A. Digitales Signieren von E-Mails

Sie können Ihr Kommunikationsprogramm entsprechend einstellen, so dass Sie in Zukunft signierte, und/oder auch verschlüsselte Nachrichten verschicken können.

A.1 mit Microsoft Outlook

Nach dem Zertifikatsimport unterstützt Microsoft Outlook sowohl das Unterzeichnen als auch das Verschlüsseln einer E-Mails mittels digitalem Zertifikat.
Die notwendigen Einstellungen dazu nehmen Sie über das Menü

- Datei -› Optionen -› Trust-Center -› Einstellungen für das Trust-Center -› E-Mail-Sicherheit

vor.

A.2 mit OWA (webmail.hs-karlsruhe.de)

Für den Versand über OWA ist das S/MIME-Steuerelement nötig (nur für den Internet Explorer verfügbar).

Sprechen Sie ggf. Ihre IT-Administration an.

A.3 mit Apple Mail

Nach dem Zertifikatsimport unter MacOS bietet Ihnen Apple Mail ohne weitere Konfiguration das Signieren von Nachrichten an. Unter IOS muß dies eingestellt werden mittels

- Einstellungen -› Accounts -› ... -› Erweiterte Einstellungen -› S/MIME -› Signieren -› Zertifikat aktivieren.

A.4 auf Smartphone unter Android

Auf der Seite der TU Dresden finden Sie eine gute Beschreibung wie unter Android mit der Anwendung CipherMail 2.1.8 signierte E-Mails verschickt werden können.

https://tu-dresden.de/zih/dienste/service-katalog/zusammenarbeiten-und-forschen/groupware/exchange/Anleitungen#section-6

Wofür kann ich Zertifikate verwenden?

Es existieren bereits viele Anwendungen, in denen Zertifikate sinnvoll integriert werden können, um die Sicherheit bezüglich der Authentizität und der Vertraulichkeit von Daten zu erhöhen, zum Beispiel:

- **Signieren von E-Mails und/oder Dokumenten,**
- **Verschlüsseln von E-Mails und/oder Dokumenten,**
- **Authentisierung von Nutzern,**
- **Identifikation von Webservern.**

Warum soll ich Zertifikate verwenden?

Wenn man eine E-Mail signiert, wird dadurch sicher gestellt, dass der Inhalt nicht verändert (Signatur ist gleichzeitig auch eine Prüfsumme) wurde und die E-Mail von der besagten Person kommt (Überprüfung anhand der Zertifikatskette, ob der Absender dem Zertifikatsinhaber entspricht).
Um zusätzlich sicherzustellen, dass niemand anderes die E-Mail auch lesen kann, wird die optionale Verschlüsselung eingesetzt.

Warum DFN-Zertifikate?

Die Hochschule arbeitet wie die meisten deutschen Forschungseinrichtungen mit dem DFN-Verein (Deutsches Forschungsnetz e.V.) zusammen, der für Mitglieder einen TÜV-IT-gesicherten Weg zur Bereitstellung von Zertifikaten anbietet. Der DFN stellt Ihnen die für die elektronische Signatur notwendigen Zertifikate aus und wir, die IZ-Benutzerberatung, authentifizieren dafür Ihre Identität (daher auch die Überprüfung des Personalausweises oder Reisepasses) gemäß den deutschlandweiten Richtlinien.

Was enthält ein Zertifikat?

Das Zertifikat setzt sich aus einem Schlüsselpaar, bestehend aus einem geheimen (privaten) und einem öffentlichen Schlüssel, zusammen, das mit einem Verwendungszweck verknüpft ist. Den geheimen (privaten) Schlüssel haben nur Sie als authentifizierte Person. Der öffentliche Schlüssel wird von anderen Personen benötigt um Ihnen eine verschlüsselte E-Mail zu schicken. Dieser wird in der Regel bei der Beantragung veröffentlicht.

IZ2019002

Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Näher dran.

IZ Informations-zentrum

E-Mail-Zertifikate

Public Key Infra-structure (PKI)

IZ-Benutzerberatung

Montag - Freitag
08h bis 14h (Vorlesungszeit)
10h bis 13h (Vorlesungsfreie Zeit)

Gebäude LI, 1. OG, Raum 133
Telefon: (0721) 925-2305
Fax: (0721) 925-2301

E-Mail: iz-helpdesk@hs-karlsruhe.de
Web: www.hs-karlsruhe.de/iz
Twitter: @hska_iz

02/2019

Wie kann ich ein Zertifikat erhalten?

Um ein Zertifikat zu erhalten, muss bei einer Zertifizierungsstelle ein Zertifikatantrag gestellt werden. Zur Erzeugung dieses Antrags wird in der Regel das Schlüsselpaar bei dem Antragsteller selbst generiert.
Dabei bleibt der **private Schlüssel bei dem Antragsteller,** der auch für dessen Speicherung und Verwaltung verantwortlich ist.

Manuelle Zertifikatsbeantragung

Für die Hochschule Karlsruhe steht die DFN-PKI unter folgender Webadresse bereit:

https://pki.pca.dfn.de/ hs-karlsruhe-ca-g2/pub

Automatisierte Zertifikatsbeantragung

1. Antragsgenerierung

Unter

https://idp.hs-karlsruhe.de/dfnaai

finden Sie eine Webseite der Hochschule, die Sie bei der DFN-Zertifikatserstellung unterstützt.

