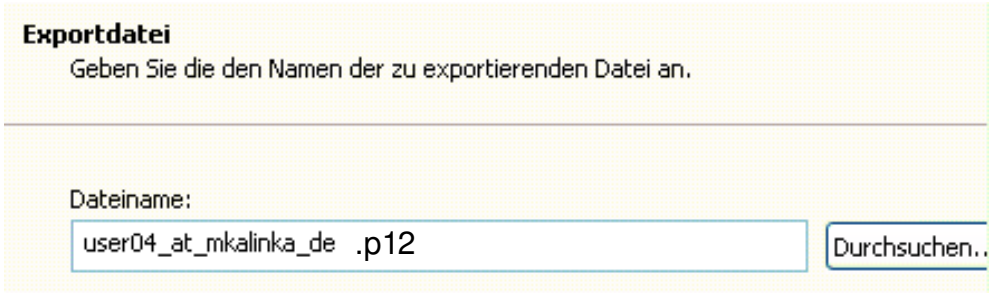


IE6 exportCert

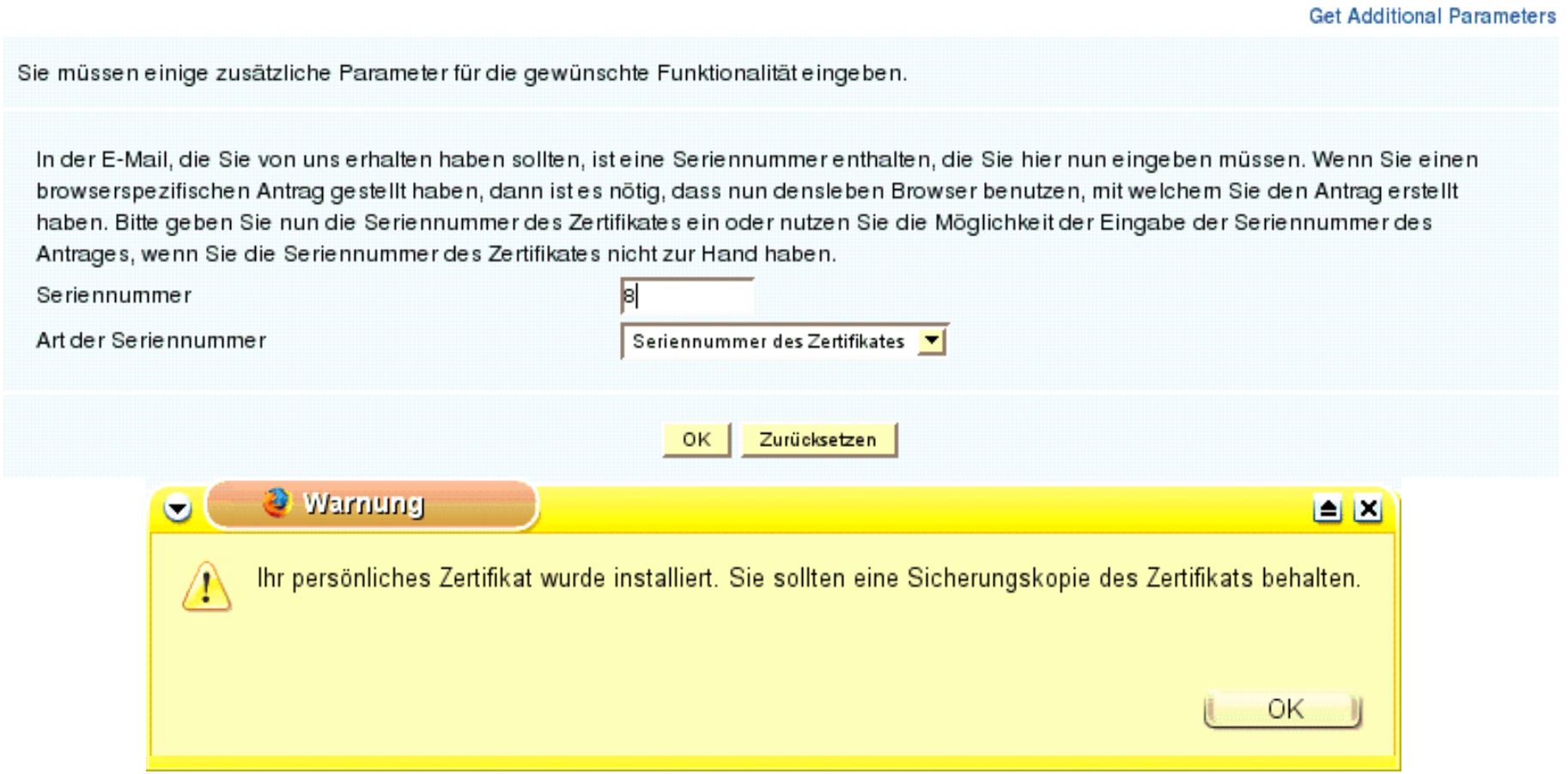


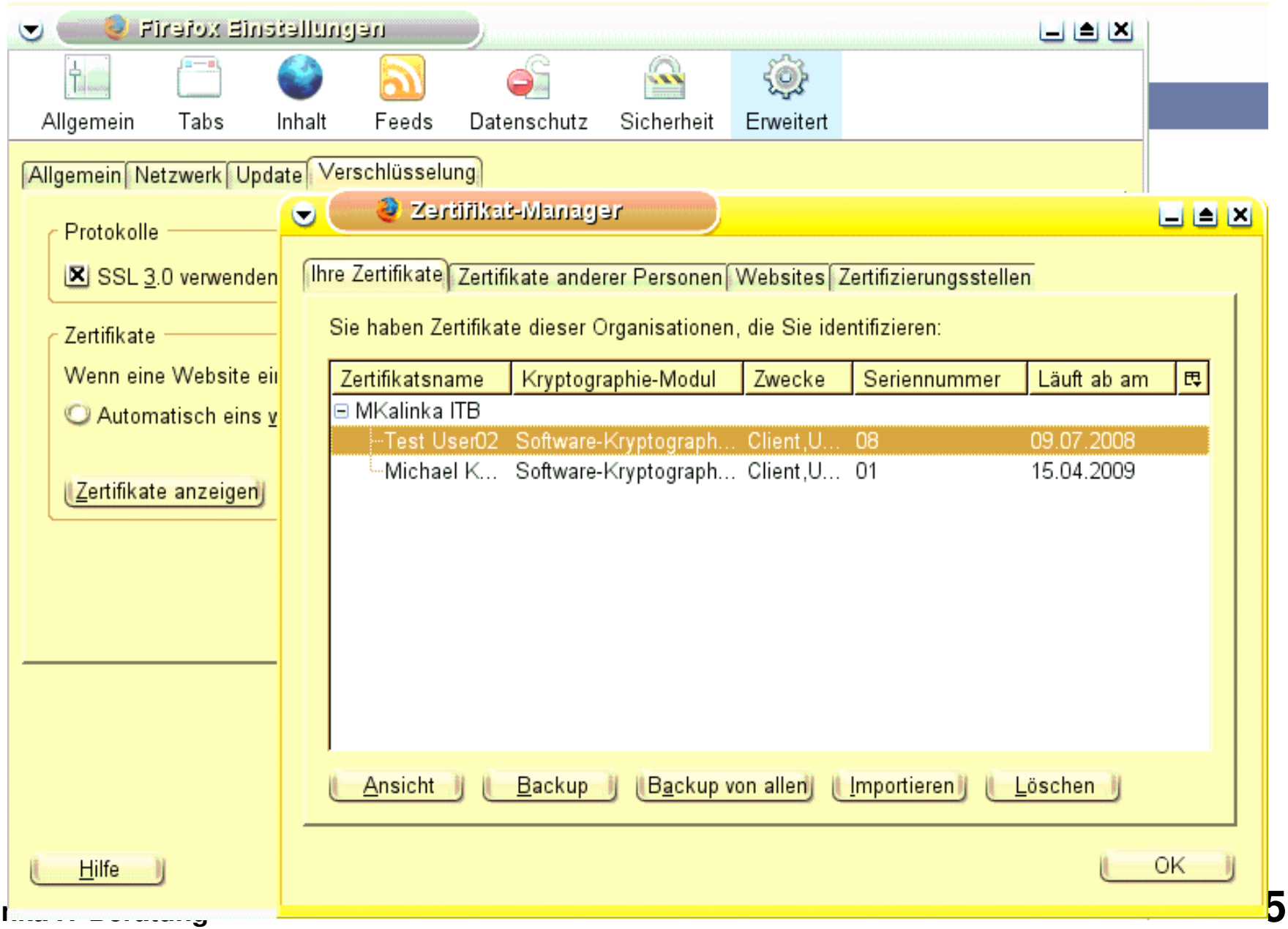
Exportdatei als .p12

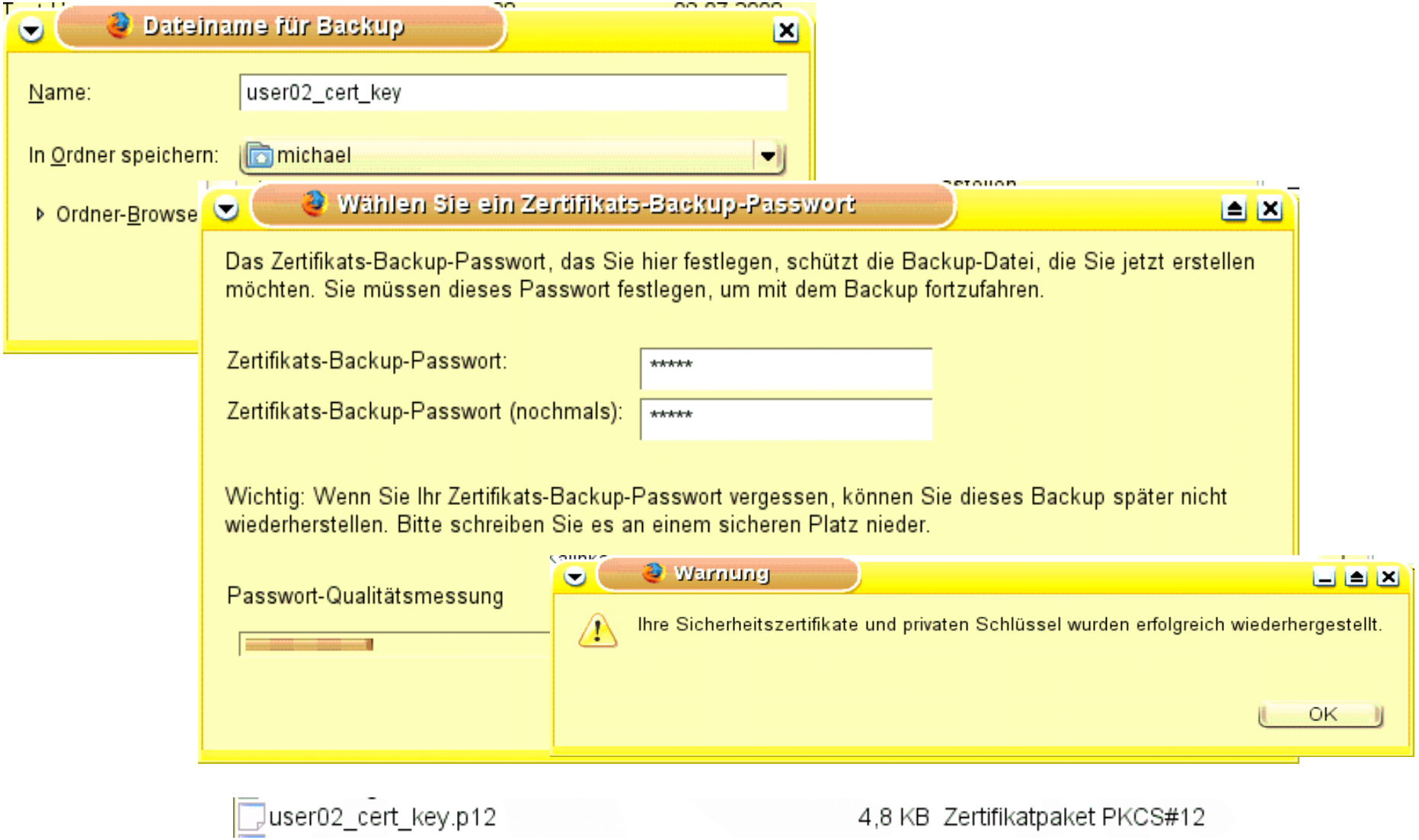




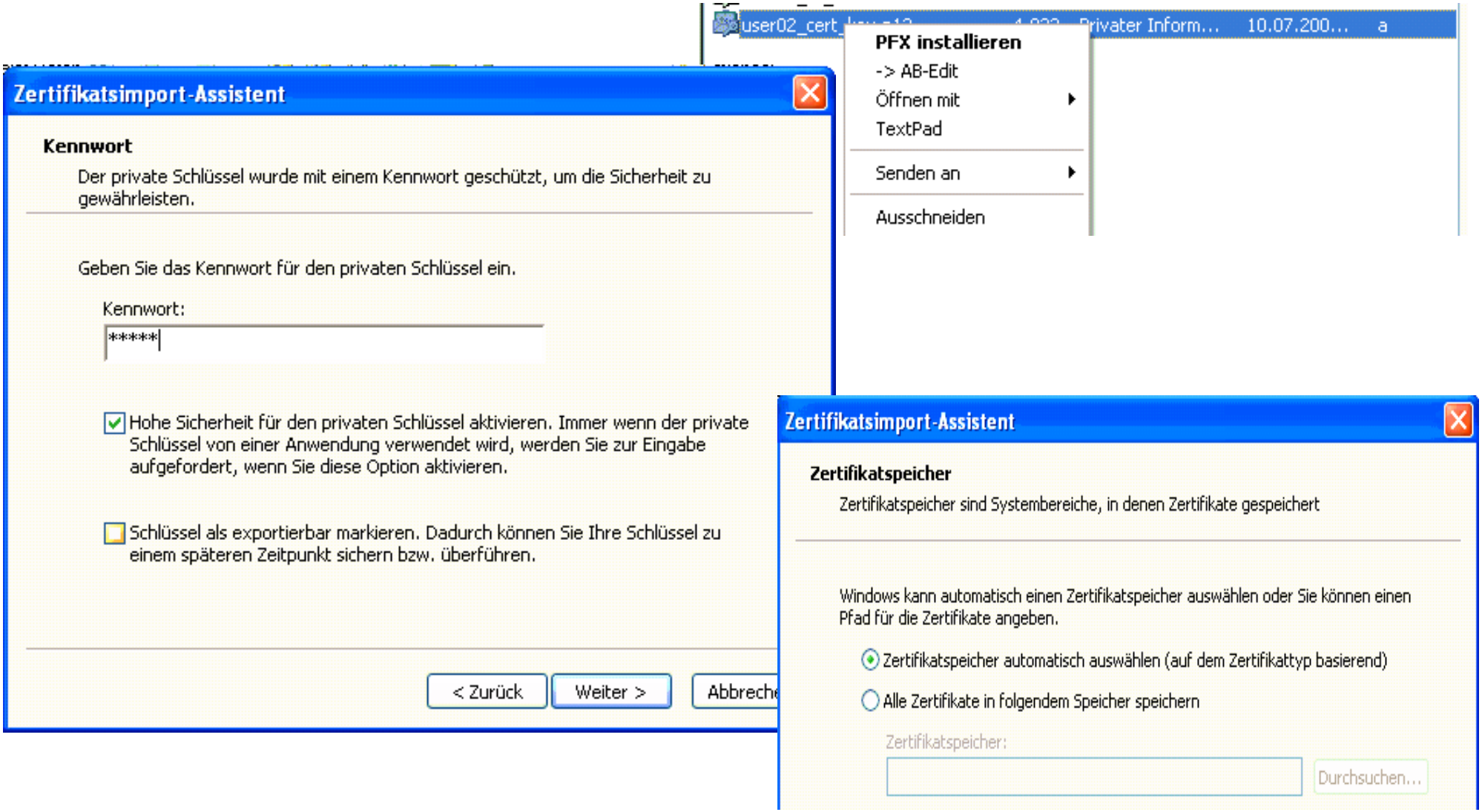
