

# E-Mail-Verschlüsselung

INSTITUT FÜR ANGEWANDTE UND NUMERISCHE MATHEMATIK



# Motivation

E-Mail ist einer Postkarte gleichzusetzen

- lesen, kopieren, verändern bzw. austauschen und wegwerfen
- vertrauliche Informationen → niemals
- E-Mail: Klartextpasswörter
- Zugang zum Mailserver



Karlsruher Institut für Technologie

Inst. für Angew. und Num. Math 1

Kaiserstr. 12

76131 Karlsruhe

**Deutschland / Germany**

# Motivation

E-Mail ist einer Postkarte gleichzusetzen

- lesen, kopieren, verändern bzw. austauschen und wegwerfen
- vertrauliche Informationen → niemals
- E-Mail: Klartextpasswörter
- Zugang zum Mailserver

Mail-Content



Karlsruher Institut für Technologie

Inst. für Angew. und Num. Math 1

Kaiserstr. 12

76131 Karlsruhe

Deutschland / Germany

Mail-Header

*„Vor allem beim Versenden von personenbezogenen und anderweitig geheimen oder zu schützenden Daten ist das Verschlüsseln dringend notwendig.“*

**Anlaufstelle:** <https://www.ca.kit.edu/>

# Bezeichnungen

## Verschlüsselung, digitale Signatur & PKI

Verschlüsselung ist die von *einem Schlüssel* abhängige Umwandlung von Klartext genannten Daten in einen Geheimtext, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

# Bezeichnungen

## Verschlüsselung, digitale Signatur & PKI

Verschlüsselung ist die von *einem Schlüssel* abhängige Umwandlung von Klartext genannten Daten in einen Geheimtext, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

Eine digitale Signatur ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels zu einer digitalen Nachricht einen Wert berechnet.

# Bezeichnungen

## Verschlüsselung, digitale Signatur & PKI

Verschlüsselung ist die von *einem Schlüssel* abhängige Umwandlung von Klartext genannten Daten in einen Geheimtext, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

Eine digitale Signatur ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels zu einer digitalen Nachricht einen Wert berechnet.

Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels die nichtabstreitbare Urheberschaft und Integrität der Nachricht zu prüfen.

# Bezeichnungen

## Verschlüsselung, digitale Signatur & PKI

Verschlüsselung ist die von *einem Schlüssel* abhängige Umwandlung von Klartext genannten Daten in einen Geheimtext, so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.

Eine digitale Signatur ist ein asymmetrisches Kryptosystem, bei dem ein Sender mit Hilfe eines geheimen Signaturschlüssels zu einer digitalen Nachricht einen Wert berechnet.

Dieser Wert ermöglicht es jedem, mit Hilfe des öffentlichen Verifikationsschlüssels die nichtabstreitbare Urheberschaft und Integrität der Nachricht zu prüfen.

Eine Public Key Infrastruktur ermöglicht das Ausstellen, die Verteilung und das Prüfen von digitalen Zertifikaten.



- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
  - Wurzelzertifikat / Root Certificate
    - Deutsche Telekom Root CA 2 (Trusted)
  - Intermediate CA / Certificates
    - DFN-Verein PCA Global - G01
    - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate
      - Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates
      - DFN-Verein PCA Global - G01
      - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate  
Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates  
DFN-Verein PCA Global - G01  
KIT-CA
  - S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
  - Schlüsselpaar (privater Schlüssel / Zertifikat)
  - Ende-zu-Ende
  - Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate  
Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates  
DFN-Verein PCA Global - G01  
KIT-CA
  - S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
  - Schlüsselpaar (privater Schlüssel / Zertifikat)
  - Ende-zu-Ende
  - Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
  - Wurzelzertifikat / Root Certificate
    - Deutsche Telekom Root CA 2 (Trusted)
  - Intermediate CA / Certificates
    - DFN-Verein PCA Global - G01
    - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate  
Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates  
DFN-Verein PCA Global - G01  
KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate
      - Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates
      - DFN-Verein PCA Global - G01
      - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
  - Schlüsselpaar (privater Schlüssel / Zertifikat)
  - Ende-zu-Ende
  - Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate
      - Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates
      - DFN-Verein PCA Global - G01
      - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)



- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate
      - Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates
      - DFN-Verein PCA Global - G01
      - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

- Transportverschlüsselung
- Client-basierend
- Public Key Infrastructure (PKI) nach X.509
  - Zertifizierungsstelle / Certification Authority (CA)
    - Wurzelzertifikat / Root Certificate
      - Deutsche Telekom Root CA 2 (Trusted)
    - Intermediate CA / Certificates
      - DFN-Verein PCA Global - G01
      - KIT-CA
- S/MIME-Standard (*Alternative*: OpenPGP/GnuPG)
- Schlüsselpaar (privater Schlüssel / Zertifikat)
- Ende-zu-Ende
- Verifikation und Verschlüsseln (ohne eigenes Schlüsselpaar)

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

**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**

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

## Nutzerzertifikat beantragen

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

### Zertifikatdaten

Die folgenden Domainnamen können Sie in E-Mail-Adressen nutzen:>>

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.

