

YES, we can!

Fälschungssichere
und vertrauliche E-Mail
mit S/MIME

15. Dezember 2010

Ingmar Camphausen <ingmar@mi.fu-berlin.de>

Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- Wie bekomme ich, was ich dafür brauche?
- „Mehrwert“: digitale Unterschrift
- Klappen umschiffen
- S/MIME vs. PGP/GnuPG, NPA und De-Mail

Motivation

- Geheime Nachrichten austauschen macht Spaß! :-)

**DIE SES TRE
NGG EHE IME
NAC HRI CHT
IST NIC HTF
UER FRE MDE
AUG ENB EST
IMM TXY**

„Früher war alles schlechter“ (< Jahr 2000)

- US-Exportverbot für Verschlüsselung („ammunition“!)
- fehlende Unterstützung in E-Mail-Programmen
- Kryptokontroverse (Schlüsselhinterlegung!)
 - USA: „Clipper-Chip“
 - DE: BMI Kanther
- Algorithmen z.T. patentiert
- Software selbst besorgen, compilieren, installieren...

„Heute ist alles besser“ :-)

- nur noch ein Schlüsselpaar erzeugen
- keine Software-Installation mehr nötig
↳ keine Admin-Rechte erforderlich!
- geeignete Software bei uns schon vorhanden
- notwendige Infrastruktur bei uns schon vorhanden
- Schlüssel des jeweiligen Komm.-Partners beschaffen
 - geht größtenteils automatisch
 - nur für verschlüsselung erforderlich (nicht für Signaturen)

Unterstützung in gängigen Mail-Programmen



MS Outlook (auch Mac-Version)



Thunderbird



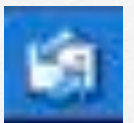
Apple Mail



KMail, Evolution



mutt, alpine

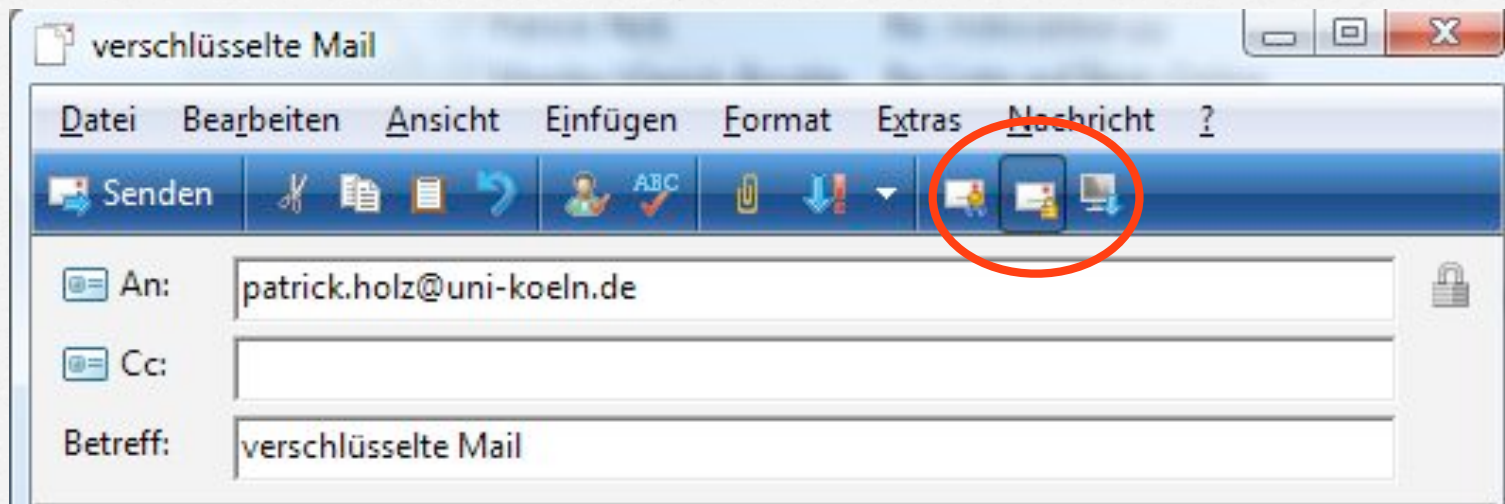


MS Outlook Express/Windows Mail



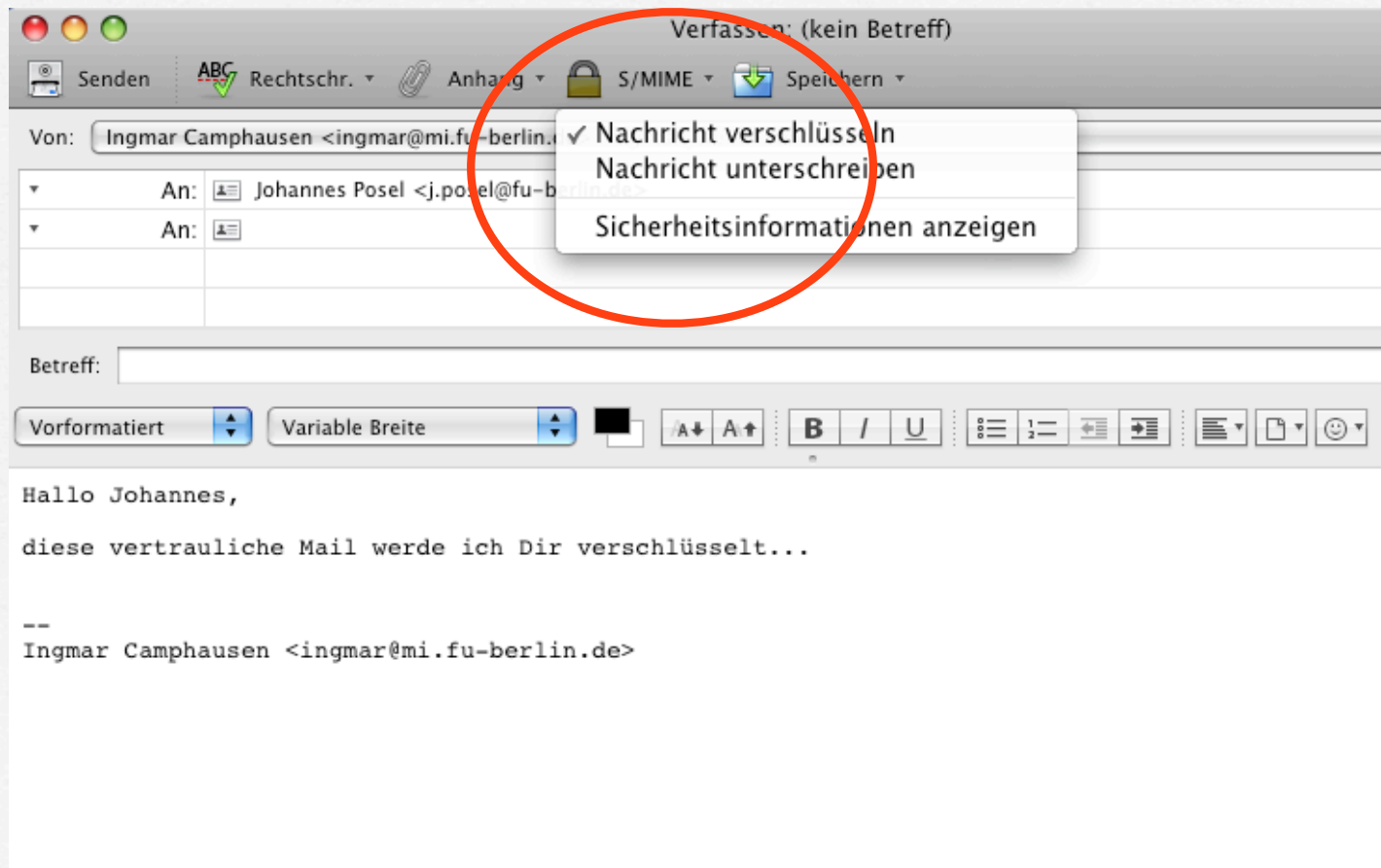
Webmailer: z.T. ja (GMX, WEB.DE)

Verschlüsselte Mail „live“ – Senden (Windows Mail)



<http://www.uni-koeln.de/rrzk/sicherheit/smime/iexplorer.html>

Verschlüsselte Mail „live“ – Senden (Thunderbird)



Verschlüsselte Mail „live“ – Senden (Apple Mail)