Zu dem dort von Ihnen angegebenen IZ-Benutzernamen werden alle aktuell zugewiesenen eMail-Adressen in einem Zertifikatsantrag zusammengefasst. Zusätzlich zu diesem Zertifikatsantrag wird ein privater Zertifikatsschlüssel erzeugt, welcher mit dem von Ihnen angegebenen Dateipassword abgesichert ist.

- ***Passwort zum Schutz der Datei bei der Zertifikatsgenerierung wählen.***

Dieses Passwort benötigen Sie wieder unter Schritt 4.

Nach Klick auf „Weiter mit Antragsgenerierung“ erhalten Sie eine E-Mail mit einer Anleitung für das weitere Vorgehen. Zur Sicherstellung der Vertrauenswürdigkeit dieser Benachrichtigung ist die Nachricht mit dem Absenderzertifikat ***iz-support@hs-karlsruhe.de*** signiert. Dies wird Ihnen in Ihrem eMail-Programm in der Regel durch ein rotes Schloßsymbol angezeigt.

Mit dieser E-Mail erhalten Sie zwei Dokumente im Anhang:

1. die Antragsdatei ***„certreq-‹username›-yyyymmttHHMMSS.pem“*** mit allen Ihnen zugeordneten eMail-Adressen, bspw. mamioo03@hs-karlsruhe.de, Micky.Maus@hs-karlsruhe.de, und micky.maus@hs-karlsruhe.de),
2. die geheime passwortgesicherte Schlüsseldatei ***„user-‹username›-yyyymmttHHMMSS.pem“*** mit Ihrem geheimen und dem öffentlichen Schlüsselpaar.

Speichern Sie bitte diese beiden Datei zur späteren Verwendung - und merken Sie sich Ihr Dateipasswort.

2. Zertifikat im DFN-Portal beantragen

Unter --- SCHRITT ZWEI --- in der E-Mail finden Sie einen personalisierten Link (sodass gewisse Teile der dort zu findenden Webmaske vorausgefüllt sind), der Sie direkt zum Antrag für ein Nutzerzertifikat im DFN-Portal führt.

Über den Knopf „Durchsuchen“ können Sie die Antragsdatei (***„certreq-‹username›-... .pem“***) hochladen und müssen anschließend nur noch eine PIN für Ihr Zertifikat, welche bei Bedarf zur Sperrung des Zertifikats verwendet wird, vergeben.
(Bitte PIN langfristig gut merken!).

3. Identitätsprüfung und Antragsbearbeitung

Drucken Sie bitte den daraufhin erscheinenden Zertifikatsantrag aus, und bringen ihn zusammen mit Ihrem Lichtbildausweis zur weiteren Bearbeitung in der IZ-Benutzerberatung vorbei. Dort wird Ihre Identität im Auftrag des DFN (Deutschen Forschungsnetz e.V.) verifiziert.
Nach Genehmigung Ihres Antrags erhalten Sie Ihr Nutzerzertifikat über eine mit dem Absenderzertifikat

dfnpki-mailsender-noreply@dfn-cert.de

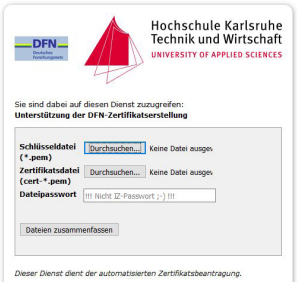
signierte Nachricht.

4. Portables Zertifikatspaar erzeugen

Um dieses Zertifikat auf Ihren unterschiedlichen Geräten zu importieren, muss es in ein allgemeines Container-Format (Dateiendung .p12) umgewandelt werden. Dafür steht Ihnen unter

https://idp.hs-karlsruhe.de/dfnaai/ dfnaai-combine

eine weitere Webseite zur Verfügung. Geben Sie dort bitte folgendes Informationen an:



- die passwortgesicherte Schlüsseldatei ***„user-‹username›-yyyymmttHHMMSS.pem“,***
- die vom DFN-Verein erhaltene Zertifikatsdatei ***„cert-‹serialNo›.pem“,***
- Ihr Dateipasswort aus **Schritt 1.**

Unmittelbar darauf erhalten Sie eine „.p12“ Datei zum Download, welche Ihr Zertifikat mit Schlüssel, geschützt durch Ihr Dateipasswort, enthält. Diese Zertifikatscontainerdatei sollten Sie dauerhaft (bspw. auf einem USB-Stick) aufbewahren. Mit dieser Datei können Sie Ihr Zertifikat auf beliebigen Geräten importieren.

5. Persönliches Zertifikat importieren

Transferieren Sie die Container-Format (PKCS#12-Datei, Dateiendung .p12) auf das gewünschte Endgerät (bspw. per USB-Stick, Dateiablage oder per eMail). Öffnen Sie die Zertifikatscontainerdatei. Dabei werden Sie nach dem Dateipasswort, welches Sie sich gut gemerkt haben, gefragt. Nun steht Ihnen Ihr persönliches Zertikat in vielen Anwendungen zur Verfügung.