





Überblick

1. Ansprechpartner

2. Zertifikate

2.1 Warum Zertifikate Verwenden?2.2 Aufbau und Funktionsweise

3. Antragsverfahren

3.1 Webformular3.2 Antrag und Identifizierung3.3 Antwortmail



Überblick

4. Import und Nutzung des Zertifikats

4.1 Antwortmail mit signiertem Zertifikat

4.2 Import des Zertifikats im Browser

4.3 Outlook Einstellungen

5. E-Mail-Signierung und –Verschlüsselung

- 5.1 Signierung
- 5.2 Verschlüsselung



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



2.1 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



2.2 Aufbau und Funktionsweise (1)

Fin 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!



2.2 Aufbau und Funktionsweise (2)

Öffentlicher und privater Schlüssel

Der öffentliche Schlüssel

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



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!



3.1 Webformular

- Bitte den Internet Explorer verwenden!
- Homepage des ITMZ: <u>www.itmz.uni-rostock.de</u>
- Im Seitenmenü "IT-Sicherheit" auswählen
- "Zertifikate" auswählen
- Den hier rot markierten Link öffnen

Service/Support	Universität Rostock Web-Mail VPN
nternet	Startseite » IT-Sicherheit » Zertifikate
Arbeitsplätze	Zertifikate
Software	Zerunkate
Anwendungen	Antragstellung
T-Sicherheit	Jeder Nutzer der Universität Rostock ist berechtigt Nutzer, und Serverzertifikate zu beantragen. Über die Webschnittstelle https://pki.pca.dfn.de/uni-rostock-ca/pub.tage.tage.utzer wahlweise
Betreiben von wanservem	Zertifikate beantragen, spenen rassen oder nach Zerunkaten suchen.
Datensicherung	Für Serverzertitikate muss der Nutzer vorher einen PKCS#10-Zertifikatantrag (PEM-tormatierte Datei) erzeugen, der in der Webschnittstelle übergeben wird. Diesen PKCS#10-Zertifikatantrag kann man
Grundregeln für sicheres Arbeiten	z.B. mit OpenSSL erzeugen (Nutzung OpenSSL.pdf oder OpenSSL-Kurzreferenz).
Gesicherte Datenübertragung	Nachdem alle erforderlichen Daten eingegeben wurden, ist der Antrag auszudrucken, auszufüllen und
Nutzung von Netzdiensten	zu unterschreiden. Der Antrag ist mit einem Lichtbildausweis dei der Registrierungsstelle im IT- und Medienzentrum der Universität Rostock zur Prüfung vorzulegen.
Einschränkung von Netzdiensten	Folgende Mitarbeiter nehmen den Antrag entgegen:
Spamabwehr	Torsten Thierbach
Verschlüsselung von lokalen Daten	Jörg Zerbe
Virenschutz	Wenn der Antrag bestätigt wurde, bekommt der Nutzer das Zertifikat per E-Mail zugeschickt. In der
Zertifikate	E-Mail stehen finnweise zum installieren des Zertlinkals.
Sicherheitskonzept für die IT- Infrastruktur	Erläuterungen
Hinweise zu externer Software	Digitale Zertfilfkate werden nach der internationalen Norm X.509 Version 3 ausgestellt. Sie dienen der Authentifizierung von Kommunikationspartnern und der Verschlüsselung von Daten für den Transport. Sie bieten eine beite Sicherbeit und eine einfache Nutzung
Beirat IKM	Der Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (DFN-Verein) stellt als einen seiner Dienste eine Public-Kev-Infrastruktur (DFN-PKI) bereit
Über uns	Die Universität Rostock hat ihren Zertifizierungsdienst bei der DFN-PKI eingebunden. Dort wird für die Universität Rostock eine ausgelagerte Zertifizierungsstelle (UNIRO-CA) betrieben. Im IT- und Universität Rostock eine ausgelagerte Zertifizierungsstelle (UNIRO-CA) betrieben. Im IT- und



3.1 Webformular

- Startseite der PKI der Uni Rostock
- Im Menü "Nutzerzertifikat" auswählen





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!