PUB : Zertifikat abholen



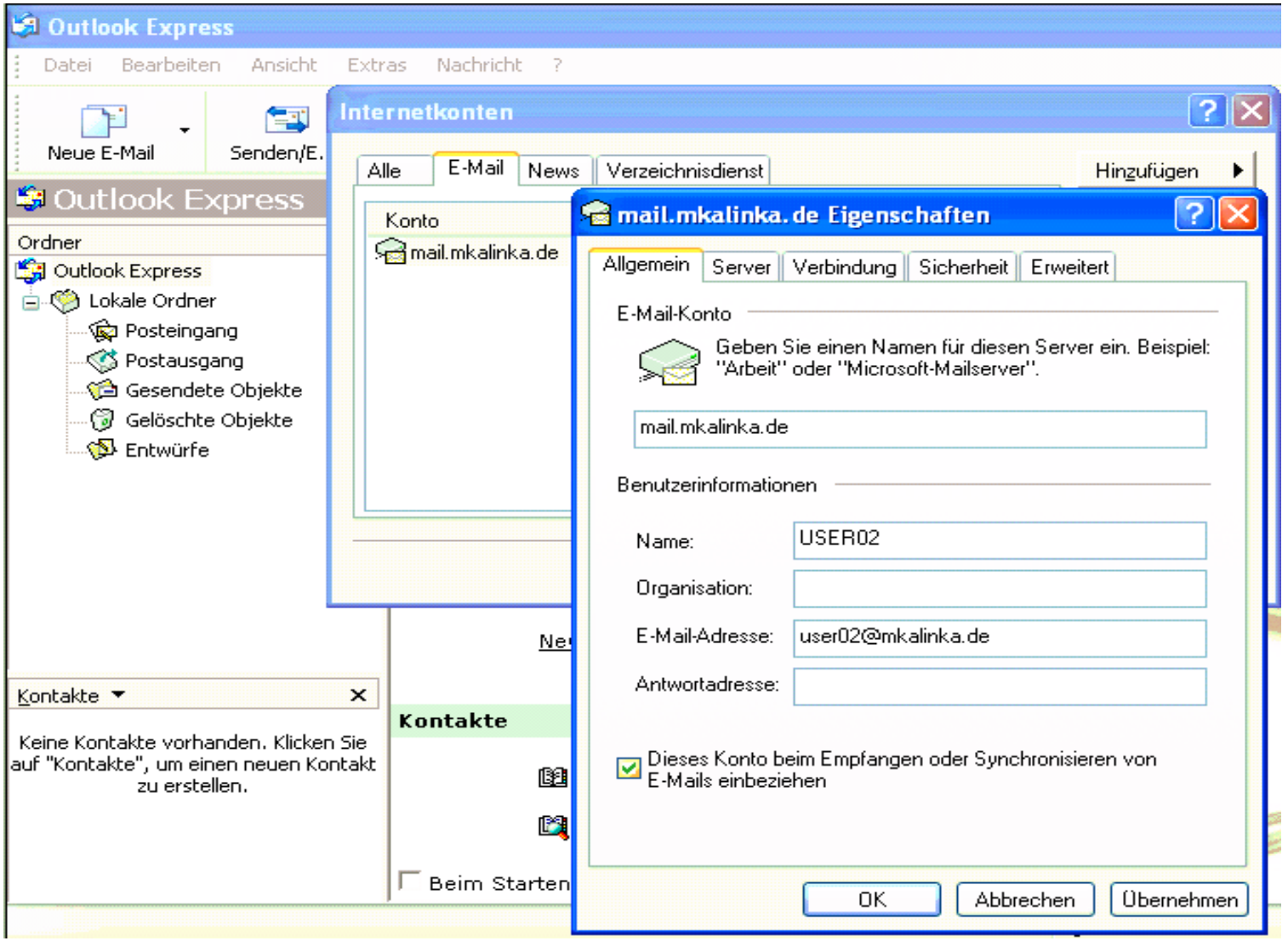

Firefox Einstellungen
Allgemein
Tabs
Inhalt
Feeds
Datenschutz
Sicherheit
Erweitert
Allgemein
Netzwerk
Update
Verschlüsselung
Protokolle
SSL 3.0 verwenden
Zertifikate
Wenn eine Website ei
Automatisch eins v
Zertifikate anzeigen
Hilfe
Zertifikat-Manager
Ihre Zertifikate
Zertifikate anderer Personen
Websites
Zertifizierungsstellen
Sie haben Zertifikate dieser Organisationen, die Sie identifizieren:
Zertifikatsname
Kryptographie-Modul
Zwecke
Seriennummer
Läuft ab am
MKalinka ITB
Test User02
Software-Kryptograph...
Client,U...
08
09.07.2008
Michael K...
Software-Kryptograph...
Client,U...
01
15.04.2009
Ansicht
Backup
Backup von allen
Importieren
Löschen
OK