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

## 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 verpflichte mich, die in den **Informationen für Zertifikatinhaber** aufgeführten Regelungen einzuhalten. \*



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](mailto:pki@dfn.de) widerrufen. Bitte beachten Sie, dass es leider **nicht** möglich ist, ein Zertifikat nachträglich doch zu veröffentlichen; im Zweifel rät die KIT-CA daher dazu, der Veröffentlichung jetzt zuzustimmen.

Weiter

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

## Nutzerzertifikat beantragen - Bestätigen

Bitte überprüfen Sie die Daten.

### Zertifikatdaten

|           |                          |
|-----------|--------------------------|
| E-Mail    | vorname.nachname@kit.edu |
| Name      | Vorname Nachname         |
| Abteilung | IANM                     |

### Weitere Angaben

|                 |    |
|-----------------|----|
| Veröffentlichen | Ja |
|-----------------|----|

Ändern

Bestätigen

**Wichtig:** Browserprofil

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

## Zertifikatantrag

Abschließend müssen Sie Ihren Zertifikatantrag ausdrucken.

- Bitte betätigen Sie die Schaltfläche "Zertifikatantrag anzeigen". Daraufhin wird der Zertifikatantrag geöffnet.
- Bitte drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn bei Ihrer Registrierungsstelle vor, um die Antragsstellung abzuschließen.
- **Bitte beachten Sie, dass Anträge nach drei Monaten automatisch gelöscht werden, wenn sie nicht bearbeitet wurden. Führen Sie daher die Identifizierung bei der Registrierungsstelle so schnell wie möglich durch!**

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

Zertifikatantrag anzeigen

# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

## Zertifikatantrag für ein Nutzerzertifikat

– an das Karlsruher Institut für Technologie –

### Angaben zum Zertifikatantrag

|                        |   |
|------------------------|---|
| Antragsnummer          | 5 743 904   |
| Eindeutiger Name (DN)  | CN=Vorname Nachname, OU=IANM, O=Karlsruhe Institute of Technology, C=DE |
| Alternativer Name      | email:vorname.nachname@kit.edu  |
| Public-Key Fingerprint | BD:65:32:DB:3B:9A:84:31:AE:CB:7D:97:B9:5D:7C:97:CE:ED:63:57             |
| Veröffentlichen        | Ja  |
| Zertifikatprofil       | User  |

### Angaben zur Person

|                    |                          |
|--------------------|--------------------------|
| Name               | Vorname Nachname         |
| E-Mail             | vorname.nachname@kit.edu |
| Abteilung/Institut | IANM                     |



# Nutzerzertifikatantrag

<https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki>

Hiermit beantrage ich ein Nutzerzertifikat in der DFN-PKI und verpflichte mich, die Regelungen der unter [https://info.pca.dfn.de/doc/Info\\_Zertifikatinhaber.pdf](https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf) veröffentlichten »Informationen für Zertifikatinhaber« einzuhalten. Das heißt insbesondere:

- Ich versichere, dass sämtliche Angaben im Antrag vollständig sind und der Wahrheit entsprechen; ist im eindeutigen Namen (DN) des Zertifikatantrags in einem OU-Feld ein Institut oder ähnliches enthalten, so ist meine Zugehörigkeit durch den entsprechenden Institutsstempel oder vergleichbares unten bestätigt.
- Ich darf den privaten Schlüssel zu dem Zertifikat nicht anderen Personen zugänglich machen. Eine Weitergabe ist nicht erlaubt.
- Jedes Gerät, auf dem ich den privaten Schlüssel speichere beziehungsweise einsetze, muss angemessen geschützt, also unter anderem frei von Schadsoftware wie Viren sein und regelmäßig mit Sicherheits-Patches versehen werden.
- Ich bin unter den folgenden Bedingungen verpflichtet, das Zertifikat sperren zu lassen:
  - Das Zertifikat enthält Angaben, die nicht mehr gültig sind, beispielsweise nach einer Namensänderung.
  - Der private Schlüssel oder die dazugehörige Passphrase wurde verloren, gestohlen, offen gelegt oder anderweitig kompromittiert oder missbraucht.
  - Ich bin nicht mehr berechtigt, das Zertifikat zu nutzen.

Ich erkläre mich mit der Verarbeitung und Nutzung der erhobenen Daten zum Zweck der Zertifikaterstellung einverstanden. Die Daten dürfen an die KIT-CA sowie den DFN-Verein übermittelt und dort beschränkt auf diesen Zweck verarbeitet und genutzt werden.

\_\_\_\_\_  
(Ort, Datum, gegebenenfalls Institutsstempel)

\_\_\_\_\_  
(Unterschrift – wie im Ausweis)

**Wird vom Teilnehmerservice ausgefüllt**

**Antragsnummer 5 743 904**

## Identitätsprüfung

Name geprüft

Unterschrift geprüft

Passbild geprüft



Ausweisnr. (letzte 5 Stellen)







KIT-Mitgliedschaft geprüft

**Prüfer**

# Zertifikatexport und -import

## E-Mail: KIT-CA Zertifikatinformation

Von ra@kit.edu   
Betreff KIT-CA Zertifikatinformation  
An Ingrid Lenhardt  13:51

 Antworten  Allen antworten  Weiterleiten  Junk  Löschen  Mehr ▾

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer 7368570169423424 ist auf den Namen CN=Ingrid Lenhardt,OU=IANM,O=Karlsruhe Institute of Technology,C=DE erstellt worden und im Anhang dieser Mail beigelegt.

