Universität Rostock Traditio et Innovatio

E-Mail-Signierung und Verschlüsselung mit Zertifikaten

Torsten Thierbach (ITMZ)

Überblick

1. Ansprechpartner

2. Zertifikate
   - 2.1 Warum Zertifikate Verwenden?
   - 2.2 Aufbau und Funktionsweise

3. Antragsverfahren
   - 3.1 Webformular
   - 3.2 Antrag und Identifizierung
   - 3.3 Antwortmail

Überblick

1. Ansprechpartner

- Daniel Erdmann
  - E-Mail: daniel.erdmann@uni-rostock.de
  - Tel.: 5384

Für Anträge:

- Torsten Thierbach
  - E-Mail: torsten.thierbach@uni-rostock.de
  - Tel.: 5328
- Jörg Zerbe
  - E-Mail: joerg.zerbe@uni-rostock.de
  - Tel.: 5320
- Jörg Maletzky
  - E-Mail: joerg.maletzky@uni-rostock.de
  - Tel.: 5339

2. Zertifikate

2.1 Warum sollte ich Zertifikate Verwenden?

- Ein Zertifikat dient der Identifizierung eines Absenders (ähnlich eines Personalausweises)
- Ist eine E-Mail mit einem Zertifikat signiert, kann man sie dem Absender eindeutig zuordnen
  - → Damit können E-Mails von gefälschten Adressen identifiziert werden (Zertifikat fehlt)
  - → Empfänger kann potentiell gefährliche E-Mails (Malware, Viren) von „bekannten“ Adressen erkennen
- Informationen können verschlüsselt ausgetauscht werden
  - → E-Mails können nur vom Empfänger mit passendem privatem Schlüssel geöffnet werden

2. Zertifikate

2.2 Aufbau und Funktionsweise (1)

Ein Zertifikat:

- enthält den Namen des Besitzers,
- enthält dessen E-Mail-Adresse,
- enthält den öffentlichen Schlüssel
- wird nach persönlicher Identifizierung mittels Lichtbildausweis ausgestellt
- ist vom Aussteller digital signiert und
- ist 3 Jahre gültig
    - Danach muss das Antragsverfahren wiederholt werden!

→ Dadurch ist die Identität des Absenders einer digital signierten E-Mail verifizierbar!

2. Zertifikate

2.2 Aufbau und Funktionsweise (2)

Öffentlicher und privater Schlüssel

Der öffentliche Schlüssel

- wird mit einer signierten Mail versendet
- dient dazu, Mails an den Eigentümer des dazugehörigen Zertifikats zu VERSCHLÜSSELN

