



17.07.2024

## Quick Guide

# Certificate Request Wizard (CRW)

**Status:** Freigegeben

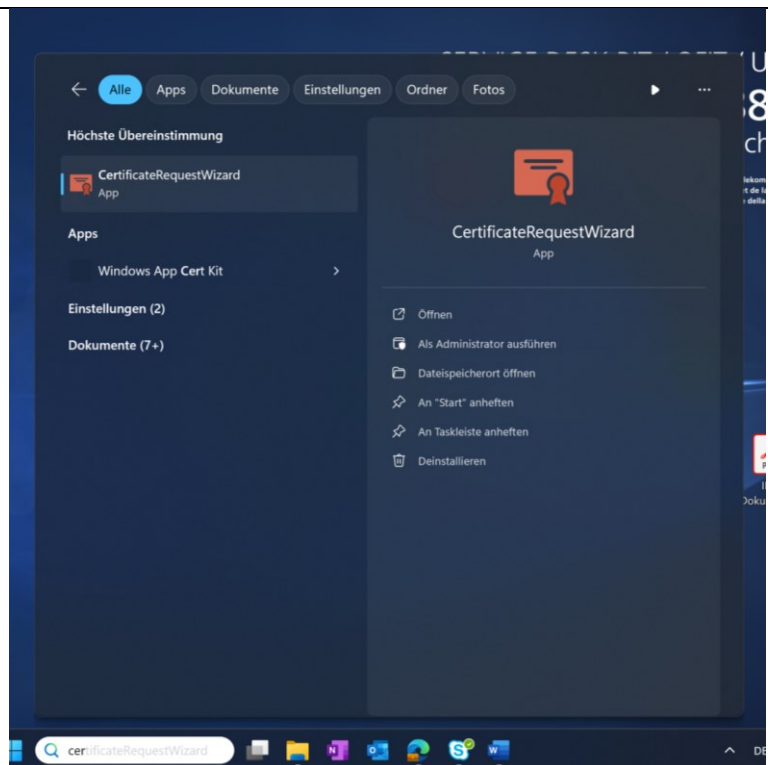
V1.2



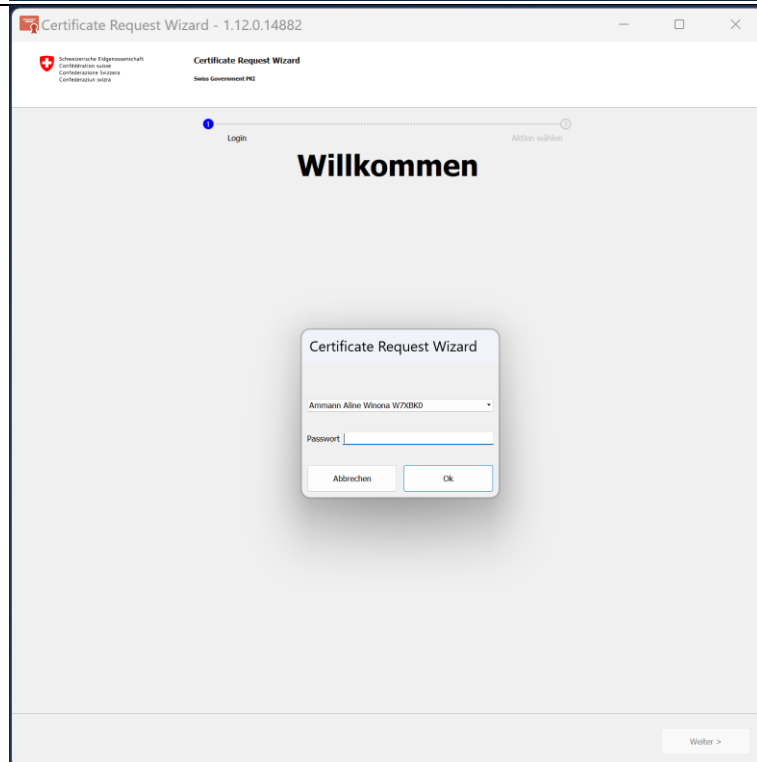
Der «Certificate Request Wizard» (CRW) ist ein eigenständiges Tool, das auf einem BAB-Client installiert wird. Mit dem CRW kann eine Person Certificate Signing Requests (CSRs) für Zertifikate, für die sie berechtigt wurde, lokal generieren. Das CRW schickt diese CSRs anschliessend automatisch an die Swiss Government PKI. Die SG-PKI lässt die erfassten Daten von der in der Mailadresse des Antrags angegebenen zertifikatsempfangende Person verifizieren und bestätigen. Danach wird das Zertifikat ausgestellt und kann von der antragstellenden Person abgeholt und an die Zertifikatsempfangende weitergeleitet werden. Alternativ zu der Erstellung des CSR durch den Wizard, kann auch ein vorbereiteter CSR in das Tool kopiert und als Antrag abgeschickt werden.