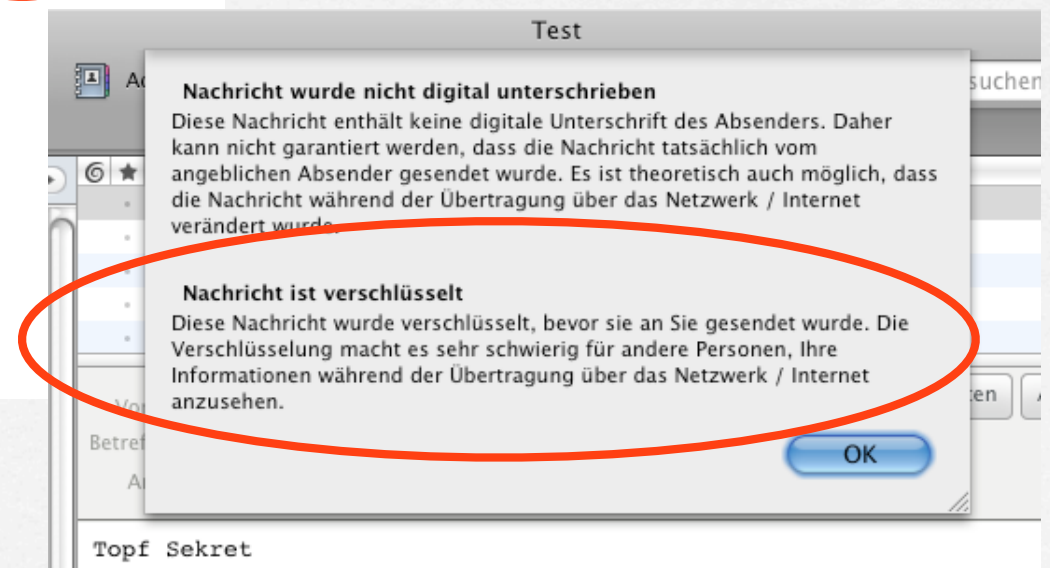
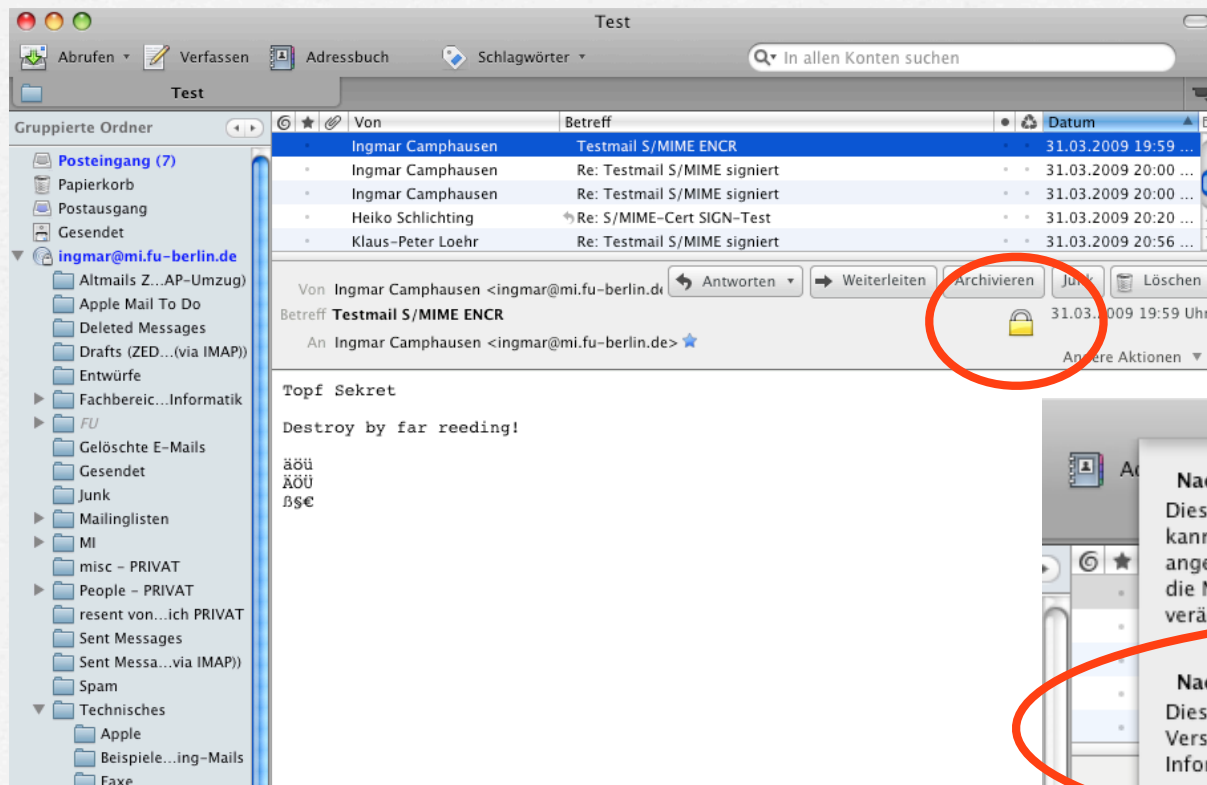
Verschlüsselte Mail „live“ – Empfangen (Windows Mail)

Von: Patrick Holz <patrick.holz@uni-koeln.de> **An:** Haiko Luepsen <luepsen@uni-koeln.de>
Betreff: Verschlüsselte Mail




<http://www.uni-koeln.de/rrzk/sicherheit/smime/iexplorer.html>

Verschlüsselte Mail „live“ – Empfangen (Thunderbird)



Verschlüsselte Mail „live“ – Empfangen (Apple Mail)


281	↳ Chr. von Stuckrad	Mist – nochmal – mutt hat den Default gelernt – ALTER key?	21. Jul 2009
285	→ BSCW Administrator	Sofortige Benachrichtigung per Email (https://bscw.zuv.fu...	24. Jul 2009
286	↳ Johannes Posel	Testnachricht S/MIME Apple Mail	11. Sep 2009
287	↳ Posel, Johannes	RE: Testnachricht S/MIME Apple Mail	11. Sep 2009
288	Ingmar Camphausen	test! (SIGN)	11. Sep 2009
289	Ingmar Camphausen	inbev -> mi	12. Sep 2009
290	↳ lens Dreier	Re: S/MIME-SIGN	20. Okt 2009
291			23. Okt 2009
292			24. Okt 2009
293			28. Okt 2009
306			21. Nov 2009
307			21. Nov 2009
308			21. Nov 2009
309			21. Nov 2009
310			22. Dez 2009
311			22. Dez 2009
312			22. Dez 2009
313			22. Dez 2009
314	↳ agathon	1. ausgehende Testmail via Exchange mittels IMAP	26. Jan 2010
315			4. Feb 2010
316	↳ Volker Roth	Re: Testmail (ich führe Digitale Signaturen vor... :-)	2. Mrz 2010

 **Mail möchte Ihre vertraulichen Informationen verwenden, die in „privateKey“ in Ihrem Schlüsselbund gesichert sind.**
Möchten Sie Zugriff auf dieses Objekt gewähren?

► Details

Immer erlauben Nicht erlauben Erlauben

264 ↳ Naumowicz Tomasz RE: Sig-Test (this mail signed b...

Von: Ingmar Camphausen <ingmar@mi.fu-berlin.de>
Betreff: S/MIME ENCR-only-Test
Datum: 31. März 2009 21:12:05 Uhr MESZ
An: Klaus-Peter Lohr <lohr@inf.fu-berlin.de>
Sicherheit:  Verschlüsselt

äöüÄÖÜ3€1s

Erstmal 'was Kleines als Fingerübung... ;-)

-I.

Ansicht in einem Programm, das S/MIME nicht unterstützt

ingmar *Ingmar Camphausen*

Webmail | Einstellungen | Services | Hilfe | Logout

Webmail | E-Mail schreiben | Adressen | Ordner | Optionen | Suchen

Aktueller Ordner: **Test**

[Nachrichtenliste](#) | [Löschen](#) | [Vorherige](#) | [Nächste](#) | [Weiterleiten](#) | [Als Anhang weiterleiten](#) | [Antworten](#) | [Allen Antworten](#)

Betreff: Testmail S/MIME ENCR
Von: "Ingmar Camphausen" <ingmar@mi.fu-berlin.de>
Datum: Di, 31.03.2009, 19:59
An: "Ingmar Camphausen" <ingmar@mi.fu-berlin.de>
Optionen: [Alle Kopfzeilen anzeigen](#) | [Druckversion zeigen](#) | [Nachrichtendetails anzeigen](#) | [Zum Adressbuch hinzufügen](#)

Anhänge:

smime.p7m	1 k	[application/pkcs7-mime]	Herunterladen
---------------------------	-----	----------------------------	-------------------------------

[Löschen & Vorherige](#) | [Löschen & Nächste](#)

Verschiebe nach:

INBOX

Verschieben

Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- Wie bekomme ich, was ich dafür brauche?
- „Mehrwert“: digitale Unterschrift
- Klappen umschiffen
- S/MIME vs. PGP/GnuPG, NPA und De-Mail

Public-Key-Verfahren

- nicht 1 Schlüssel „für alle/alles“
- nicht 1 Schlüssel für jedes Pärchen Sender - Empfänger
(Mathematiker sehen: das wären $n(n-1)/2$ Schlüssel bei n Beteiligten!)
- sondern 1 Schlüsselpaar pro Beteiligtem:
 - öffentliche Komponente („public key“),
kann und muss verteilt werden;
geheime Komponente („private key“
oder „secret key“)
- löst (fast) das Problem der sicheren Schlüssel-Verteilung
- bekanntestes Public-Key-Verfahren: RSA



Zertifikat

- bestätigt die Zugehörigkeit eines öffentl. Schlüssels zu einer Person (oder allgemein: zu einer Identität)
- ist gegen Manipulation geschützt (Urkunde mit „Siegel“)
- enthält keine geheimen Informationen!



S/MIME- Zertifikat (Beispiel)



Ingmar Camphausen

Ausgestellt von: Freie Universitaet Berlin - FU-CA - G01

Gültig bis: Freitag, 30. März 2012 14:55:07 Uhr MESZ

✔ Dieses Zertifikat ist gültig.

► Vertrauen

▼ Details

Name des Inhabers

Ländername DE

Bundeslands- oder Bezirksname Berlin

Ortsname Berlin

Organisation Freie Universitaet Berlin

Organisationseinheit Fachbereich Mathematik und Informatik

Organisationseinheit Rechnerbetrieb

Allgemeiner Name Ingmar Camphausen

Name des Ausstellers

Ländername DE

Bundeslands- oder Bezirksname Berlin

Ortsname Berlin

Organisation Freie Universitaet Berlin

Organisationseinheit ZEDAT

Allgemeiner Name Freie Universitaet Berlin - FU-CA - G01

E-Mail-Adresse ca@FU-Berlin.DE

Seriennummer 233934907

Version 3

Signaturalgorithmus SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)

Parameter Ohne

Erst gültig ab Dienstag, 31. März 2009 14:55:07 Uhr MESZ

Nur gültig bis Freitag, 30. März 2012 14:55:07 Uhr MESZ

Öffentlicher Schlüssel

Algorithmus RSA-Verschlüsselung (1 2 840 113549 1 1 1)

Parameter Ohne

Öffentlicher Schlüssel 256 Byte : AE 10 79 9F 22 E8 B1 78 ... ↻

Exponent 65537

Schlüssellänge 2048 Bit

Schlüsselverwendung Verschlüsseln, Überprüfen, Einpacken, Ableiten


Signatur 256 Byte : 62 7B F9 1D 19 BE FC CA ... ↻

Zertifikat – 2. Beispiel: gesicherte Webseite

Zugang nur für ZEDAT-Account Inhaber

fu-berlin.de <https://portal.zedat.fu-berlin.de/einstellungen/> Google

Zugang nur für ZEDAT-Account In...

Freie Universität  Berlin | Home | Kontakt | Impressum

ZEDAT | Webmail | Portal | Shell

zedat Z E D A T Enter

Seiteninformation – <https://portal.zedat.fu-berlin.de/einstellungen/ui.php?w=1>

Allgemein | Medien | Berechtigungen | **Sicherheit**

ZEDAT-Portal
Hier finden Sie:
- Webmail
- Konfiguration
- Möglichkeit Passwortänderung
- und vieles mehr

ung für
Server, so
möglich ist.

