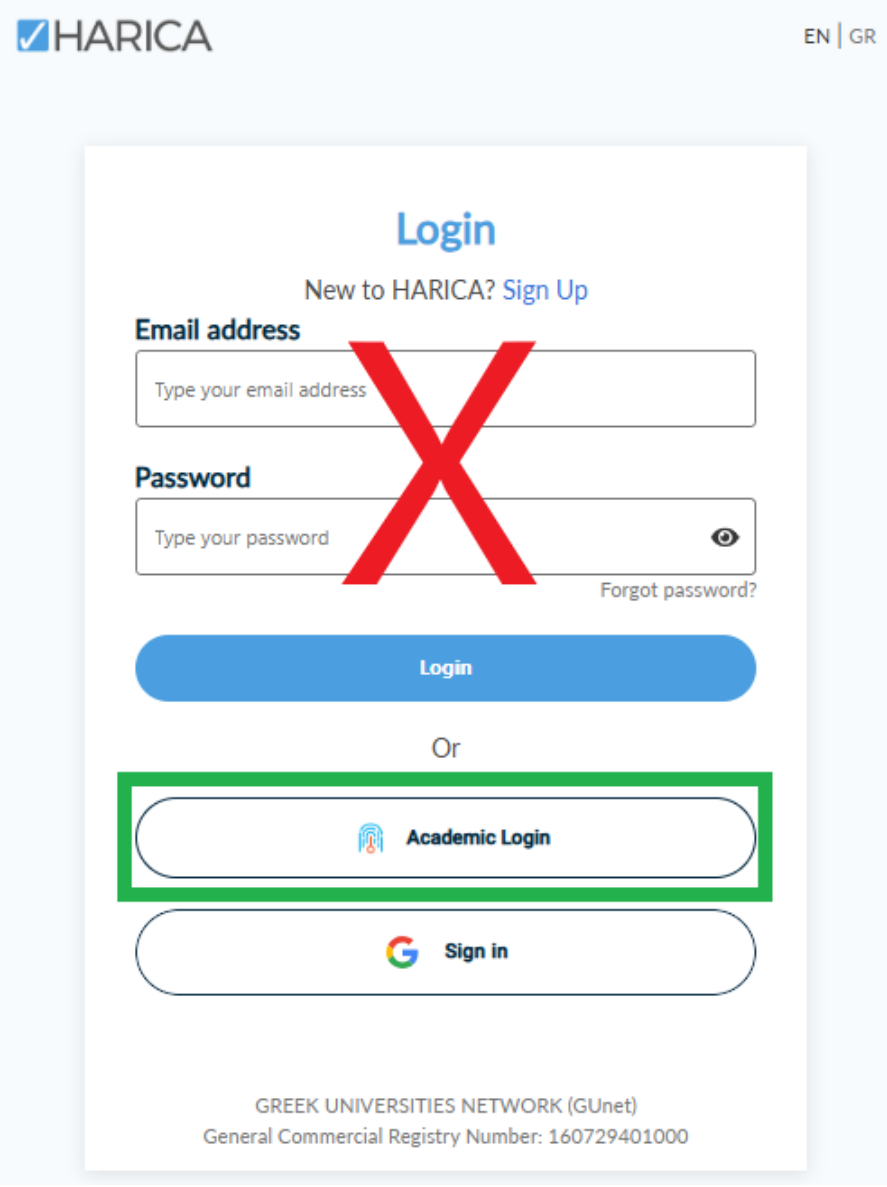
Inhalt

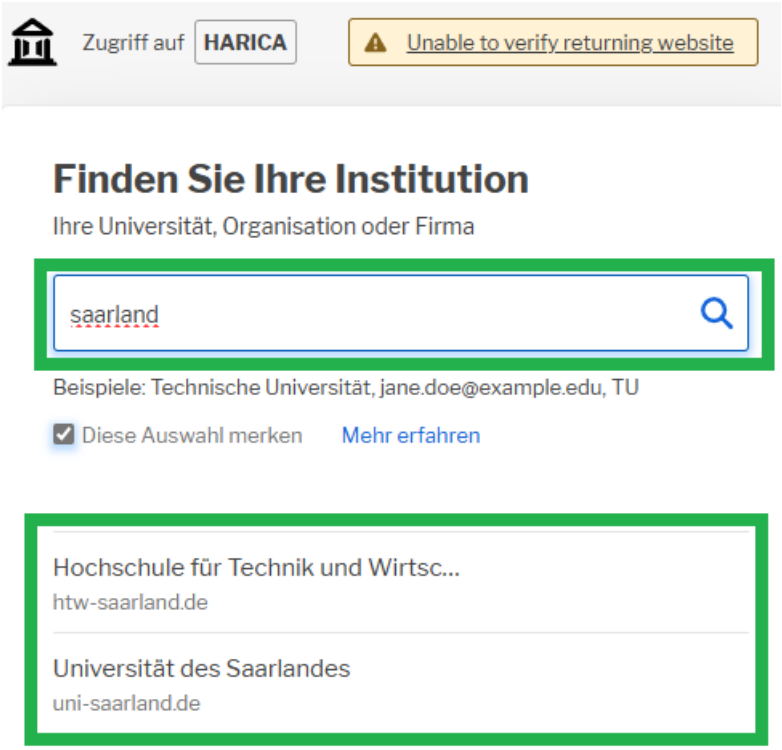
I. Aufrufen des HARICA-Portals zur Zertifikatsbeantragung

1. Rufen Sie folgenden Link auf und klicken Sie dort auf Academic Login

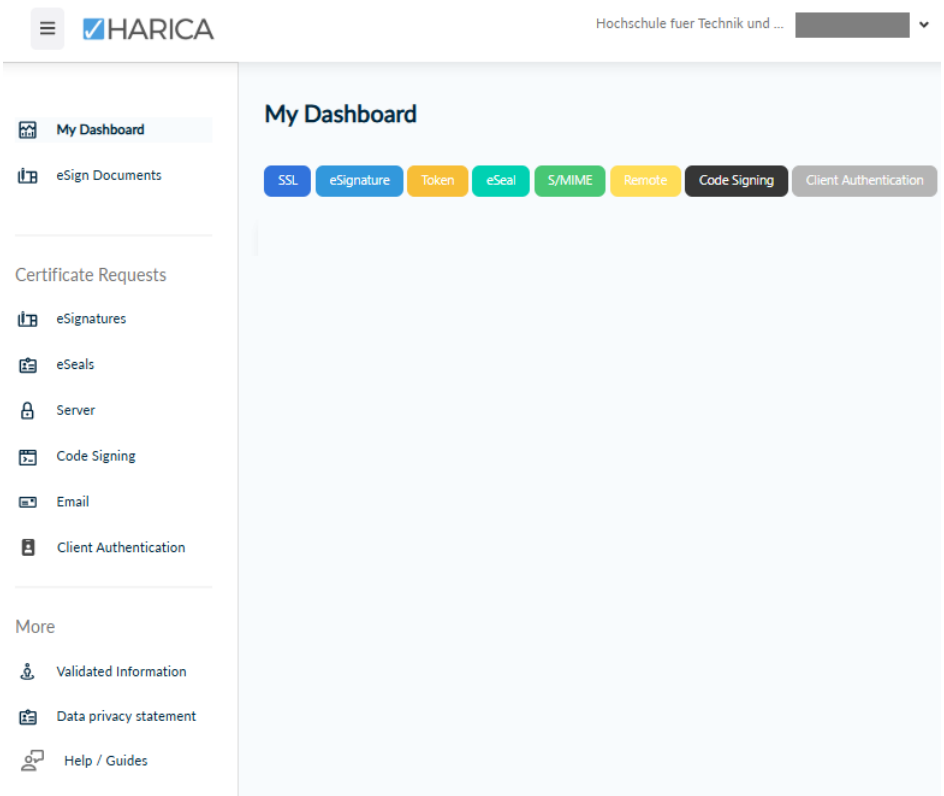
https://cm.harica.gr/



Sie werden dann zu einer Webseite zur Authentifizierung geleitet. Suchen Sie dort nach Ihrer Hochschule (HTW oder UdS) und wählen sie entsprechend aus. Auf der folgenden Seite geben Sie Ihre Benutzerkennung ein und bestätigen sie.

