

Sicherheit durch Kryptographie

Sicherheit durch Kryptographie

- Vertraulichkeit
- Integrität
- Authentizität und digitale Signaturen
- Zertifikate



Sicherheit durch PKI

- Schlüsselmanagement
- 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

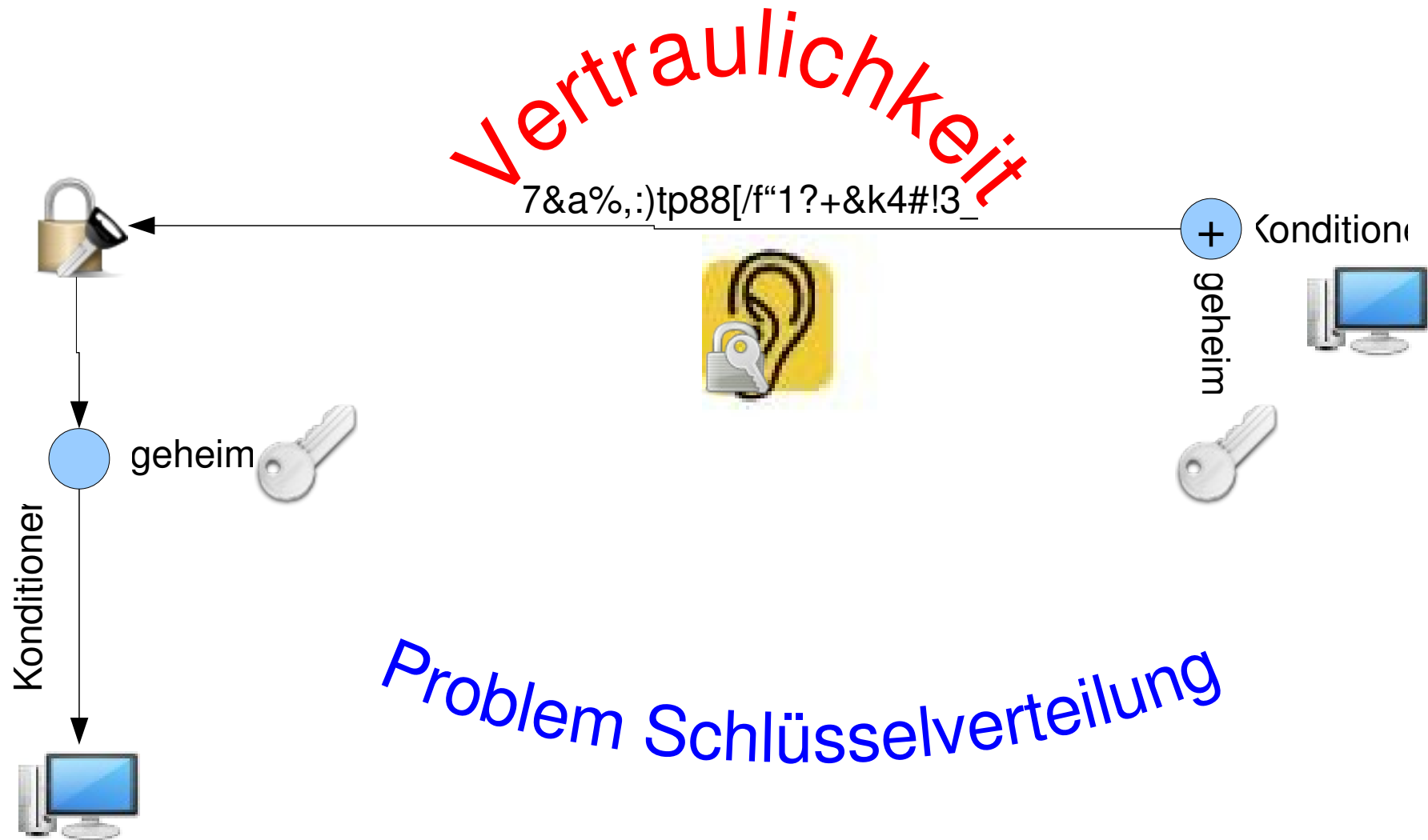
==> Schlüssellänge groß (ab 128 bit, Brute Force langwierig)

*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 <i>Aus den Daten wird eine Zahl errechnet (Hashwert, Digest, Fingerprint)</i>
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 <i>Verwendung zweier Schlüssel</i> <i>privatekey + publickey</i>
Verfahren	RSA, DSA, PGP, GPG
Vorteil	A) Lösung des Schlüsselveilteilungsproblems 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

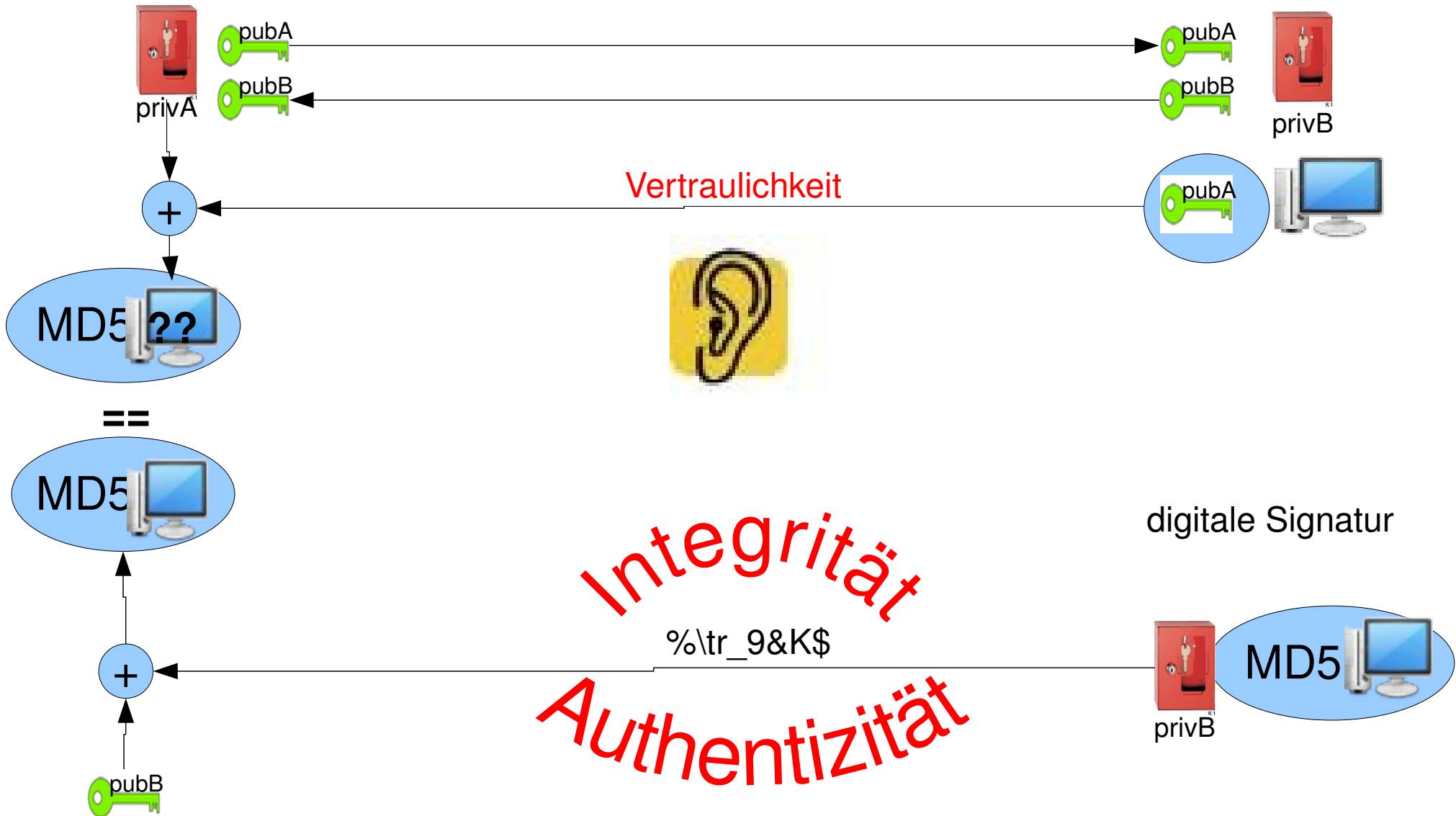
Bob



Alice

und

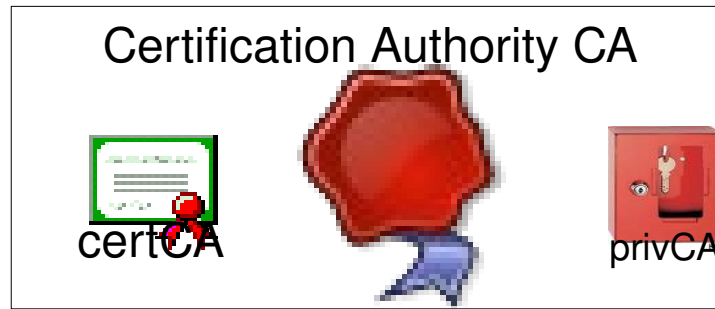
Bob



Und wer signiert die public keys ?

Zertifikate

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

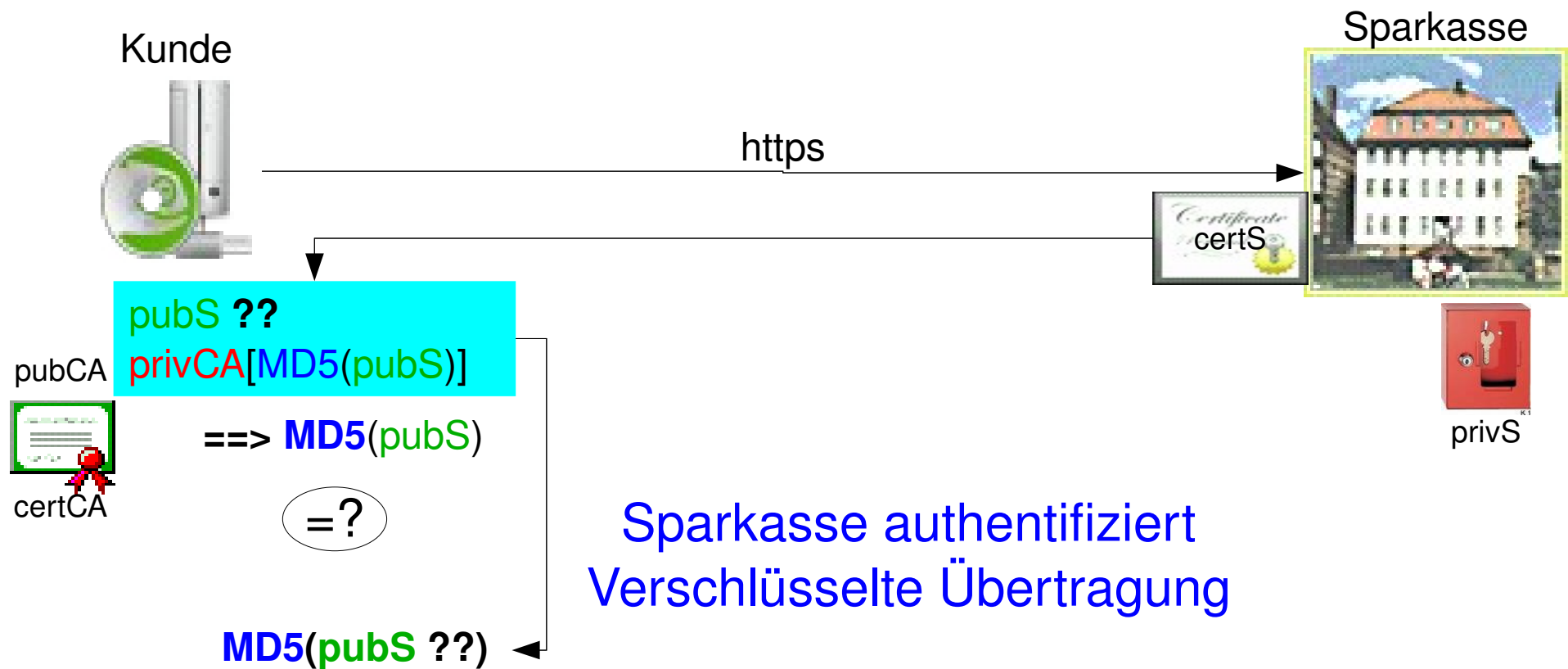
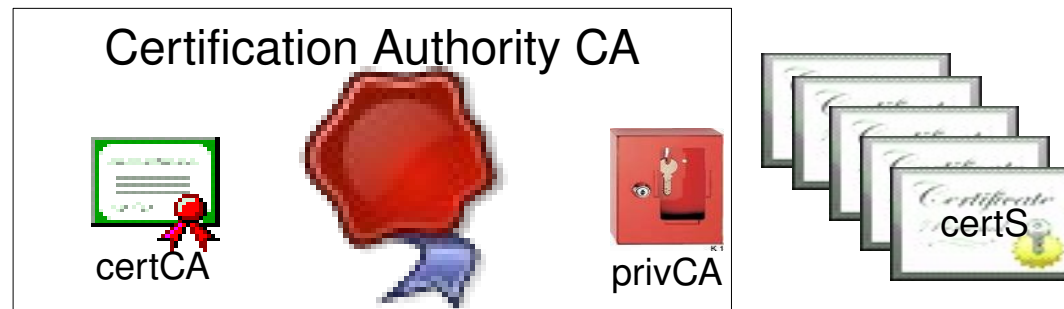


