

CSR unter macOS

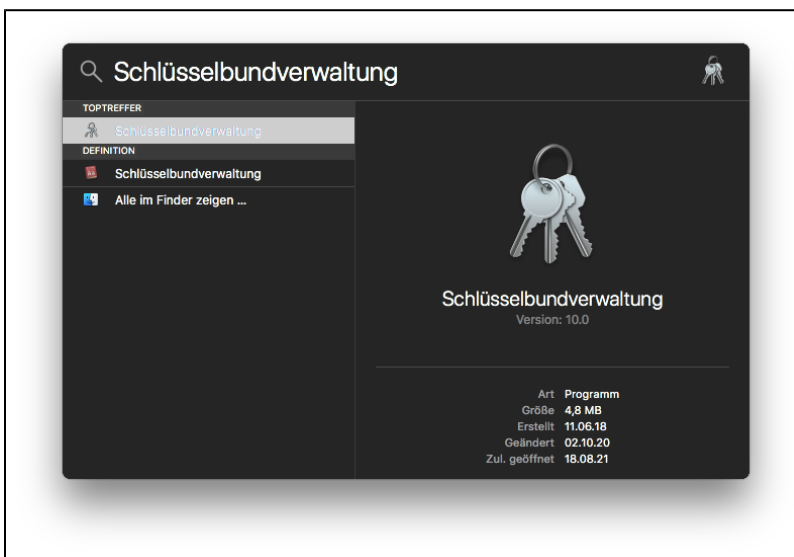
 Diese Seite befindet sich aktuell noch im Aufbau 

Wie Sie einen CSR (Certificate Signing Request, deutsch: Zertifikatsignierungsanforderung) unter macOS erstellen, erfahren Sie in den 8 Schritten der Schritt-für-Schritt-Anleitung.

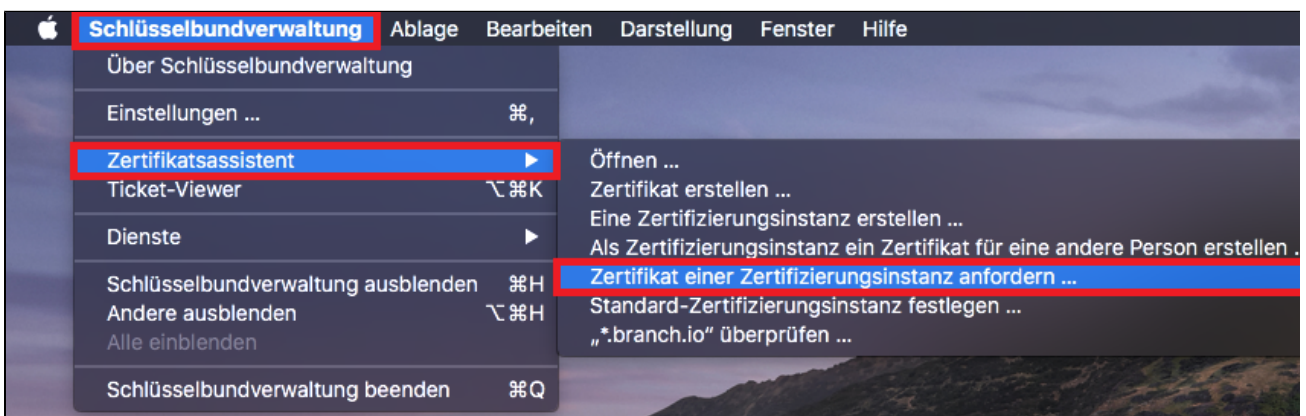
Um ein Nutzerzertifikat von einer CA (Certificate Authority) anzufordern, muss ein **"Certificate Signing Request" (CSR)** erstellt werden. Ein CSR ist ein digitaler Antrag, aus einem öffentlichen Schlüssel ein digitales Zertifikat zu erstellen.

Schritt-für-Schritt-Anleitung

1. Öffnen Sie die App **„Schlüsselbundverwaltung“**. Sie finden die App im Finder unter „Programme/Dienstprogramme/Schlüsselbundverwaltung.app“ oder nutzen Sie die Spotlight-Suche („CMD + Leerzeichen“).