2. Zertifikate

2.2 Aufbau und Funktionsweise (3)

Öffentlicher und privater Schlüssel

Der private Schlüssel

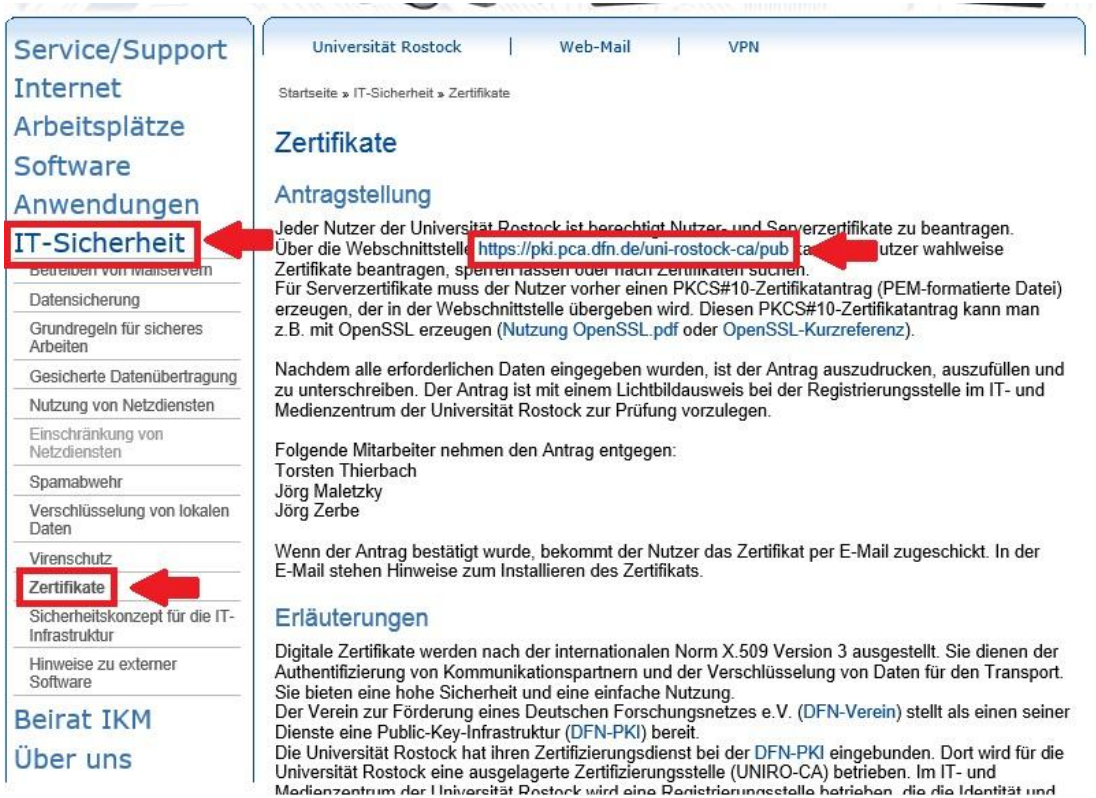
- wird zum ENTSCHLÜSSELN einer E-Mail benötigt
- existiert nur auf dem Rechner des Zertifikateigentümers!
- bei Verlust können E-Mails, welche mit dem dazugehörigen öffentlichen Schlüssel verschlüsselt wurden nicht mehr entschlüsselt werden!

→ Das Zertifikat sollte inklusive privatem Schlüssel exportiert und auf einem externen Medium (z.B. USB-Stick) gespeichert werden!

3. Antragsverfahren

3.1 Webformular

- **Bitte den Internet Explorer verwenden!**
- Homepage des ITMZ: www.itmz.uni-rostock.de
- Im Seitenmenü „IT-Sicherheit“ auswählen
- „Zertifikate“ auswählen
- Den hier rot markierten Link öffnen