© 2006 ZEDAT

Fertig

Website-Identität

Website: **portal.zedat.fu-berlin.de**
Besitzer: **Diese Website stellt keine Informationen über den Besitzer zur Verfügung.**
Validiert von: **Freie Universitaet Berlin**

Zertifikat anzeigen

Datenschutz & Chronik


Habe ich diese Website früher schon einmal besucht? **Ja, 30 Mal**

Speichert diese Website Daten (Cookies) auf meinem Computer? **Nein** **Cookies anzeigen**

Habe ich Passwörter für diese Website gespeichert? **Nein** **Gespeicherte Passwörter anzeigen**

Technische Details

Verbindung verschlüsselt: Hochgradige Verschlüsselung (AES-256 256 bit)
Die Seite, die Sie ansehen, wurde verschlüsselt, bevor sie über das Internet übermittelt wurde.
Verschlüsselung macht es für unberechtigte Personen sehr schwierig, zwischen Computern übertragene Informationen anzusehen. Daher ist es sehr unwahrscheinlich, dass jemand diese Seite gelesen hat, als sie über das Netzwerk gesendet wurde.



Zertifizierungsstelle (CA – Certification Authority)

- auch „Trustcenter“
- beglaubigt („zertifiziert“) öffentliche Schlüssel nach festgelegten, publizierten Regeln
 - vorherige Prüfung der Identität
- sollte möglichst vertrauenswürdig sein
- DFN: Zertifizierungs-Infrastruktur (ab 1997)
- auch Freie Universität Berlin hat eigene CA

Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- *Wie bekomme ich, was ich dafür brauche?*
- „Mehrwert“: digitale Unterschrift
- Klippen umschiffen
- S/MIME vs. PGP/GnuPG, NPA und De-Mail

Wo/wie bekomme ich Schlüssel und Zertifikat?

- Schlüssel (paar): selbsterzeugen!
 - erzeugt der eigene Rechner (Browser)
<http://www.zedat.fu-berlin.de/Zertifikate>
- Zertifikat (für FU-Angehörige):
 - von FU-CA ausstellen lassen, dazu
 - persönlicher Besuch bei der zuständ.
Registrierungsstelle (RA) erforderlich

FU-CA Registrierungsstellen

- RAs an folgenden Fachbereichen:
 - FB Geowissenschaften
 - FB Geschichts- und Kulturwissenschaften
 - FB Mathe + Informatik
 - FB Physik
 - Zentrale Uni-Verwaltung (ZUV)
 - ZEDAT
- E-Mail: ra@<BEREICH>.fu-berlin.de

Andere Einrichtungen

- TU Berlin (TU-CampusCard!):

<https://www.tubit.tu-berlin.de/trustcenter/>

- HU Berlin (HU-Smartcard!):

<http://www.cms.hu-berlin.de/dl/zertifizierung/>

- Sonstige Forschungseinrichtungen (D):

<https://info.pca.dfn.de/>

- Personen aus DFN-Einrichtungen ohne eig. CA:

<http://www.dfn.de/organisation/geschaeftsstelle/>

- zur privaten Nutzung (kostenlos!):

http://www.trustcenter.de/products/tc_internet_id.htm

Ablauf Schlüssel-Zertifizierung

1. Antragsformular auf RA-Webseite abschicken
↳ Browser erzeugt Schlüsselpaar
2. Antrag ausdrucken, zuständige RA aufsuchen
wichtig: Antrag und amtliches ID-Dokument
(Personalausweis o. Pass) mitnehmen!
3. RA prüft Identität und gibt Antrag frei
4. FU-CA stellt Zertifikat aus
5. Installation des Zertifikats auf eigenem PC

Zertifikate

CA-Zertifikate

Gesperrte Zertifikate

Policies

Hilfe

Beenden

Nutzerzertifikat

Serverzertifikat

Zertifikat sperren

Zertifikat suchen

Willkommen zur DFN-PKI

Schnittstelle für Nutzer und Administratoren - Zertifikate

Hier können Sie Zertifikate beantragen, sperren lassen und nach Zertifikaten suchen.

- Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte "CA-Zertifikate".
- Bitte wählen Sie aus den Registerkarten eine Funktion aus.

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

Impressum

[Zertifikate](#)[CA-Zertifikate](#)[Gesperrte Zertifikate](#)[Policies](#)[Hilfe](#)[Beenden](#)[Nutzerzertifikat](#)[Serverzertifikat](#)[Zertifikat sperren](#)[Zertifikat suchen](#)

Nutzerzertifikat beantragen

Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (*) müssen ausgefüllt werden.

Zertifikatdaten

E-Mail *

Name *

Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:" voran. Verwenden Sie keine Umlaute.

Abteilung

Wenn Sie hier eine Abteilung angeben, wird diese in den Zertifikatnamen aufgenommen.

Weitere Angaben

Diese Angaben werden nicht in das Zertifikat übernommen.

PIN (Mindestens 8 beliebige Zeichen) *

Nochmalige Eingabe der PIN zur Bestätigung *

Die PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen oder um dieses einzulesen, wenn Sie einer Veröffentlichung nicht zustimmen. Bitte notieren Sie sich die PIN.

Ich stimme der [Zertifizierungsrichtlinie](#) zu. *Ich stimme der [Veröffentlichung des Zertifikats](#) mit meinem darin enthaltenen Namen und der E-Mail-Adresse zu.

Sie können diese Einwilligung jederzeit mit Wirkung für die Zukunft durch eine E-Mail an pki@dfn.de widerrufen.



Zertifikate | CA-Zertifikate | Gesperrte Zertifikate | Policies | Hilfe | Beenden

Nutzerzertifikat | Serverzertifikat | Zertifikat sperren | Zertifikat suchen

Nutzerzertifikat beantragen - Bestätigen

Bitte überprüfen Sie die Daten.

Zertifikatdaten

E-Mail ingmar@math.fu-berlin.de
Name Ingmar Camphausen
Abteilung IT-Service

Weitere Angaben

Veröffentlichen Ja

Ändern

Bestätigen

Impressum



Zertifikatantrag

Abschließend müssen Sie Ihren Zertifikatantrag ausdrucken.

- Bitte betätigen Sie die Schaltfläche "Zertifikatantrag anzeigen". Daraufhin wird der Zertifikatantrag in einem neuen Fenster geöffnet.
- Bitte drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn bei Ihrer Registrierungsstelle vor, um die Antragsstellung abzuschließen.

Nachdem Sie den Zertifikatantrag ausgedruckt haben, können Sie diese Schnittstelle über die Registerkarte "Beenden" verlassen.

Zertifikatantrag anzeigen

Impressum

Zertifikatantrag mit Identifizierung

Antragsnummer 244256
Eindeutiger Name emailAddress=ingmar@math.fu-berlin.de, CN=Ingmar Camphausen, OU=IT-Service, OU=Fachbereich Mathematik und Informatik, O=Freie Universitaet Berlin, L=Berlin, ST=Berlin, C=DE
Public Key Fingerprint 85:75:4E:14:D0:83:3C:6B:0C:58:F3:46:01:F5:75:CA:80:AE:D6:ED
Schlüssellänge 2048
Veröffentlichen Ja

Angaben zur Person Frau Herr

Vorname Nachname Ingmar Camphausen

E-Mail ingmar@math.fu-berlin.de

Telefonnummer _____

Ausweis (Art u. letzte
5 Zeichen der Nummer) _____

Abteilung / Institut IT-Service

Straße u. Hausnummer _____

Postleitzahl u. Ort _____

- Ich versichere, dass sämtliche Angaben im Antrag vollständig sind und der Wahrheit entsprechen.
- Ich kenne die gültigen Zertifizierungsrichtlinien und die Erklärung zum Zertifizierungsbetrieb und stimme ihnen zu.
- Ich stimme der Verarbeitung und Speicherung der bei der Zertifizierung anfallenden Daten zu. Die Daten werden gemäß den geltenden Datenschutzbestimmungen vertraulich behandelt.

(Ort, Datum)_____
(Unterschrift - wie im Ausweis)**Wird von der Registrierungsstelle ausgefüllt**

Prüfung der Ausweisdaten:

Bereits geprüft

ihnen zu.

- Ich stimme der Verarbeitung und Speicherung der bei der Zertifizierung anfallenden Daten zu. Die Daten werden gemäß den geltenden Datenschutzbestimmungen vertraulich behandelt.

(Ort, Datum)

(Unterschrift - wie im Ausweis)

Wird von der Registrierungsstelle ausgefüllt

Prüfung der Ausweisdaten:

Name

Unterschrift

Bild

Bereits geprüft

Gültigkeit

Nummer

Name des Prüfers _____

Zugehörige Registrierungsstelle _____

(Datum, Unterschrift des Prüfers)

fu-ca

Zertifikate

CA-Zertifikate

Gesperrte Zertifikate

Policies

Hilfe

Beenden

Nutzerzertifikat

Serverzertifikat

Zertifikat sperren

Zertifikat suchen

Laden des beantragten Zertifikats

Benutzen Sie den Button, um Ihr Zertifikat in Ihren Browser zu importieren.

Bitte beachten Sie, dass einige Browser einen erfolgreichen Import nicht gesondert melden.