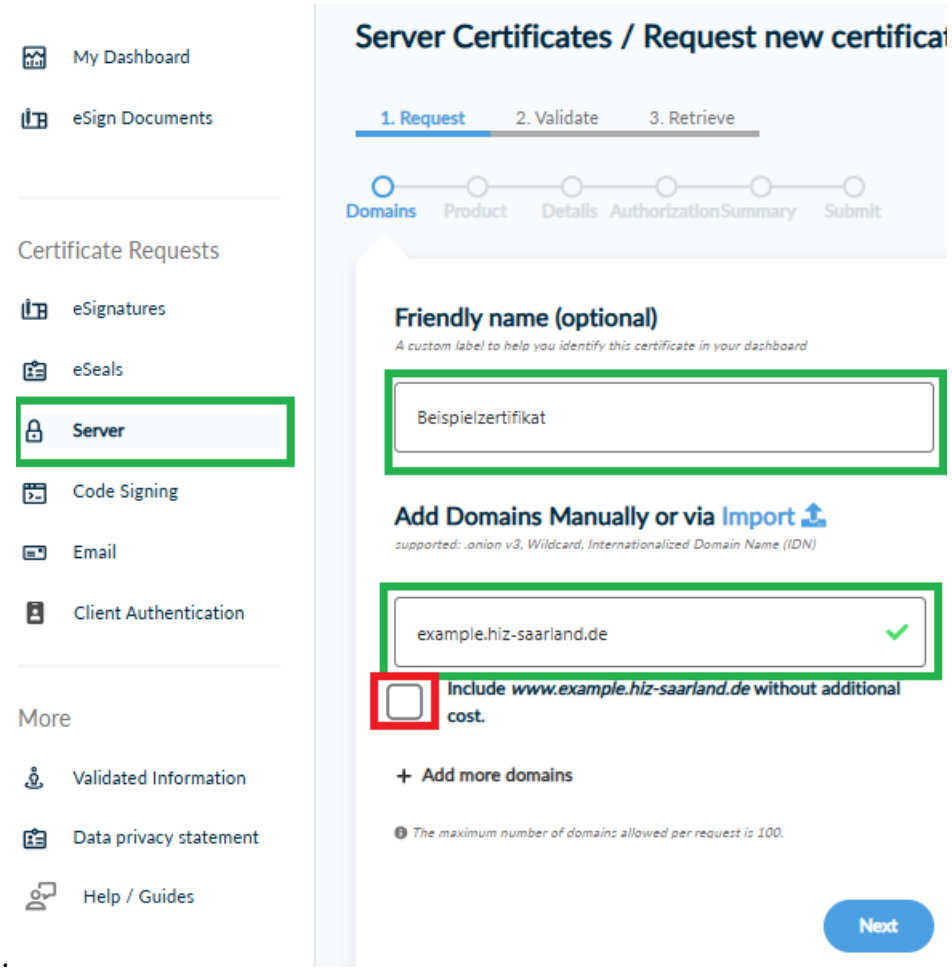


2. Sie gelangen dann auf die Startseite des HARICA-Portals

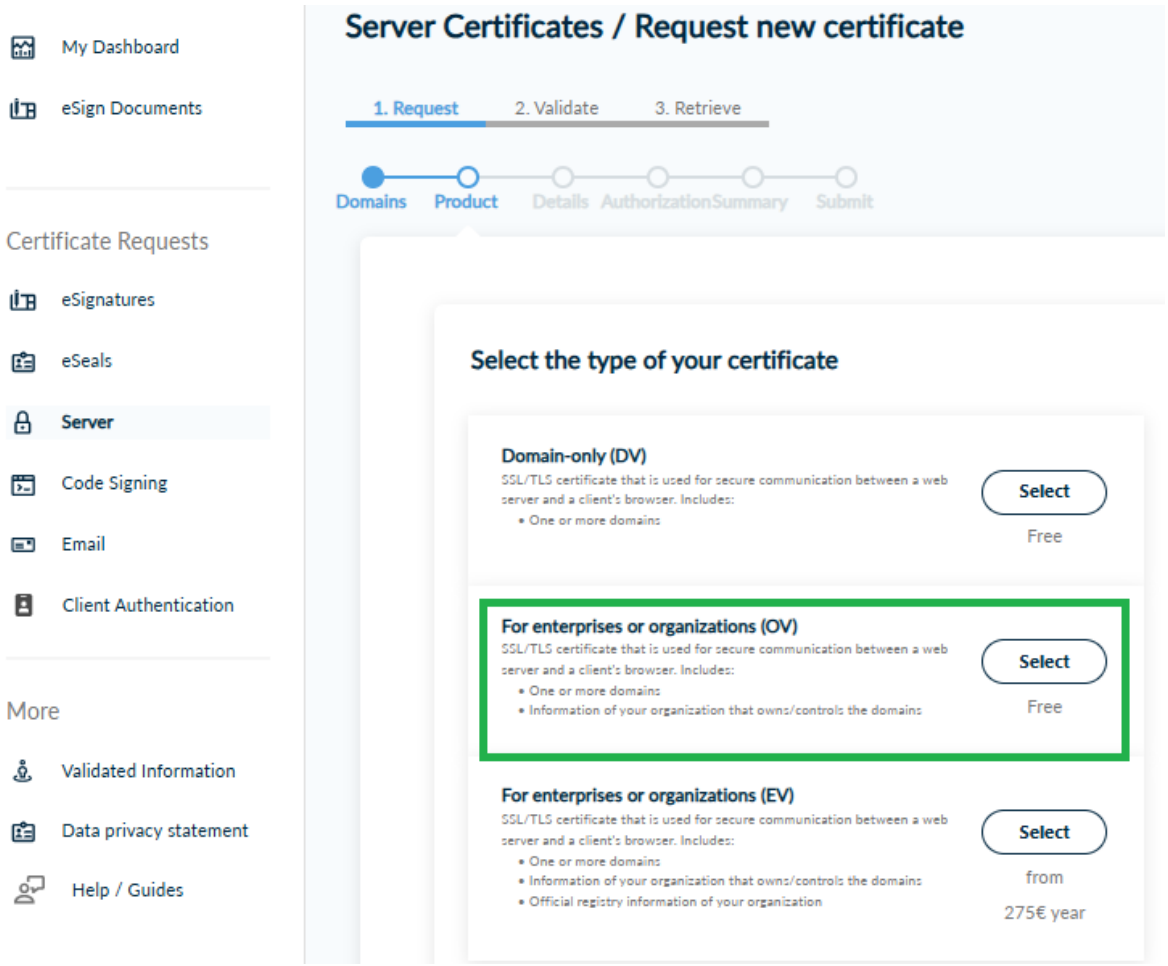


II. Anleitung zur Betragung von SSL-Serverzertifikaten

1. Wählen Sie im Portal auf der linken Seite „**Server**“ aus. Geben Sie dann einen selbstgewählten Anzeigenamen des Antrags (nur sichtbar im Portal) und alle im Zertifikat benötigten Domainnamen ein. Entfernen Sie das Häkchen bei „Include www.…“ wenn Sie nicht wirklich diese Namen im Zertifikat benötigen.