3. Antragsverfahren

3.1 Webformular

- Startseite der PKI der Uni Rostock
- Im Menü „Nutzerzertifikat“ auswählen

3. Antragsverfahren

3.1 Webformular

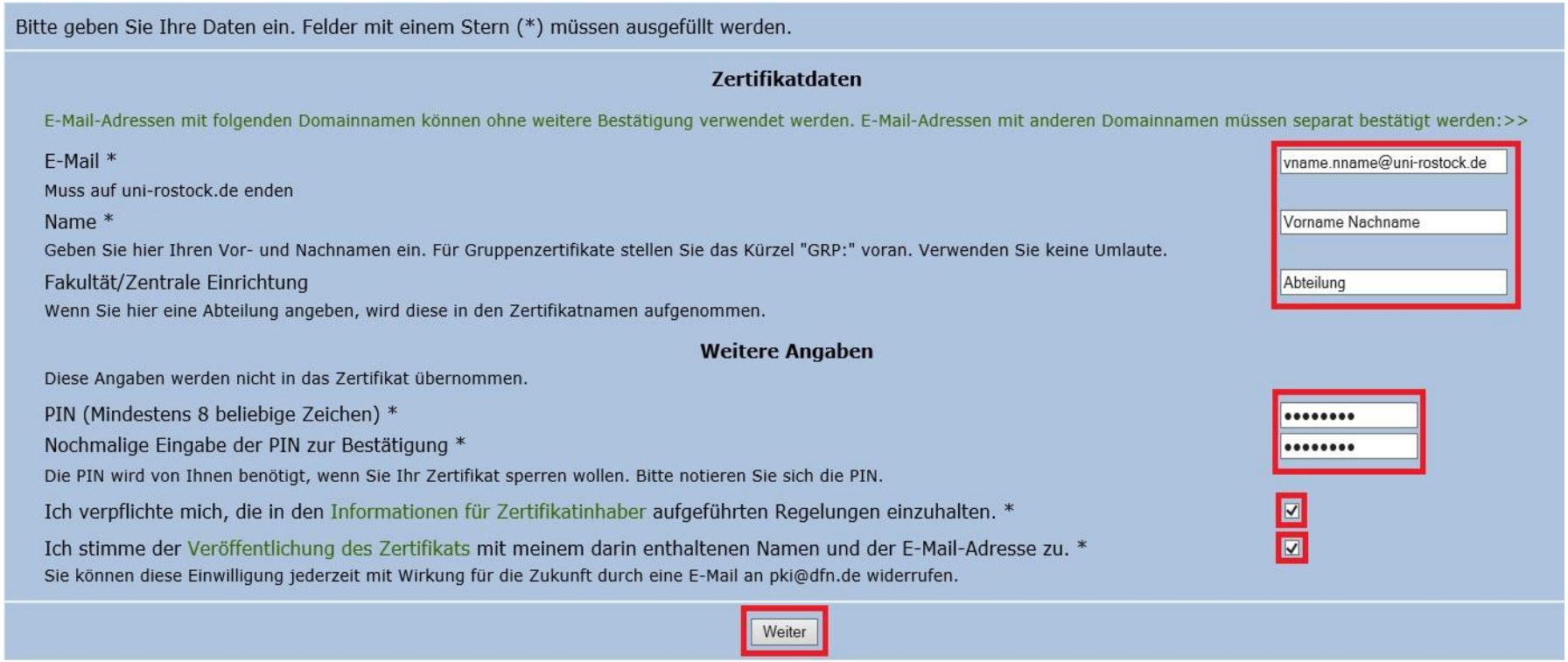
WICHTIG:

- Beim Ausfüllen des Formulars: im Feld „Fakultät/Zentrale Einrichtung“ keine Sonderzeichen verwenden (ä, ö, :, etc)!

- In Allen Feldern darauf achten, dass am Ende keine Leerzeichen sind!

3. Antragsverfahren

3.1 Webformular



3. Antragsverfahren

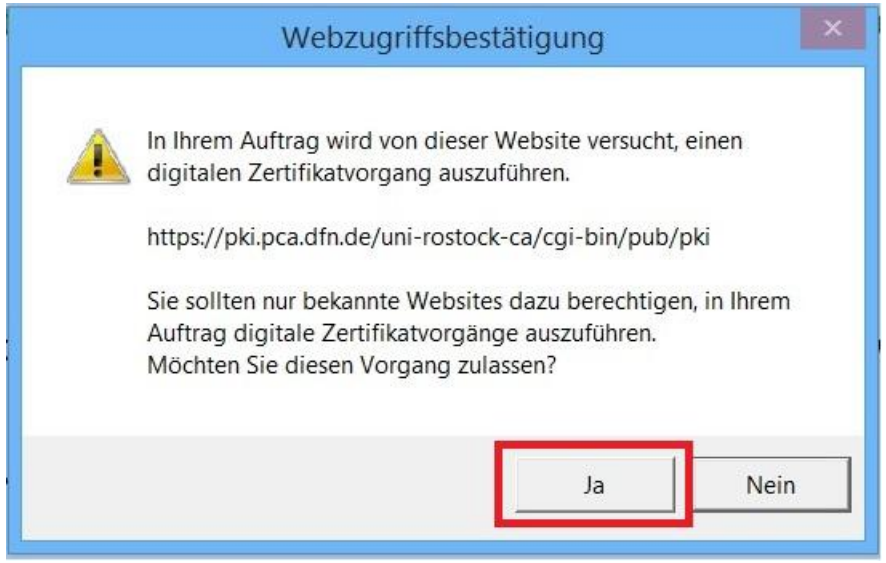
3.1 Webformular

- Sind die Daten korrekt bitte auf „Bestätigen“ klicken
- Für Korrekturen auf „Ändern“ klicken, NICHT den „Zurück“-Button im Browser nutzen!