Sie benötigen die Seriennummer, um Ihr Zertifikat gegebenenfalls sperren zu können.

Um Ihr Zertifikat nutzen zu können, müssen Sie alle folgenden Zertifikate in Ihren Browser importieren. Achten Sie darauf, dass Sie die Zertifikate auf dem Rechner importieren, von dem aus Sie den Antrag gestellt haben, weil sich dort der zugehörige Schlüssel befindet.

1. Für die CA-Zertifikate wählen Sie bitte die Seite

<https://pki.pca.dfn.de:443/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=index;id=2>

und folgen den Anweisungen.


2. Ihr eigenes Zertifikat erhalten Sie direkt über folgenden Link:

<https://pki.pca.dfn.de:443/kit-ca/cgi-bin/pub/pki?cmd=getcert&key=7368570169423424&type=CERTIFICATE>

Befolgen Sie bitte die in dem Dokument "Informationen für Zertifikatinhaber" aufgeführten Regelungen: [https://info.pca.dfn.de/doc/Info\\_Zertifikatinhaber.pdf](https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf)

Mit freundlichen Grüßen

Ihr PKI-Team der Karlsruhe Institute of Technology

 1 Anhang: cert-7368570169423424.pem 2.0 KB

 Speichern ▾

# Zertifikatexport und -import

## Browserimport: Firefox

**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.**

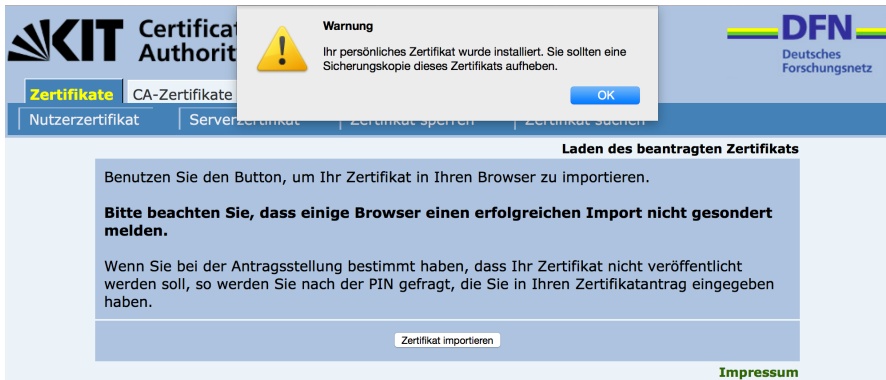
Wenn Sie bei der Antragsstellung bestimmt haben, dass Ihr Zertifikat nicht veröffentlicht werden soll, so werden Sie nach der PIN gefragt, die Sie in Ihren Zertifikatantrag eingegeben haben.

Zertifikat importieren

**Impressum**

# Zertifikatexport und -import

## Browserimport: Firefox



**KIT** Certificate Authority

**DFN**  
Deutsches Forschungsnetz

**Zertifikate** CA-Zertifikate

Nutzerzertifikat | Serverzertifikat | Zertifikat sperren | Zertifikat suchen

**Warnung**  
Ihr persönliches Zertifikat wurde installiert. Sie sollten eine Sicherungskopie dieses Zertifikats aufheben.

OK

**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.**

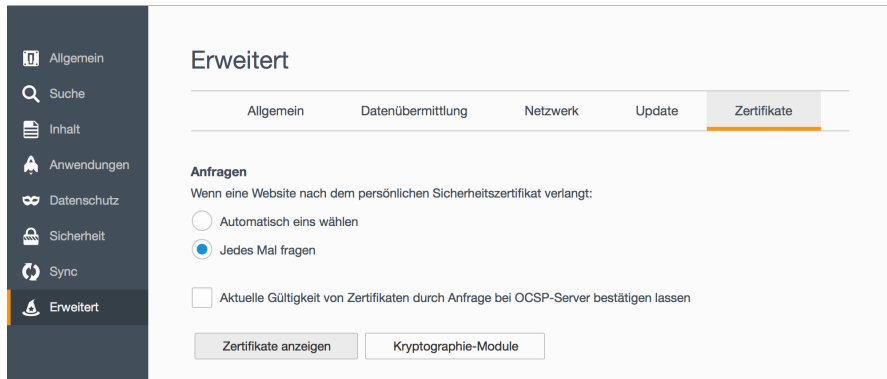
Wenn Sie bei der Antragsstellung bestimmt haben, dass Ihr Zertifikat nicht veröffentlicht werden soll, so werden Sie nach der PIN gefragt, die Sie in Ihren Zertifikatantrag eingegeben haben.

