## **CSR unter macOS**

(i)	Diese Seite befindet sich aktuell noch im Aufbau	<u> </u>	
-----	--	----------	--

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 ...".

Ś	Schlüsselbundverwaltung	Ablage	Bearbeite	en Darstellung	Fenster	Hilfe
	Über Schlüsselbundverwaltu	ng				the second
	Einstellungen		ж,			
	Zertifikatsassistent		•	Öffnen		
	Ticket-Viewer		́СЖК	Zertifikat erstell	en	
	Dienste		►	Eine Zertifizieru Als Zertifizierun	ngsinstanz gsinstanz (	z erstellen ein Zertifikat für eine andere Person erstellen
(Selficiency)	Schlüsselbundverwaltung au	sblenden	жн	Zertifikat einer 2	Zertifizieru	ngsinstanz anfordern
	Andere ausblenden Alle einblenden		Ҡӝн	Standard-Zertifi "*.branch.io" üb	zierungsin erprüfen	istanz festlegen
	Schlüsselbundverwaltung be	enden	жQ	-	100	All and a start of the start of

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".

Г

Allgemeiner Name E-Mail der ZertInstanz: Anfrage: An die ZertInstanz mailen Auf der Festplatte sichern Eigene Schlüsselpaarinformationen festlegen		Gib die Informationen für das angeforderte Zertifikat ein. Klicke auf "Fortfahren", um ein Zertifikat von der Zertifizierungsinstanz anzufordern.
	Cer	Allgemeiner Name E-Mail der ZertInstanz: Anfrage: An die ZertInstanz mailen Auf der Festplatte sichern Z Eigene Schlüsselpaarinformationen festlegen

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

Sichern unter	CSR	•
Tags:		
Ort:	🔁 Schreibtisch 🗘	
	Abbrechen Sichern	

5. Wählen Sie nun die Schlüsselpaarinformationen "Schlüssellänge" und "Algorithmus" aus den Dropdown-Menüs. Klicken Sie anschließend auf "For tfahren".

(i)	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.	

<b>- -</b>	Lonnatodobioton
	Informationen zum Schlüsselpaar
	Gib die Schlüssellänge und den Algorithmus an, mit dem dein Schlüsselpaar erstellt werden soll.
C	Das Schlüsselpaar besteht aus deinem privaten und deinem öffentlichen Schlüssel. Der private Schlüssel ist der Teil des Schlüsselpaars, der geheim bleibt und an niemanden weitergegeben werden darf. Der öffentliche Schlüssel ist öffentlich verfügbar als Teil des digitalen Zertifikats.
	Schlüssellänge: 8192 Bit
	Algorithmus: RSA
	Weitere Informationen
	Fortfahren

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.

	Zusammenfassung
	Deine Zertifikatsanfrage wurde auf der Festplatte erstellt.
Ce	Im Finder zeigen
	Fertig

		Schlusselbundverwaltung			
Klicke hier, um der	n Schlüsselbund "Anmeldung" zu sperren.				imej 🛛 😒
Schlüsselbunde Anmeldung Lokale Objekte System System-Roots	[Vorname] [Nachname] Art: Öffentlicher Schlüssel, E Verwendung: Beliebig	CDSA, 521-bit			
	Name	∧ Art	Geändert	Verfällt	Schlüsselbund
	[Vorname] [Nachname] [Nachname] [Vorname]	Öffentlicher Schlüssel			Anmeldung
	[Vorname] [Nachname] [ [ ] [ ] [ ] ] [ ] ] ] ] [ ] ] ] ] [ ] [ ] ] [ ] ] [ ] ] [ ] [ ] ] [ ] ] [ ] ] [ ]	Privater Schlüssel			Anmeldung
Alle Objekte					
	+ i Kopieren	_	2 Objekte	_	_

## 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
MB8GA1UECgwYSW50ZXJuZXQgV21kZ210cyBQdHkgTHRkMIGbMBAGByqGSM49AgEG
BSuBBAAjA4GGAAQBpbiPH0XWzTXy7WP3QGxP5x4yTp5KqV9SQnV5qRkWZqp3fXIe
YnN39/MmUYxUNNG/ly970hHYxAeig1k6sFljaVUAlYPVMzMnWbs8GhNioXuA3GnV
5JtiizJ35ABZ51NGOI1fm8h+DInMsrlGw+Eo21nqSfYV2m5cifMG4tvI/9PZoAWg
ADAKBggqhkjOPQQDAgOBiwAwgYcCQU2Pbmg6FKQdtgLUzspUZBKOu3ccxBSvCQlK
UDGkguCG9oQF61xSrUg+6z/qRyyiMVuQ/0kAgOHm5Z471gyRARjBAkIA/VfcpPtR
0WvhsFvTrD8nvgblJGT+kk4jj42gf7n+q710mtrNh9jTAuzz+fC1F+Taq56KX1Ku
2SKzOn2OSUJBAuY=
END CERTIFICATE REQUEST

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