3. Antragsverfahren

3.1 Webformular

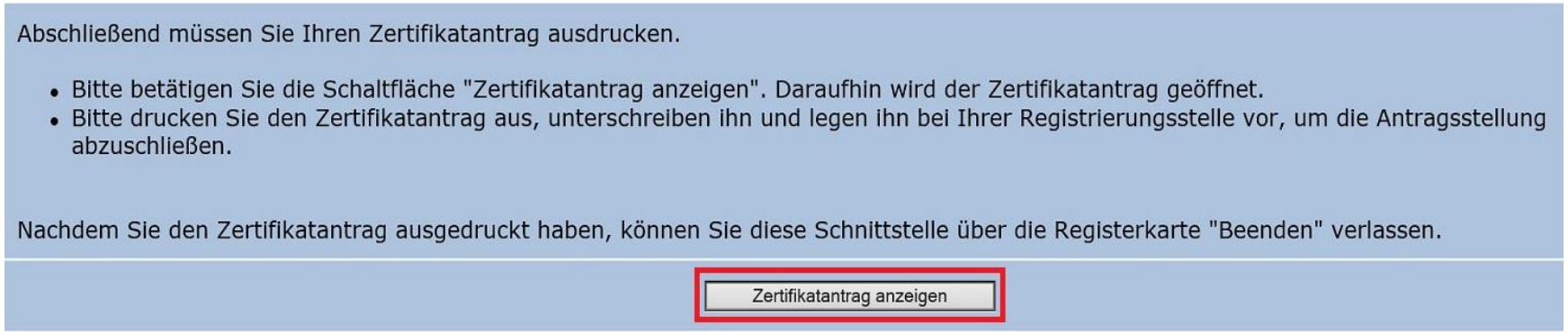
- Es wird auf Ihrem PC ein zu dem Zertifikat gehörender privater Schlüssel generiert
- Sollte folgende Warnung angezeigt werden, bitte mit „Ja“ bestätigen



3. Antragsverfahren

3.1 Webformular

- Der Antrag muss nun ausgedruckt werden
- Dazu bitte auf „Zertifikatsantrag anzeigen“ klicken



3. Antragsverfahren

3.1 Webformular

Nach dem Anklicken des Buttons „Zertifikatantrag anzeigen“ wird, je nach Einstellungen des Browsers, entweder die .pdf-Datei geöffnet, oder das oben gezeigte Feld im unteren Bereich des Browsers angezeigt.
In diesem Fall können Sie auswählen, ob Sie den Antrag speichern oder direkt öffnen möchten. Wo der Antrag gespeichert wird, hängt von Ihren Browsereinstellungen ab. Bei Fragen wenden Sie sich bitte an den zuständigen Administrator!

3. Antragsverfahren

3.2 Antrag und Identifizierung

Den Antrag bitte

- Ausdrucken
- Ort und Datum eintragen
- Unterschreiben
- PERSÖNLICH bei Hr. Thierbach / Hr. Zerbe / Hr. Maletzky abgeben
  - → Bei der Abgabe bitte einen amtlichen Lichtbildausweis zur Identifizierung mitbringen!

4. Import und Nutzung des Zertifikats

4.1 Antwortmail mit signiertem Zertifikat

- Nachdem der Antrag genehmigt wurde, bekommen Sie innerhalb weniger Minuten eine E-Mail von „ca@uni-rostock.de“
- Öffnen Sie den Link unter „2. Ihr eigenes Zertifikat erhalten Sie direkt über folgenden Link:“ (siehe nächste Folie)
- → Hierzu bitte denselben Browser benutzen, mit dem auch der Antrag erstellt wurde (nur dieser hat Zugriff auf den privaten Schlüssel)!

