

# Erstellung eines DFN-Serverzertifikats

Für die Erstellung eines DFN-Serverzertifikats gibt es zwei Wege:

---

## Weg 1: Eigenen privaten Schlüssel erstellen (empfohlen)

Wenn Sie Ihren privaten Schlüssel selbst erstellen möchten, gehen Sie wie folgt vor:

**Schritt 1:** Erstellen Sie zunächst lokal einen privaten Schlüssel, einen öffentlichen Schlüssel und eine CSR-Datei (Certificate Signing Request). Eine detaillierte Anleitung finden Sie [hier](#).

**Schritt 2:** Laden Sie anschließend die CSR-Datei über die [DFN-Webseite](#) hoch. Wählen Sie dazu die Option „**Eigene CSR-Datei (PKCS#10) einreichen**“.

**Schritt 3:** Geben Sie Ihre Daten an und legen Sie einen Sperr-PIN fest. Achten Sie dabei oben das richtige Zertifikatsprofil auszuwählen.

**Schritt 4:** Weiter mit Schritt 5.

---

## Weg 2: Schlüsselerstellung durch den DFN

Wenn Sie dem DFN vertrauen, können Sie die Erstellung des privaten und öffentlichen Schlüssels Ihren Browser überlassen. Die Schlüssel verlassen dabei Ihren Rechner nicht.

**Schritt 1:** Wählen Sie auf der [DFN-Webseite](#) die Option „**Serverzertifikat (inkl. Schlüsselerzeugung)**“.

**Schritt 2:** Wählen Sie das richtige Zertifikatsprofil und verwenden Sie als Schlüsseltyp „**EC P-384**“. Wenn der Server damit Probleme haben sollte, können auch noch das alte „**RSA 4096**“ Format verwenden.

**Schritt 3:** Geben Sie Ihre Daten an und legen Sie einen Sperr-PIN fest.

**Schritt 4:** Auf der nächsten Seite prüfen Sie Ihre Daten und speichern Sie die Antragsdatei (.json). Merken Sie sich das Passwort gut, Sie benötigen beides später, wenn Sie Ihr Zertifikat abholen wollen.

---

**Schritt 5:** Speichern und senden Sie die Antragsquittung (**die PDF-Datei**) als **signierte E-Mail** an: [ca-btu@b-tu.de](mailto:ca-btu@b-tu.de) (Eine signierte E-Mail ist ausreichend, eine handschriftliche Unterschrift ist nicht notwendig)

**Schritt 6:** Der Antrag wird geprüft und genehmigt. Das kann unter Umständen bis zum nächsten Werktag dauern, da dies aktuell noch manuell durchgeführt wird.

**Schritt 7:** Sie bekommen eine E-Mail vom DFN (Betreff: DFN-Verein Community CA Zertifikatsinformation). Darin enthalten ist ihr Zertifikat.

**Schritt 8 – Weg 1:** Wenn Sie das Zertifikat über Weg 1 beantragt haben, können sie über den zweiten Link in der E-Mail, noch die CA-Zertifikate herunterladen.

**Schritt 8 - Weg 2:** Wenn Sie das Zertifikat über Weg 2 beantragt haben, klicken Sie auf den erst Link. Daraufhin öffnet sich eine Webseite auf der Sie die in Schritt 2 erstellen Zertifikate runterladen können. Über den zweiten Link können sie noch die Ca-Zertifikate herunterladen.