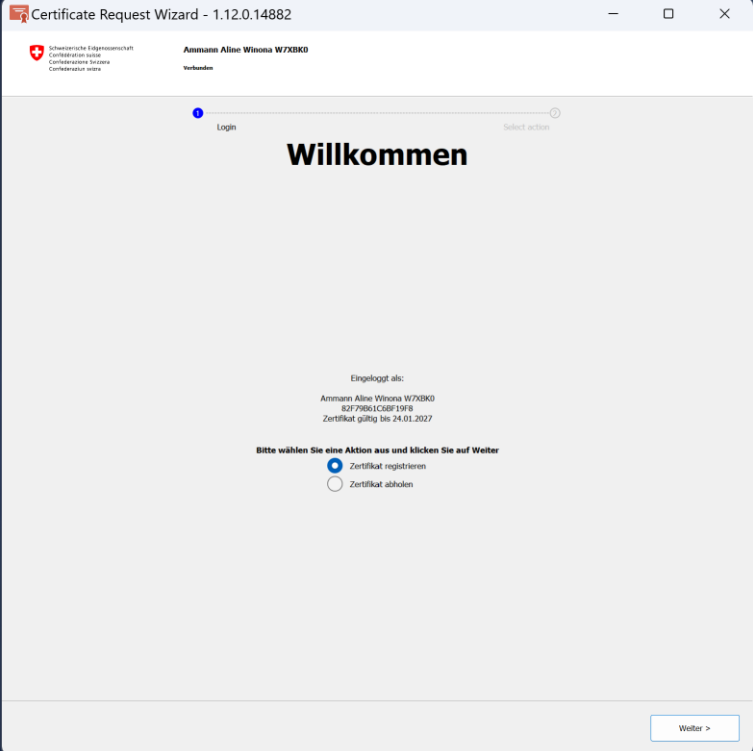
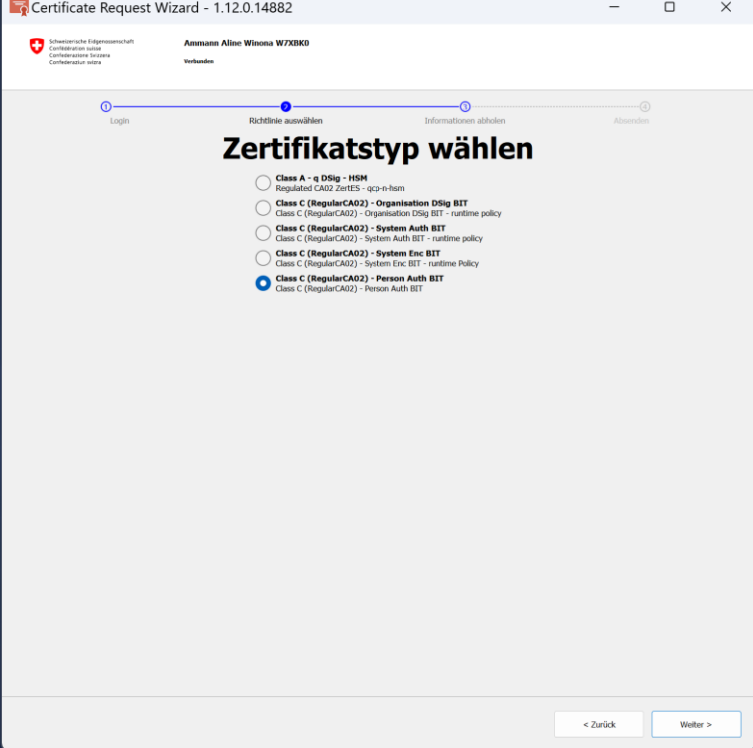
## Zertifikat registrieren

Starten Sie die CRW Applikation.