3.1 Webformular

Bitte geben Sie Ihre Daten ein. Felder mit einem Stern (*) müssen ausgefüllt werden. Zertifikatdaten E-Mail-Adressen mit folgenden Domainnamen können ohne weitere Bestätigung verwendet werden. E-Mail-Adressen mit anderen Domainnamen müssen separat bestätigt werden:>> E-Mail * vname.nname@uni-rostock.de Muss auf uni-rostock.de enden Name * Vorname Nachname Geben Sie hier Ihren Vor- und Nachnamen ein. Für Gruppenzertifikate stellen Sie das Kürzel "GRP:" voran. Verwenden Sie keine Umlaute. Fakultät/Zentrale Einrichtung 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. 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 widerrufen. Weiter

29.10.2015 © 2009 UNIVERSITÄT ROSTOCK | IT- und Medienzentrum



3.1 Webformular

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

tung Ja
ern Bestätigen



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



29.10.2015 © 2009 UNIVERSITÄT ROSTOCK | IT- und Medienzentrum



3.1 Webformular

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

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.

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

Zertifikatantrag anzeigen



3.1 Webformular

Möchten Sie "Zertifikatantrag.pdf" von "pki.pca.dfn.de" öffnen oder speichern?	
--	--

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.

Öffnen

Speichern

Abbrechen

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!



3.2 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!



4.1 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 <u>denselben</u> Browser benutzen, mit dem auch der Antrag erstellt wurde (nur dieser hat Zugriff auf den privaten Schlüssel)!



4.1 Antwortmail mit signiertem Zertifikat

Sehr geehrte Nutzerin, sehr geehrter Nutzer,

die Bearbeitung Ihres Zertifizierungsantrags ist nun abgeschlossen.

Ihr Zertifikat mit der Seriennummer der Kerten ist auf den Namen CN= 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=

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

&type=CERTIFICATE

Mit freundlichen Grüßen

Ihr PKI-Team der Universitaet Rostock

29.10.2015 © 2009 UNIVERSITÄT ROSTOCK | IT- und Medienzentrum



4.2 Import des Zertifikats im Browser

- Auf der sich öffnenden Webseite bitte "Zertifikat importieren" klicken

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



4.2 Import des Zertifikats im Browser

- Sollte folgende Warnung angezeigt werden, bitte mit "Ja" bestätigen





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





- 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





- 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)



Vertrauenswürdige Herausgeber Datenschutzoptionen Verschlüsselte E-Mail-Nachrichten E-Mail-Sicherheit Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln Anlagenbehandlung Signierte Nachrichten digitale Signatur hinzufügen Automatischer Download SyMIME-Bestätigung anfordern, wenn mit S/MIME signiert Standardeinstellungen Digitale IDs (Zertifikate) Digitale IDs (Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden kann. In GAL veröffentlichen Importieren/Exportieren Als Nur-Text lesen		Trust Center ? ×
Standardnachrichten im Nur-Text-Format lesen Digital signierte Nachrichten im Nur-Text-Format lesen	Vertrauenswürdige Herausgeber Datenschutzoptionen E-Mail-Sicherheit Anlagenbehandlung Automatischer Download Makroeinstellungen Programmgesteuerter Zugriff	Verschlüsselte E-Mail-Nachrichten Inhalt und Anlagen für ausgehende Nachrichten verschlüsseln Ausgehenden Nachrichten digitale Signatur hinzufügen Signierte Nachrichten als Klartext senden S/MIME-Bestätigung anfordern, wenn mit S/MIME signiert Standardeinstellung: Meine S/MIME-Einstellungen Oigitale IDs (Zertifikate) Digitale IDs bzw. Zertifikate sind Dokumente, mit denen die Identität in elektronischen Transaktionen nachgewiesen werden kann. In GAL veröffentlichen Importieren/Exportieren Digitale ID anfordern Als Nur-Text lesen Standardnachrichten im Nur-Text-Format lesen Digital signierte Nachrichten im Nur-Text-Format lesen
Skript in Ordnern Skript in freigegebenen Ordnern zulassen Skript in Öffentlichen Ordnern zulassen		Skript in Ordnern Skript in freigegebenen Ordnern zulassen Skript in Öffentlichen Ordnern zulassen



Meine S/MIME-Einstellungen		@uni-rostock.de)	
Kryptografieformat:	S/MIME		
Standardsicherheitseinstellu	ng fūr alle krypto	grafischen Nachrid	:hten
-	-1.1.	4 . <u> </u>	
Zertifikate und Algorithmen			
Zertifikate und Algorithmen — Signaturzertifikat:	Universitaet Rost	tock ID von	Auswählen
Zertifikate und Algorithmen — Signaturzertifikat: Hashalgorithmus:	Universitaet Rost	tock ID von	Auswählen
Zertifikate und Algorithmen — Signaturzertifikat: Hashalgorithmus: Verschlüsselungszertifikat:	Universitaet Rost SHA1 Universitaet Rost	tock ID von V tock ID von	Auswählen



- 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?

29.10.2015 © 2009 UNIVERSITÄT ROSTOCK | IT- und Medienzentrum