4. Import und Nutzung des Zertifikats

4.1 Antwortmail mit signiertem Zertifikat

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer [redacted] ist auf den Namen CN=[redacted] OU=ITMZ,O=Universitaet Rostock,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/uni-rostock-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/uni-rostock-ca/cgi-bin/pub/pki?cmd=getcert&key=[redacted]&type=CERTIFICATE

Befolgen Sie bitte die in dem Dokument "Informationen für Zertifikatinhaber" aufgeführten Regelungen: https://info.pca.dfn.de/doc/Info_Zertifikatinhaber.pdf

Mit freundlichen Grüßen

Ihr PKI-Team der Universitaet Rostock

4. Import und Nutzung des Zertifikats

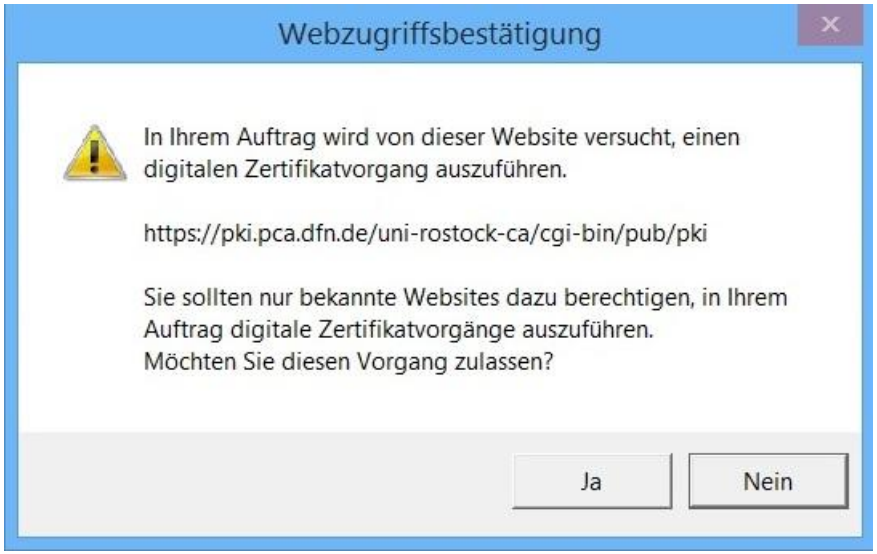
4.2 Import des Zertifikats im Browser

- Auf der sich öffnenden Webseite bitte „Zertifikat importieren“ klicken

4. Import und Nutzung des Zertifikats

4.2 Import des Zertifikats im Browser

- Sollte folgende Warnung angezeigt werden, bitte mit „Ja“ bestätigen



4. Import und Nutzung des Zertifikats

4.3 Outlook Einstellungen

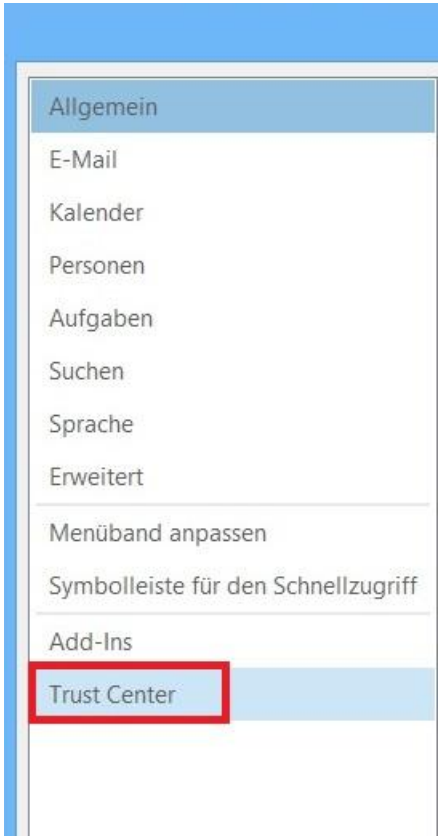
- Bitte öffnen Sie Outlook
- Das „Datei“-Menü öffnen
- Den Punkt „Optionen“ auswählen

4. Import und Nutzung des Zertifikats

4.3 Outlook Einstellungen

- Im neuen Fenster den Punkt **„Trust Center“** (je nach Spracheinstellung kann es auch **„Sicherheitscenter“** heißen) auswählen

- Dann rechts auf den Button „Einstellungen für das Trust Center (oder Sicherheitscenter)…“ klicken