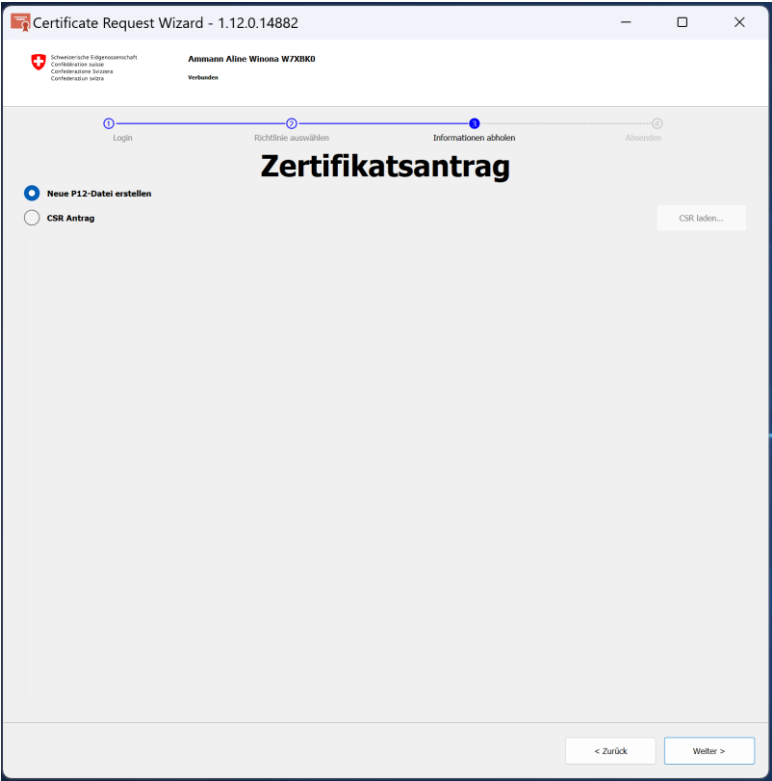
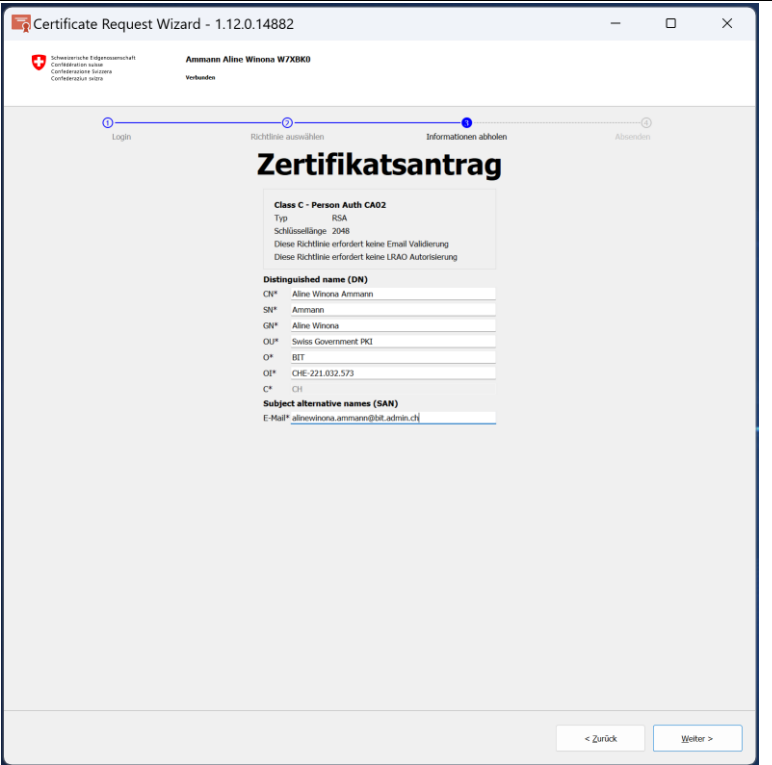
Nach dem Start der Anwendung erscheint ein Anmeldefenster. Geben Sie hier die PIN Ihres berechtigten Klasse B Zertifikates ein und bestätigen Sie mit "OK".