Zertifikat importieren

**Impressum**

# Zertifikatexport und -import

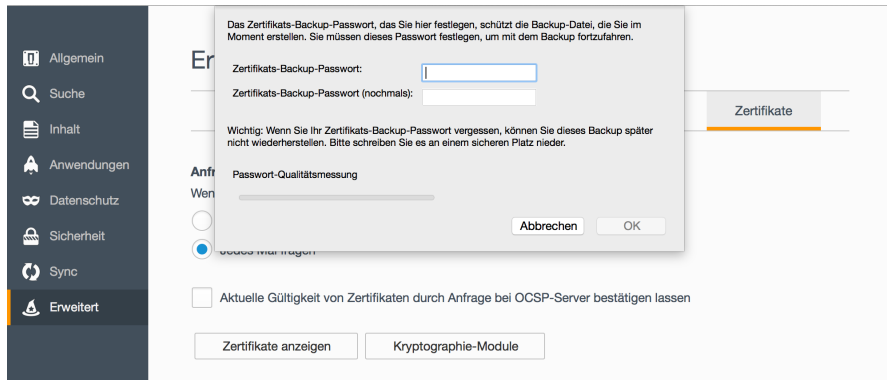
## Browserexport: Firefox



The screenshot shows the 'Erweitert' (Advanced) settings page in Firefox. On the left is a dark sidebar with navigation icons and labels: Allgemein, Suche, Inhalt, Anwendungen, Datenschutz, Sicherheit, Sync, and Erweiterter (highlighted). The main content area has a title 'Erweitert' and a horizontal menu with tabs: Allgemein, Datenübermittlung, Netzwerk, Update, and Zertifikate (selected). Below the tabs is a section titled 'Anfragen' with the text 'Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:'. There are three radio button options: 'Automatisch eins wählen', 'Jedes Mal fragen' (selected), and 'Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen'. At the bottom are two buttons: 'Zertifikate anzeigen' and 'Kryptographie-Module'.

# Zertifikatexport und -import

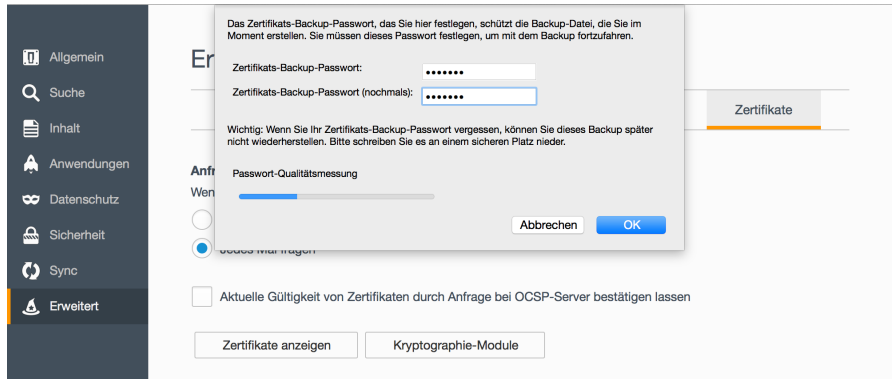
## Browserexport: Firefox



The screenshot shows the Firefox Certificate Manager interface. On the left is a dark sidebar with navigation options: Allgemein, Suche, Inhalt, Anwendungen, Datenschutz, Sicherheit, Sync, and Erweitert (highlighted). The main content area is titled 'Zertifikate' and contains a dialog box for creating a certificate backup. The dialog box text reads: 'Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Backup-Datei, die Sie im Moment erstellen. Sie müssen dieses Passwort festlegen, um mit dem Backup fortzufahren.' It includes two input fields for the password, a warning: 'Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können Sie dieses Backup später nicht wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder.', and a 'Passwort-Qualitätsmessung' section with a progress bar. At the bottom of the dialog are 'Abbrechen' and 'OK' buttons. Below the dialog, there is a checkbox for 'Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen' and two buttons: 'Zertifikate anzeigen' and 'Kryptographie-Module'.

# Zertifikatexport und -import

## Browserexport: Firefox



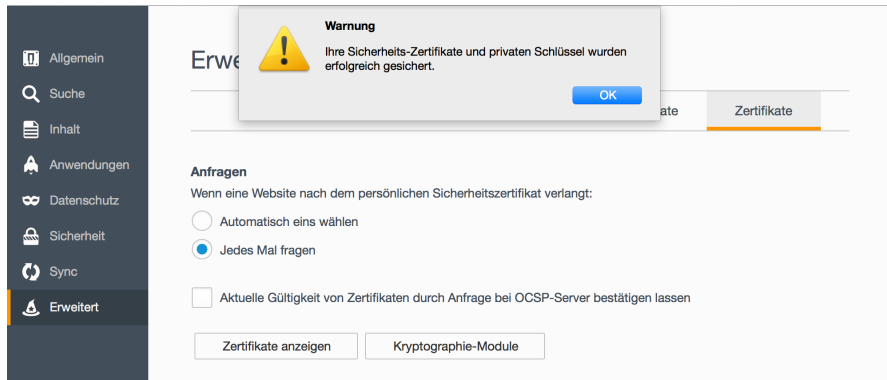
The screenshot shows the Firefox settings page with the 'Erweitert' (Advanced) section selected in the left sidebar. A dialog box is open for creating a certificate backup. The dialog contains the following text and elements:

- Header: **Er**
- Text: Das Zertifikats-Backup-Passwort, das Sie hier festlegen, schützt die Backup-Datei, die Sie im Moment erstellen. Sie müssen dieses Passwort festlegen, um mit dem Backup fortzufahren.
- Form fields: Two input fields for 'Zertifikats-Backup-Passwort:' and 'Zertifikats-Backup-Passwort (nochmals):', both containing six dots.
- Text: Wichtig: Wenn Sie Ihr Zertifikats-Backup-Passwort vergessen, können Sie dieses Backup später nicht wiederherstellen. Bitte schreiben Sie es an einem sicheren Platz nieder.
- Section: **Anf** Passwort-Qualitätsmessung
- Progress bar: A blue progress bar indicating password strength.
- Buttons: 'Abbrechen' (Cancel) and 'OK'.
- Text: **Wen**
- Radio buttons: Two radio buttons, the second one is selected.
- Text: **Wen** jedes Mal fragen
- Text:  Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen
- Buttons: 'Zertifikate anzeigen' and 'Kryptographie-Module'

In the background, the 'Zertifikate' (Certificates) section of the settings is visible, with a 'Zertifikate' button highlighted.

# Zertifikatexport und -import

## Browserexport: Firefox



The screenshot shows the Firefox 'Erweitert' (Advanced) settings page. A warning dialog box is overlaid on top, stating: 'Warnung: Ihre Sicherheits-Zertifikate und privaten Schlüssel wurden erfolgreich gesichert.' (Warning: Your security certificates and private keys were successfully backed up.) The dialog has a yellow warning icon and an 'OK' button. Below the dialog, the 'Erweitert' settings are visible, with the 'Zertifikate' (Certificates) section selected. Under the 'Anfragen' (Ask) section, the option 'Jedes Mal fragen' (Ask every time) is selected. There are also buttons for 'Zertifikate anzeigen' (Show Certificates) and 'Kryptographie-Module' (Cryptographic Modules).

**Warnung**  
Ihre Sicherheits-Zertifikate und privaten Schlüssel wurden erfolgreich gesichert.

OK

Erweitert

Zertifikate

**Anfragen**  
Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

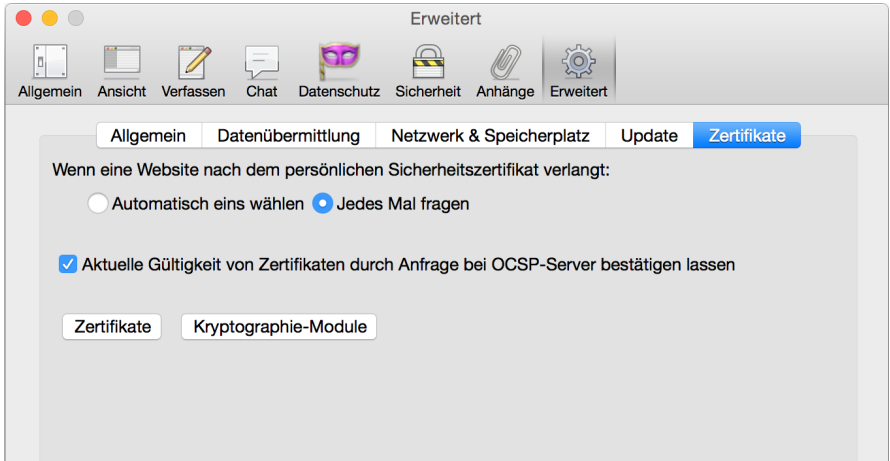
- Automatisch eins wählen
- Jedes Mal fragen
- Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Zertifikate anzeigen    Kryptographie-Module



# Zertifikatexport und -import

## Mailclientimport: Thunderbird



The screenshot shows the 'Erweitert' (Advanced) settings window in Thunderbird. The 'Zertifikate' (Certificates) tab is selected. The window title is 'Erweitert'. The top toolbar includes icons for Allgemein, Ansicht, Verfassen, Chat, Datenschutz, Sicherheit, Anhänge, and Erweitert. The main content area has tabs for Allgemein, Datenübermittlung, Netzwerk & Speicherplatz, Update, and Zertifikate. The text reads: 'Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:'. There are two radio buttons: 'Automatisch eins wählen' (unselected) and 'Jedes Mal fragen' (selected). Below this is a checked checkbox: 'Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen'. At the bottom, there are two buttons: 'Zertifikate' and 'Kryptographie-Module'.

Erweitert

Allgemein Ansicht Verfassen Chat Datenschutz Sicherheit Anhänge Erweitert

Allgemein Datenübermittlung Netzwerk & Speicherplatz Update **Zertifikate**

Wenn eine Website nach dem persönlichen Sicherheitszertifikat verlangt:

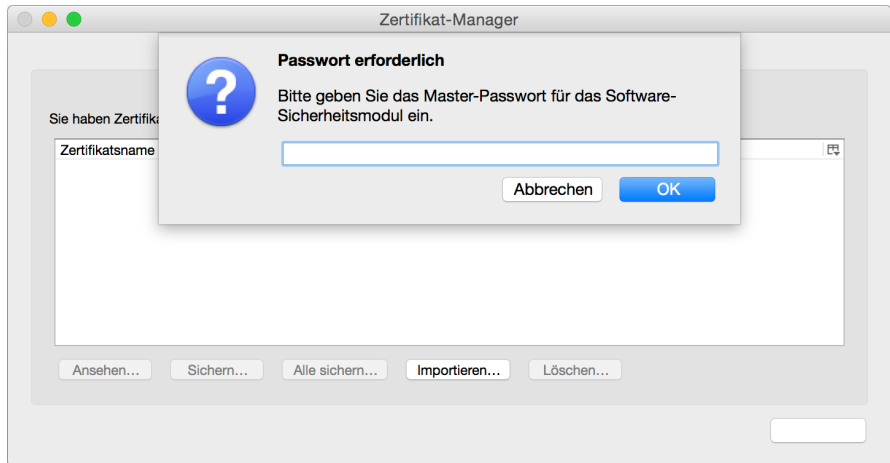
Automatisch eins wählen  Jedes Mal fragen

Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen

Zertifikate Kryptographie-Module

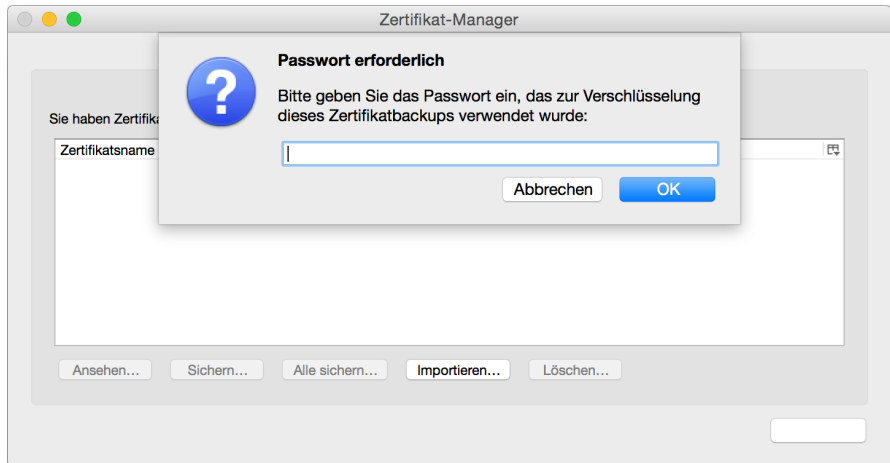
# Zertifikatexport und -import

## Mailclientimport: Thunderbird



# Zertifikatexport und -import

## Mailclientimport: Thunderbird



# Zertifikatexport und -import

## Mailclientimport: Thunderbird



### Konten



[Konten-Einstellungen bearbeiten](#)



Neues Konto erstellen:



E-Mail



Chat



Newsgroups



Feeds

### ▼ KIT (NA)

Server-Einstellungen

Kopien & Ordner

Verfassen & Adressieren

Junk-Filter

Synchronisation & Speicherplatz

OpenPGP-Sicherheit

Empfangsbestätigungen (MDN)

S/MIME-Sicherheit

VERSCHLUSS

Folgendes :

Standard-V

Nie (kein

Notwend

Zertifikate

▼ KIT (NA)

Server-Einstellungen

Kopien & Ordner

Verfassen & Adressieren

Junk-Filter

Synchronisation & Speicherplatz

OpenPGP-Sicherheit

Empfangsbestätigungen (MDN)

S/MIME-Sicherheit

Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.

### Digitale Unterschrift

Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben:

Auswählen...

Leeren

Nachrichten digital unterschreiben (als Standard)

### Verschlüsselung

Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:

Auswählen...

Leeren

Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:

Nie (keine Verschlüsselung verwenden)

Notwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen)

### Zertifikate

Zertifikate verwalten...

Kryptographie-Module verwalten...

# Mailclientkonfiguration

## Thunderbird

Zertifikat: Karlsruhe Institute of Technology ID von Ingrid Lenhardt [1A:2D:AC:EF:73:76:40]

Details des gewählten Zertifikats:

Ausgestellt auf: CN=Ingrid Lenhardt,OU=IANM,O=Karlsruhe Institute of Technology,C=DE

Seriennummer: 1A:2D:AC:EF:73:76:40

Gültig von 02.10.15 09:16:47 bis 01.10.18 09:16:47

Verwendung eines Zertifikatsschlüssels: unterzeichne,Non-repudiation,Schlüssel-Verschlüsselung

E-Mail: ingrid.lenhardt@kit.edu

Ausgestellt von: E=ca@kit.edu,CN=KIT-CA,OU=Steinbuch Centre for Computing,O=Karlsruhe Institute of Technology,L=Karlsruhe,ST=Baden-Wuerttemberg,C=DE

Gespeichert in: das Software-Sicherheitsmodul

Abbrechen

OK

**3 Jahre Gültigkeit** → dennoch Aufbewahren!





### Thunderbird

Möchten Sie das gleiche Zertifikat verwenden, um an Sie gesendete Nachrichten zu ver- und entschlüsseln?

Nein

Ja

Um verschlüsselte Nachrichten zu senden und zu empfangen, sollten Sie sowohl ein Zertifikat für Verschlüsselung als auch eines für digitale Unterschrift angeben.

### Digitale Unterschrift

Folgendes Zertifikat verwenden, um Nachrichten digital zu unterschreiben:

Karlsruhe Institute of Technology ID von Ingrid Lenhardt

Auswählen...

Leeren

Nachrichten digital unterschreiben (als Standard)

### Verschlüsselung

Folgendes Zertifikat verwenden, um Nachrichten zu ver- und entschlüsseln:

Karlsruhe Institute of Technology ID von Ingrid Lenhardt

Auswählen...