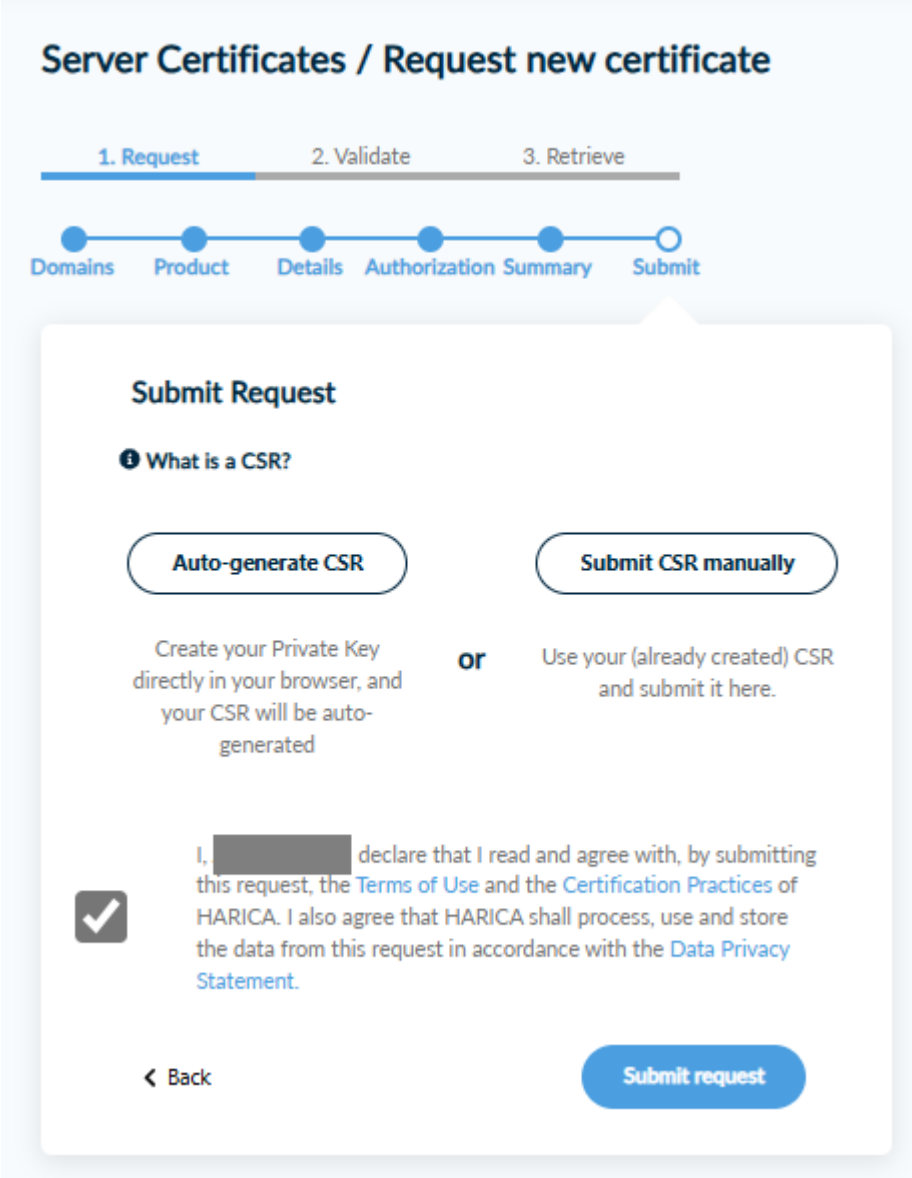


2. Wählen Sie im nächsten Schritt „For enterprises or organisations (OV) aus“

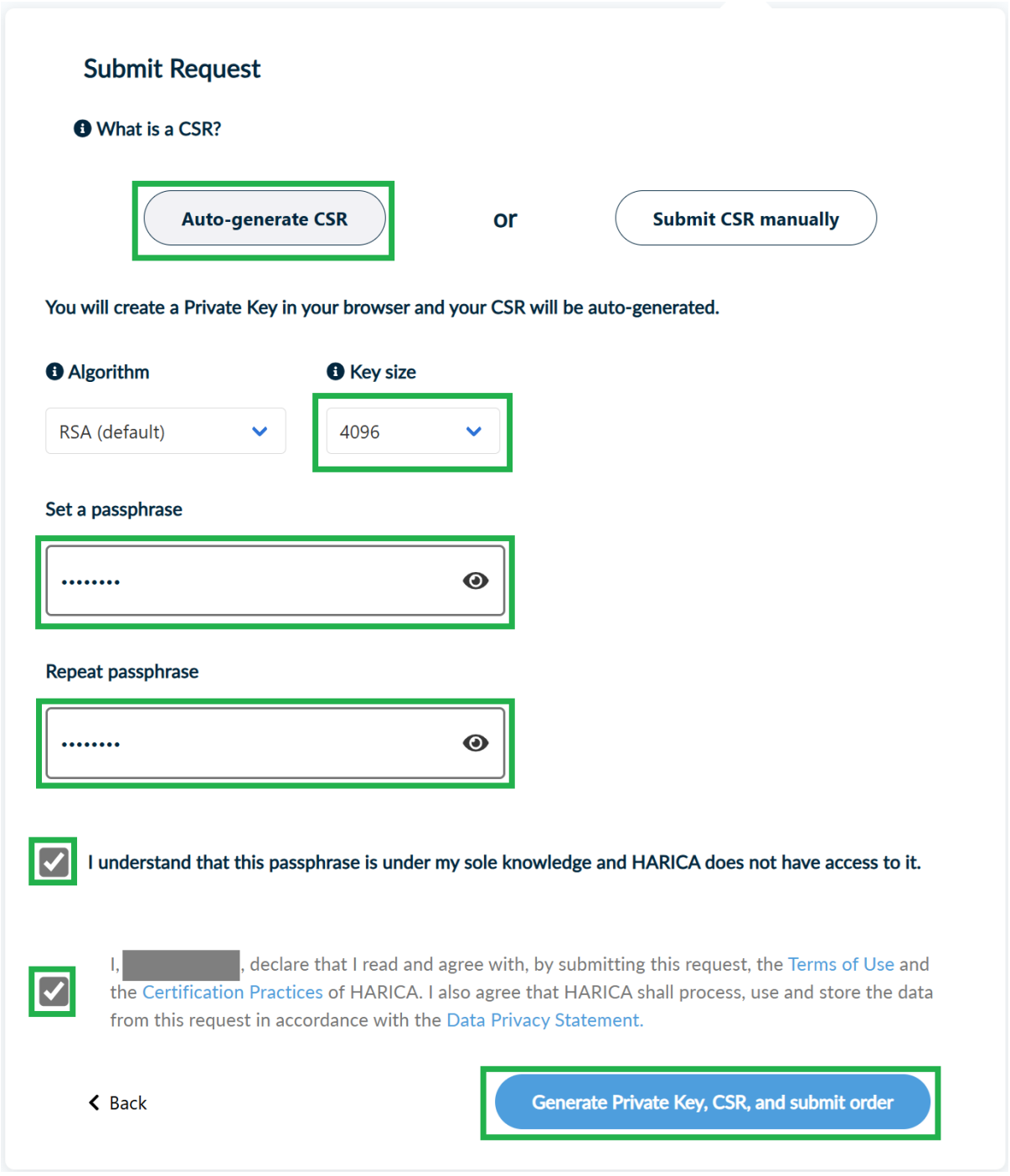


3. Anschließend erhalten Sie die Auswahl zwischen zwei Möglichkeiten, die sogenannten Zertifikatsignierungsanforderung (Certificate Signing Request (CSR)), hochzuladen.