$$\text{signCA}(\text{pubS}) = \text{privCA}[\text{MD5}(\text{pubS})]$$



←----- Certificate Signing Request CSR ----->





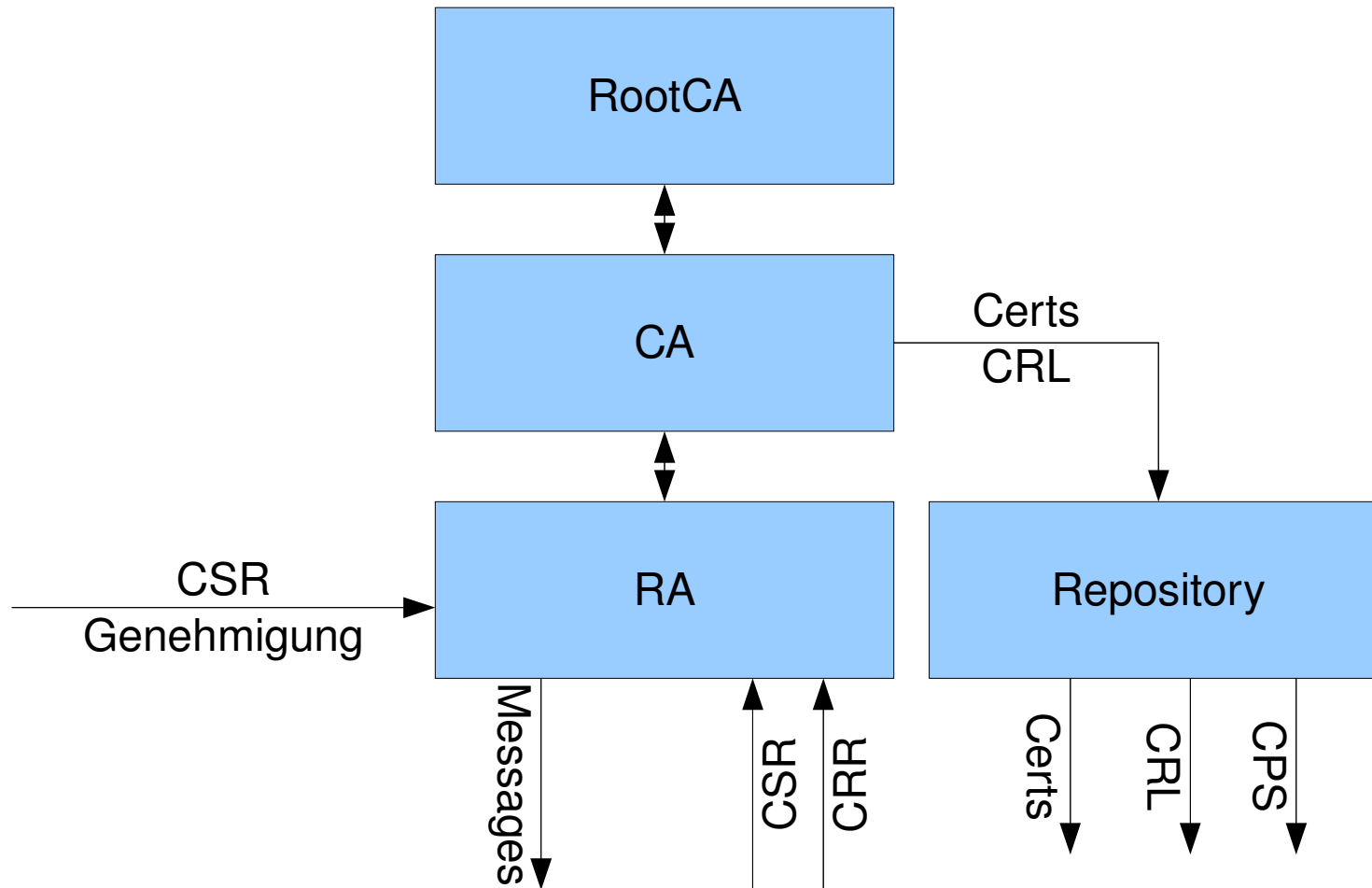
Und woher kommt das CA-Zertifikat ?

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

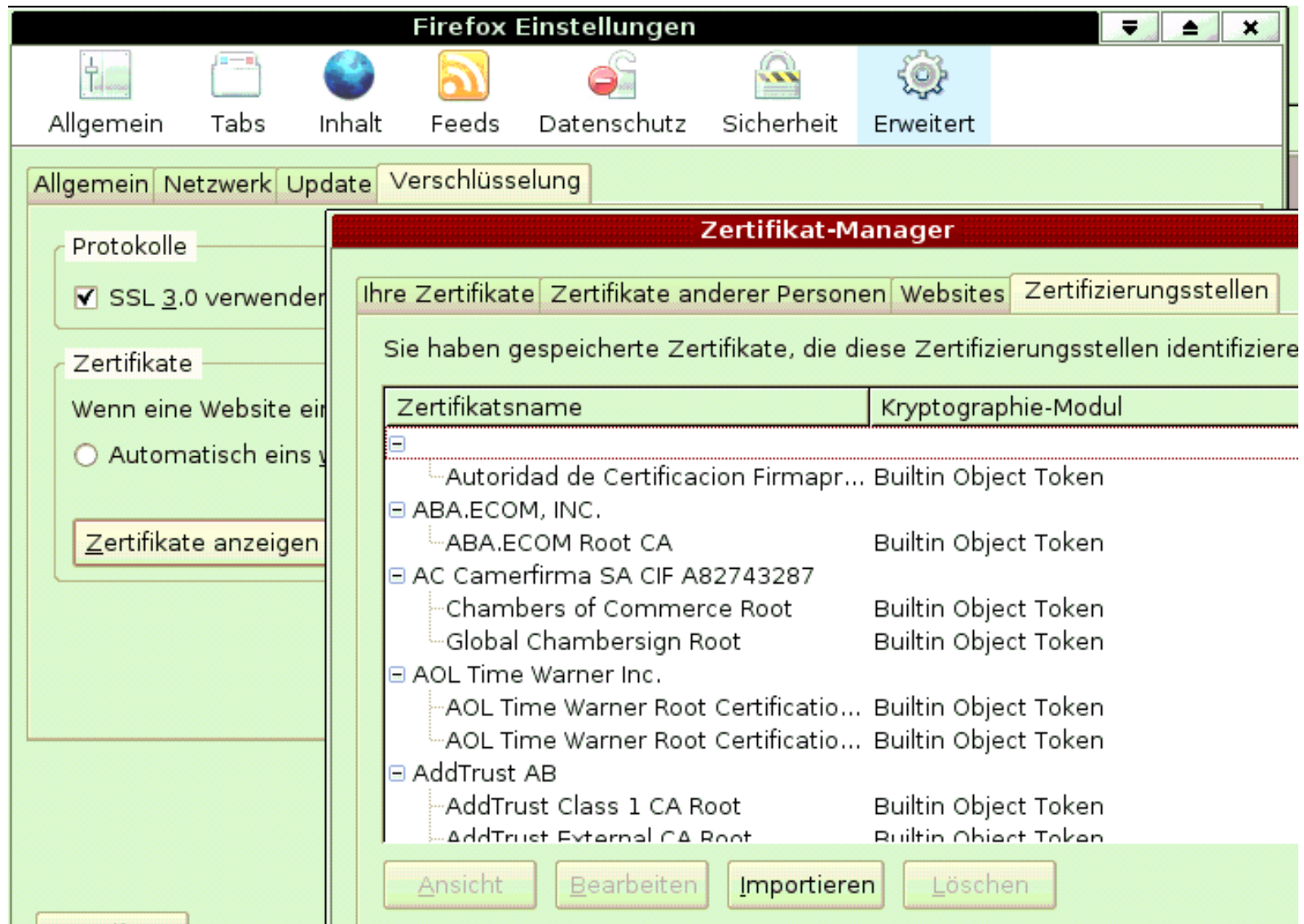
PKI



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

Internetoptionen

Verbindungen | Programme | Erweitert | Inhalte

Allgemein | Sicherheit | Datenschutz

Inhaltsratgeber

Filter helfen Ihnen bei der Kontrolle der Internetaktivitäten auf diesem Computer angezeigt werden können

Altivieren...

Zertifikate

Verwenden Sie Zertifikate, um sich selbst, Zertifikatsagenturen und Herausgeber zuverlässig zu identifizieren

Zertifikate...

Persönliche Informationen

Mit AutoVervollständigen werden Ihre Eingaben gespeichert und Übereinstimmungen vorgeschlagen

AutoVervollständigen

Microsoft Profil-Assistent speichert Ihre persönlichen Informationen.

OK Abbrechen

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-Clie...	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

Introduction

It's been a long t...

For years we've a...

The primary goal...

Inclusion into...

To provide a t...

For general docu...

[Latest News - \[1 \]](#)

CAcert Board

As the new secr...

President Robert...

declared vacant t...

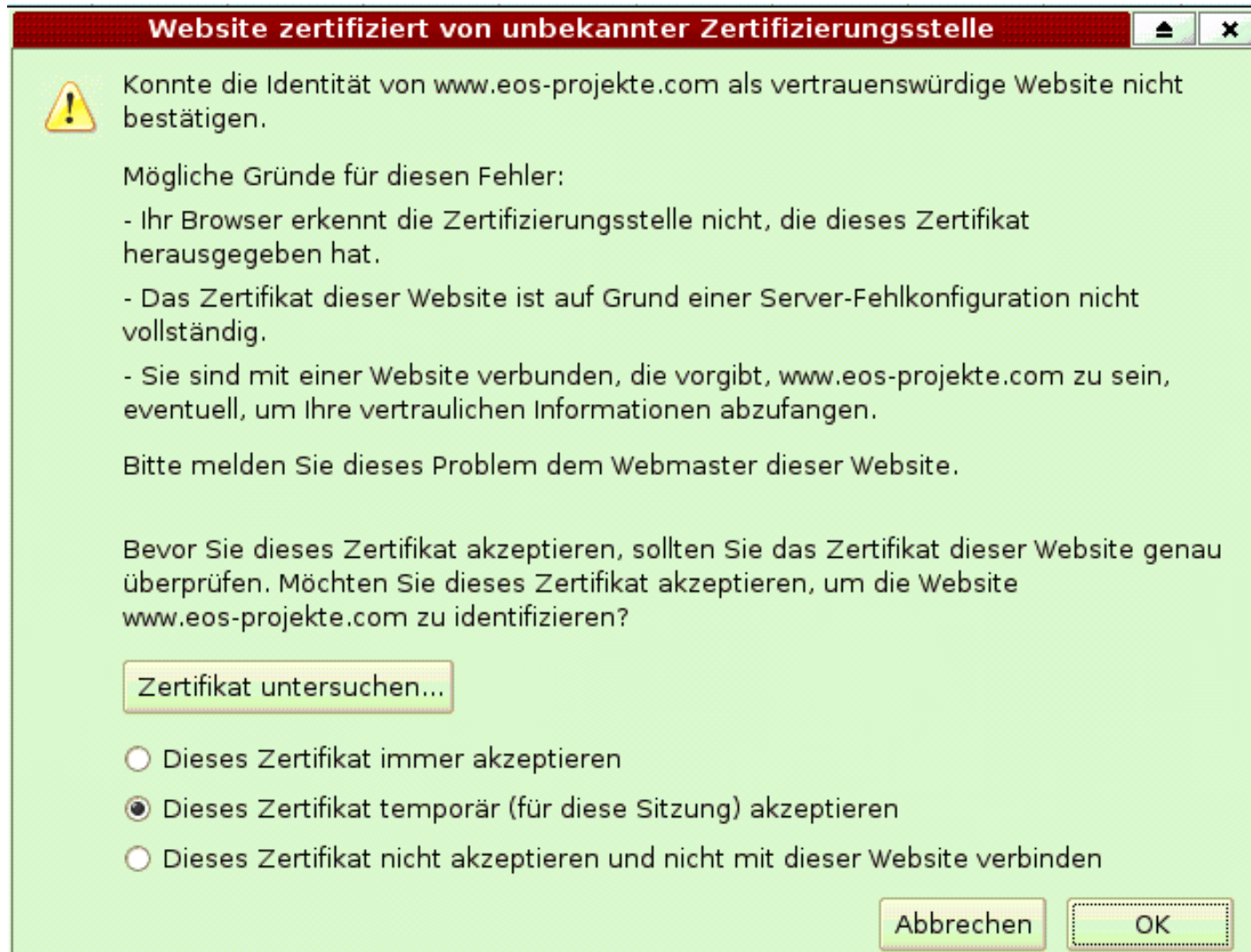
[\[Full Story \]](#)

CAcert Inc. S...