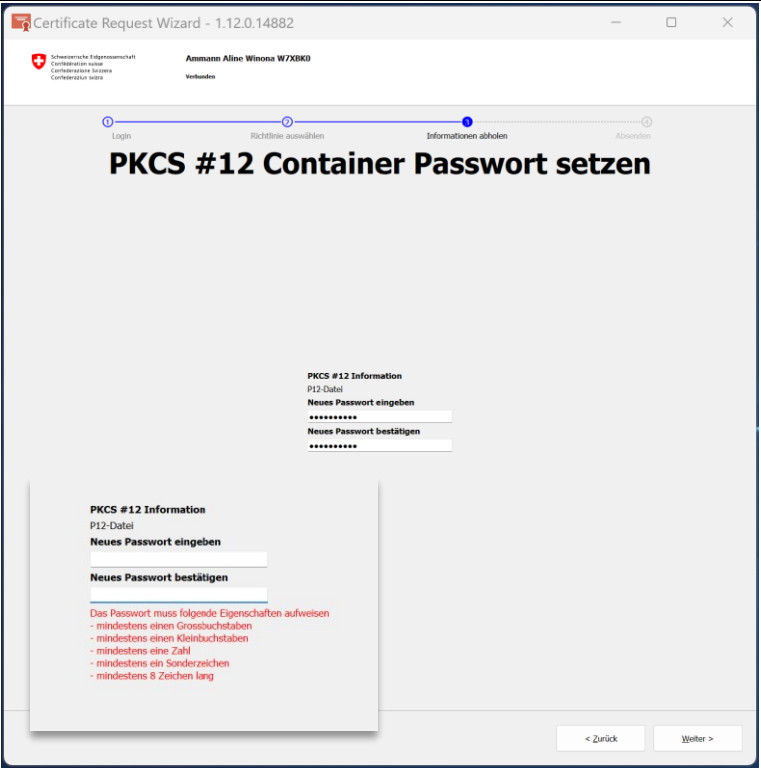
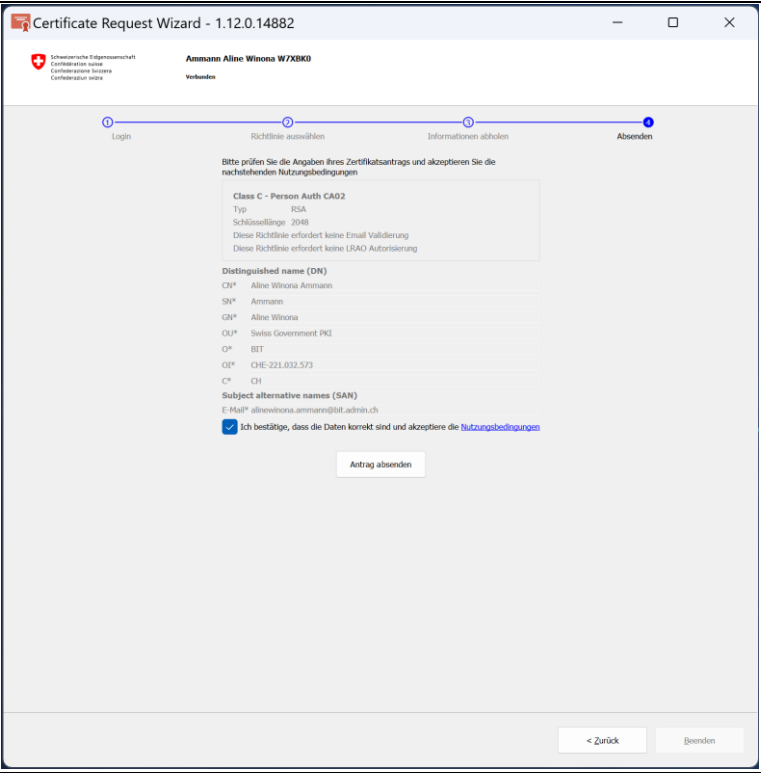


<p>Wählen Sie „Zertifikat registrieren“ aus und klicken Sie auf den Knopf „Weiter“.</p>	
<p>Wählen Sie die gewünschte Policy (je nach Berechtigungen können mehrere zur Auswahl stehen), und klicken Sie danach auf „Weiter“.</p>	