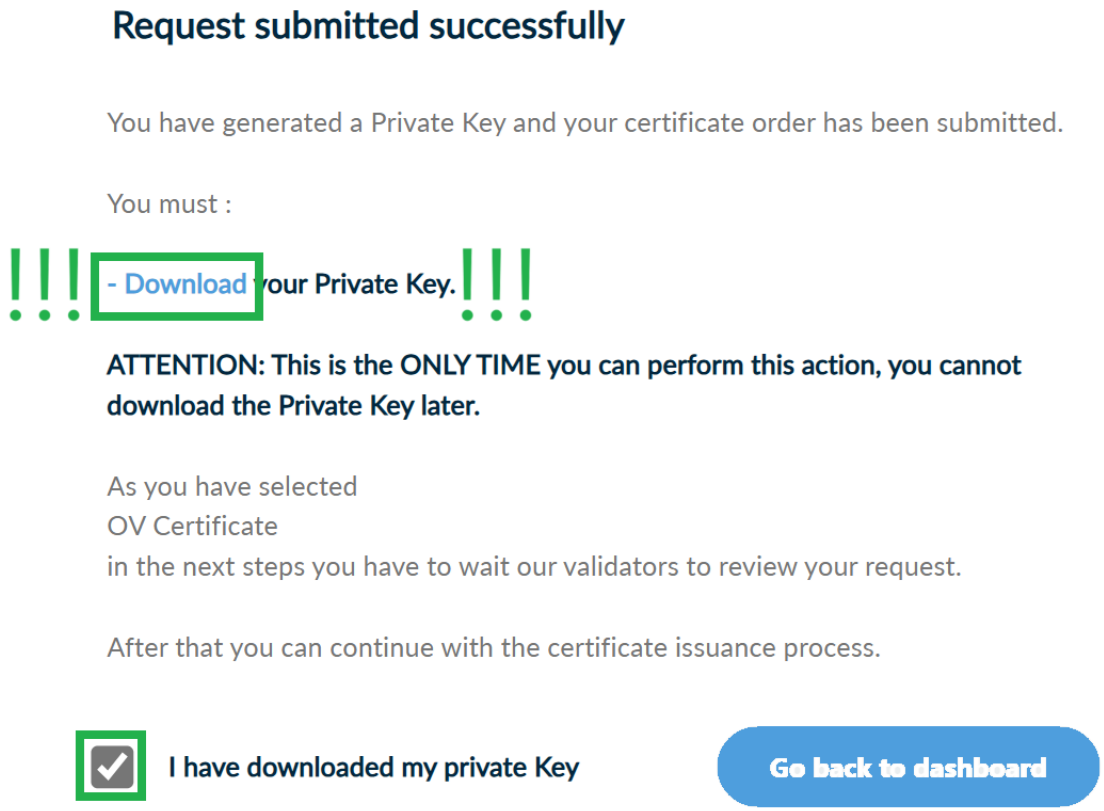
   Technischer Hintergrund
   Die standardisierte und obligatorische CSR-Datei enthält neben den Domainnamen selbst auch die kryptografischen Informationen, damit das später ausgestellte Zertifikat überhaupt zu dem privaten Schlüssel (key) passt, der vertraulich und abgesichert zusätzlich zum Zertifikat selbst in Ihrer Anwendung hinterlegt sein muss. Die CSR-Datei kann (meist bei kommerziellen Anwendungen) direkt generiert werden, oder Sie können Sie mit dem openssl-Toolkit über die Kommandozeile selbst erzeugen. Bei Harica steht Ihnen nun auch eine komfortable dritte Möglichkeit zur Verfügung den CSR während der Beantragung automatisch erzeugen zu lassen.



4. Wenn Sie sich für Auto-generate CSR entschieden haben wählen Sie eine Schlüssellänge von 4096 bit, wenn Sie den verbreitetsten Algorithmus RSA verwenden möchten. Der moderne ECDSA-Algorithmus steht aber auch zur Verfügung.
   Zuletzt müssen Sie noch ein Passwort setzen, mit dem die Key-Datei geschützt ist.
   ACHTUNG: DIESES PASSWORT BENÖTIGEN SIE SPÄTER UNBEDINGT, SONST IST DER KOMPLETTE BEANTRAGUNGS-PROZESS HINFÄLLIG.



5. Das Generieren des Schlüsselpaares dauert einige Sekunden im Browser. Bitte brechen Sie den Vorgang nicht ab. Anschließend erscheint die finale Seite der Beantragung.
   ACHTUNG: LADEN SIE UNBEDINGT DEN KEY AUF DIESER SEITE HERRUNTER. DER VORGANG KANN SPÄTER NICHT WIEDERHOLT WERDEN UND IST NUR AN DIESER STELLE UND EINMALIG MÖGLICH.



6. Nur müssen Sie etwas warten, bis der Antrag genehmigt ist. Die ist ein manueller Prozess. Sie erhalten nach Abschluss eine E-Mail.