4. Import und Nutzung des Zertifikats

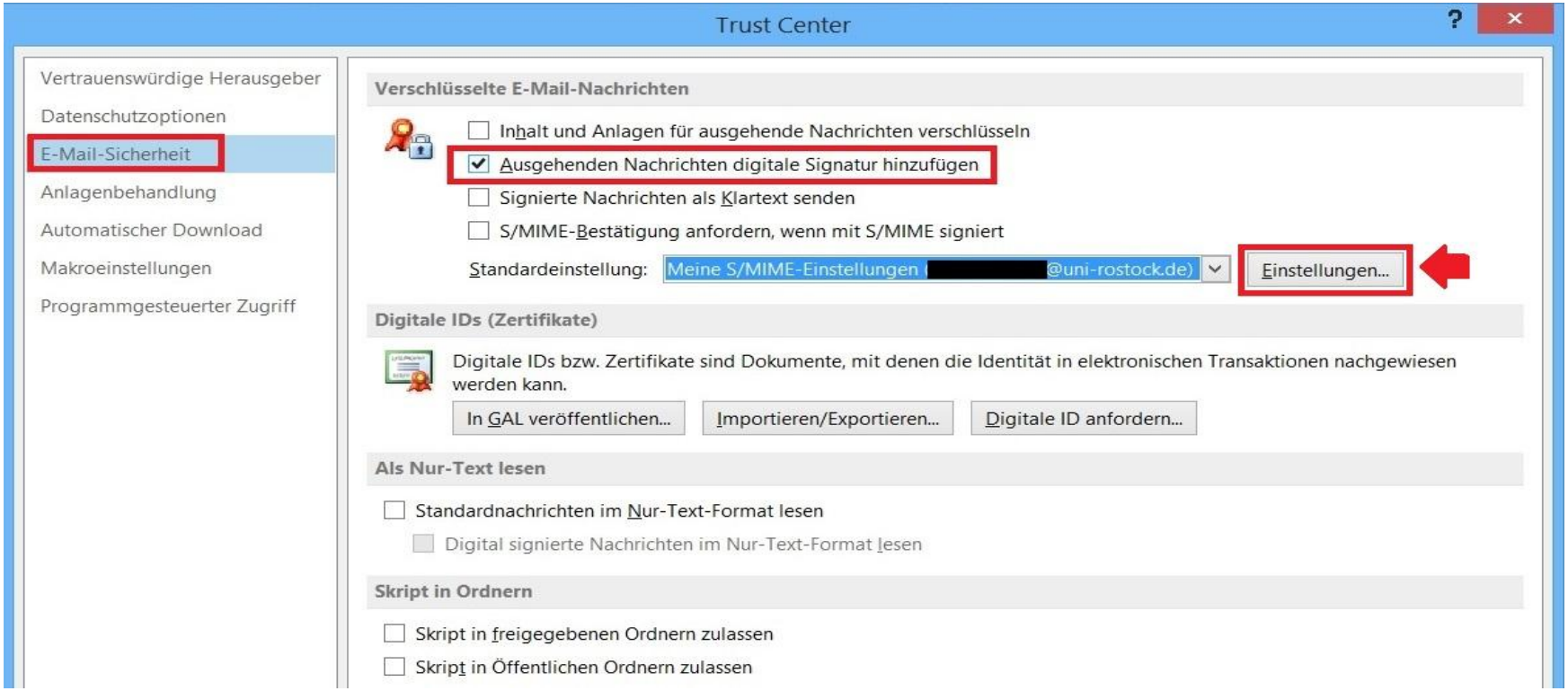
4.3 Outlook Einstellungen

- Im „Trust Center“ bzw. „Sicherheitscenter“-Fenster den Punkt „E-Mail Sicherheit“ auswählen
- In der Menügruppe „Verschlüsselte E-Mail-Nachrichten“ einen Haken im Kästchen neben „Ausgehenden Nachrichten digitale Signatur hinzufügen“ setzen
- Den Button „Einstellungen“ klicken und das sich öffnende Fenster mit „OK“ bestätigen (hier müssen keine Einstellungen geändert werden!)