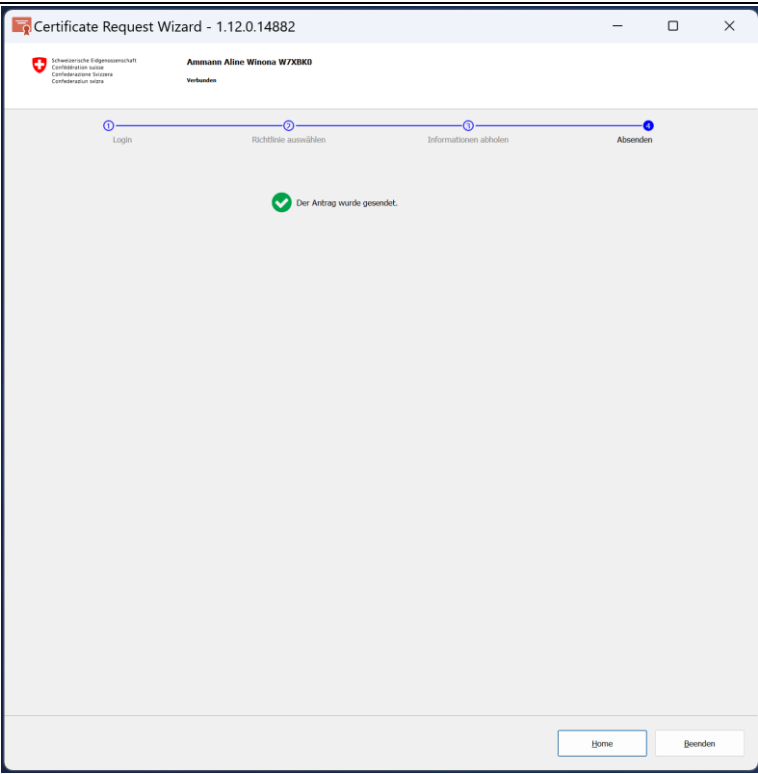
Variante 1: P12 ausstellen (Schlüsselpaar und Zertifikat)

Bei diesem Vorgang erstellt das Tool automatisch ein Certificate Signing Request (CSR), das online versendet wird. Das Resultat sind die beiden Schlüssel, sowie das Zertifikat in einer P12-Datei

<p>Wählen Sie die Option «Neue P12 Datei erstellen» und fahren Sie mit „Weiter“ fort.</p>	
<p>Je nach ausgewählter Policy sind die Felder des Distinguished Name (DN) unterschiedlich auszufüllen. Fixe Einträge sind schattiert und können nicht bearbeitet werden. Füllen Sie die nötigen Felder aus (siehe Kapitel Policy) und klicken Sie danach erneut auf „Weiter“.</p>	

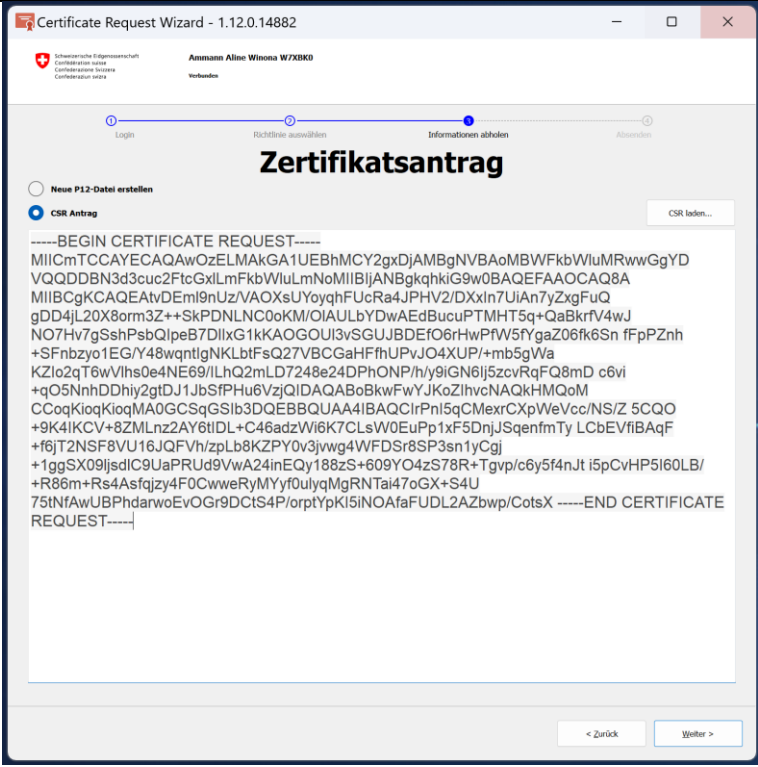
<p>Geben Sie ein Passwort für Ihr P12-File ein. Die Richtlinien für das Passwort werden angezeigt, wenn die Eingabe diese nicht erfüllt. Drücken Sie danach "Weiter".</p>	
<p>Prüfen Sie die Angaben. Setzen Sie anschliessend das Häkchen bei der Bestätigung (Lesen Sie die Nutzungsbedingungen). Schicken Sie den Antrag ab und drücken Sie auf den Knopf "Beenden".</p> <p>Die antragstellende Person kann nun die E-Mail-Validierung durchführen, sofern dies die Policy verlangt.</p>	