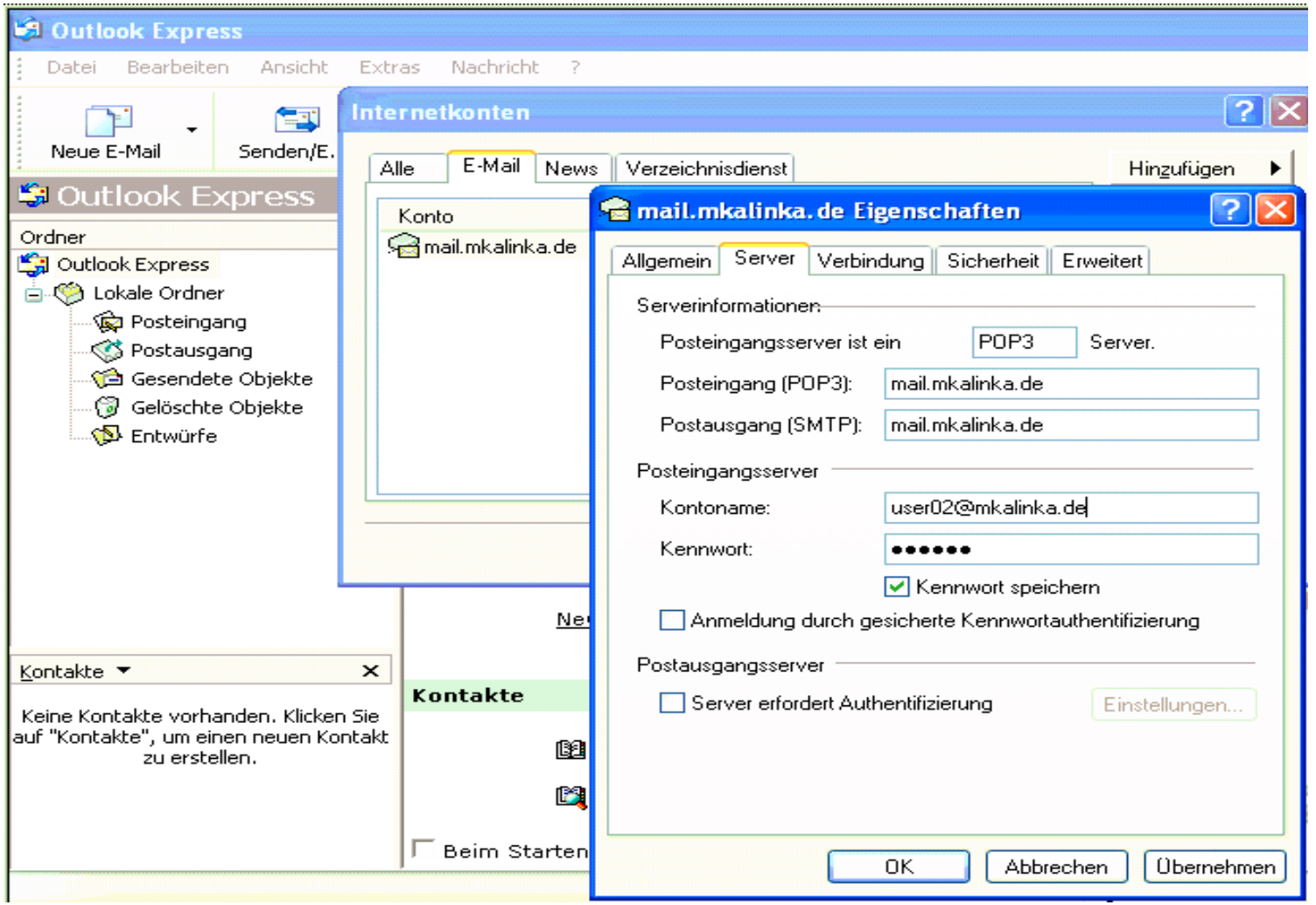
Windows Import .p12



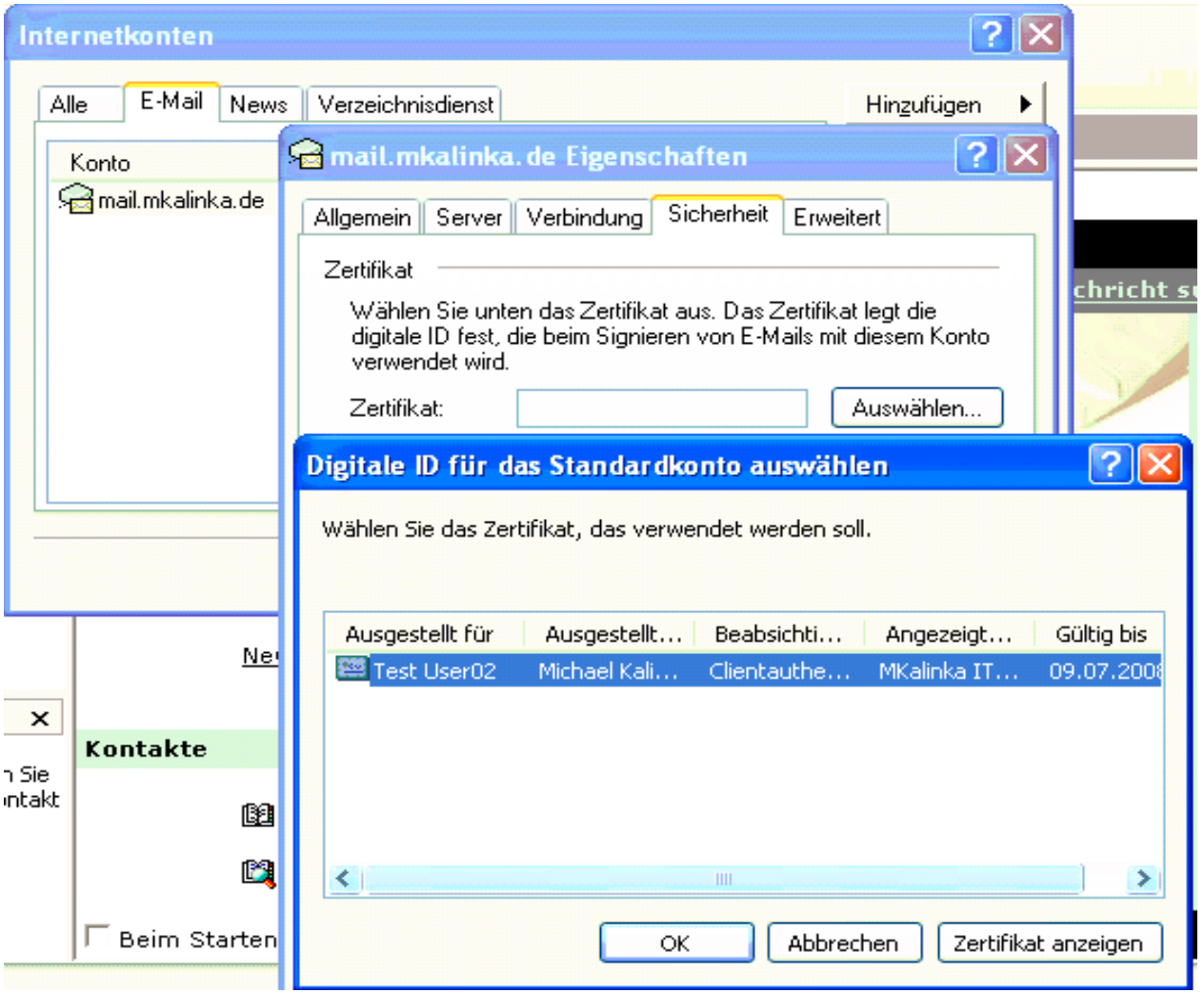