Leeren

Standard-Verschlüsselungseinstellung beim Senden von Nachrichten:

Nie (keine Verschlüsselung verwenden)

Notwendig (Senden nur möglich, wenn alle Empfänger ein Zertifikat besitzen)

### Zertifikate

Zertifikate verwalten...

Kryptographie-Module verwalten...

#### ▼ KIT (NA)

Server-Einstellungen

Kopien & Ordner

Verfassen & Adressieren

Junk-Filter

Synchronisation & Speicherplatz

OpenPGP-Sicherheit

Empfangsbestätigungen (MDN)

S/MIME-Sicherheit

# Symbolik im Thunderbird

## Beispiele 1/4

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

Betreff Nicht verschlüsselt / nicht signiert

25.09.15 18:14

An Christian Knieling★

---

Nicht verschlüsselt / nicht signiert

Größe: 724 Byte

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

Betreff Nicht verschlüsselt / signiert



25.09.15 18:13

An Christian Knieling★

---

Nicht verschlüsselt / signiert

Größe: 8.577 Byte

# Symbolik im Thunderbird

## Beispiele 2/4

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

Betreff **Verschlüsselt / nicht signiert**



25.09.15 18:14

An Christian Knieling★

---

Verschlüsselt / nicht signiert

Größe: 1.789 Byte

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

Betreff **Verschlüsselt / signiert**



25.09.15 18:13

An Christian Knieling★

---

Verschlüsselt / signiert

Größe: 12.543 Byte

# Symbolik im Thunderbird

## Beispiele 3/4

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

**Betreff Nicht verschlüsselt / signiert und Betreff geändert**



25.09.15 18:13

An Christian Knieling★

---

Nicht verschlüsselt / signiert

Von Christian Knieling★

↩ Antworten

➡ Weiterleiten

🗑 Junk

🗑 Löschen

Mehr ▾

**Betreff Nicht verschlüsselt / signiert und Nachrichteninhalte geändert**



25.09.15 18:13

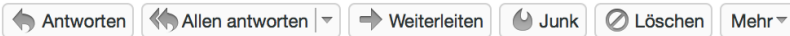
An Christian Knieling★

---

Nicht verschlüsselt / signiert und Nachrichteninhalte geändert

# Symbolik im Thunderbird

## Beispiele 4/4



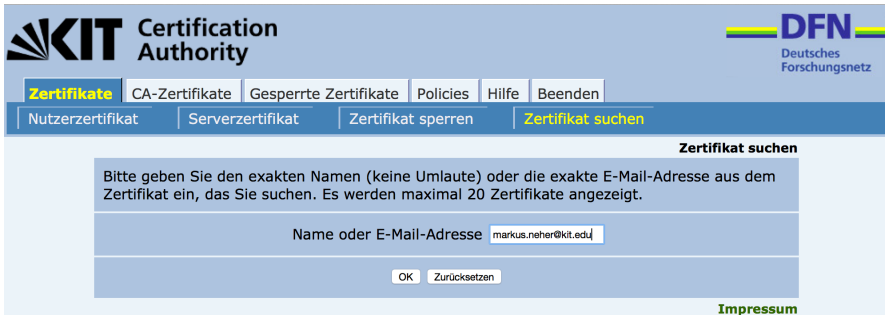
im★, David Hipp★, Marlis Hochbruck★, Jonas Käppler★, Christian Knie **8 weitere**



16.09.15 19:15

# Zertifikate auffinden

`https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=search_cert`



The screenshot shows the web interface of the KIT Certification Authority. At the top left is the KIT logo and the text "Certification Authority". At the top right is the DFN logo with the text "Deutsches Forschungsnetz". Below the logos is a navigation bar with several tabs: "Zertifikate" (highlighted in yellow), "CA-Zertifikate", "Gesperrte Zertifikate", "Policies", "Hilfe", and "Beenden". Below this is a secondary navigation bar with tabs: "Nutzerzertifikat", "Serverzertifikat", "Zertifikat sperren", and "Zertifikat suchen" (highlighted in yellow). The main content area is titled "Zertifikat suchen" and contains the following text: "Bitte geben Sie den exakten Namen (keine Umlaute) oder die exakte E-Mail-Adresse aus dem Zertifikat ein, das Sie suchen. Es werden maximal 20 Zertifikate angezeigt." Below this text is a text input field with the label "Name oder E-Mail-Adresse" and the value "markus.neher@kit.edu". At the bottom of the input area are two buttons: "OK" and "Zurücksetzen". In the bottom right corner of the interface is a link labeled "Impressum".

# Zertifikate auffinden

`https://pki.pca.dfn.de/kit-ca/cgi-bin/pub/pki?cmd=getStaticPage;name=search_cert`



**Certification  
Authority**



**Zertifikate**

CA-Zertifikate

Gesperrte Zertifikate

Policies

Hilfe

Beenden

Nutzerzertifikat


Serverzertifikat

Zertifikat sperren

**Zertifikat suchen**

## Zertifikat suchen - Ergebnisse

Klicken Sie auf die Seriennummer eines Zertifikats, um es in Ihren Browser zu importieren.