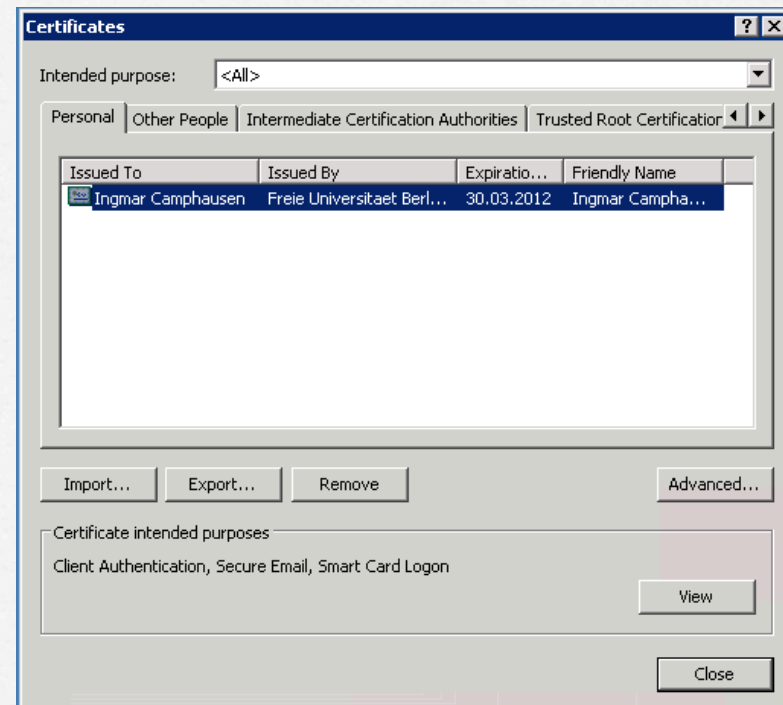
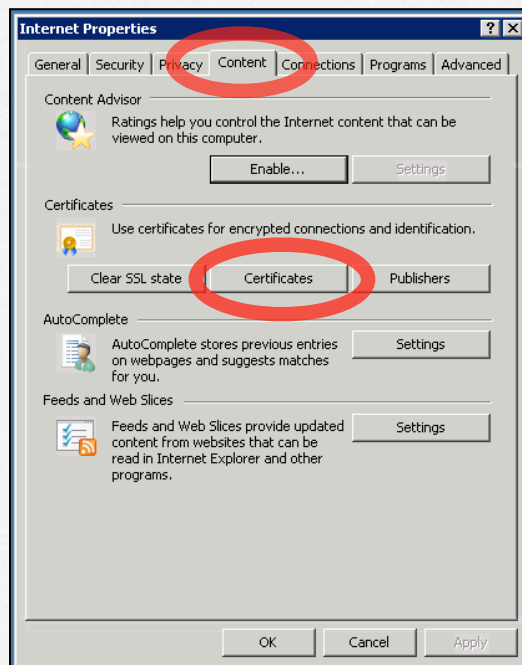
Wenn Sie bei der Antragsstellung bestimmt haben, dass Ihr Zertifikat nicht veröffentlicht werden soll, so werden Sie nach der PIN gefragt, die Sie in Ihren Zertifikatantrag eingegeben haben.

Zertifikat importieren

[Impressum](#)

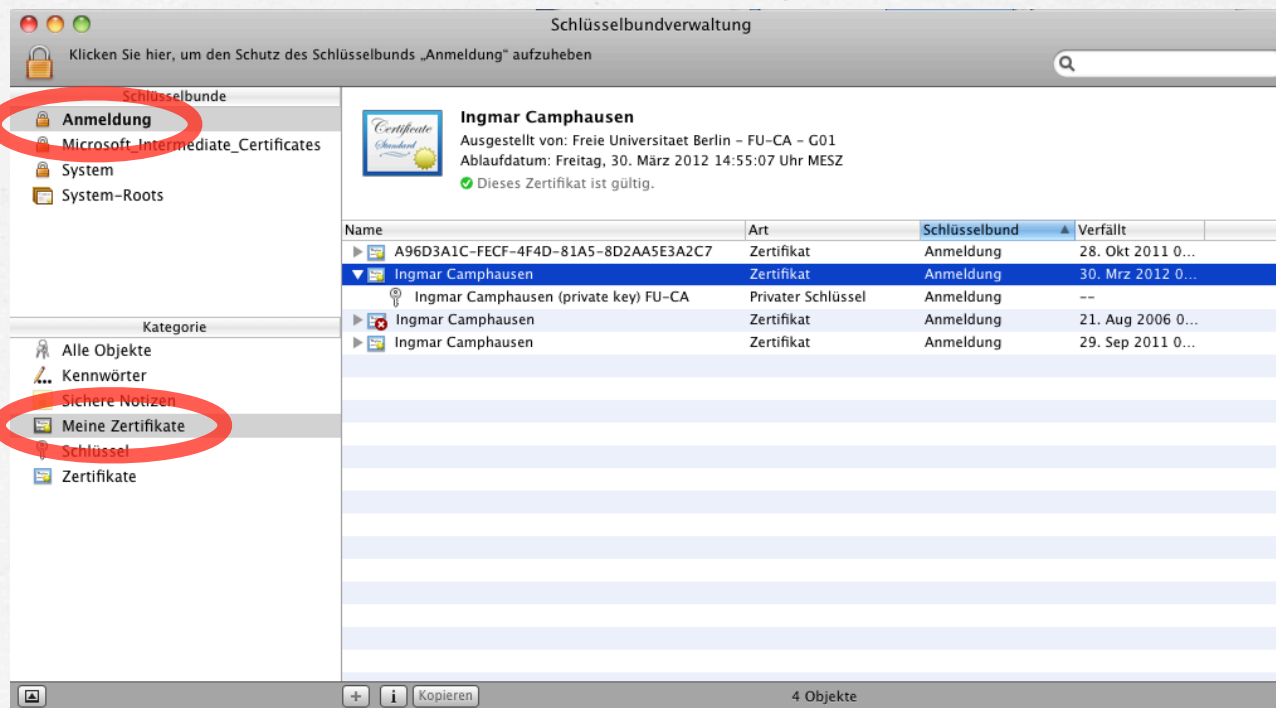
Wo landet das Zertifikat? – MS Windows

- Start > Control Panel > Internet Options > Content (!) > Certificates > Personal



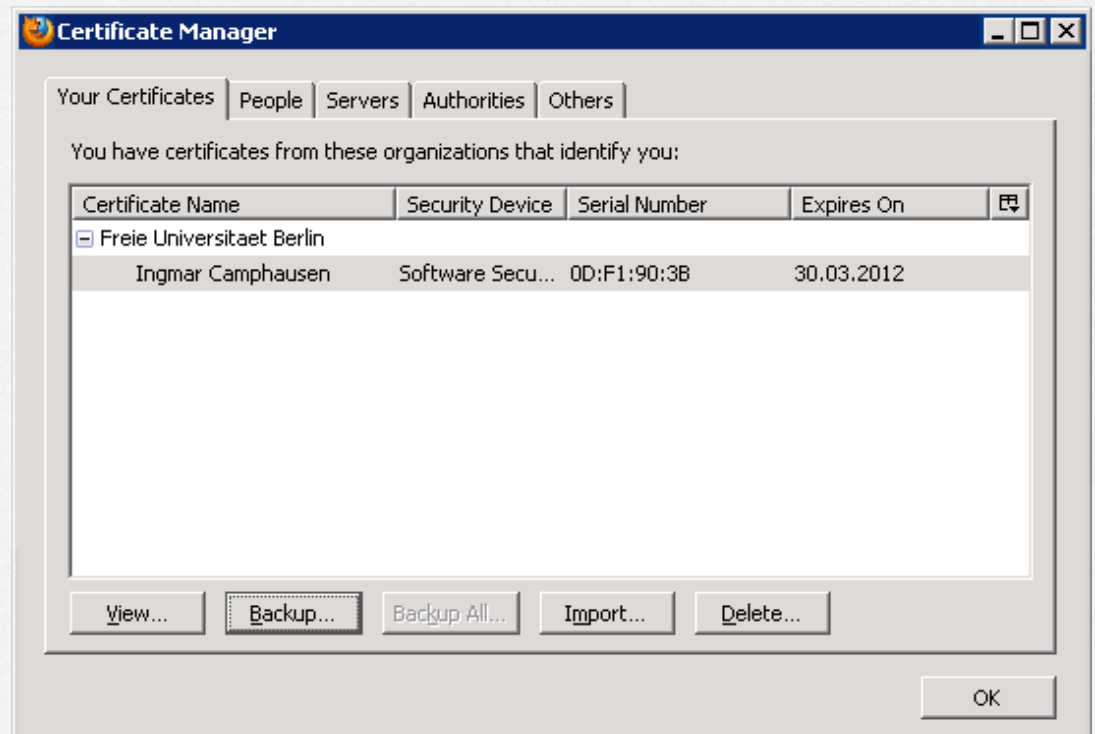
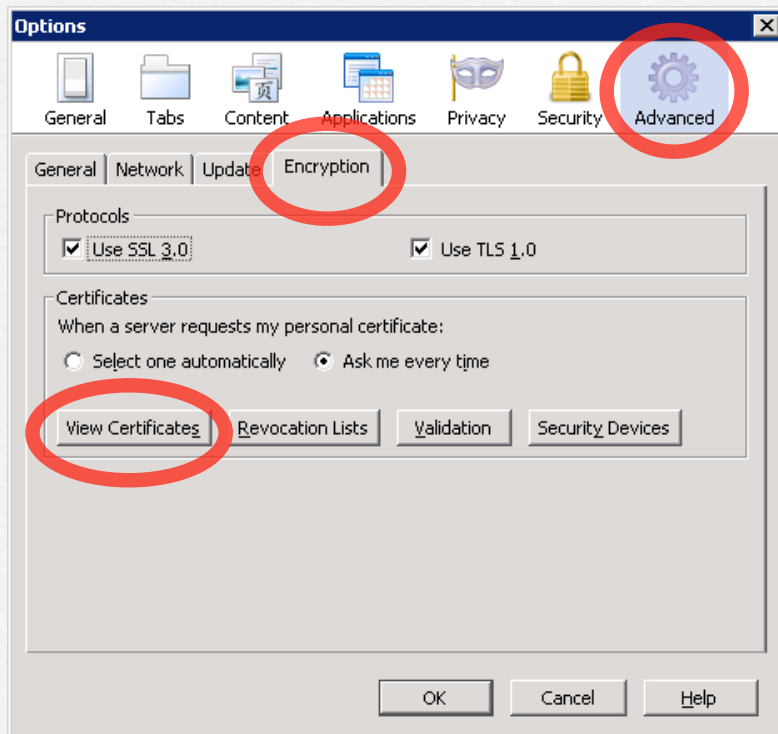
Wo landet das Zertifikat? – Mac OS X

- Programme > Dienstprogramme > Schlüsselbundverwaltung > Schlüsselbund „Anmeldung“ > Meine Zertifikate



