



## Anleitung Serverzertifikat beantragen DFN-PKI

[Link zur Antragsseite](#)

Ergänzen Sie die geforderten Angaben und wählen Ihren Request (CSR) aus.

### Eigene CSR-Datei (PKCS#10) einreichen

Hier können Sie ein neues Zertifikat beantragen.

Zertifikatsprofil **Web Server** ▾

Mit dem Zertifikatsprofil legen Sie den Einsatzzweck des Zertifikats fest. ([Beschreibung der Zertifikatsprofile](#))

Die folgenden Domainnamen können Sie in E-Mail-Adressen nutzen: ▾

Die folgenden Domainnamen können Sie im CN-Attribut und in SubjectAlternativeNames (SaN) des Typs 'DNS' nutzen: ▾

Um einen CSR (PKCS10) einreichen zu können, müssen Sie diesen vorher erstellt haben, z.B. mit openssl.

CSR (PKCS#10) Datei (e.g. .pem)

Browse

Ihr vorhandener CSR (PKCS#10) im PEM-Format. Gebräuchliche Dateierendungen sind .pem und .csr.

### Ihre Daten

Diese Daten werden nicht in Ihr Zertifikat aufgenommen.

Vollständiger Name \*

Geben Sie hier Ihren vollständigen Vor- und Nachnamen an

E-Mail \*

Ihre E-Mail-Adresse

Abteilung

Abteilungsname Ihrer Abteilung

Sperr-PIN \*

Sperr-PIN - Mindestens 8 beliebige Zeichen



Sperr-PIN - Bestätigung \*

Nochmalige Eingabe der Sperr-PIN zur Bestätigung



Diese PIN wird von Ihnen benötigt, wenn Sie Ihr Zertifikat sperren wollen. Bitte notieren Sie sich die PIN.

### Persönliche Notiz

Hier können Sie eine persönliche Notiz zu diesem Zertifikatantrag eingeben. Diese Notiz wird ausschließlich lokal mit der Antragsdatei abgespeichert.

Geben Sie die geforderten Informationen in die Felder des Formulars ein und wählen das entsprechende Zertifikatsprofil aus. Klicken Sie auf "Weiter".

Auf der nächsten Seite sehen Sie eine Zusammenfassung Ihrer Angaben, wenn Sie Änderungen daran vornehmen wollen, benutzen Sie bitte den Zurückbutton Ihres Browsers.

