Zertifikate

Zertifikate

Digitale Zertifikate

Allgemeines

Verschiedene Server und Personen der Hochschule nutzen digitale Zertifikate, um einen sicheren Datenaustausch mit den Clients zu gewährleisten. Realisiert wird dies mit Hilfe eines digitalen Schlüsselpaars, einem öffentlichen und einem privaten Schlüssel sowie einer eindeutigen ID, dem Zertifikat.

Serverzertifikat

Ein Serverzertifikat ist auf dem Server installiert. Es enthält den Hostnamen (FQDN - full qualified domain name) des Servers und bestätigt die Identität des Servers (z. B. Webserver) gegenüber dem Client (z. B. Webbrowser).

Mit Hilfe eines Serverzertifikats können **verschlüsselte Verbindungen von einem Server zu den Clients** hergestellt werden. Bei einem Webserver werden verschlüsselte Verbindungen über HTTPS bereit gestellt.

Wenn der Browser eine TLS gesicherte Verbindung mit einem Webserver hergestellt hat, beginnt die Adresse (URL) mit „https://“

Wenn Sie ein Serverzertifikat online beantragen, benötigen Sie eine CSR-Datei. Eine genaue Anleitungen mit allen Einzelheiten finden Sie im -> Tab "Anleitung"

Nutzerzertifikat

Das Nutzerzertifikat wird für Personen oder Gruppen ausgestellt. Es enthält den Vor- und Nachname sowie die E-Mail-Adresse der Person, bzw. der Gruppe.

Mit einem Nutzerzertifikat können E-Mails digital signiert und/oder verschlüsselt werden. Die digitale Signatur dient der **Unverfälschbarkeit und Authentisierung** einer E-Mail. Die Verschlüsselung stellt die **Vertraulichkeit** einer E-Mail sicher.

Details zur Vorgehensweise beim Beantragen eines Nutzerzertifikat erhalten Sie -> Tab "Anleitung"

Zertifizierungsstelle der Hochschule

Die Hochschule Offenburg ist Teil der Public-Key-Infrastruktur (PKI) des DFN und hat Ihre Zertifizierungsstelle an die DFN ausgelagert. In diesem Rahmen betreibt die Hochschule eine Registrierungsstelle.

Registrierungstelle der Hochschule

Über die Registrierungsstelle können digitale Zertifikate gemäß dem X.509-Standard beantragt werden. Das beinhaltet Serverzertifikate für Dienstanbieter und Nutzerzertifikate für Endanwender. Die Registierungsstelle ist für das Bearbeiten von Zertifikat- und Sperranträgen verantwortlich.

Zertifikate beantragen

....hier geht es gleich zur Webanwendung, um Zertifikate online zu beantragen

Seiteninhalt

Serverzertifikat beantragen

Zur Hilfestellung haben wir alle notwendigen Informationen in einer **ausführlichen Anleitung** sowie den internen **Workflow** zusammengestellt.

Kurzanleitung

1. Um Online ein Serverzertifikat zu beantragen benötigen Sie

- *CSR-Datei* (Certificate Signing Request - CSR). Diese müssen Sie zurvor erzeugen (siehe ausführliche Anleitung).
- *E-Mail-Adresse* des Administrators
- Eine von Ihnen gewählte PIN, um im Falle eines Falles einen Sperrantrag für das Zertifikat zu beantragen.

2. Verwenden Sie unsere **Webschnittstelle**

- Laden Sie die CRS.pem hoch
- Geben Sie die benötigten Daten ein

3. Drucken Sie anschließend den Zertifikatantrag aus und vereinbaren Sie einen Termin in der Registrierungsstelle,

- Vor der Genehmigung Ihres Zertifikats wird der Zertifikatantrag durch die Registrierungsstelle überprüft. Bringen Sie daher den ausgefüllten und unterschriebenen Zertifikatantrag mit.