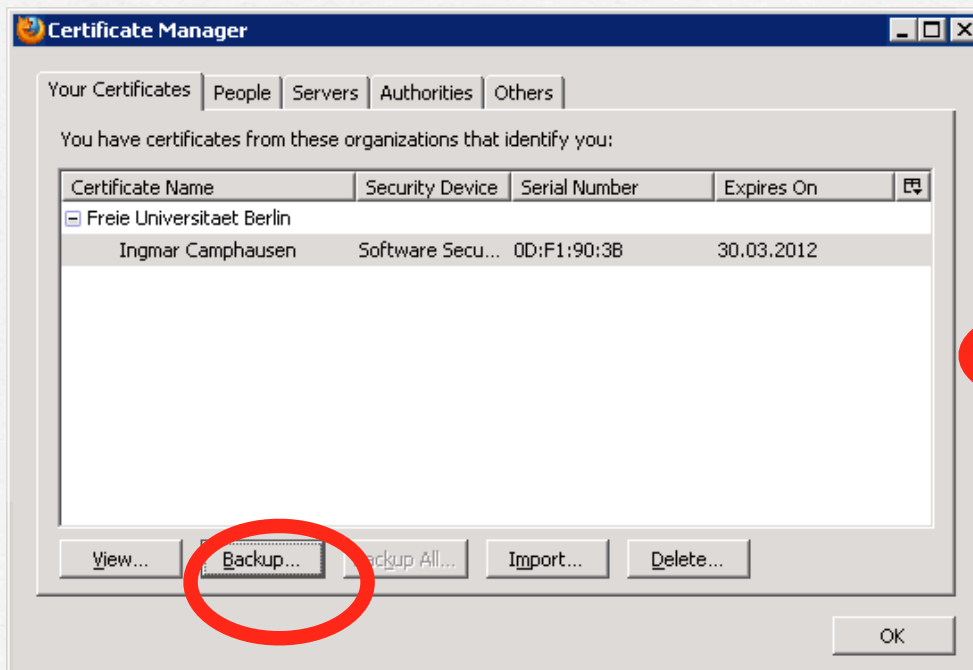
Wo landet das Zertifikat? – Firefox (Windows)

- Tools > Options > Advanced (!) > Encryption > View Certificates > Your Certificates



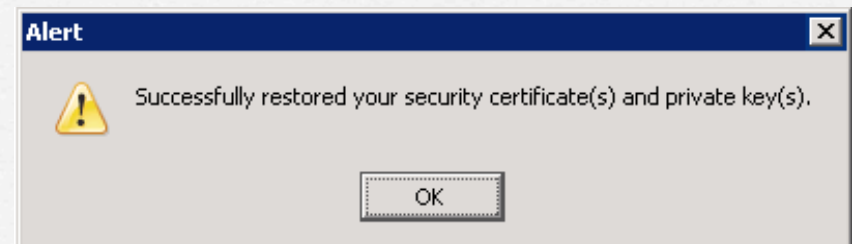
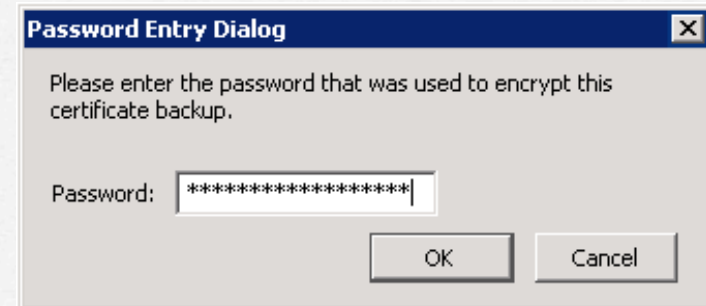
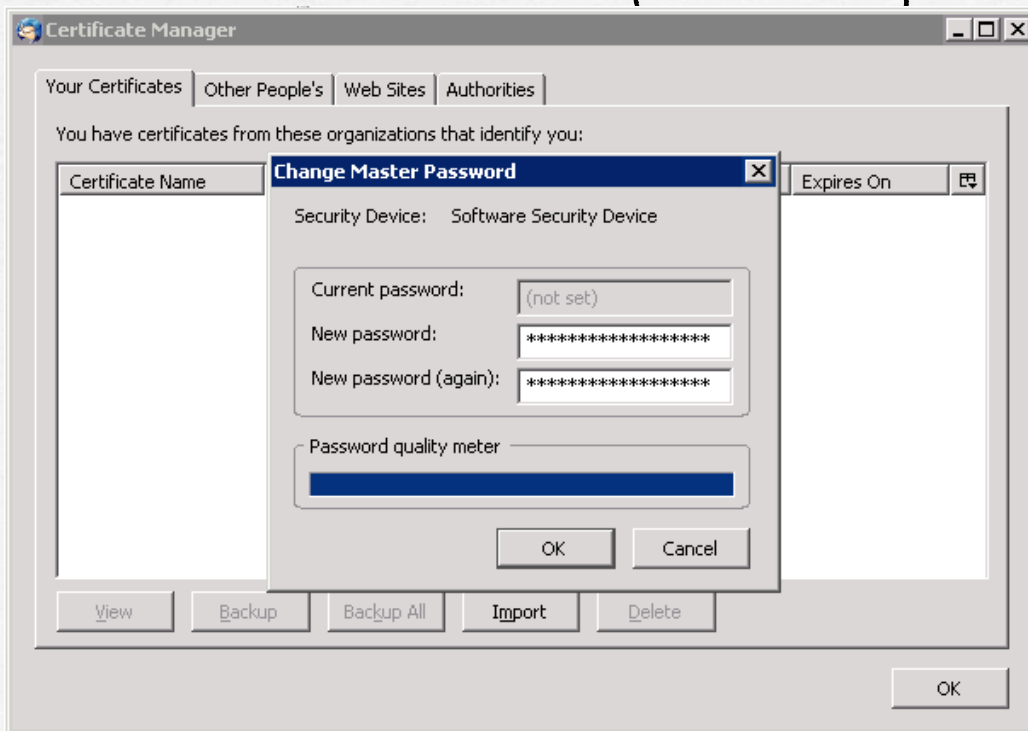
Transfer Zertifikat + Schlüssel Firefox > Thunderbird (1)

- Firefox > Tools > Options > Advanced (!)
 - > Encryption > view Certificates
 - > Your Certificates > Backup



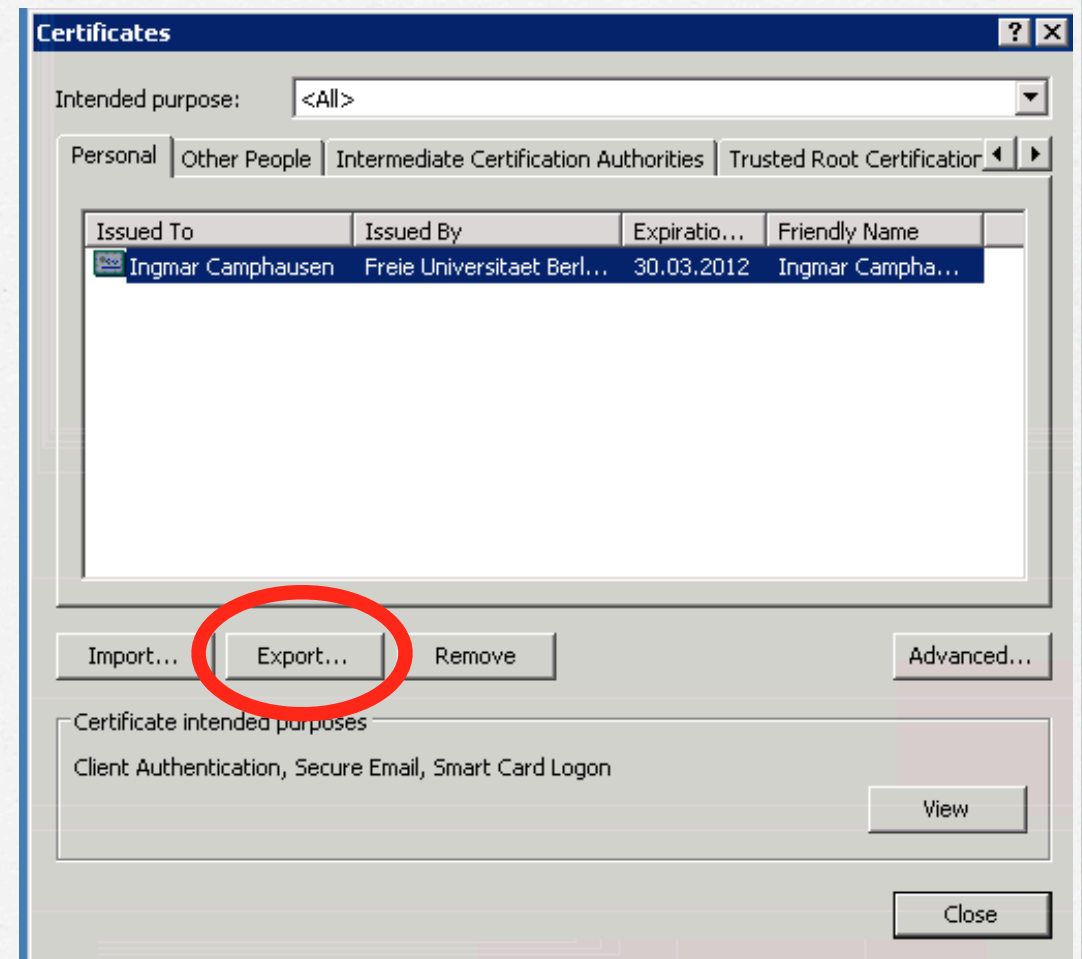
Transfer Zertifikat + Schlüssel Firefox > Thunderbird (2)

- Thunderbird > Tools > Options
 - > Advanced (!) > Certificates
 - > View Certificates > Your Certificates > Import