2. Klicken Sie in der Menüleiste neben dem Apfel-Symbol auf **„Schlüsselbundverwaltung“**. Im Dropdown-Menü klicken Sie auf **„Zertifikatsassistent“** und **„Zertifikat einer Zertifizierungsinstanz anfordern ...“**.



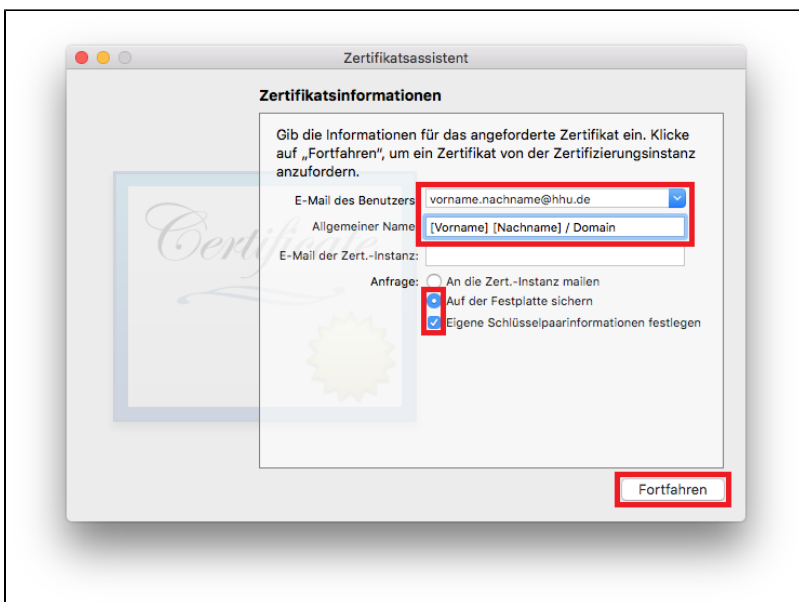
3. Im Zertifikatsassistenten geben Sie zunächst Ihre **„E-Mail-Adresse“** im Format **vorname.nachname@hhu.de** ein. Denken Sie unbedingt daran, die richtige E-Mail-Adresse anzugeben!

Unter „**Allgemeiner Name**“ tragen Sie **Ihren Namen** ein. Wenn Sie ein Zertifikat für eine *.hhu.de-Domain beantragen möchten, tragen Sie stattdessen den **Domainnamen** ein (bspw. testseite.hhu.de).

Das Dritte Feld „E-Mail der Zert.-Instanz“ bleibt leer.

Setzen Sie jeweils einen Haken bei „**Auf der Festplatte sichern**“ und „**Eigene Schlüsselpaarinformationen festlegen**“.

Klicken Sie anschließend auf „**Fortfahren**“.



4. Wählen Sie im angezeigten Dialogfeld einen Dateinamen für Ihren CSR („**Sichern unter**“) und den Speicherort („**Ort**“). Klicken Sie anschließend auf „**Sichern**“.



5. Wählen Sie nun die Schlüsselpaarinformationen „**Schlüssellänge**“ und „**Algorithmus**“ aus den Dropdown-Menüs. Klicken Sie anschließend auf „**Fortfahren**“.