Beachten Sie die allgemeinen FAQs der DFN PKI und lesen Sie die **Informationen für Zertifikatinhaber**

Nutzerzertifikat beantragen

Detaillierte Anleitung wie Sie einen Antrag stellen, sowie zur Verwendung des Nutzerzertifikat im E-Mail-Programm (anhand vom GroupWise Client).

Zusätzlich haben wir ein **Kurzanleitung** sowie den **Vorgang als Übersicht** bereit gestellt

Kurzanleitung

1. Verwenden Sie unsere **Webschnittstelle**

Benutzen Sie für diesen wichtigen Schritt **KEINEN ÖFFENTLICHEN COMPUTER**, sondern stets Ihren persönlichen Computer sowie Ihren persönlichen Account auf Ihrem Arbeitsrechner.

- Für das Beantragen eines Nutzerzertifikates benötigen Sie

- *Vorname* und *Name*
- *E-Mail-Adresse* an der Hochschule Offenburg
- Eine von Ihnen gewählte PIN. Die PIN benötigen Sie, falls Sie Ihr Zertifikat sperren lassen möchten.

- Zum Abschließen des Online-Antrag lesen Sie die **Informationen für Zertifikatinhaber** und stimmen Sie der *Zertifizierungsrichtlinie* sowie der *Veröffentlichung des Zertifikats* zu.

2. Drucken Sie anschließend den Zertifikatsantrag aus und lassen Sie Ihr Zertifikat in unserer Registrierungsstelle, persönlich registrieren. Dafür benötigen Sie neben dem ausgefüllten und unterschriebenen Zertifikatsantrag einen amtlich gültigen Lichtbildausweis.

Bitte beachten Sie auch die allgemeinen FAQs der DFN PKI.

Gruppenzertifikat beantragen

Gruppenzertifikate werden nur für Funktions E-Mail-Adressen ausgestellt. Die Vorgehensweise ist fast analog wie beim Beantragen eines Nutzerzertifikat. Die schrittweise detaillierte Vorgehensweise wird in der **genauen Anleitung** beschrieben.

Zum Verständnis stellen wir den Vorgang in einer **Übersicht als Workflow** bereit.

Kurzanleitung

Gehen Sie zunächst so vor als würden Sie ein Nutzerzertifikat beantragen.

Bei der E-Mail-Adresse muss es sich um eine gültige Adresse, aus dem Bereich hs-offenburg.de handeln.

Geben Sie beim Ausfüllen im Web-Formulars bei Name die vier Zeichen „GRP:“ und dahinter so exakt wie möglich die Funktion (das Amt, die Gruppe, ...) an. Das gilt auch, wenn immer nur eine Person die Funktion ausübt. Dabei muss es sich um eine Funktion aus dem Bereich der Hochschule handeln. Auch hier müssen Umlaute als ae/oe/ue/ss geschrieben werden.

Beispiel:

- E-Mail: chancengleichheit@hs-offenburg.de
- Name: GRP: Beauftragte für Chancengleichheit

Registrierungsstelle, RA

Ihre Ansprechpartner in der RA der Hochschule Offenburg

Rechenzentrum
Renate Becker
Raum B208b
Telefon 0781-205-298
r.becker@hs-offenburg.de

Informationszentrum:
Christian Obermann
Raum D206
Telefon 0781-205-4728
christian.obermann@hs-offenburg.de

Falultät B+W
Steffen Schlager
Raum BC 2.2.16
Telefon 07803 9698 4491
steffen.schlager@hs-offenburg.de

Herunterladen und Suchen von Zertifikaten

Siehe -> Tab "Download/Links"

Erhalt der Zertifikate

Die Zertifikatanträge werden von der RA der Hochschule auf Ihre Richtigkeit überprüft und anschließend signiert. Nach Ende dieses Prozeß erhalten Sie Ihr Zertifikat per E-Mail.

Das digitale Zertifikat kann nun in Ihre Anwendung eingebunden werden.