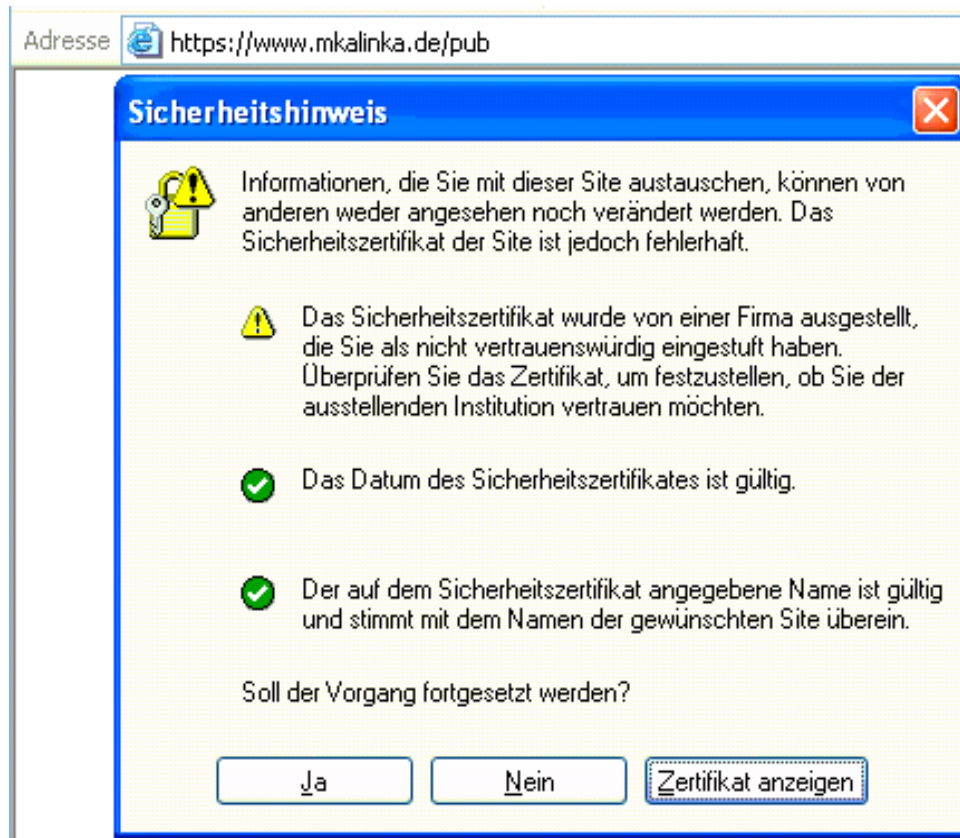
At the 25th of M...

and Greg Rose on the CAcert Inc. Committee (board). The resignat...

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>

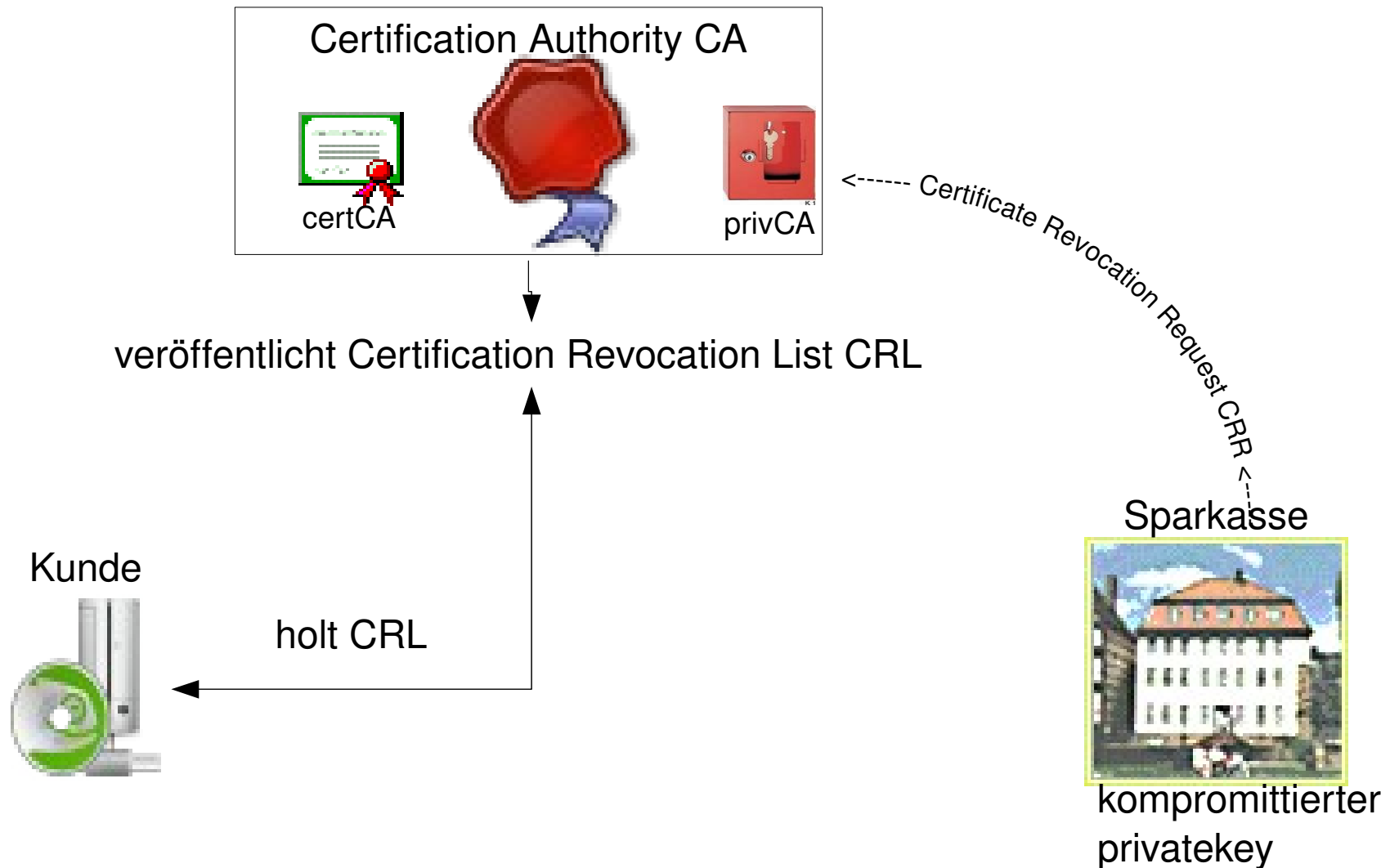
Netscape CA Revocation Url:

<http://www.mkalinka.de/pub/crl/cacrl.crl>

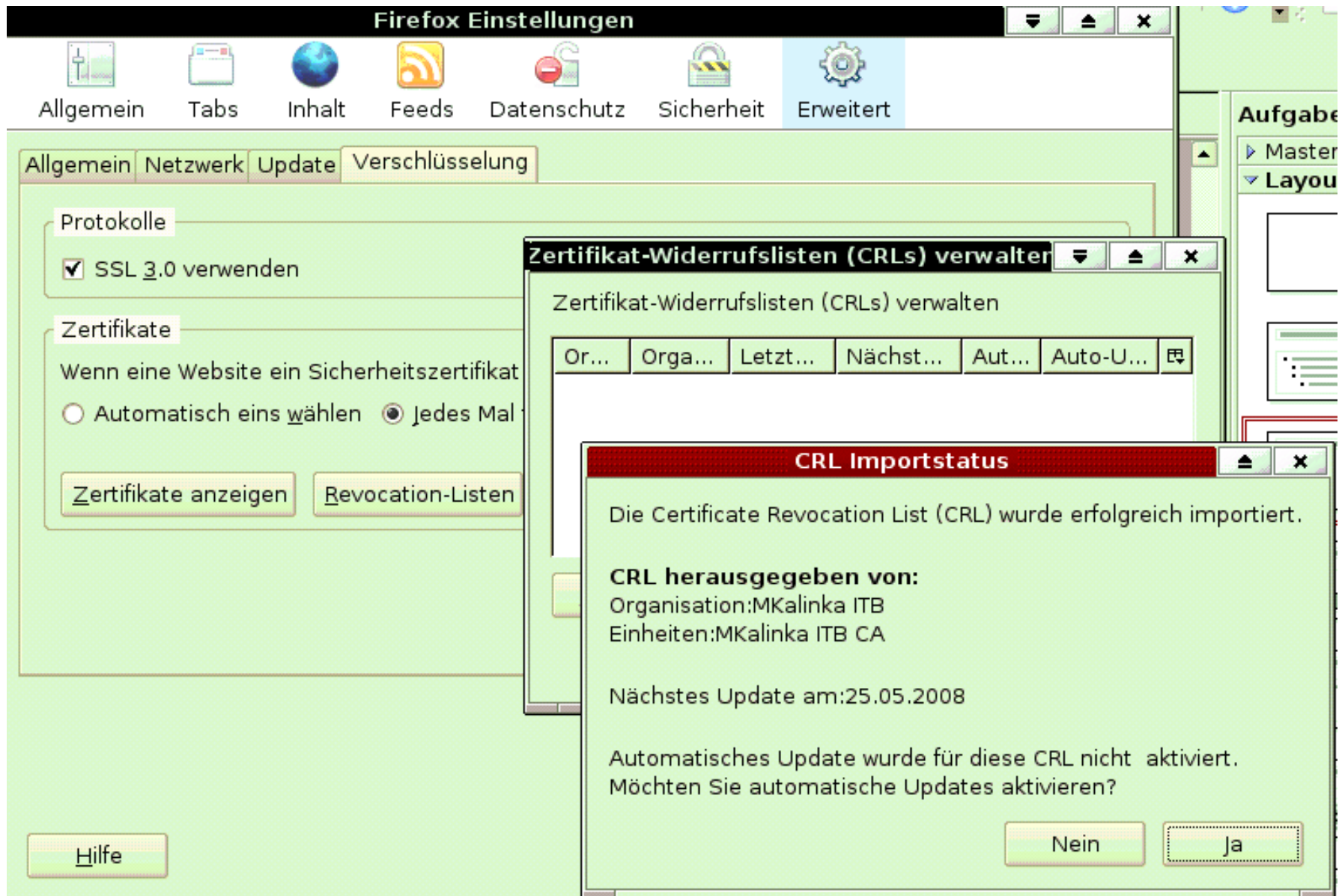
Netscape Revocation Url:

<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
Online **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`

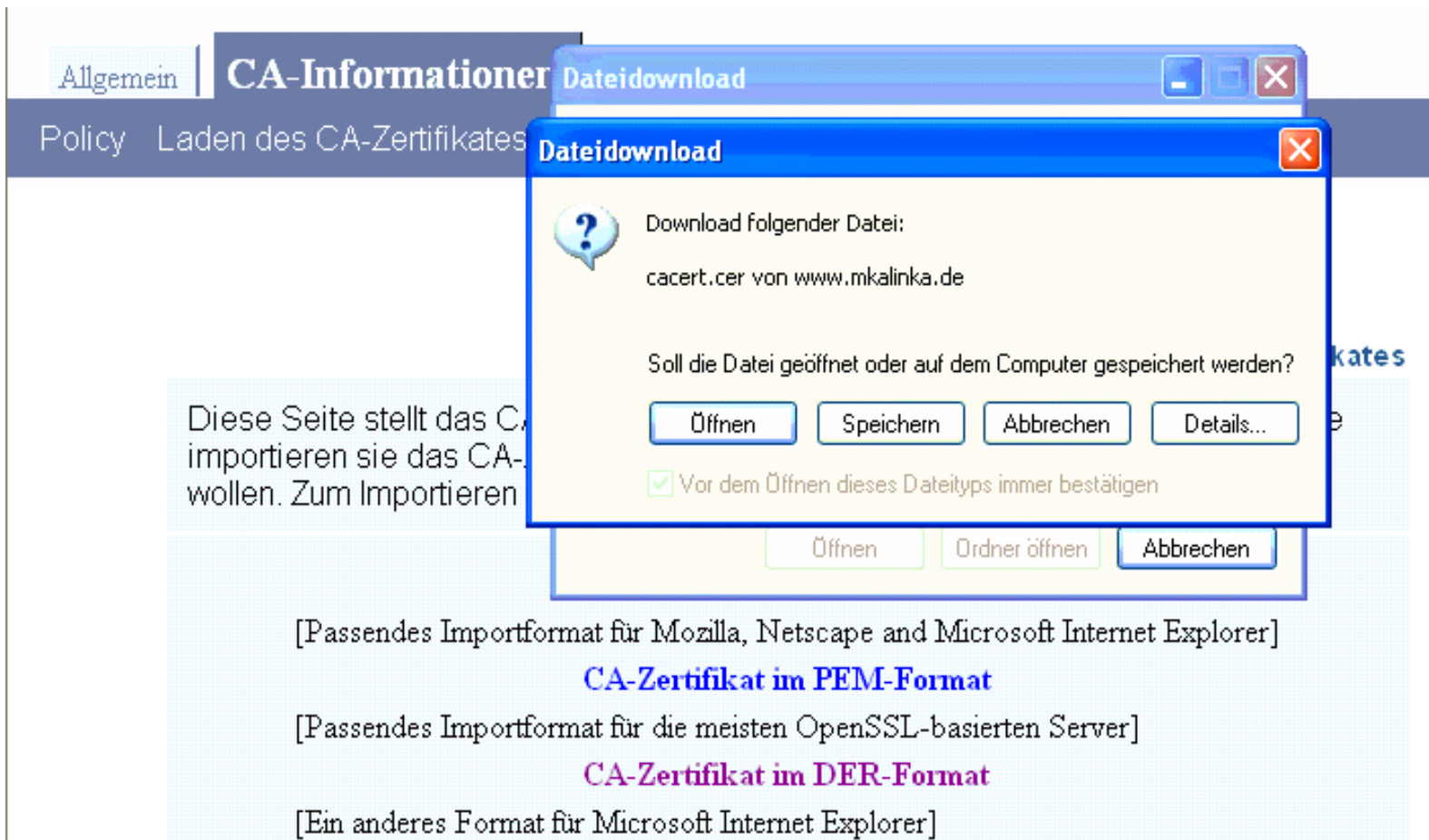
- PFX to p12 (Microsoft-proprietär)