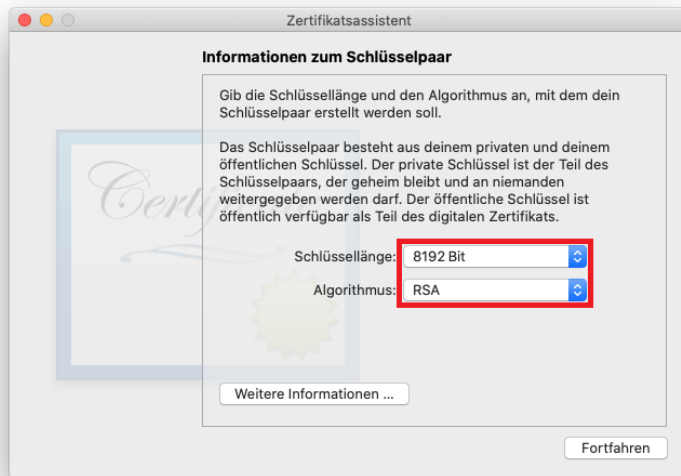


Empfehlung

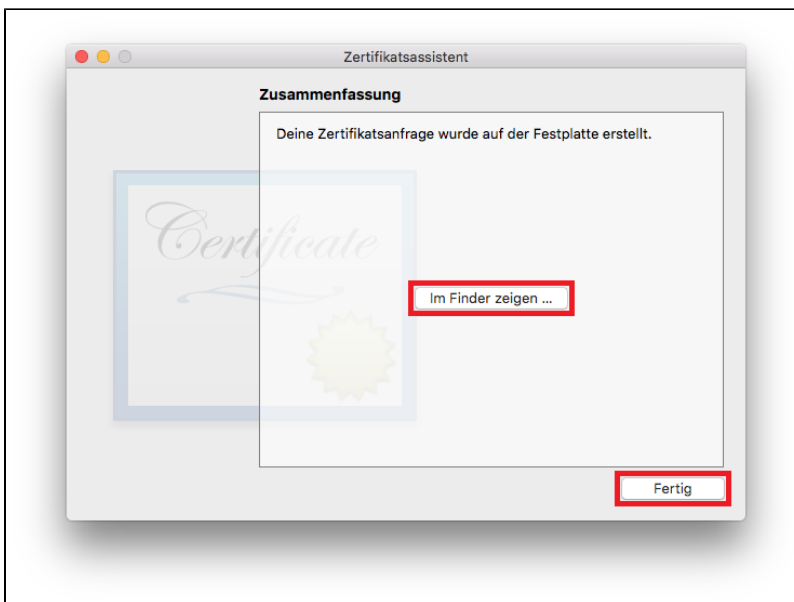
Schlüssellänge: **4096 Bit**

Algorithmus: **RSA**

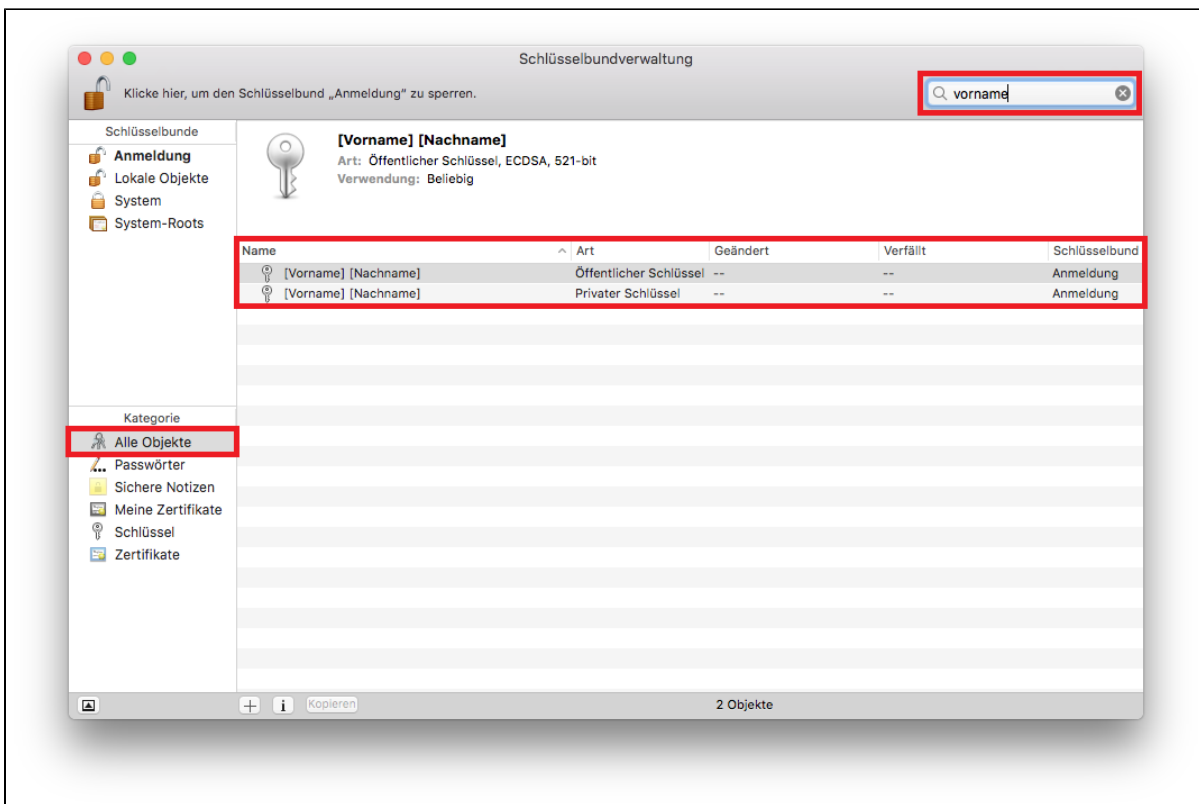
Grund: Nutzerzertifikate mit den ECC-Schlüsseltypen 384 und 265 können nur für Signatur und Authentisierung, aber nicht für Verschlüsselung verwendet werden.