OE Mail-Konto



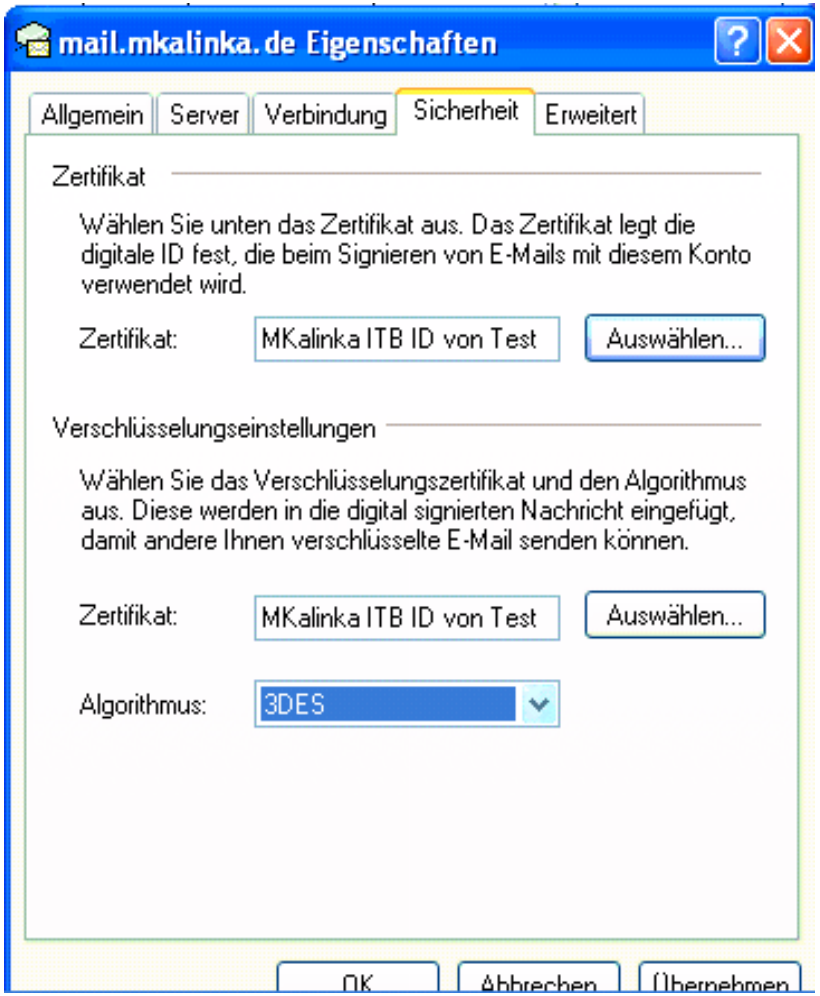
OE Mail-Server



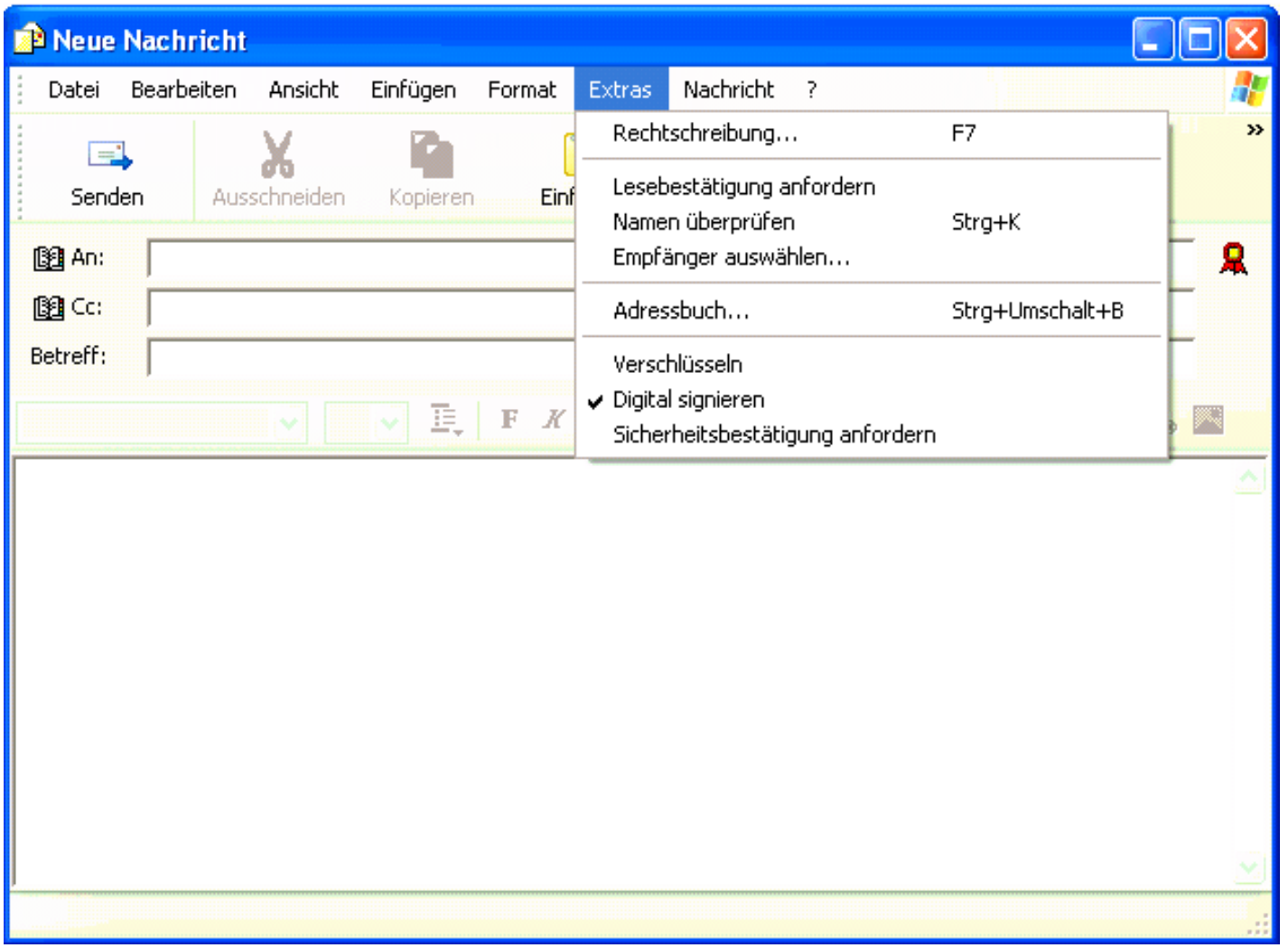