- `cp cert_key.pfx cert_key.p12`

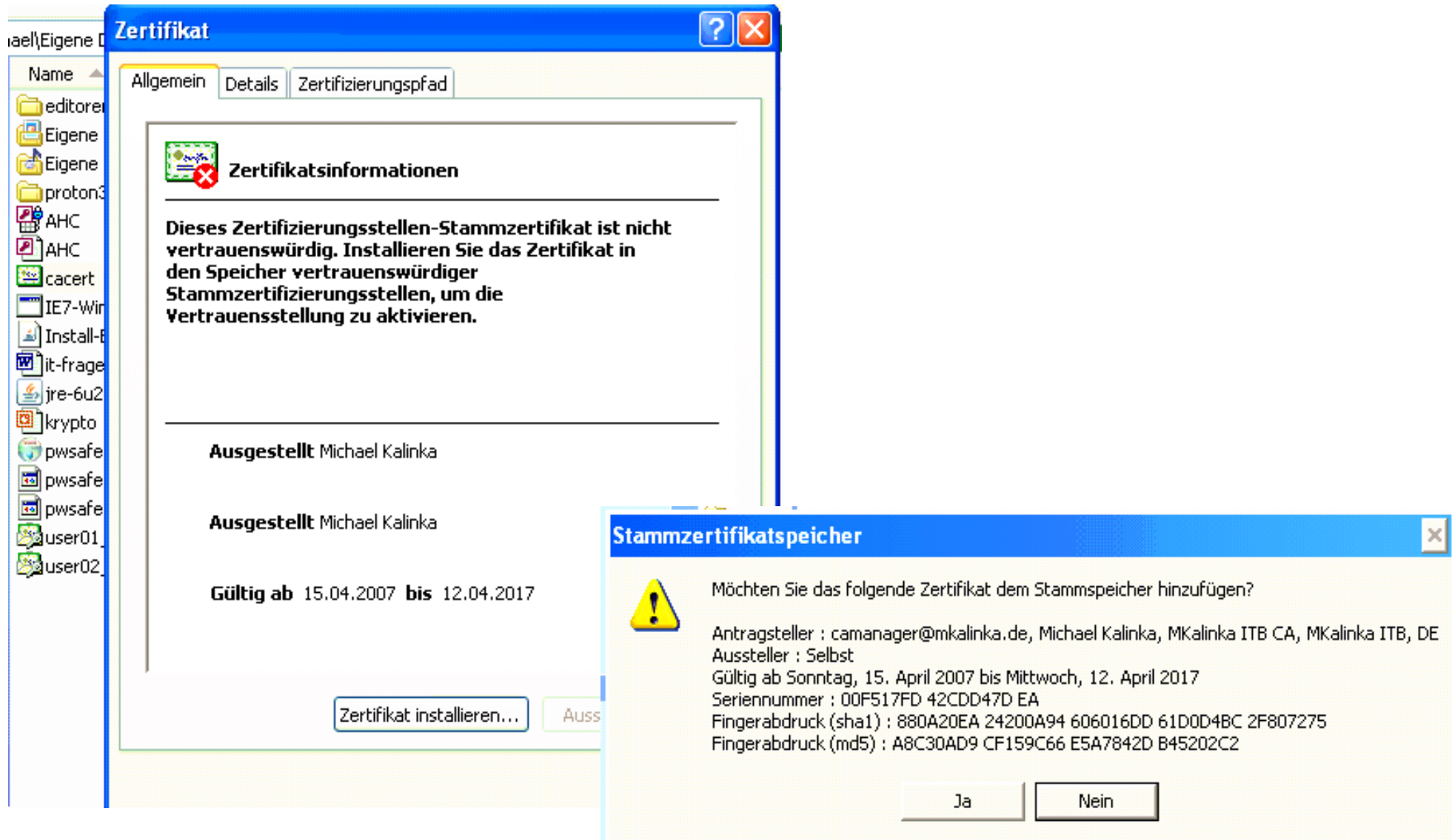
Literatur

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/verschlueselung_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		

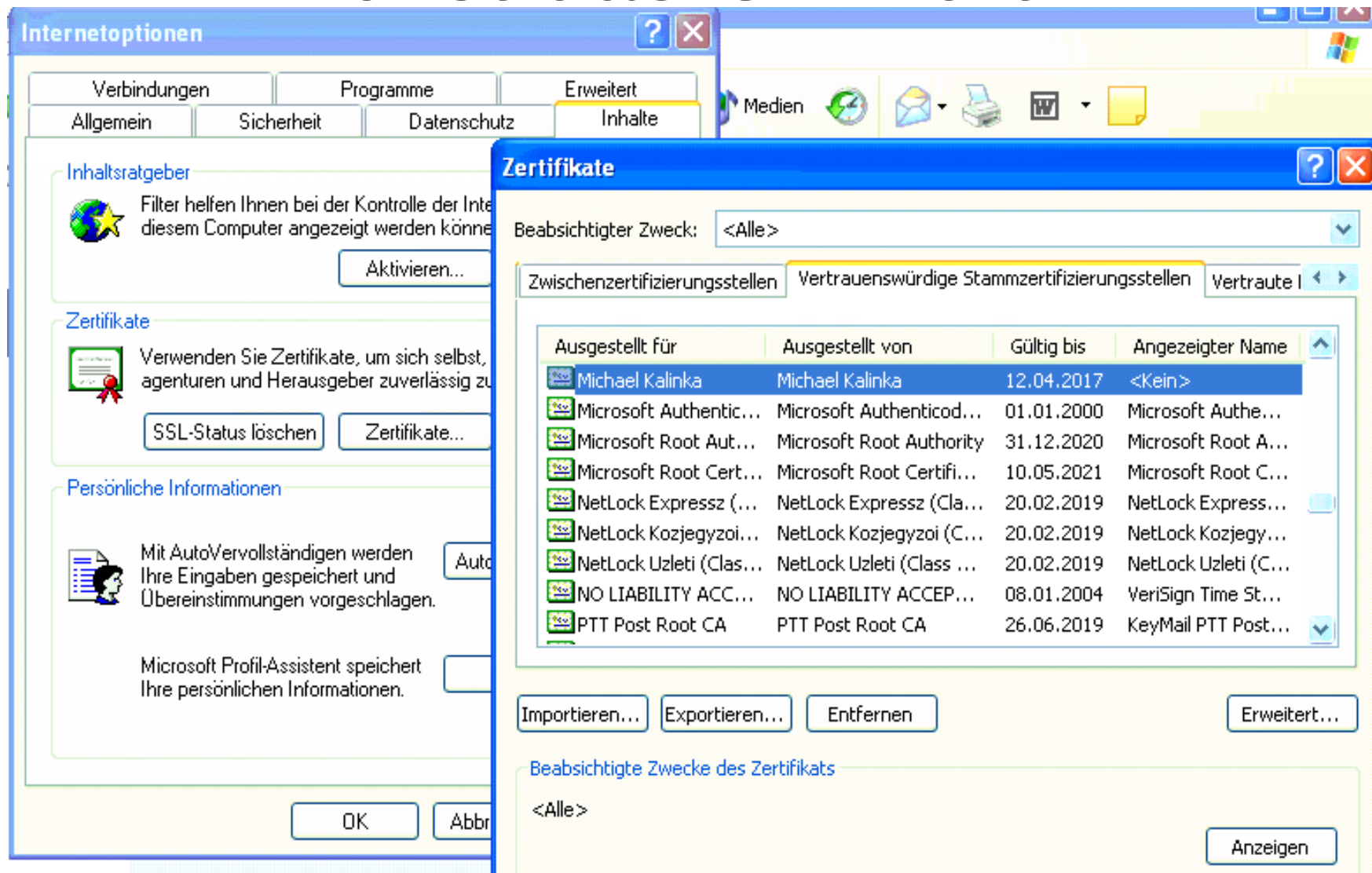
CA-Zert download



CA-Zert installieren



Wo ist das CA-Zert ?



IE6 : CSR erstellen



Navigation: Allgemein | CA-Informationen | **Nutzer** | Zertifikate | Anträge | Language

Beantragen eines Zertifikates | Laden des beantragten Zertifikates | Test Certificate | Zertifikat löschen

Beantragen eines Zertifikates mit automatischer Browsererkennung
[Benutzen Sie diesen Link, wenn Sie nicht wissen, was Sie tun sollen]

Allgemeiner Zertifizierungsantrag
[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]

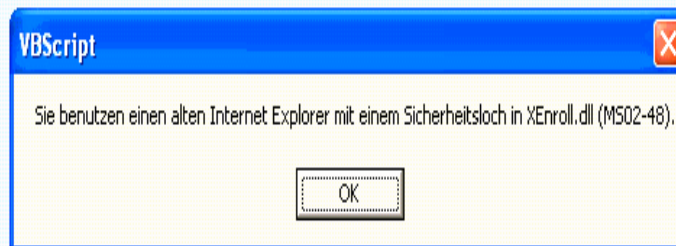
IE6 CSR Daten

E-Mail	<input type="text" value="user04@mkalinka.de"/>
Name	<input type="text" value="Unknown User Nr 4"/>
Organisationseinheit	<input type="text" value="Internet"/>
alternative email	<input type="text" value="user04@mkalinka.de"/>
IP address	<input type="text"/>
DNS name	<input type="text"/>
DNS name	<input type="text"/>
User Data	
Name (Vor- und Nachname)	<input type="text" value="Unknown User Nr 4"/>
E-Mail	<input type="text" value="user04@mkalinka.de"/>
Einrichtung	<input type="text" value="MKalinka ITB"/>
Telefon	<input type="text"/>
Niveau der Identifizierung (LOA) wählen Sie das Niveau der Identifizierung, welches Sie erfüllen wollen	<input type="text" value="Test"/>
Rolle	<input type="text" value="Mail Server"/>
Registrierungsinstanz (RA) wählen Sie die Registrierungsinstanz, welche Sie benutzen wollen	<input type="text" value="Trustcenter selbst"/>
PIN [used to verify the certification request, min 10 chars (please write it down for later usage)]	<input type="text" value="....."/>
Nochmalige Eingabe der PIN zur Bestätigung	<input type="text" value="....."/>

IE6 CSR privatekey

Bestätigung des Zertifizierungsantrages

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



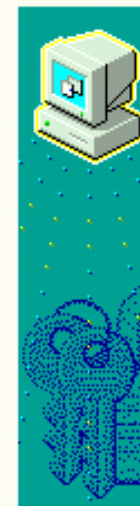
DNS name

DNS name

User Data

Name (Vor- und Nachname)	Unknown User Nr 4
E-Mail	user04@mkalinka.de
Einrichtung	MKalinka ITB
Telefon	
Niveau der Identifizierung (LOA) Test	
Rolle	Mail Server
Registrierungsinstanz	Trustcenter selbst
Schlüssellänge	1024
Kryptografisches Gerät	Standard

Ein neuer RSA-Austauschschlüssel wird erstellt.



Eine Anwendung erstellt ein geschütztes Objekt.

Privater Schlüssel des Cry

Sie haben die mittlere
Sicherheitsstufe gewählt

Sicherheitsstufe...

OK

Abbrechen

Details...

VBSript

Der Zertifikatsantrag wurde erfolgreich erzeugt.