Nutzerzertifikat	Serverzertifikat	Zertifikat sperren	Zertifikat suchen
<b>Serverzertifikat beantragen - Bestätigung</b>			
Die folgenden Daten wurden eingetragen:			
<p>PKCS#10-Zertifikatantrag -----BEGIN CERTIFICATE REQUEST-----  MIIEEDCCAvqCAQAvgawxCzAJBgNVBAYTAkRFMSgwJgYDVQQKEw9IdW11b2xkdC1V  bm12ZXJzaXRhZXQgenUgQmVybGluNScwJQYDVQQLEx5aRSBDb21wdXRlc1OgdW5k  IE11ZG1lbnN1cnZpY2UxIjAgBgNVBANTG1haWxob3N0LmNtcy5odS11ZXJsaW4u  ZGUxJjAkBgkqhkiG9w0BCQEFWF3Bvc3RtYXNOZXJaaHUtYmVybGluLmR1MIIBIjAN  BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYro6HmgMBRMAL4dz2HEYIzt1a0FE  dtpnVmOxqoDw2vrwp6Gk+POO6LZHo0z+afSDnOerBfUQIHk1CixwfOX+0tbUWh+/  1GR+r7m2DpmEtav1oOQ9K4mUdBD5BKCnKYuz4VzYDHL1VU06+Hg7ID+CGTjHM29Y  3FfJ9jXUEhANaQcYytm5NUC0m86R0d3Y8AvA11EzZ+M3qpch4mR8851e5KtT60W6  X89ug77UPvYiI/cUWdms1r/tg2hMChK/k/+Om65Zy1Omxo1rwbYyOI4CIVJSSXf  9cpkxkZLa1g1NB4GDUQZzuoIkosKGAxPz+Y1EbYNM0naOHVO41jzjzq5MwIDAQAB  oIBHDDCCARgGCSqGS1b3DQEJJDjCAQkwwgEFMIIBAQYDVROBRIHSHIH2gRdwb3NO  bWFzdGVyQGh1LWJlcmxpb15kZyI2bWVpbGhvc3QuY21zLmhlLWJlcmxpb15kZyIY  bWVpbGhvc3QuenouaHUtYmVybGluLmR1ghppcjEtcMVsYXkuY21zLmhlLWJlcmxp  b15kZyEjRQBk4IaaXIyLXJlbGF5LmNtcy5odS11ZXJsaW4uZGWHBIOUAZWCHHNT  dHBob3N0LmFsdW1uaS5odS11ZXJsaW4uZGWHBIOUAZaHBIOUAZeCG21yMS1tYW5h  Z2UuY21zLmhlLWJlcmxpb15kZyIbaXIyLW1hbWFnZSS5bXMuaHUtYmVybGluLmR1  MAOGCSqGS1b3DQEBBQUAA4IBAQBvziKNI7z3fkFH6wJWR+cSDvqUSEVseOXXJumf  HRtu2jnMkdYwUMyXOIYw1hHtSckfW1/gBx65xScZwf22hejX1rHrZxgcJK2yVNA  CxHOR9JZvIvg4EXp101yY+VfQNs1vP15rJRI+WznYm5qKHdrQpXkrz+1CscUhDY  G13IOx3pvGDkah7bREZ8PYzE2Q9tpgRuuoDma3ORXEOXbzZeOgMUKLOVLRdKv7K  PSa5my4t31sdkhvCzHtbYk/ANGIOasjC1S1vUFq6UxqfMcE5u0qFIMERefhjr/vt  Aot3+jT57iRjVoaxOPxhpYXXLa5e6Ie6oFuhh0+sfh1VdqH  -----END CERTIFICATE REQUEST-----</p>			
Zertifikatsprofil	Web Server		
Algorithmus des öffentlichen Schlüssels	rsaEncryption		
Schlüssellänge	2048		
Eindeutiger Name	emailAddress=postmaster@hu-berlin.de,CN=mailhost.cms.hu-berlin.de,OU=ZE Computer- und Medienservice,O=Humboldt-Universitaet zu Berlin,C=DE		
Alternativer Name des Zertifikats	DNS:ir1-manage.cms.hu-berlin.de, DNS:ir1-relay.cms.hu-berlin.de, DNS:ir2-manage.cms.hu-berlin.de, DNS:ir2-relay.cms.hu-berlin.de, DNS:mailhost.cms.hu-berlin.de, DNS:mailhost.rz.hu-berlin.de, DNS:smtphost.alumni.hu-berlin.de, email:postmaster@hu-berlin.de, IP:141.20.1.147, IP:141.20.1.149, IP:141.20.1.150, IP:141.20.1.151		
Veröffentlichen	Ja		
Name (Vor- und Nachname)	Vorname Nachname		
E-Mail	admin@webserver.hu-berlin.de		

Zusammenfassung der Daten aus ihrem Request und ihrer Angaben

Klicken Sie auf "Bestätigen". Im nächsten Fenster klicken Sie auf "Zertifikatantrag anzeigen".

Zertifikate	CA-Zertifikate	Gesperrte Zertifikate	Polices	Hilfe	Beenden
Nutzerzertifikat	Serverzertifikat	Zertifikat sperren	Zertifikat suchen		
<b>Zertifikatantrag</b>					
Abschließend müssen Sie Ihren Zertifikatantrag ausdrucken.					
<ul style="list-style-type: none"> <li>• Bitte betätigen Sie die Schaltfläche "Zertifikatantrag anzeigen". Daraufhin wird der Zertifikatantrag geöffnet.</li> <li>• Bitte drucken Sie den Zertifikatantrag aus, unterschreiben ihn und legen ihn bei Ihrer Registrierungsstelle vor, um die Antragsstellung abzuschließen.</li> </ul>					
Nachdem Sie den Zertifikatantrag ausgedruckt haben, können Sie diese Schnittstelle über die Registerkarte "Beenden" verlassen.					
<input type="button" value="Zertifikatantrag anzeigen"/>					

Zertifikatantrag anzeigen

## **Zertifikatantrag**

Um den Request zu bearbeiten, schicken Sie bitte den ergänzten und unterschriebenen Antrag per signierter E-Mail an "pki@hu-berlin.de".

## **Ausstellung des Zertifikates**

Nachdem Ihr Request durch die CA signiert wurde, erhalten Sie eine E-Mail an die von Ihnen im Formular angegebene E-Mailadresse. Darin enthalten ist ein Link zum Download des Zertifikates, sowie das Zertifikat selbst.