OE Mail-Sicherheit



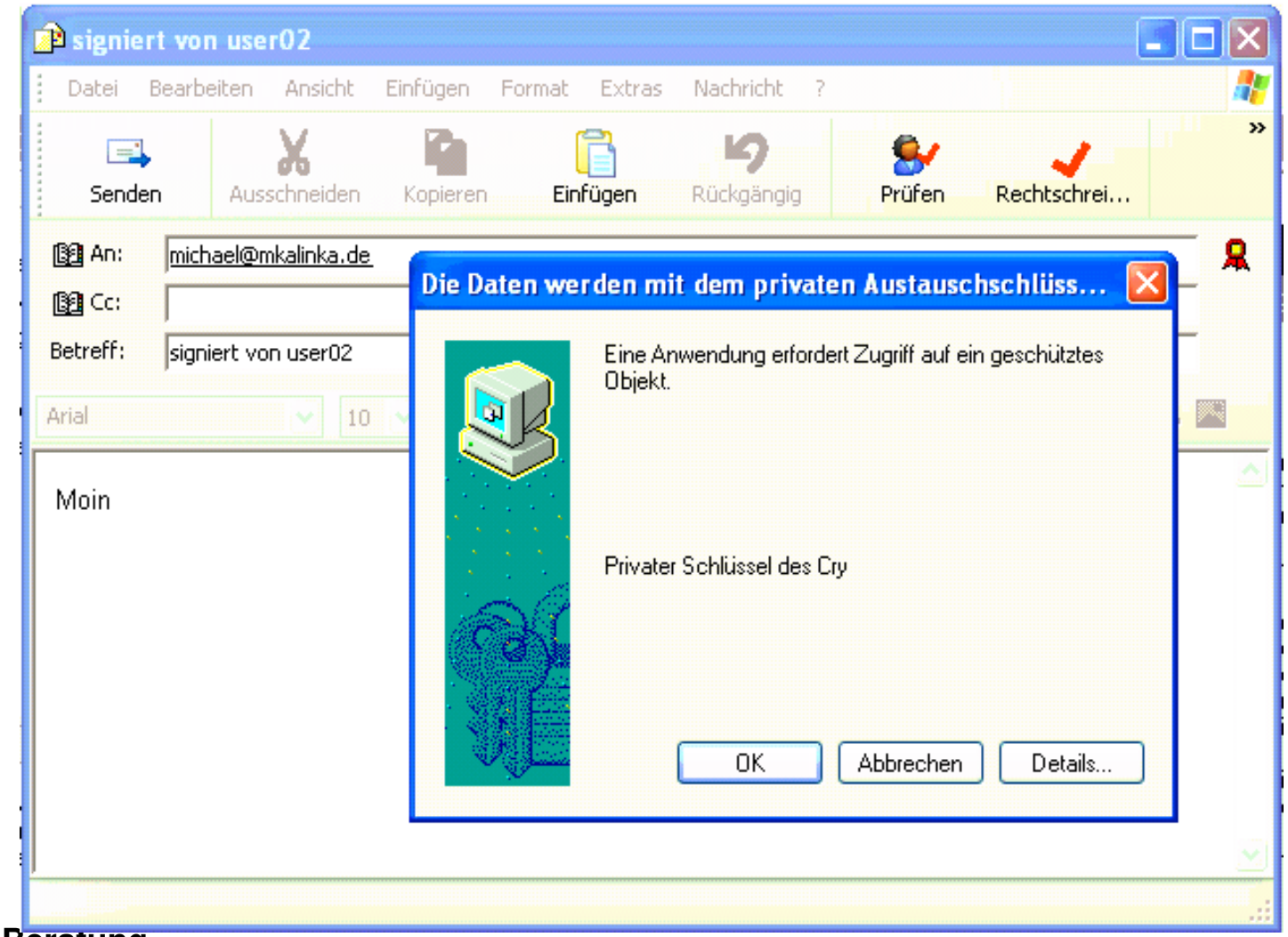
OE Userzertifikat