- (siehe nächste Folie)

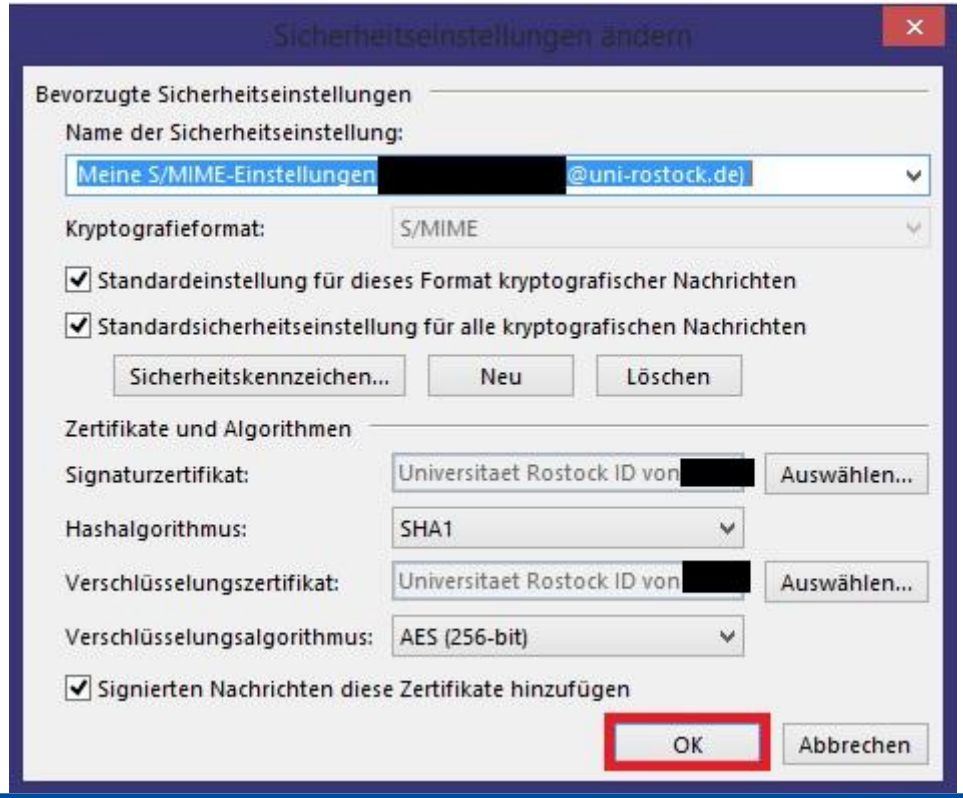
4. Import und Nutzung des Zertifikats

4.3 Outlook Einstellungen



4. Import und Nutzung des Zertifikats

4.3 Outlook Einstellungen



4. Import und Nutzung des Zertifikats

4.3 Outlook Einstellungen

- Jetzt wird automatisch Ihr Zertifikat an jede Ihrer ausgehenden E-Mails gehängt (kann bei jeder Mail auch einzeln abgeschaltet werden)

- Damit sind Sie eindeutig als Absender identifizierbar

5. E-Mail-Signierung und –Verschlüsselung

- Sie können bei jeder E-Mail festlegen, ob diese Signiert/Verschlüsselt wird
- Dazu in der Menüleiste auf „Optionen“ klicken
  - Sollten ihre neuen / Antwort-Mails nicht in einem eigenen Fenster geöffnet werden, so ist diese Menüleiste nicht sichtbar!
  - Dann bitte das Bearbeitungsfenster über den Button „Abdocken“ in einem eigenen Fenster öffnen
- Je nach bedarf die Optionen „Signieren“ und „Verschlüsseln“ anklicken (aktive Auswahl = Blau oder Gelb hinterlegt) (siehe nächste Folie)

- **Bitte Beachten:** um verschlüsselte Mails zu versenden benötigen Sie den öffentlichen Schlüssel des Empfängers!
- Dieser muss ihnen eine signierte E-Mail zusenden!
- Auf diese können Sie dann Antworten und die Option „Verschlüsseln“ auswählen

5. E-Mail-Signierung und –Verschlüsselung

In diesem Beispiel ist „Signieren“ aktiv und „Verschlüsseln“ inaktiv

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?