OK

Firefox CSR



Firefox CSR Daten

Zertifikatsdaten	
E-Mail	<input type="text" value="user02@mkalinka.de"/>
Name	<input type="text" value="Test User02"/>
Organisationseinheit	<input type="text" value="Internet"/>
alternative email	<input type="text"/>
IP address	<input type="text"/>
DNS name	<input type="text"/>
DNS name	<input type="text"/>

User Data	
Name (Vor- und Nachname)	<input type="text" value="Test User02"/>
E-Mail	<input type="text" value="user02@mkalinka.de"/>
Einrichtung	<input type="text" value="MKalinka ITB"/>
Telefon	<input type="text" value="+49 431 728426"/>
Niveau der Identifizierung (LOA) wählen Sie das Niveau der Identifizierung, welches Sie erfüllen wollen	<input type="text" value="Test"/>
Rolle	<input type="text" value="User"/>
Registrierungsinstanz (RA) wählen Sie die Registrierungsinstanz, welche Sie benutzen wollen	<input type="text" value="Trustcenter selbst"/>
PIN [used to verify the certification request, min 10 chars (please write it down for later usage)]	<input type="text" value="*****"/>
Nochmalige Eingabe der PIN zur Bestätigung	<input type="text" value="*****"/>
Wählen einer Schlüssellänge	<input type="text" value="1024"/>

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) ▼

Kein Hinweis auf den privatekey

Weiter

RA : CSR bearbeiten

OpenCA - Mozilla Firefox <2>

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.mkalinka.de/cgi-bin/ra/RAServer

Google

Allgemein **Aktive CSRs** Aktive CRRs Information Hilfsmittel Language

Neu Erneuert In Bearbeitung Auf weitere Genehmigung wartend

Neue Zertifizierungsanträge

Dienstag den 10. Juli 06:55:25 (UTC)

Seriennummer	Name des Absenders	Übermittelt am	Beantragte Rolle	Beantragte Identifizierung des Nutzers (LOA)
2592	emailAddress=user02@mkalinka.de, CN=Test User02, OU=Internet, O=MKalinka ITB, C=DE	Tue Jul 10 06:51:13 2007 UTC	User	Test

Weitere Ergebnisse <

Fertig

www.mkalinka.de

RA : CSR bearbeiten

Variable	Wert		
Antragsversion	1		
Seriennummer	2592		
Name	Test User02		
E-Mail	user02@mkalinka.de		
Alternativer Name des Zertifikats	email.O=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	7d7099dfd4835647b5a7fa877e be9bd3529573a0		
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:f0:2b:04:4b:6c:00:2a: 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

Alternativer Name:		
emailAddress	user02@mkallinka.de	+
CM	Test User02	+
OU	Interne I	+
O	MKallinka ITB	+
C	DE	+
Rolle	User	
Valid for ## days	365	
Notafter (YYYY-MM-DD hh:mm:ss)		
Notbefore (YYYY-MM-DD hh:mm:ss)		
LOA	Test I	
Benutzt PIN zur Identifizierung	7d7099dd1b4830647b0a71b877ebesbdc3029073a0	
Schlüsselgröße (Modulus)	1024	
Algorithmus des öffentlichen Schlüssels	rsaEncryption	
Signaturalgorithmus	nicht vorhanden	
Name (Vor- und Nachname)	Test User02	
E-Mail	user02@mkallinka.de	
Einrichtung	MKallinka ITB	
Telefon	+49 431 728426	
RA	Trustcenter selbst	

Gültigkeitsdauer eintragen

Genehmigung ohne Signatur

Gültigkeitsdauer eintragen
Genehmigung ohne Signatur

CA : CSR finden

OpenCA - Mozilla Firefox <2>

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

https://www.mkalinka.de/cgi-bin/ca/ca

Allgemein **Normale Operationen** Aktive CSRs Aktive CRRs Information Language

Genehmigte Zertifizierungsanträge Genehmigte Rückrufe Erstellen einer neuen CRL Issue certificates (automaticly) Revoke certificates (a

Genehmigte Zertifizierungsanträge

Dienstag den 10. Juli 07:08:40 (UTC)

Operator	Seriennummer	Name des Absenders	Genehmigt am	Beantragte Rolle	Beantragte Identifizierung des Nutzers (LOA)
nicht vorhanden	2592	emailAddress=user02@mkalinka.de, CN=Test User02, OU=Internet, O=MKalinka ITB, C=DE	nicht vorhanden	User	Test

Keine weiteren Ergebnisse

CA : CSR signieren

Sie sehen nun die Details des Zertifizierungsantrages (CSR).

Dienstag den 10. Juli 07:11:28 (UTC)

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)	365
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

[CA Login für kryptographisches Gerät](#)

Bitte geben Sie Ihre Daten in das folgende Formular ein.

Passwort

[OK](#)

[Zurücksetzen](#)

Exponent: 65537 (0x10001)

Signaturalgorithmus	nicht vorhanden
Name (Vor- und Nachname)	Test User02
E-Mail	user02@mkalinka.de
Einrichtung	MKalinka ITB
Telefon	+49 431 738426

Operationen

[Zertifikatausstellen](#)

[Zertifikat ausstellen](#)

[Delete request](#)

[Delete request](#)

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 Zertifikats	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

Get Additional Parameters

Sie müssen einige zusätzliche Parameter für die gewünschte Funktionalität eingeben.

In der E-Mail, die Sie von uns erhalten haben sollten, ist eine Seriennummer enthalten, die Sie hier nun eingeben müssen. Wenn Sie einen browserspezifischen Antrag gestellt haben, dann ist es nötig, dass nun denselben Browser benutzen, mit welchem Sie den Antrag erstellt haben. Bitte geben Sie nun die Seriennummer des Zertifikates ein oder nutzen Sie die Möglichkeit der Eingabe der Seriennummer des Antrages, wenn Sie die Seriennummer des Zertifikates nicht zur Hand haben.

Seriennummer

Art der Seriennummer

Seriennummer des Zertifikates ▼

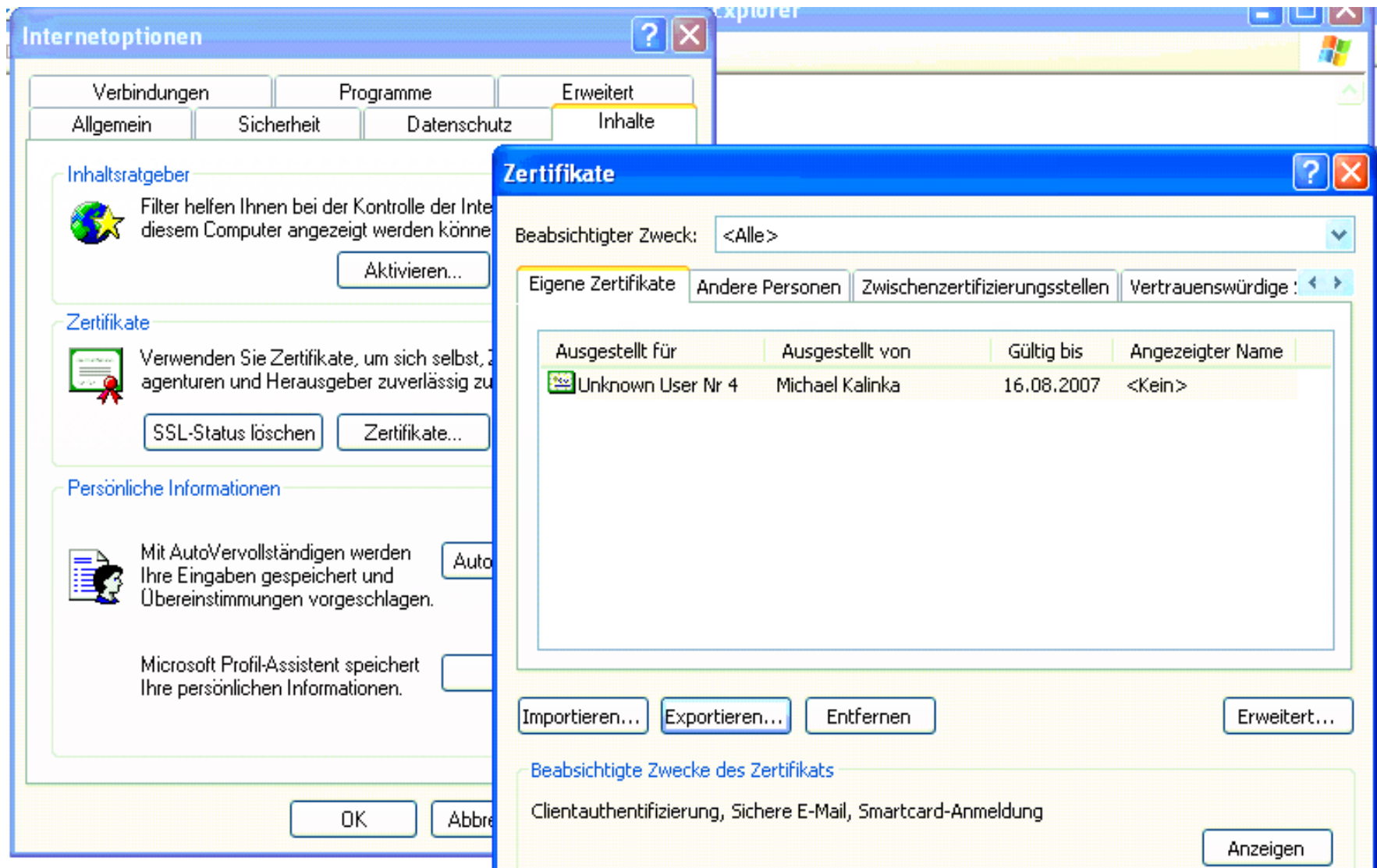
Zertifikatsinstallation für Internet Explorer - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zertifikatsinstallation für Internet Explorer

Das Zertifikat wurde erfolgreich installiert.

IE6 wo ist das Zert ?



IE6 exportCert

The screenshot shows the 'Zertifikatsexport-Assistent' (Certificate Export Wizard) in Internet Explorer 6. The wizard is divided into two main sections: 'Privaten Schlüssel exportieren' (Export Private Key) and 'Exportdateiformat' (Export File Format).

Privaten Schlüssel exportieren
Sie können den privaten Schlüssel mit dem Zertifikat exportieren.

Private Schlüssel sind kennwortgeschützt. Wenn Sie das ausgewählte Zertifikat exportieren möchten, müssen Sie ein Kennwort eingeben.

Möchten Sie mit dem Zertifikat auch den privaten Schlüssel exportieren?

- ☒ Ja, privaten Schlüssel exportieren
- ☐ Nein, privaten Schlüssel nicht exportieren

Exportdateiformat
Zertifikate können in verschiedenen Dateiformaten exportiert werden.

Wählen Sie das gewünschte Format:

- ☐ DER-codiert-binär X.509 (.CER)
- ☐ Base-64-codiert X.509 (.CER)
- ☐ Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
 - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- ☒ Privater Informationsaustausch - PKCS #12 (.PFX)
 - ☐ Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
 - ☒ Verstärkte Sicherheit aktivieren (IE 5.0, NT 4.0 SP4 oder höher erforderlich)
 - ☐ Privaten Schlüssel nach erfolgreichem Export löschen

Kennwort
Der private Schlüssel muss mit einem Kennwort geschützt zu gewährleisten.

Geben Sie ein Kennwort ein und bestätigen Sie dieses.

Kennwort:

Kennwort bestätigen:

Buttons: Importieren..., Exportieren..., < Zurück, Weiter >, Abbrechen

Exportdatei als .p12

Kennwort

Der private Schlüssel muss mit einem Kennwort geschützt zu gewährleisten.

Geben Sie ein Kennwort ein und bestätigen Sie dieses.