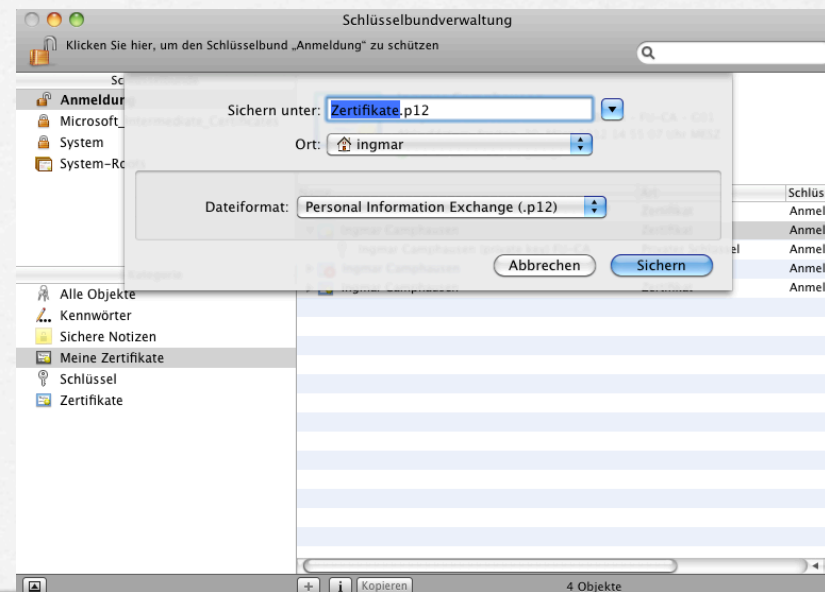
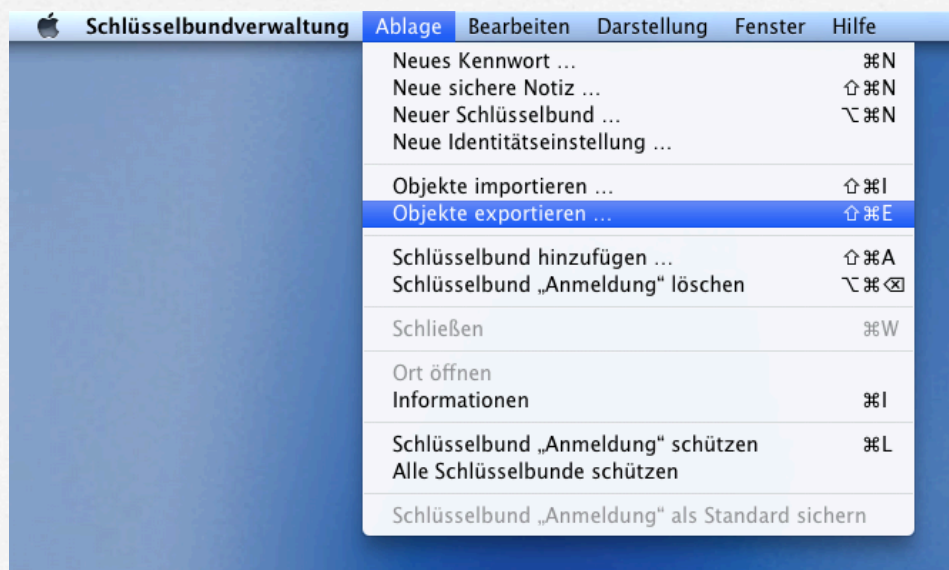
Export/Backup Zertifikat + Schlüssel (Windows)

- Start >
Control Panel >
Internet Options >
Content (!) >
Certificates >
Personal > Export
(Wizard...)
- Dateiformat:
PKCS#12, private
key mit exportieren



Export/Backup Zertifikat + Schlüssel (Mac OS X)

- Programme > Dienstprogramme > Schlüsselbundverwaltung > Ablage > Objekte exportieren ...
- Dateiformat: Personal Information Exchange (.p12)



Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- Wie bekomme ich, was ich dafür brauche?
- „Mehrwert“: digitale Unterschrift
- Klippen umschiffen
- S/MIME vs. PGP/GnuPG, NPA und De-Mail

Digitale Signaturen

- Public-Key-Verfahren ermöglichen nicht nur Verschlüsselung!
- bieten auch Mechanismen für elektronisches Pendant zur Unterschrift: „Digitale Signatur“
 - ↳ signieren von E-Mails! (kein „Footer“!)
- Signaturen nutzen auch Leuten, die selbst noch keine Schlüssel haben!

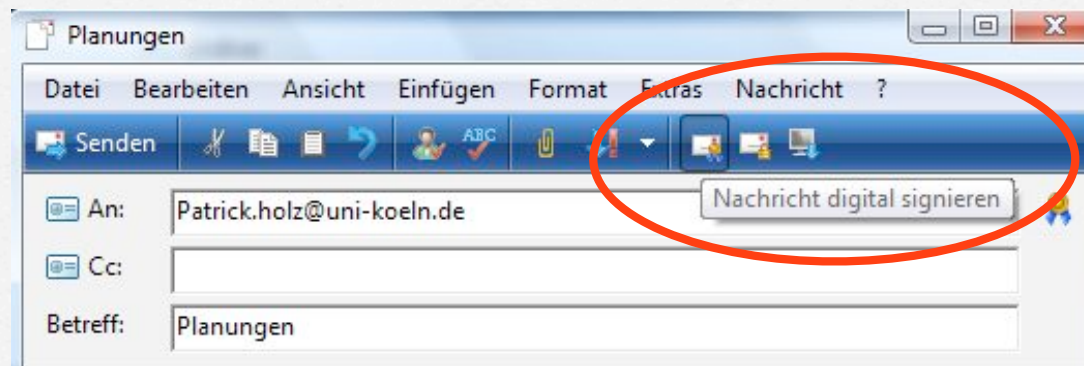
Vorteile signierter E-Mails

- Urheber nachprüfbar (Authentizität)
- machen versehentliche oder mutwillige Änderungen erkennbar (Integrität)
- Nicht-Abstreitbarkeit (Non-Repudiation)
(in gewissen Grenzen)

Signatur (Schema)

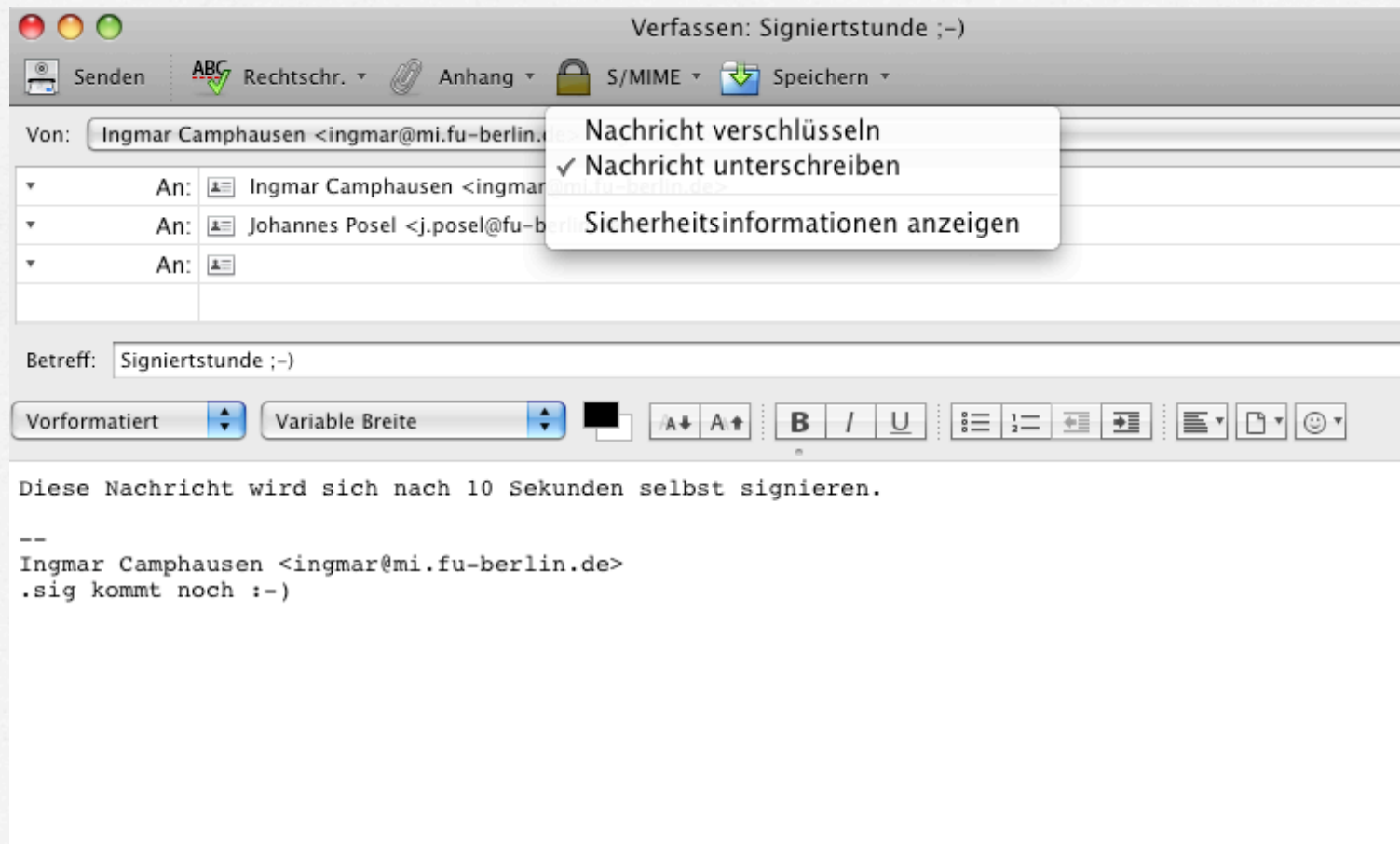
- Urheber einer Nachricht berechnet Prüfsumme über der Nachricht und „verschlüsselt“ sie mit seinem private key
- Urheber schickt Nachricht zusammen mit „verschlüsselter“ Prüfsumme + seinem Zertifikat
- Empfänger berechnet Prüfsumme über erhaltener Nachricht und „entschlüsselt“ mitgeschickte Prüfsumme mit public key des Absenders
- stimmen beide Prüfsummen überein, wurde die Nachricht unterwegs nicht verändert
- zusätzlich bei E-Mail: Plausibilitätsprüfung, ob E-Mail-Adresse im Zertifikat mit „From:“-Adresse der Nachricht übereinstimmt

Signierte Mail „live“ – Senden (Windows Mail)