Konfiguration Serverzertifikate

Meist muss die Chain (CA-Zertifikatskette) in der Serverkonfiguration hinterlegt werden.

Die Chain kann im Tab "Downloads/Links" herunter geladen werden.

Wichtig
CA Zertifikate oder die CA-Zertifikatkette der DFN PKI G2 (zweiten Generation) sind nur gültig für Zertifikate der zweiten Gerneration. Diese werden seit 2017 ausgestellt.

Sie können CA Zertifikate oder CA-Zertifikatketten aus der DFN PKI G1 (ersten Generation) nicht mit Zertifikaten ausgestellt über die DFN PKI G2 kombinieren.

Serverzertifikate in Chain einbinden:
Häufig muss in Ihrer Serverkonfiguration, das Serverzertifikat in der Chain enthalten sein.

Kopieren Sie den Inhalt der ASCII kodierten Serverzertifikats-Datei an den Anfang der Chain-Datei. Speichern Sie die Datei als .pem- Datei bzw. in dem Format, das auf dem Server benötigt wird.

Alle anzeigen / Alle verbergen

⊞ **Wo gibt es weitere Hilfe?**

www.pki.dfn.de/faqpki/

⊞ **Warum kann ich den Online Antrag für ein Nutzerzertifikat nicht abschließen?**

Sie erhalten folgende Meldung beim Abschließen bzw. Drucken Ihres Online Antrag für ein Nutzerzertifikat:

Ihr Browser hat keinen korrekten öffentlichen Schlüssel geschickt. Haben Sie "Abbrechen" in einem Passwort-Prompt bestätigt? Bitte versuchen Sie es erneut.

Diese Meldung erscheint, wenn Sie einen der folgenden Browser verwenden: Google Chrome oder Win 10 Edge Browser

Lösung:

Downloads und Links der DFN Zertifizierungstelle

Zertifikate beantragen

Nachfolgend finden Sie die aktuellen Links seit 2017. Das sind die Links der zweiten Generation der DFN PKI (public key infrastructure) G2. Neu zu beantragende Zertifikate werden nur noch hier ausgestellt.

- Über Webschnittstelle **Online-Antrag** stellen
- Zur Hilfestellung stehen die **FAQ** zu Zertifikaten in der DFN-PKI zur Verfügung

CA Zertifikate und CA-Zertifikatkette (Chain) der DFN PKI

Fileserver-Zugriff auf die DFN PKI CA-Zertifikate (alle Dateiformate und die Chain sind hinterlegt):

mit OES-Client	I:\Zertifikate\Stammzertifikate DFN
mit CIFS/SMB-Client	\\fs1-2-common\common\Zertifikate\Stammzertifikate DFN
Filr	https://filr.hs-offenburg.de -> Netzwerkordner -> Zertifikate -> Stammzertifikate DFN
Filr-Permalink	Stammzertifikate

> Beachten Sie die Liesmich-Dateien in den Verzeichnissen

Webserver-Zugriff auf die DFN PKI CA-Zertifikate:

	CA Zertifikate	**Chain**
DFN PKI G2 (gültig für alle Zertifikate ausgestellte ab 2017)	CA Zertifikate G2 *(Binärformat zum Import in Anwedungen, z.B. Webbrowser und E-Mail-Programme)*	Chain G2 *(Textformat)*
DFN PKI G1 (gültig für alle Zertifikate ausgestellt vor 2017)	CA Zertifikate G1 *(Binärformat zum Import in Anwedungen, z.B. Webbrowser und E-Mail-Programme)*	Chain G1 *(Textformat)*
Alternativ über DFN Webseite	CA Zertifikate *(alle Formate verfügbar)*	

TIPP: Wenn Sie die Chain über den Webserver herunter laden, kopieren Sie den gesamtem Inhalt der Chain in eine ASCII-Datei.

Downloads und Links für Zertifikate ausgestellt über das RZ CA

Diese Informationen und Downloads erscheinen erst, wenn Sie sich am **Website-Login** angemeldet haben.