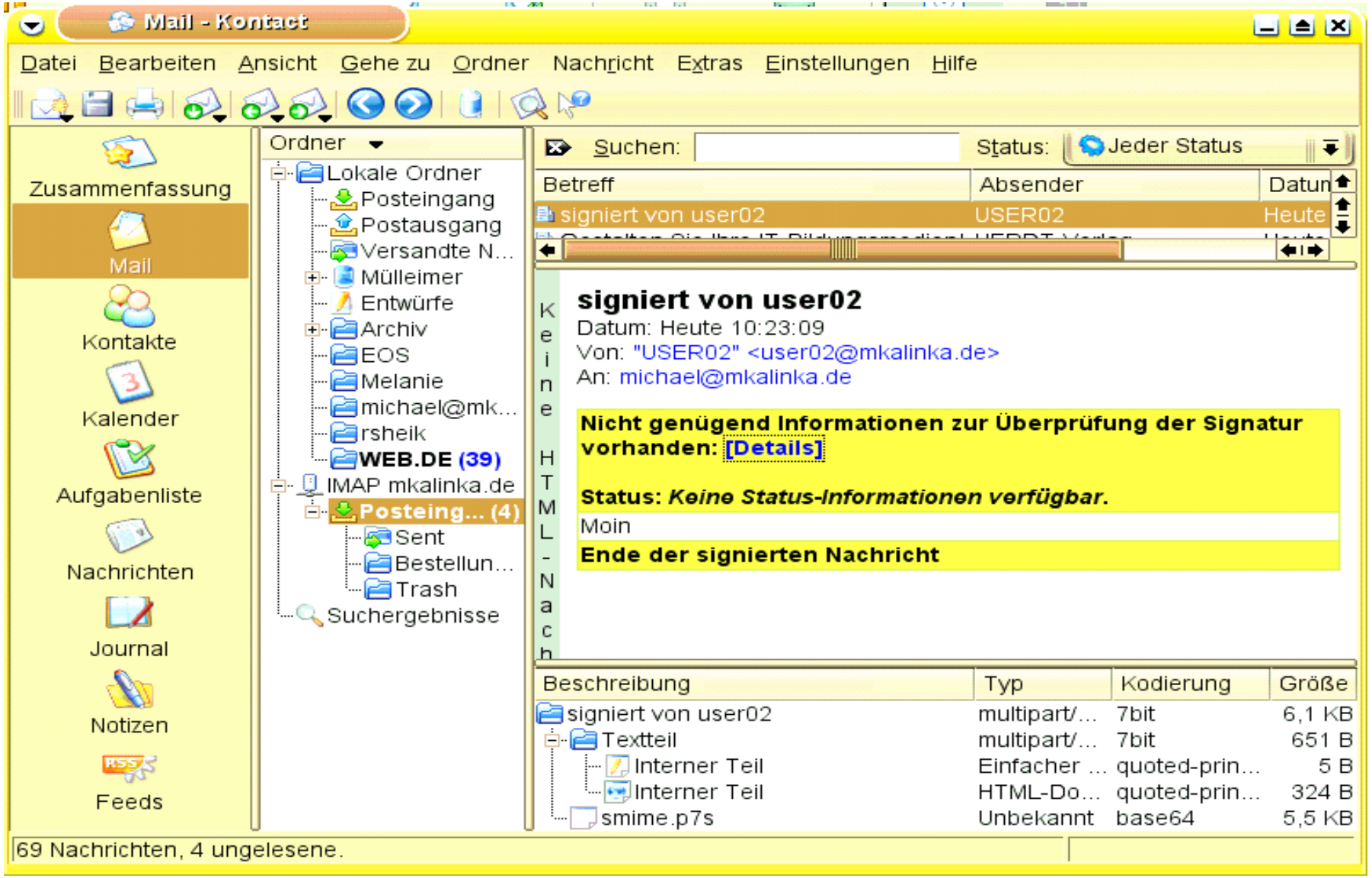
OE Signatur



OE Versand



KMail Empfang ohne Zertifikat



Kmail Signaturprüfung ok