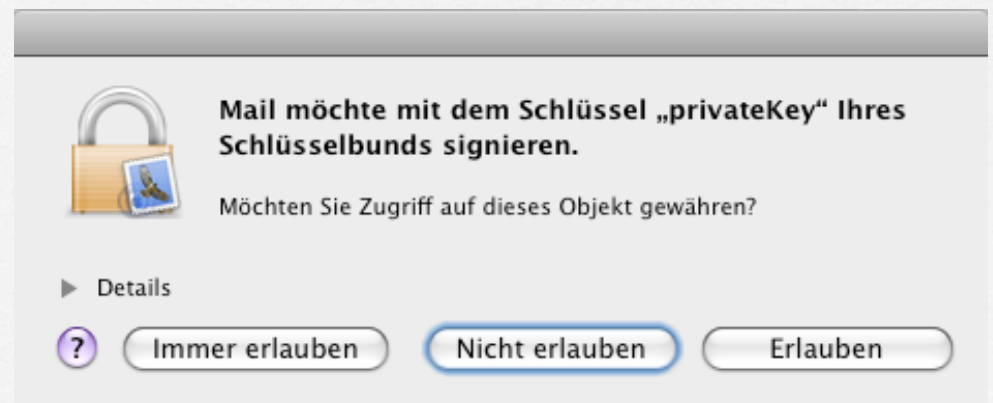
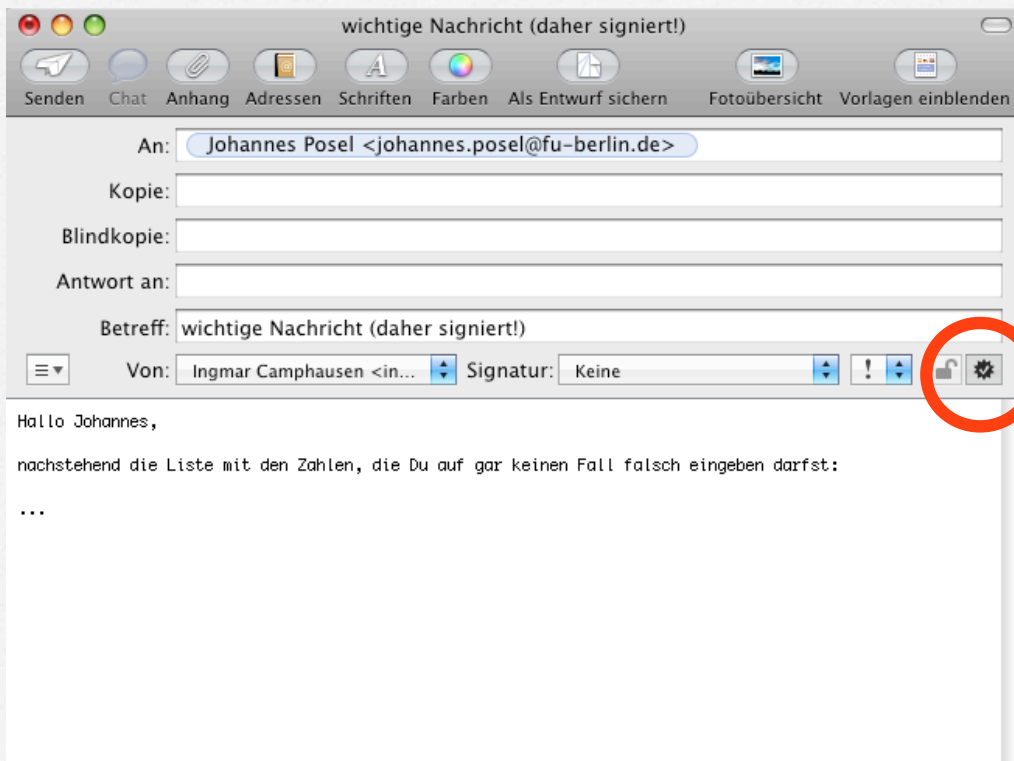


<http://www.uni-koeln.de/rrzk/sicherheit/smime/iexplorer.html>

Signierte Mail „live“ – Senden (Thunderbird)



Signierte Mail „live“ – Senden (Apple Mail)



Signierte Mail „live“ – Empfangen (Windows Mail)

Von: Patrick Holz <patrick.holz@uni-koeln.de> **An:** Haiko Luepsen <luepsen@uni-koeln.de>
Betreff: Re: logfile auswertung



<http://www.uni-koeln.de/rrzk/sicherheit/smime/iexplorer.html>

Signierte Mail „live“ – Empfangen (Thunderbird)

The screenshot shows the Thunderbird 'Posteingang' (Inbox) window. The email list includes:

Von	Betreff	Datum
efskultur Berlin	efskultur-Newsletter Juli 2010	10:48 Uhr
Ingmar Camphausen	Testmail aus Thunderbird	11:36 Uhr
Ingmar Camphausen	Signiertstunde ;-)	11:50 Uhr
Posel, Johannes	Re: Demo (ENCR)	11:50 Uhr

The selected email is from 'Posel, Johannes' with subject 'Re: Demo (ENCR)'. The interface shows buttons for 'Antworten', 'Weiterleiten', 'Archivieren', 'Junk', and 'Löschen'. A red circle highlights the 'Junk' button and the email icon with a lock symbol. The email content is:

Hallo Ingmar,

| diese vertrauliche Mail werde ich Dir verschlüsselt...

Und auf diesem Weg eine vertrauliche, verschlüsselte Mail zurück 😊

Beste Grüße,
Johannes

The dialog box displays the following information:

Nachricht wurde unterschrieben
Diese Nachricht enthält eine gültige digitale Unterschrift. Die Nachricht wurde nicht verändert, seit sie gesendet wurde.

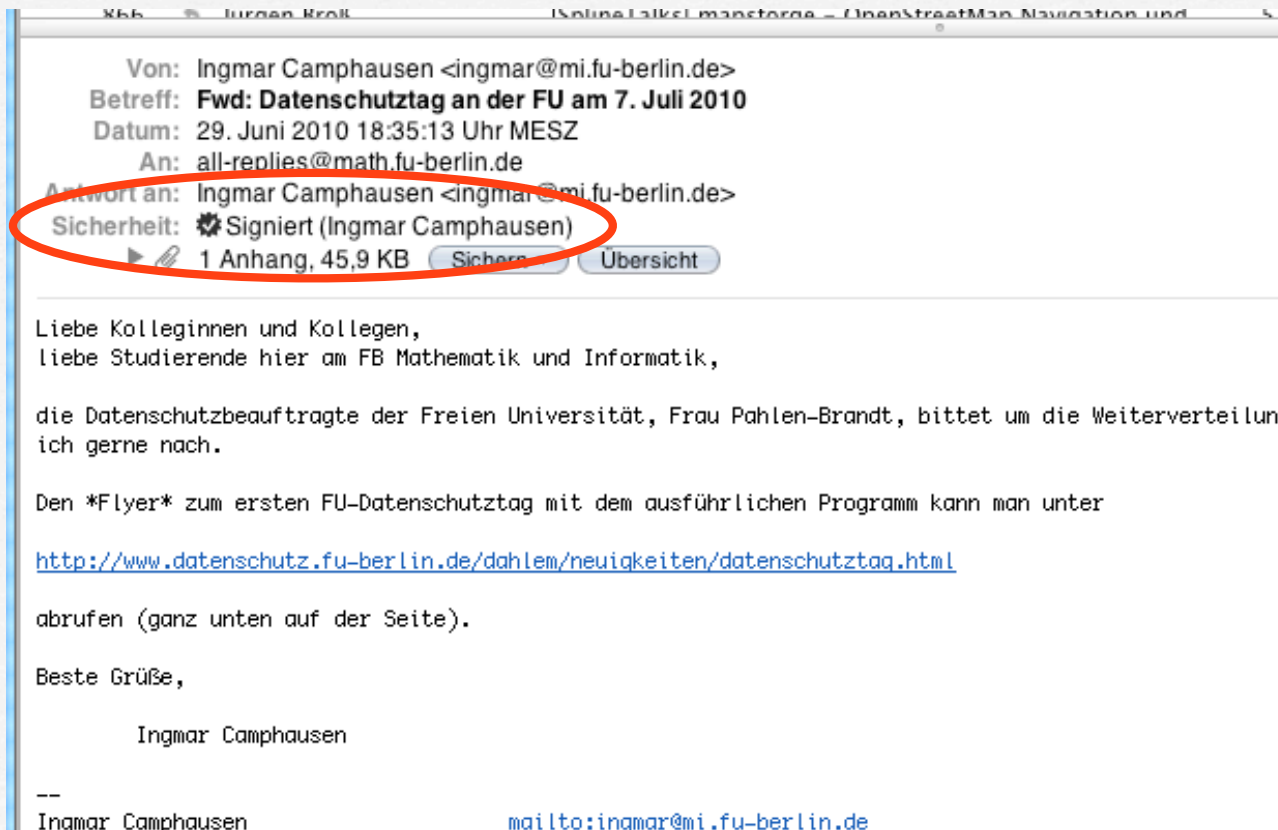
Unterschrieben von: Johannes Posel
E-Mail-Adresse: j.posel@fu-berlin.de
Zertifikat herausgegeben von: Freie Universitaet Berlin - FU-CA - G01




[Unterschriftszertifikat ansehen](#)

Nachricht ist verschlüsselt
Diese Nachricht wurde verschlüsselt, bevor sie an Sie gesendet wurde. Die Verschlüsselung macht es sehr schwierig für andere Personen, Ihre Informationen während der Übertragung über das Netzwerk / Internet anzusehen.

[OK](#)

Signierte Mail „live“ – Empfangen (Apple Mail)



Von: Ingmar Camphausen <ingmar@mi.fu-berlin.de>
Betreff: Fwd: Datenschutztag an der FU am 7. Juli 2010
Datum: 29. Juni 2010 18:35:13 Uhr MESZ
An: all-replies@math.fu-berlin.de
Antwort an: Ingmar Camphausen <ingmar@mi.fu-berlin.de>
Sicherheit:  Signiert (Ingmar Camphausen)
1 Anhang, 45,9 KB   Übersicht

Liebe Kolleginnen und Kollegen,
liebe Studierende hier am FB Mathematik und Informatik,

die Datenschutzbeauftragte der Freien Universität, Frau Pahlen-Brandt, bittet um die Weiterverteilung
ich gerne nach.

Den *Flyer* zum ersten FU-Datenschutztag mit dem ausführlichen Programm kann man unter
<http://www.datenschutz.fu-berlin.de/dahlem/neuigkeiten/datenschutztag.html>
abrufen (ganz unten auf der Seite).