Der Prozess ist nun abgeschlossen. Mit dem Button «Home» kommen Sie direkt auf die Startseite zurück. Andernfalls können Sie die Applikation mit dem Knopf «Beenden» schliessen.



Variante 2: CSR Antrag

Wählen Sie die Option «CSR Antrag» aus. Laden Sie entweder das CSR aus einer Datei mit dem Knopf «CSR laden», oder kopieren Sie den Text des CSRs wie im Beispiel gezeigt direkt in das freie Feld. Drücken Sie anschliessend auf «Weiter».

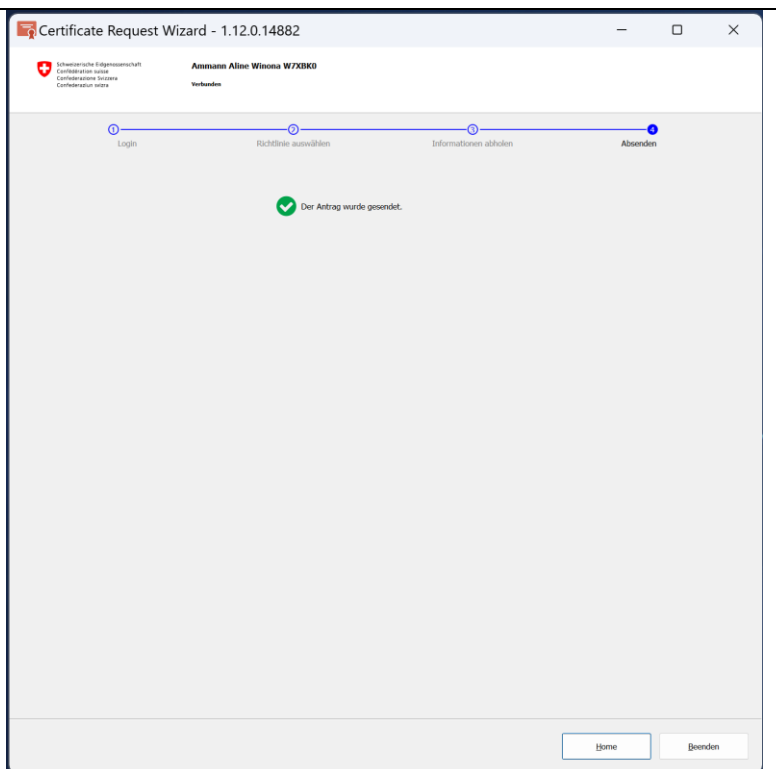


Mit dem CSR sind die Felder des Distinguished Name bereits ausgefüllt. Prüfen Sie die Angaben anhand der Policy Vorgaben und nehmen Sie, wenn nötig, Anpassungen vor. Fixe Einträge sind schattiert und können nicht bearbeitet werden. Fahren Sie danach mit "Weiter" fort.

Prüfen Sie die Angaben. Setzen Sie anschliessend das Häkchen bei der Bestätigung (Lesen Sie die Nutzungsbedingungen). Schicken Sie den Antrag ab und drücken Sie auf den Knopf "Beenden".

Die antragstellende Person kann nun die E-Mail-Validierung durchführen, sofern das die Policy verlangt.