Kennwort:

Kennwort bestätigen:

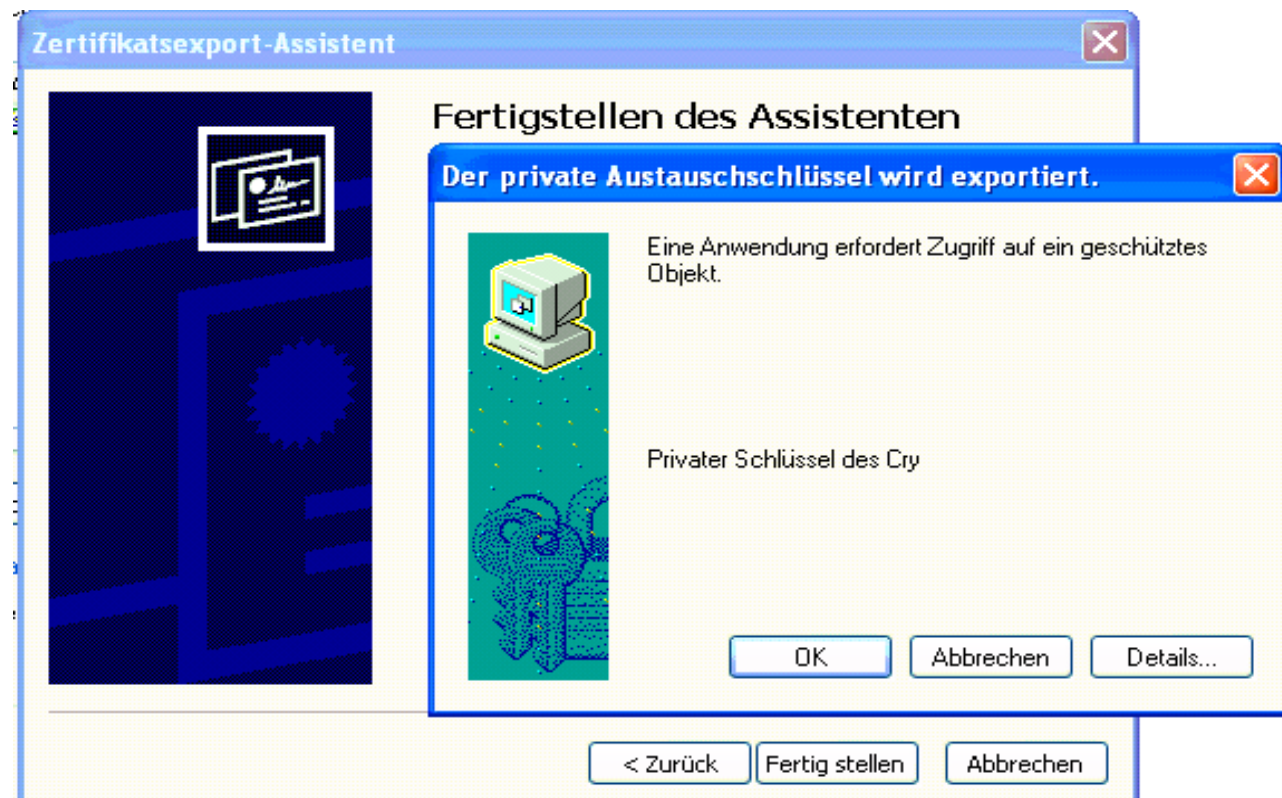
Exportdatei

Geben Sie die den Namen der zu exportierenden Datei an.

Dateiname:

user04_at_mkalinka_de .p12

Durchsuchen..



PUB : Zertifikat abholen

[Get Additional Parameters](#)

Sie müssen einige zusätzliche Parameter für die gewünschte Funktionalität eingeben.

In der E-Mail, die Sie von uns erhalten haben sollten, ist eine Seriennummer enthalten, die Sie hier nun eingeben müssen. Wenn Sie einen browserspezifischen Antrag gestellt haben, dann ist es nötig, dass nun denselben Browser benutzen, mit welchem Sie den Antrag erstellt haben. Bitte geben Sie nun die Seriennummer des Zertifikates ein oder nutzen Sie die Möglichkeit der Eingabe der Seriennummer des Antrages, wenn Sie die Seriennummer des Zertifikates nicht zur Hand haben.

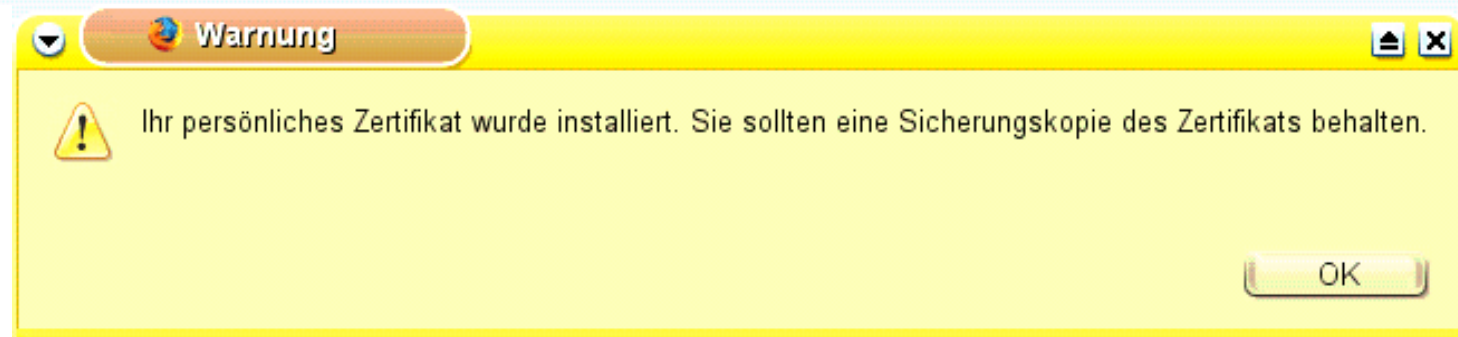
Seriennummer

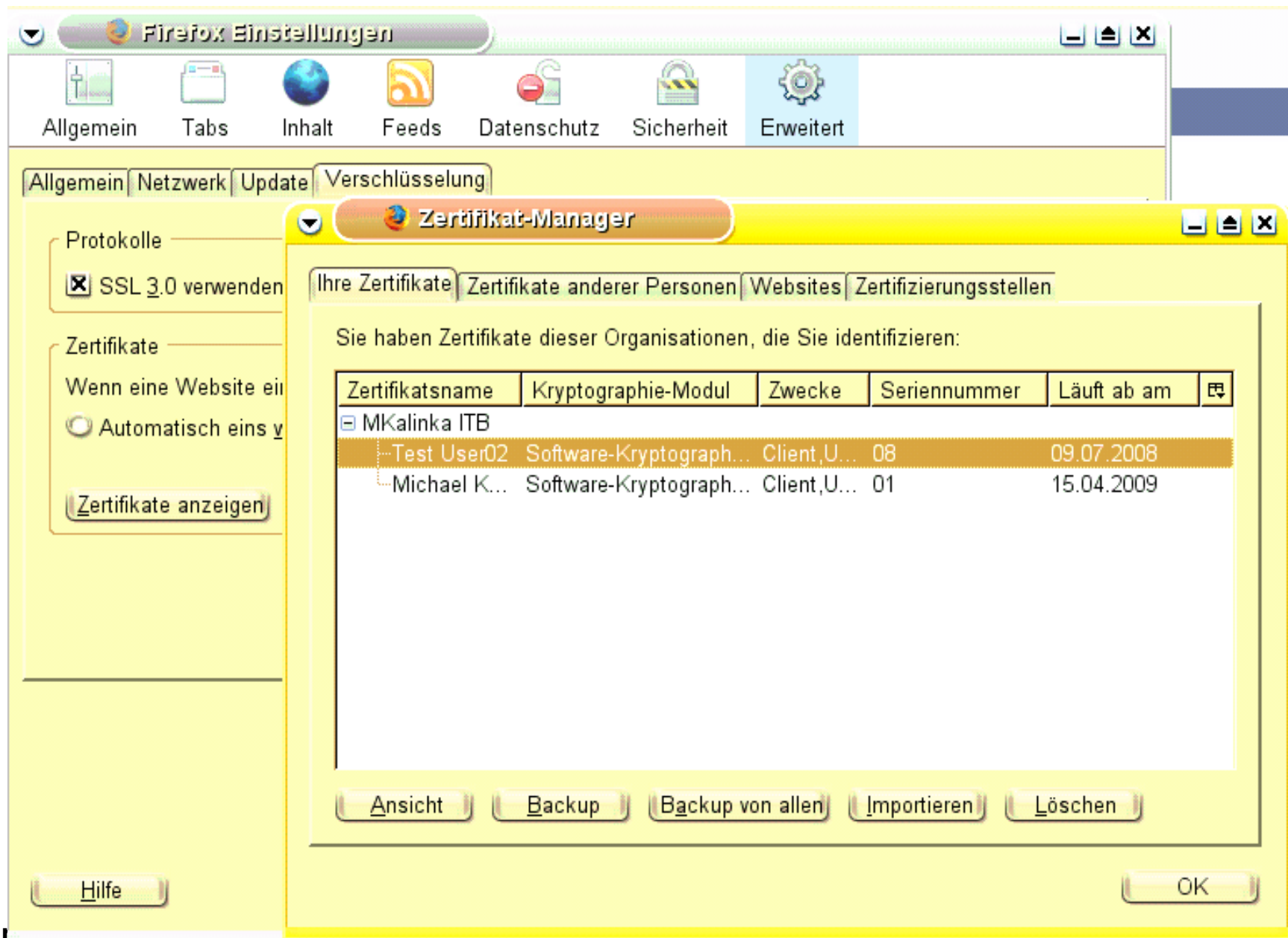
Art der Seriennummer

Seriennummer des Zertifikates ▼

OK

Zurücksetzen





Dateiname für Backup

Name:

In Ordner speichern:

Ordner-Browse

Wählen Sie ein Zertifikats-Backup-Passwort

Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Backup-Datei, die Sie jetzt erstellen möchten. Sie müssen dieses Passwort festlegen, um mit dem Backup fortzufahren.

Zertifikats-Backup-Passwort:

Zertifikats-Backup-Passwort (nochmals):


Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können Sie dieses Backup später nicht wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder.

Passwort-Qualitätsmessung

Warnung

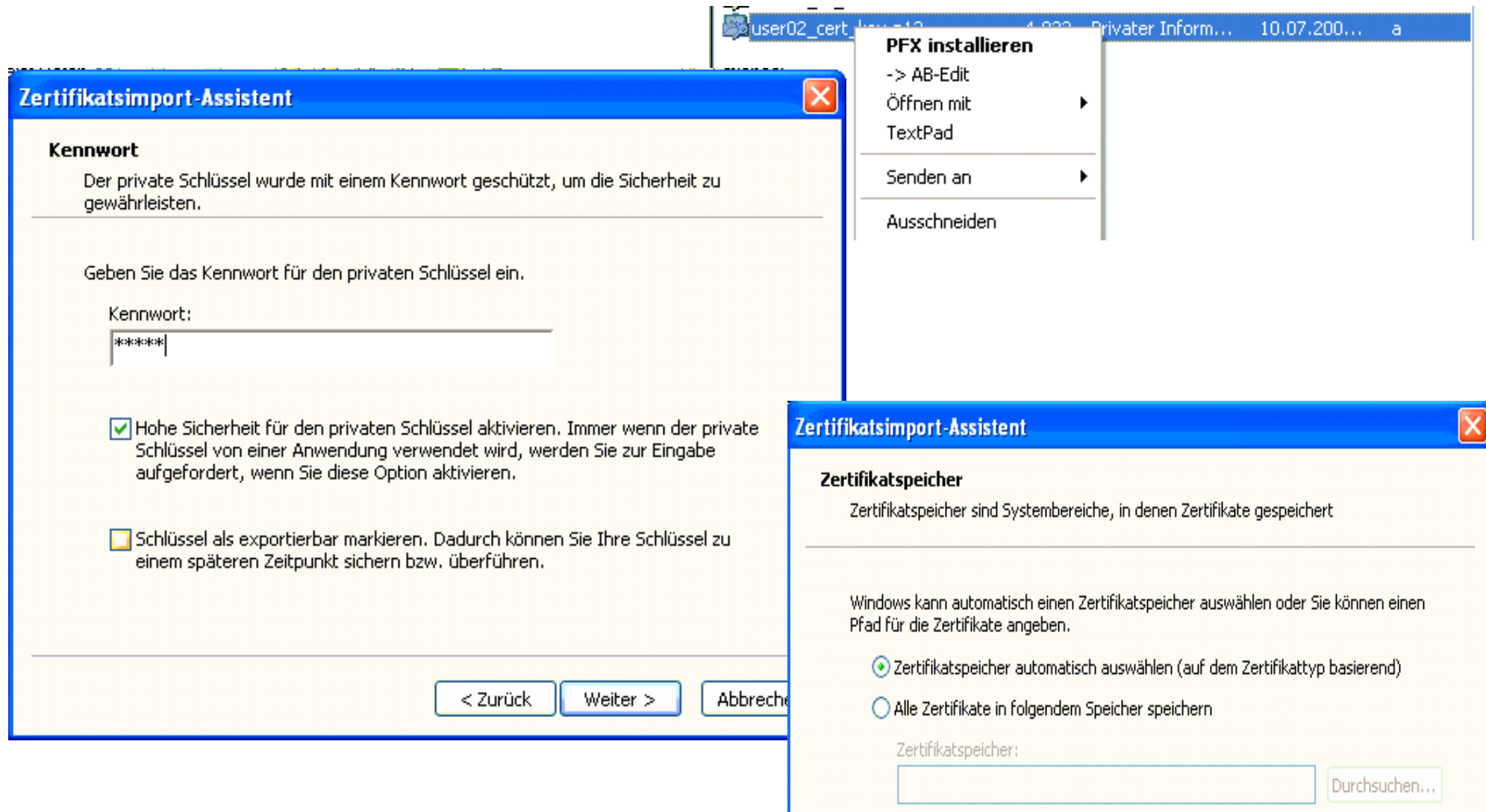
! Ihre Sicherheitszertifikate und privaten Schlüssel wurden erfolgreich wiederhergestellt.