Beste Grüße,
Ingmar Camphausen

--
Ingmar Camphausen <mailto:ingmar@mi.fu-berlin.de>

Signierte Mail in Mail-Programmen ohne S/MIME-Unterstützung

The screenshot shows a webmail interface for 'ingmar Ingmar Camphausen'. The navigation bar includes 'Webmail', 'Einstellungen', 'Services', 'Hilfe', and 'Logout'. Below this, there are tabs for 'Webmail', 'E-Mail schreiben', 'Adressen', 'Ordner', 'Optionen', and 'Suchen'. The current folder is 'Test'. The email header shows: 'Betreff: Testmail S/MIME signiert', 'Von: "Ingmar Camphausen" <ingmar@mi.fu-berlin.de>', 'Datum: Di, 31.03.2009, 19:57', 'An: Klaus-Peter Löhr <lohr@inf.fu-berlin.de>', and 'Cc: ca@mi.fu-berlin.de'. The email body contains a message in German about S/MIME signing and fingerprint verification. At the bottom, the attachment 'smime.p7s' (6.6 k, application/pkcs7-signature) is highlighted with a red circle. The interface also shows a 'Verschieben' button and a dropdown menu for moving the email to the 'INBOX'.

ingmar Ingmar Camphausen

Webmail Einstellungen Services Hilfe Logout

Webmail E-Mail schreiben Adressen Ordner Optionen Suchen

Aktueller Ordner: Test

[Nachrichtenliste](#) | [Löschen](#) | [Vorherige](#) | [Nächste](#) | [Weiterleiten](#) | [Als Anhang weiterleiten](#) | [Antworten](#) | [Allen Antworten](#)

Betreff: Testmail S/MIME signiert
Von: "Ingmar Camphausen" <ingmar@mi.fu-berlin.de>
Datum: Di, 31.03.2009, 19:57
An: Klaus-Peter Löhr <lohr@inf.fu-berlin.de>
Cc: ca@mi.fu-berlin.de
Optionen: [Alle Kopfzeilen anzeigen](#) | [Druckversion zeigen](#) | [Dies als Datei herunterladen](#) | [Nachrichtendetails anzeigen](#) | [Zum Adressbuch hinzufügen](#)

Hallo Peter,

wenn alles geklappt hat, sollte diese Mail an Dich S/MIME-signiert von mir mit einem Key mit FU-CA-Zertifikat sein.

Wir können gerne bei Gelegenheit den Fingerprint vergleichen, oder Du importierst über den Link unten am Ende der Webseite

das Wurzelzertifikat der Telekom-CA, unter der die DFN-PKI "aufgehängt" ist. (Die Telesec hat die DFN-PCA zertifiziert, d.h. wenn Du auf dem Mac das Telekom-Root-Zertifikat in die Liste der "System-Roots" importierst, müsstest Du meine Signatur ohne weiteres verifizieren können! Und vielleicht kannst Du mir dann mal an meinen Key verschlüsselt antworten?

Danke und Gruß,
Ingmar

Anhänge:
[smime.p7s](#) 6.6 k [application/pkcs7-signature] [Herunterladen](#)

[Zurück zur Übersicht](#) | [Löschen & Nächste](#)

Verschiebe nach: INBOX

Verschieben

Signierte Mail „live“ – manipuliert (Apple Mail)



Die E-Mail-Signatur konnte nicht überprüft werden.



Details e

Von: Johannes Posel <johannes@posel.name>

Betreff: Testnachricht S/MIME Apple Mail

Datum: 11. September 2009 14:44:13 Uhr MESZ

An: Ingmar Camphausen <ingmar@mi.fu-berlin.de>

Sicherheit: Verschlüsselt, Signiert (Johannes Posel -- q7369271)

1 Anhang, 41,2 KB [Sichern](#) [Übersicht](#)

Hi Ingmar,

zumindest auf dem Snow Leopard Apple Mail ist die S/MIME-Integration eigentlich bei jeder Mail drinnen, auch bei empfangenen Nachrichten (siehe Attachment). Ist das bei Dir nicht dabei?

Beste Grüße,
Johannes

„Gratis-Zugabe“: Signaturen in Adobe Acrobat

- Voraussetzungen:
 - eigenes Schlüsselpaar + Zertifikat
 - Adobe Acrobat (nicht Acrobat Reader!)
- Vorbereitung:
 - Import eigenes Zertifikat in Acrobat
- zusätzlicher „Goodie“:
Zeitstempeldienst des DFN
<http://zeitstempel.dfn.de>

Vorbereitungen

- *Advanced > Security Settings > Digital IDs*
 - entweder „Windows Digital IDs“ mitnutzen (unter MS Windows) oder
 - Zugriff auf Datei mit Zertifikat etc.

- *Root-Zertifikat muss zusätzlich installiert werden (Telekom Root CA 2):*
 - *Advanced > Manage trusted identities > Certificates*

Mittwoch, 7. Juli 2010

- Sign Document
- Place Signature
- Apply Ink Signature
- Certify with Visible Signature
- Certify without Visible Signature
- Validate All Signatures

heute:

Compf

keine

(inst

notw

Berei

einm

Schli

(größt

„Früher war alles

heute

Sign Document

Sign As: Ingmar Camphausen

Certificate Issuer: Freie Universität Berlin - FU-CA - G01

Appearance: Standard Text

Digitally signed by Ingmar Camphausen
DN: c=DE, st=Berlin, l=Berlin, o=Freie Universität Berlin, ou=Fachbereich Mathematik und Informatik, ou=Rechnerbetrieb, cn=Ingmar Camphausen
Date: 2010.12.15 13:49:07 +01'00'

Lock Document After Signing

Sign Cancel

einmaliger Aufwand: eig

Schlüssel des jeweiligen (Arbeits-)teils automatisch

Signatures

Validate All

Rev. 1: Signed by Ingmar Camphausen
Document Locked by Signature

Mittwoch, 7. Juli 2010

Ingmar Camphausen

Digitally signed by Ingmar Camphausen
DN: c=DE, st=Berlin, l=Berlin, o=Freie
Universität Berlin, ou=Fachbereich
Mathematik und Informatik,
ou=Rechnerbetrieb, cn=Ingmar Camphausen
Date: 2010.12.15 13:50:07 +01'00'

heute:

- Computer übernimmt die Arbeit
- keine Software-Installation
(insbes.: keine Admin-Rech)
- notwendige Infrastruktur an
Bereichen schon vorhanden
- einmaliger Aufwand: eigenen
Schlüssel des jeweiligen Koi
(größtenteils automatisch)

„Früher war alles s

Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- Wie bekomme ich, was ich dafür brauche?
- „Mehrwert“: digitale Unterschrift
- Klippen umschiffen
- S/MIME vs. PGP/GnuPG, NPA und De-Mail

Klappen umschiffen

- selben Rechner + Browser für Beantragung und Abholen des Zertifikats benutzen!
- Backup des geheimen Schlüssels machen + Transport-Passwort notieren!!
- Passworte/PINs auseinanderhalten!
- eigene Schlüssel + Zertifikat auf allen Rechnern installieren, von denen man mailt
- Verhalten bei Verlust oder Kompromittierung?

Überblick

- Verschlüsselte E-Mails „live“
- 3 wichtige Begriffe
- Wie bekomme ich, was ich dafür brauche?
- „Mehrwert“: digitale Unterschrift
- Klappen umschiffen
- S/MIME vs. PGP, WPA und De-Mail

S/MIME vs. PGP/GnuPG



- Gemeinsamkeiten
 - Public-Key-basiert
 - Algorithmen „sicher“ (Stand heute)
 - „kostenlos“ verfügbar
 - Formate usw. standardisiert und offen verfügbar
 - Komm.-Partner muss es unterstützen

- Unterschiede
 - S/MIME: PKI, PGP: Web of Trust
 - PGP: extra Plugin/SW muss installiert werden
 - PGP: mehr Interop.-Probleme?
 - PGP/GnuPG: Quellen verfügbar (PGP: z.Z. nur in USA)

- Parallelnutzung möglich! (Thunderbird: Enigmail-PGP-Plugin; Apple Mail: GPGmail-Plugin, mutt: kann beides)

S/MIME und nPA



- neuer Personalausweis (nPA) unterstützt qualifizierte digitale Signaturen (§22 PersAuswG)
 - nur optional, via Drittanbieter (ca. €50)
- qualif. Signatur sagt nichts über Verschlüsselung
 - Plugins für gängige Mail-Programme zur „AusweisApp“, sollen angeblich auch Verschlüsselung beherrschen (AusweisApp erst ab 01/2011 verfügbar)
- nPA setzt HW-Kartenleser voraus (ca. €100-€150)
 - erst ein (1) Leser zertifiziert (Stand 12.12.2010)
- nPA ist kontaktlos (vorhandene Leser nicht nutzbar)

De-Mail



- Ziel: Sichere Kommunikationsinfrastruktur (elektronische Nachrichten) für Bürger, Unternehmen und Verwaltung
- Feldversuch mit div. großen Anbietern in 2010
- Gesetzentwurf in der Beratung
(1. Lesung, Stellungnahme BRat liegt vor)
↳ Details teilweise noch offen/strittig
- Anbieter müssen sich akkreditieren lassen
- Nutzung per Web-Browser, ohne SW-Installation
- Zusätzliche Versand- bzw. Zustelloptionen
- keine Ende-zu-Ende-Verschlüsselung

Kontakt

□ Ingmar Camphausen

Tel. -75179

ingmar@mi.fu-berlin.de

□ Diese Vortragsfolien:

<http://page.mi.fu-berlin.de/ingmar/>

□ Registrierungsstelle am FB MI:

<http://www.mi.fu-berlin.de/RA>

<mailto:ra@mi.fu-berlin.de>

Links

- Zertifikate an der Freien Universität:
<http://www.zedat.fu-berlin.de/Zertifikate>
- DFN-Zertifizierungsinfrastruktur:
<https://www.pki.dfn.de/>
- S/MIME: RFC 5750, 5751, 5752
<http://www.rfc-editor.org/rfc/rfc5750.txt>
- Krypto-Kontroverse (ca. 1996-1998):
<http://www.iks-jena.de/mitarb/lutz/security/criptoban/>
- „Clipper-Chip“:
http://en.wikipedia.org/wiki/Clipper_chip

Links (2)

- Personalausweis-Portal:

<http://www.personalausweisportal.de/>

- De-Mail Übersichtsseite des BSI:

https://www.bsi.bund.de/cln_183/DE/Themen/EGovernment/DeMail/DeMail_node.html

- PGP

<http://www.pgp.com>

- Gnu Privacy Guard

<http://www.gnupg.org>

A dark blue, spiral-bound notebook cover is shown. The spiral binding is visible at the top edge. The cover has a fine, pebbled texture. Centered on the cover is the text "Vielen Dank!" followed by "– Fragen?" in a white, sans-serif font.

Vielen Dank!
– Fragen?