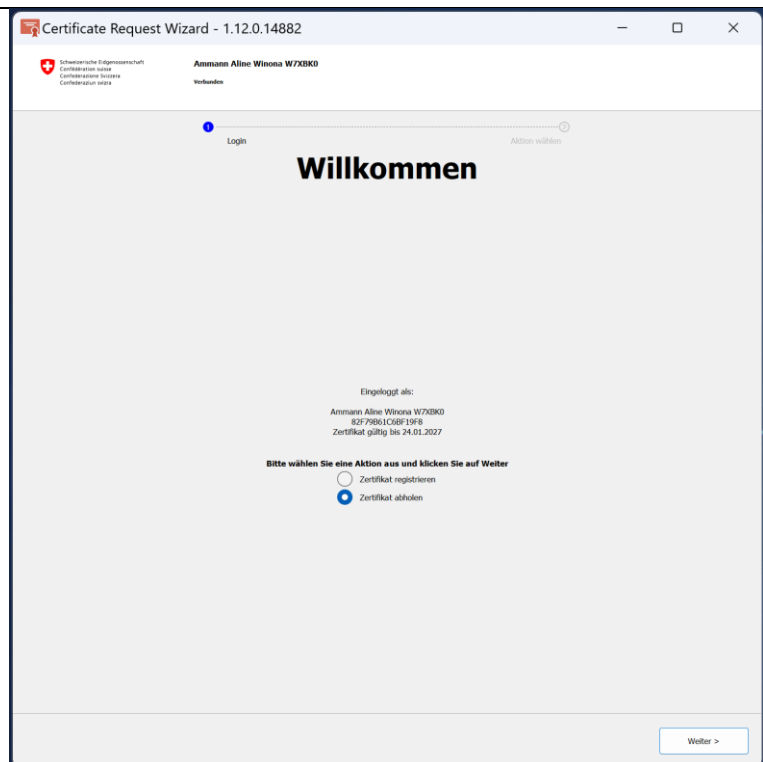
Der Prozess ist nun abgeschlossen. Mit dem Button «Home» kommen Sie direkt auf die Startseite zurück. Andernfalls können Sie die Applikation mit dem Knopf «Beenden» schliessen.



## Zertifikat abholen

Sie können ein Zertifikat entweder direkt nach der Registrierung oder, wenn es durch die Policy bedingt ist, nach der E-Mail-Validierung der antragstellenden Person abholen.

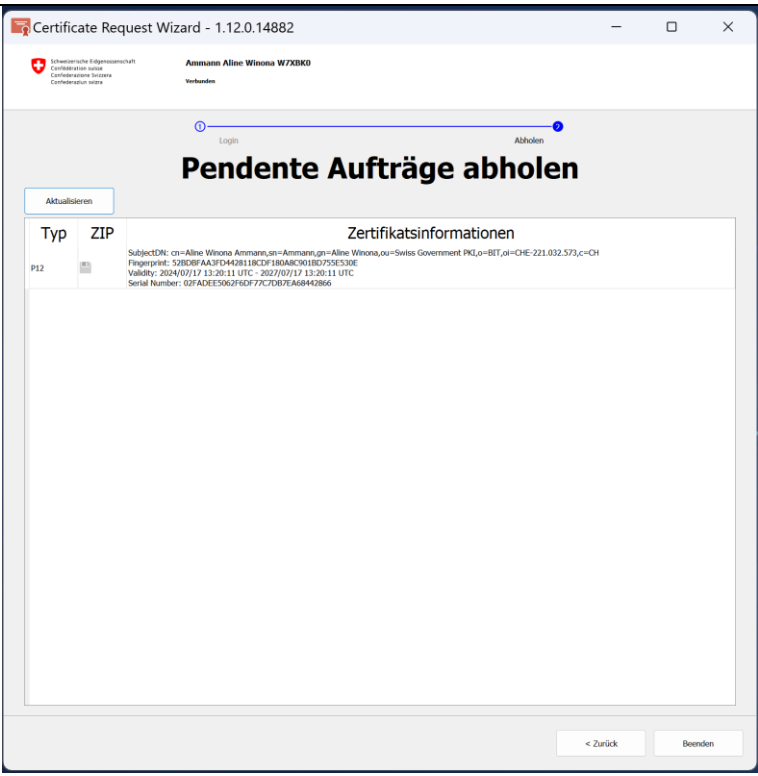
Melden Sie sich, wenn nötig, in der Anwendung gemäss Beschreibung in Kapitel 1 an. Wählen Sie dann die Option «Zertifikat abholen» und drücken Sie «Weiter».





Klicken Sie auf „Aktualisieren“, um die pendenten Aufträge aufzulisten. Klicken Sie in der Spalte ZIP auf das Diskettensymbol, um das jeweilige Zertifikat herunterzuladen.