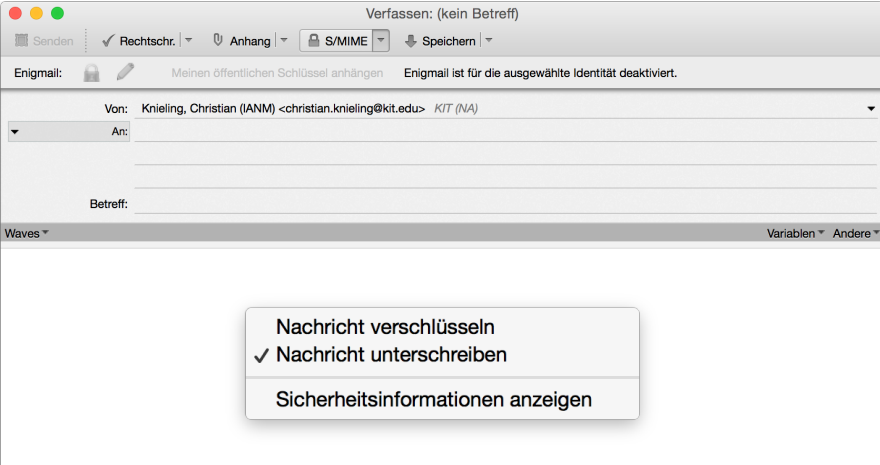
|   | <b>Seriennummer</b> | <b>Name</b>  | <b>E-Mail</b>        | <b>Rolle</b> |
|---|---------------------|--------------|----------------------|--------------|
|  | 6703553609674164    | Markus Neher | markus.neher@kit.edu | User         |

**Impressum**



# E-Mail verfassen

## Hinweise





The screenshot shows an email composition window titled "Verfassen: (kein Betreff)". The top toolbar includes buttons for "Senden", "Rechtschr.", "Anhang", "S/MIME", and "Speichern". Below the toolbar, there is a status bar for "Enigmail" with a lock icon and a pencil icon, and the text "Meinen öffentlichen Schlüssel anhängen" and "Enigmail ist für die ausgewählte Identität deaktiviert." The main area contains fields for "Von:" (Knieling, Christian (IANM) <christian.knieling@kit.edu> KIT (NA)), "An:", and "Betreff:". At the bottom, there are "Waves" and "Variablen" buttons. A callout box in the center highlights three options: "Nachricht verschlüsseln", "✓ Nachricht unterschreiben", and "Sicherheitsinformationen anzeigen".

# E-Mail verfassen

## Hinweise

Verfassen: (kein Betreff)

Senden Rechtschr. Anhang S/MIME Speichern

Enigmail:  

Von: Kr  
An: Ne  
An:   
Betreff:   
Waves

Bitte beachten Sie: Betreffzeilen von Nachrichten werden nie verschlüsselt.

Die Inhalte Ihrer Nachricht werden wie folgt gesendet:

Digital unterschrieben: Ja  
Verschlüsselt: Nein

Zertifikate:

| Empfänger:           | Status: | Herausgegeben: | Läuft ab: |
|----------------------|---------|----------------|-----------|
| markus.neher@kit.edu | Gültig  | 30.06.14       | 29.06.17  |

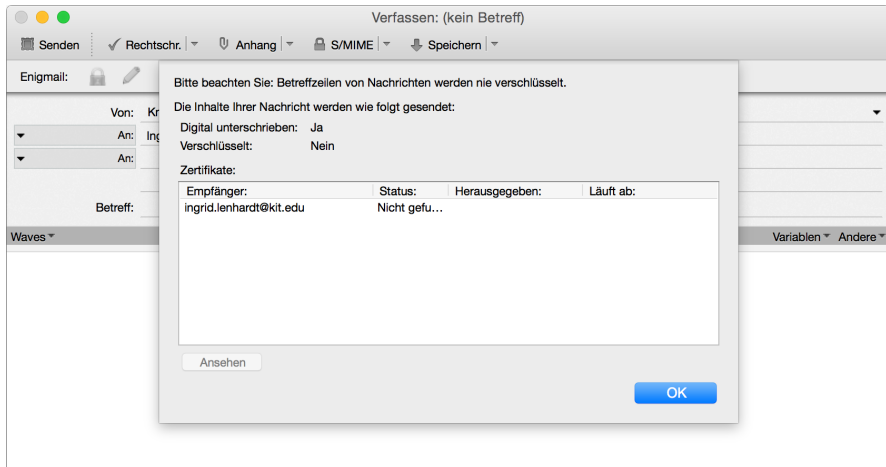
Ansehen

OK

Variablen Andere

# E-Mail verfassen

## Hinweise



### Anhänge sind Mail-Content

- Signierung
- Verschlüsselung
- nicht mehr abtrennbar

Öffnen  
Speichern...

Abtrennen...  
Löschen

OpenPGP-Schlüssel importieren  
Entschlüsseln und Öffnen  
Entschlüsseln und Speichern unter...  
Unterschrift überprüfen

Öffnen  
Speichern...

Abtrennen...  
Löschen

OpenPGP-Schlüssel importieren  
Entschlüsseln und Öffnen  
Entschlüsseln und Speichern unter...  
Unterschrift überprüfen

# Fragen oder Ungereimtheiten?



Vielen Dank für die Aufmerksamkeit.