6. Ihr CSR wird an dem von Ihnen angegebenen Speicherort auf der Festplatte gespeichert. Mit Klick auf „**Im Finder zeigen ...**“ öffnen Sie ein Finder-Fenster mit der CSR-Datei. Mit Klick auf „**Fertig**“ beenden Sie den Zertifikatsassistenten.



7. Prüfen Sie die Generierung und Installation des Schlüsselpaars, indem Sie in der Schlüsselbundverwaltung in der linken Spalte auf „**Alle Objekte**“ klicken und anschließend oben Rechts über die Suchfunktion Ihren eigenen Namen oder den Namen der *.hhu.de-Domain suchen (also das, was Sie in Punkt 3 unter „Allgemeiner Name“ eingetragen haben).



Hinweis

Der **private Schlüssel** sollte immer auf eigens verwalteten Systemen erzeugt und gespeichert werden und **niemals Dritten** in die Hände gegeben werden - auch nicht der signierenden CA.

8. Die Zertifikatsdatei ist **fertig** und besteht - wie auch der private Schlüssel - aus einer einfachen Text-Datei mit kryptischem Inhalt. Mit Doppelklick auf die CSR-Datei öffnet sich der Inhalt im Texteditor.

Beispiel:

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBhzCB6gIBADBFMQswcQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEh
MB8GA1UECgwYSW50ZXJuZXQvZ2lkZ2l0cyBqdHkgTHRkMIGbMBAGByqGSM49AgEG
BSuBBAAjA4GGAAQBpbipHOXWzTXy7WP3QGxP5x4yTp5KqV9SQnV5qRkZWqp3fXIe
YnN39/MmUYxUNNG/ly970hHYxAeig1k6sFljaVUALYPVMzMnWbs8GhNioXuA3GnV
5JtiizJ35ABZ51NGOI1fm8h+DInMsr1Gw+Eo21nqSfYV2m5cifMG4tVI/9PZoAWg
ADAKBggqhkJOPQDAG0BiwAwgYcCQU2PbmG6FKQdtgLUzspUZBK0u3ccxBSvCQ1K
UDGkguCG9oQF61xSrUg+6z/qRyyiMVuQ/OkAgOHm5Z471gyRARjBAKIA/VfcpPtR
0WvhsFvTrD8nvgblJGT+kk4jj42gf7n+q710mtrNh9jTAuzz+fC1F+Taq56KX1Ku
2SKz0n20SUJBAuY=
-----END CERTIFICATE REQUEST-----
```

Die erste und letzte Zeile sind Teil der Zertifikatsdatei und dürfen nicht entfernt werden.