# digitale Zertifikate

Digitale Zertifikate dienen meist der Authentizifierung von Dokumenten und der Sicherung von Kommunikationswegen. Seltener werden sie für das Signieren von Programmcode genutzt.
Die TU Dresden ist eine offizielle Zertifizierungsstelle des DFN, d.h. sie kann Zertifikate für die Angelegenheiten in ihrem Kontrollbereich (unter anderem Subdomains und E-Mail-Adressen, die vom ZIH verwaltet werden) ausstellen. Weiterhin gibt es natürlich auch externe Zertifizierungsstellen, diese verlangen meist eine Jahresgebühr für die ausgestellten Zertifikate. Einer der wenigen kostenlosen Zertifizierungsstellen ist CaCert.org.

## Zertifikatsstelle TU Dresden

Die Zertifikatstelle der TU Dresden ist ein Dienst des ZIH. Auf der Webseite des PKI sind die Informationen, die Teilnahmebedingungen sowie die genauen Informationen zum Antragsverfahren hinterlegt. Die Online-Zertifikatsstelle der TU-Dresden beim DFN für das Zertifikatmanagement ist unter https://pki.pca.dfn.de/tu-dresden-ca/cgi-bin/pub/pki erreichbar. Als Zertifizierungsstelle zur Validierung dienen die Zertifizierungsserver des DFN.

### Nutzer-Zertifikat

Das vom PKI TU Dresden ausgestellte Nutzerzertifikat ist für nachfolgende Anwendungsfälle brauchbar.

#### E-Mail

Für E-Mail-Adressen, die direkt vom ZIH verwaltet werden, können beim PKI TU Dresden ein entsprechendes Nutzer-Zertifikat beantragt werden. Mit diesem Zertifikat ist eine Signierung und/oder eine Verschlüsselung von E-Mails möglich.

#### PDF-Dokumente

Nit den Nutzer-Zertifikaten ist die Signierung und das digitale Unterschreiben von PDFs möglich.

### Nutzer-Zertifikat für Code Signierung

Das Standard-Nutzer-Zertifikat kann nicht zur Signierung von Programmcode verwendet werden. Für diesen Anwendungsfall muss folgendermaßen vorgegangen werden:

1. Es ist online ein Nutzerertifikat zu beantragen
2. bei der Identitätsprüfung beim ServiceDesk muss die für Benutzung des Zertifikats zum Code signieren dem Teilnehmerservice-Mitarbeiter mitgeteilt werden, damit er das Zertifikatsprofil

vor der Zertifizierung auf 'CodeSigning' umstellt

### Server-Zertifikat

Für Rechner, die über den Nameserver der TU Dresden erreichbar sind und den Namenskonventionen für Rechner erfüllen, kann für verschiedene Anwendungsfälle ein Server-Zertifikat beantragt werden.

## Zertifikatsstelle Cacert.org

Da der Studentenrat seinen Mail-Server und die dazugehörige Nutzerverwaltung selbst betreibt, weigert sich das PKI, entsprechende Nutzerzertifikate für E-Mail-Adressen der Subdomain stura.tu-dresden.de auszustellen. Eine Alternative ist ein Zertifikat einer externen Zertifizierungsstelle wie beispielsweise cacert.org. Nach der kostenlosen Registrierung kannst du dir für deine StuRa-E-Mail-Adresse ein Zertifikat beantragen, welches für ein halbes Jahr ab Ausstellungsdatum gültig ist.

From:
https://wiki.stura.tu-dresden.de/ - **StuRa-Wiki**

Permanent link:
**https://wiki.stura.tu-dresden.de/doku.php?id=allgemein:digitale_zertifikate&rev=1421058172**

Last update: **2021/01/30 12:55**