OK

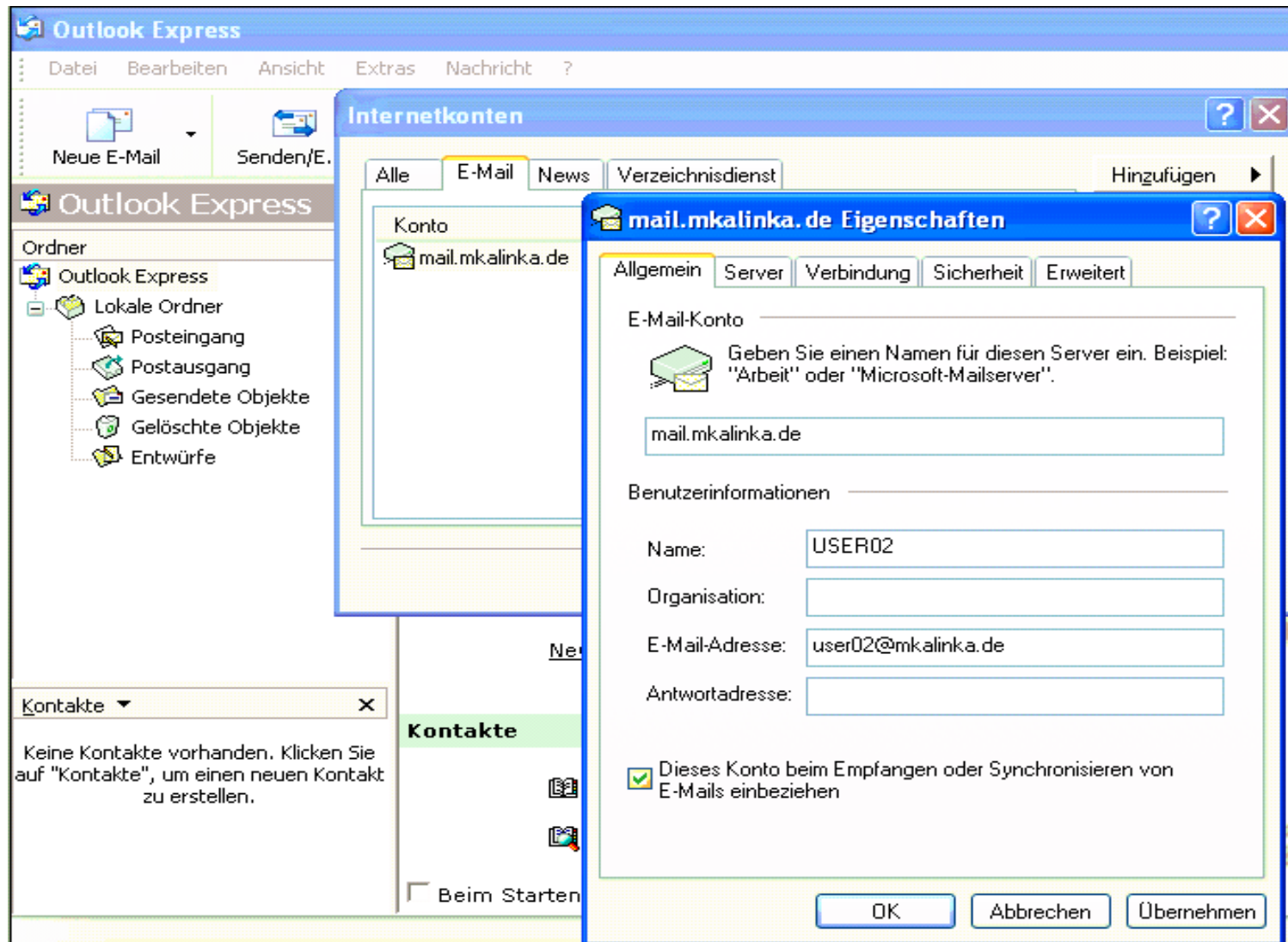
 user02_cert_key.p12

4,8 KB Zertifikatpaket PKCS#12

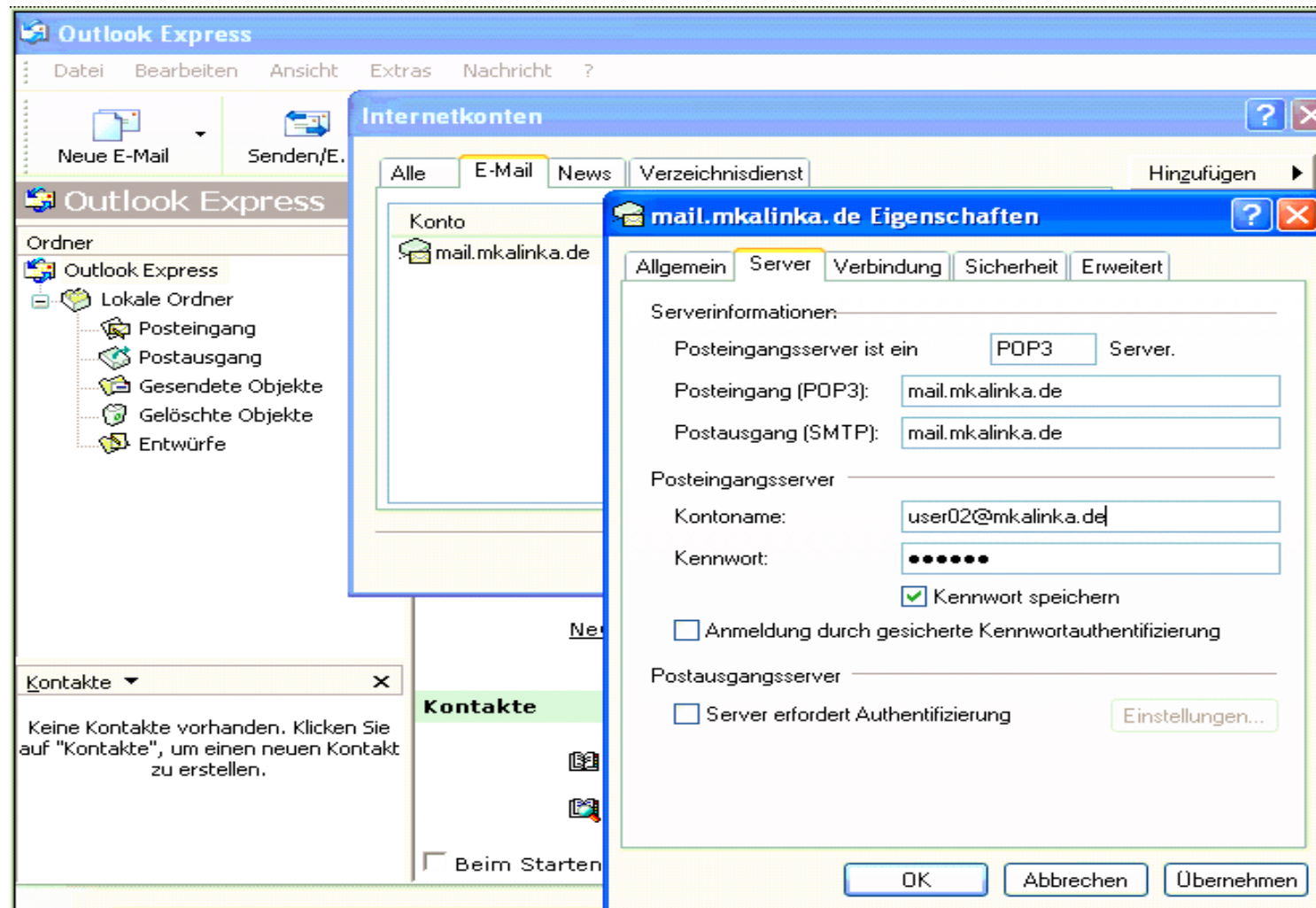
Windows Import .p12



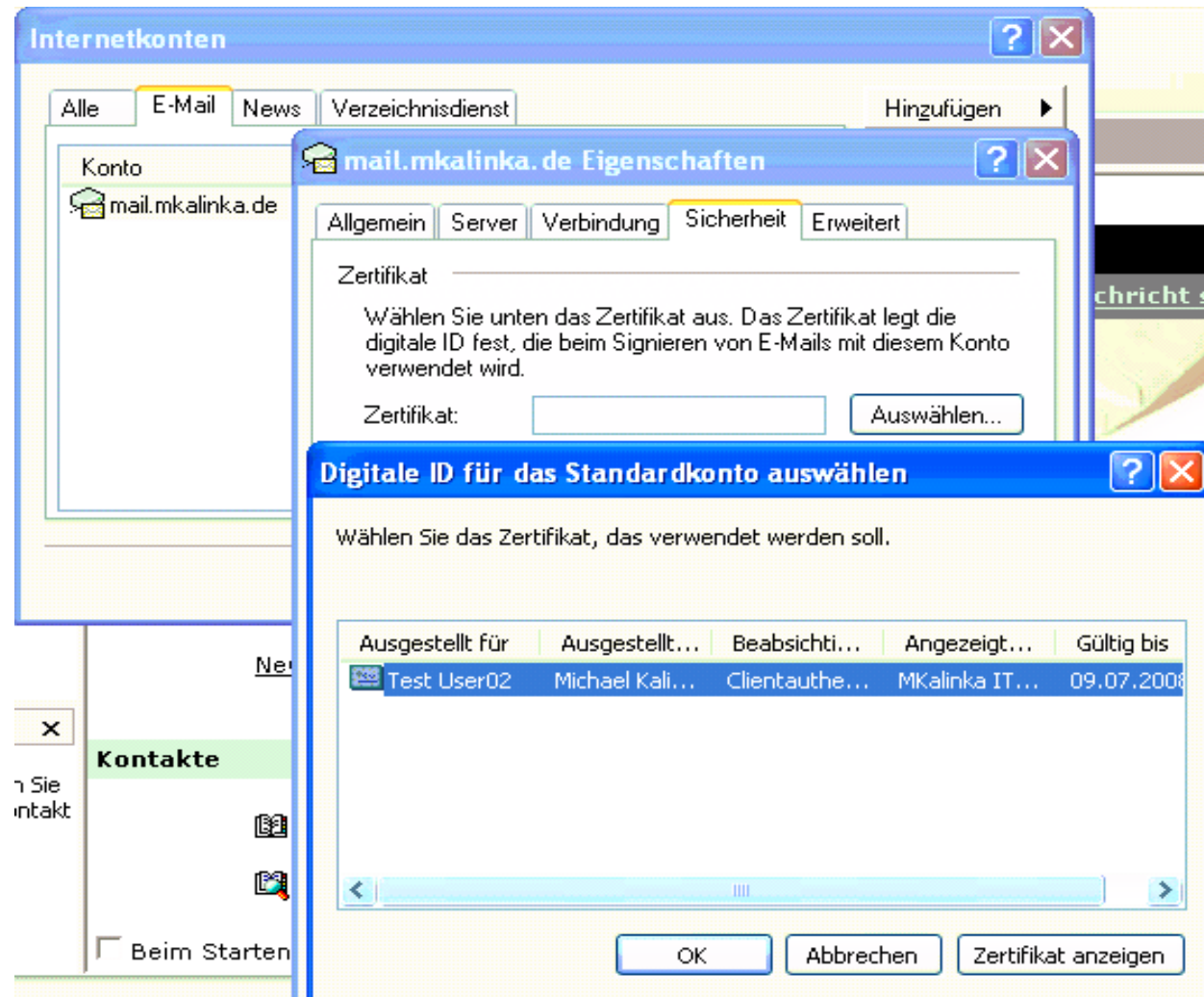
OE Mail-Konto



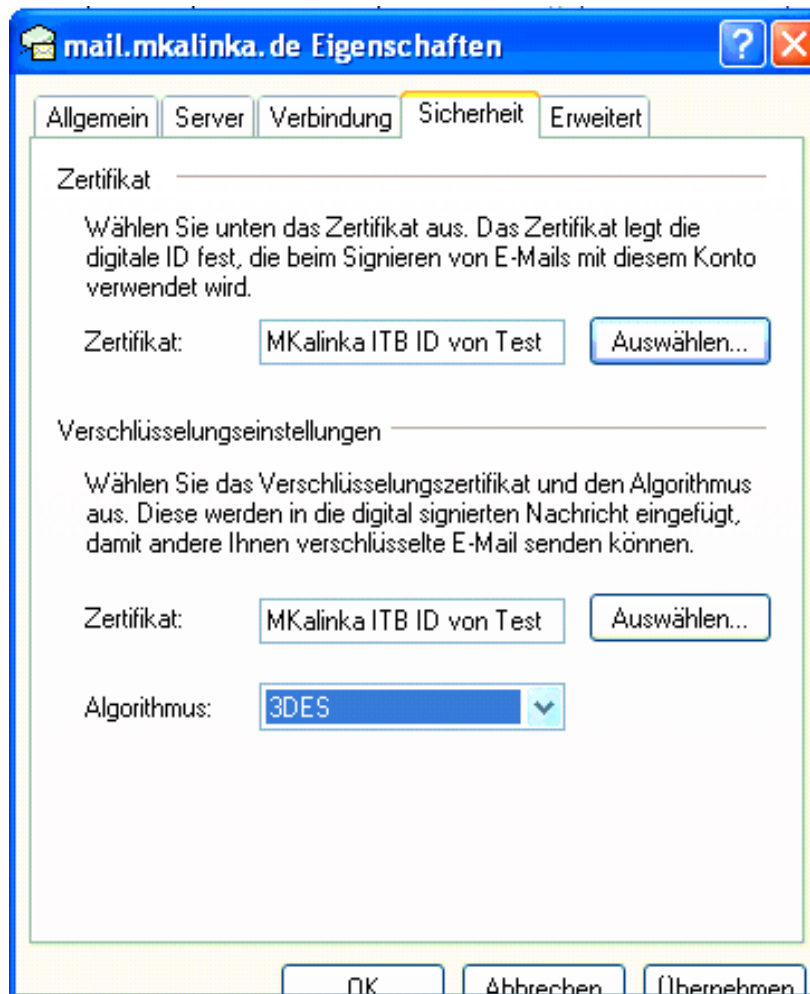
OE Mail-Server



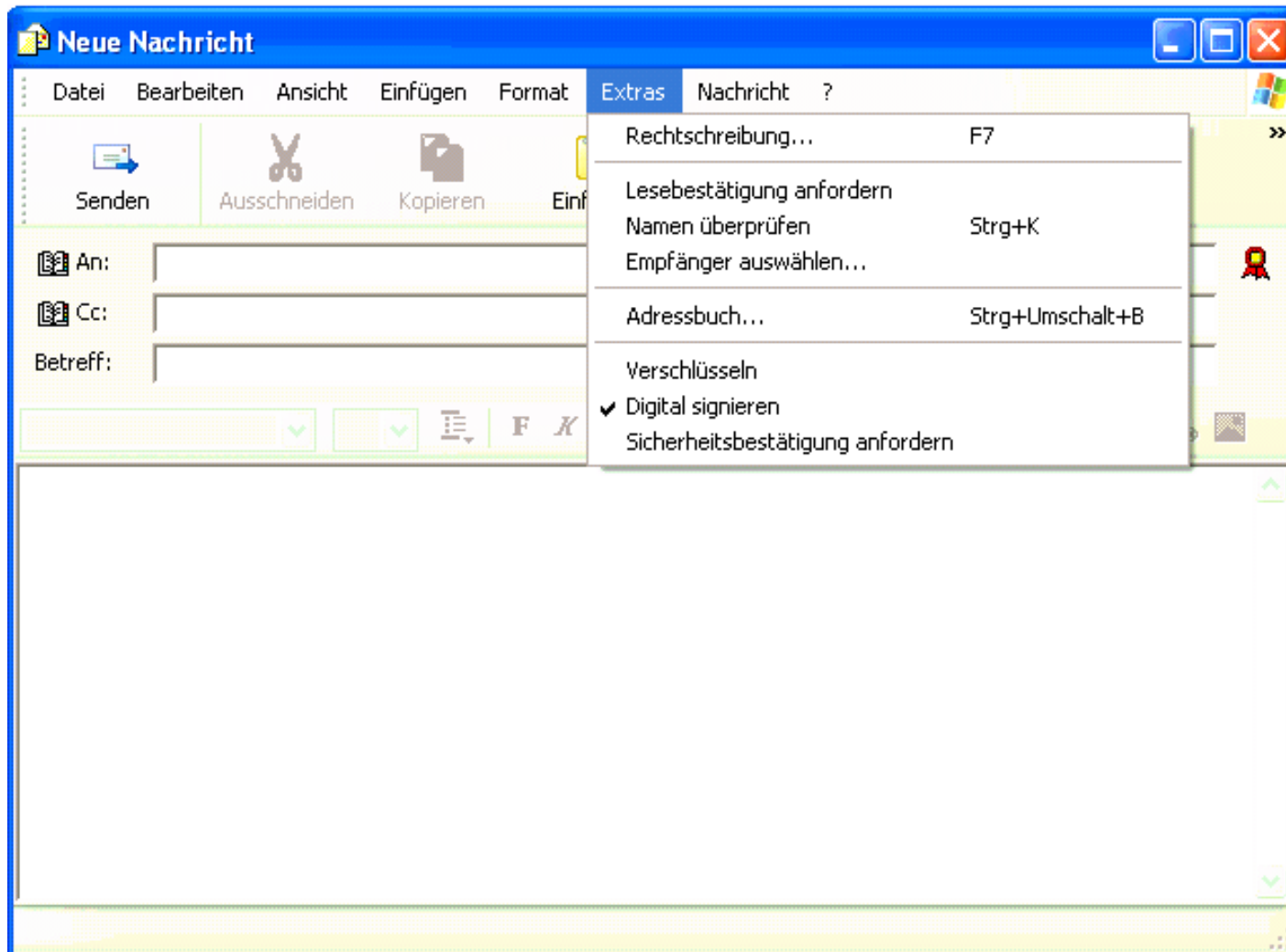
OE Mail-Sicherheit



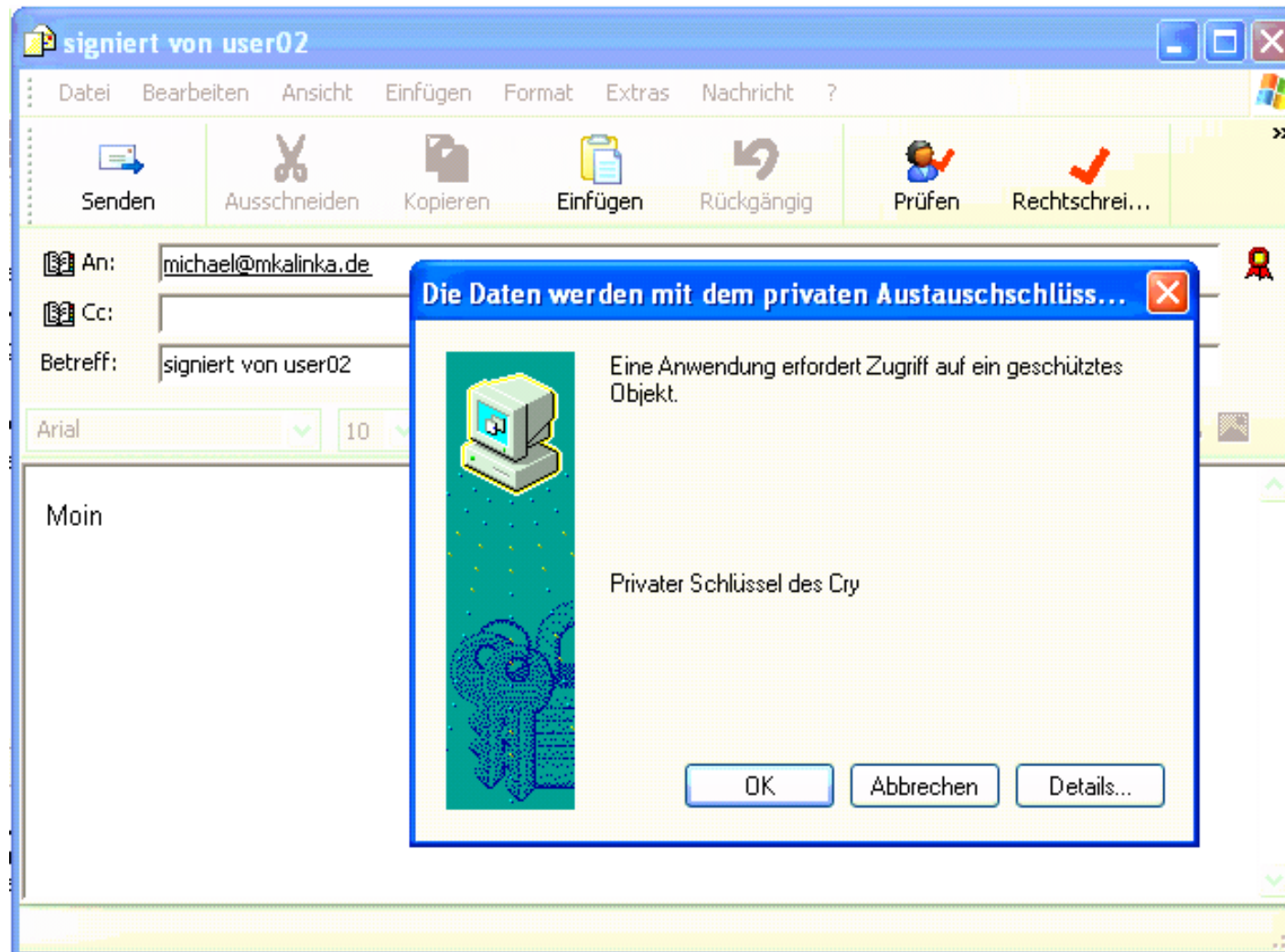
OE Userzertifikat



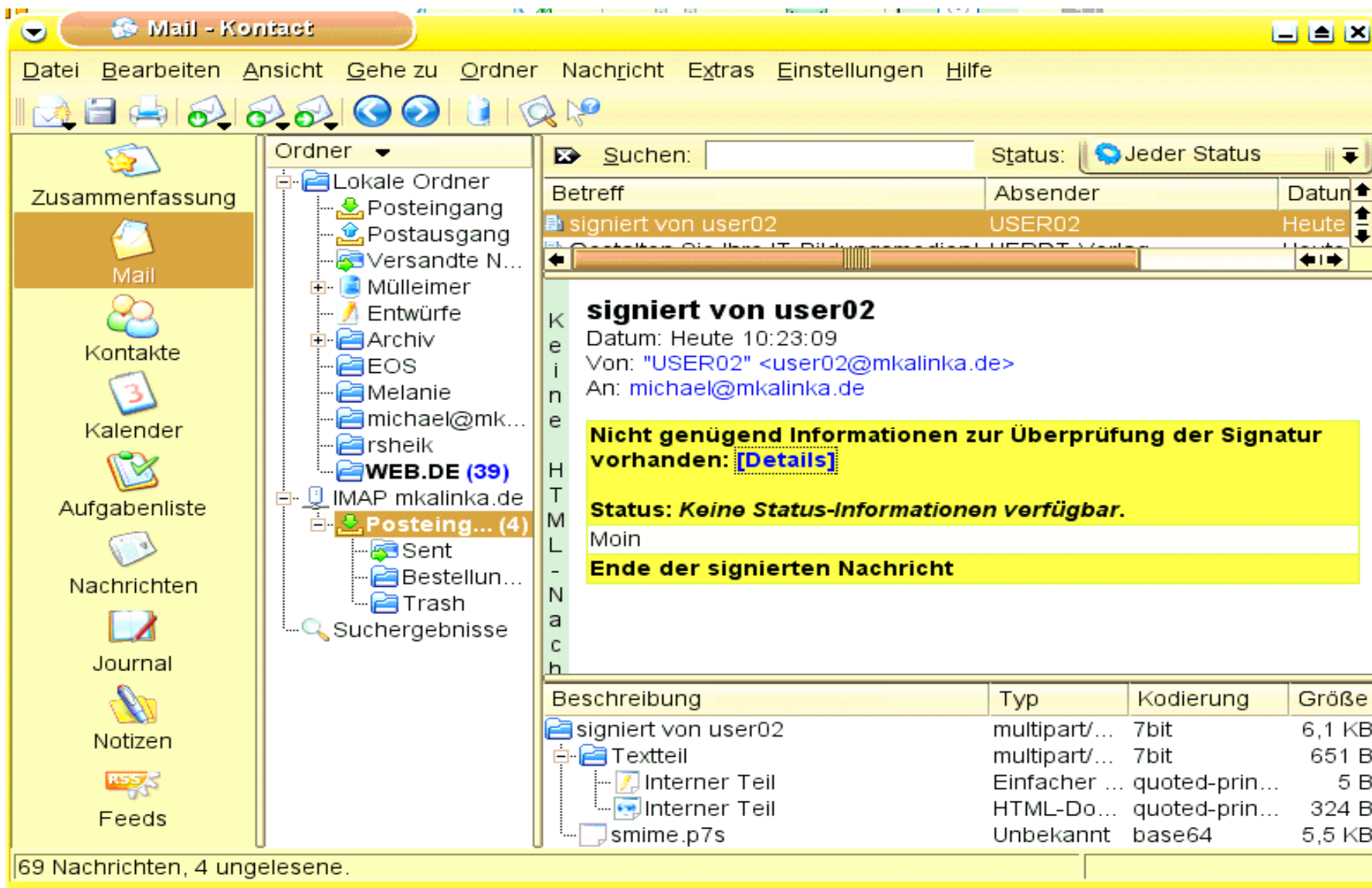
OE Signatur



OE Versand




KMail Empfang ohne Zertifikat



Kmail Signaturprüfung ok

K
e
i
n
e

H
T
M
L
-
N
a
c
h
r
i
c
h
t

signed from user04	
Von:	user04@mkalinka.de
An:	user01@mkalinka.de
Datum:	Heute 14:20:11
Spam-Status:	Spamassassin 

Die Nachricht wurde von CN=Unknown User Nr 4, OU=Internet, SerialNumber=10, DC=mkalinka, DC=de auf 17.07.2007 14:20 mit dem Schlüssel 0xCC393DB55CEF2B38 signiert.

Status: Korrekte Signatur.

Moin user 01

Ende der signierten Nachricht