**Achtung:** Ein Auftrag kann nur einmal abgeholt werden. Danach wird er nicht mehr aufgelistet.



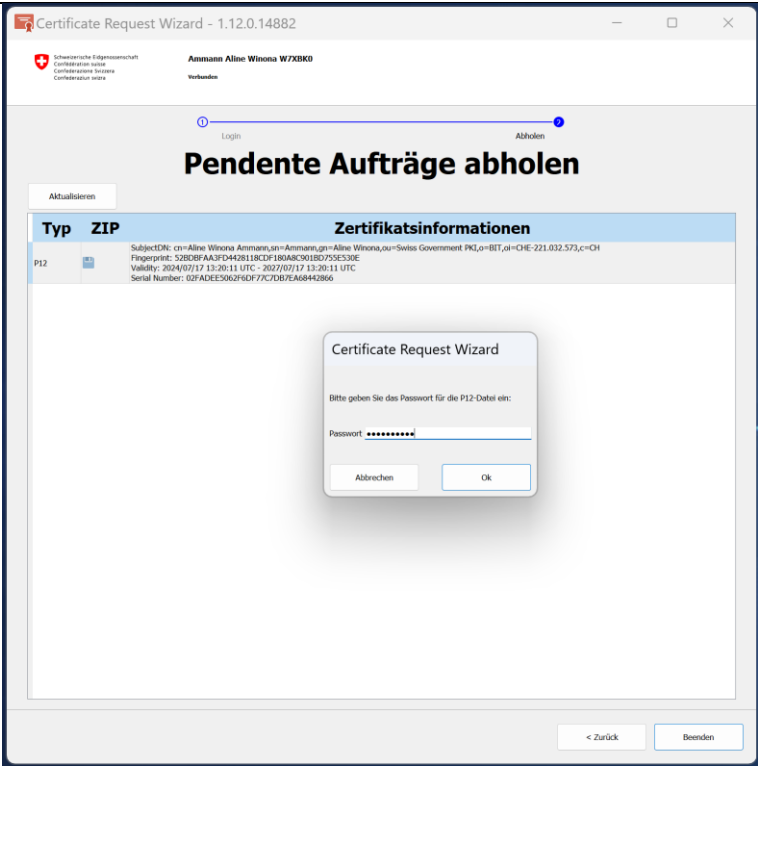
Bei der Variante P12 werden Sie nach dem Passwort des privaten Schlüssels gefragt. Geben Sie dieses in das Fenster ein (hier ist **NICHT** die Smartcard-PIN gemeint).

Bestimmen Sie danach den Speicherort Ihrer Datei.

Falls die Variante CSR gewählt wurde, wird beim Herunterladen kein Passwort verlangt. In der ZIP-Datei des CSR-Auftrags ist zudem auch keine P12-Datei.

Beenden Sie danach den CRW.

**Beachten Sie, dass die Zertifikate nur durch die inhabende Person archiviert werden dürfen, und dass das P12 File nur auf demselben PC, mit welchem der Antrag gestellt wurde, auch downloaded werden kann, da es auf der Festplatte (C:/) zwischengespeichert wird.**



## Policy

Klasse C Standardzertifikate unterscheiden sich in den anwendbaren DNs wie folgt:

Distinguished Name für Personenzertifikate*	
<b>CN =</b>	CN= Common Name: Nachname(n) Vorname(n), Bsp.: <b>Mustermeier Hanspeter</b>
<b>SN =</b>	SN = Surname: Nachname(n)
<b>GN =</b>	GN= Givenname: Vorname(n)
<b>OU =</b>	OU= Organisationseinheit: <b>Frei wählbar</b> , z.B. Abteilung, Bereich, etc... Bsp.: <b>Bundesamt für Zukunftsforschung (BFZ) - Büroautomation</b>
<b>O =</b>	O= Organisation: <b>Auswählbar</b> , zw. Administrative Einheit Bsp.: <b>BFZ</b>
<b>OI =</b>	OI= Organisation Identity: UID gemäss <a href="#">UID-Register</a> , Bsp.: <b>CHE-123.456.789</b>
<b>C =</b>	C= Country: <b>Fixer Eintrag: CH</b>
Distinguished Name für Systemzertifikate	
<b>CN =</b>	CN= Common Name: System Name, Bsp.: <b>TUSER-SYSP-SCPP123</b>
<b>OU =</b>	OU= Organisationseinheit: <b>Frei wählbar</b> , z.B. Abteilung, Bereich, etc... Bsp.: <b>Bundesamt für Zukunftsforschung (BFZ)-Büroautomation</b>
<b>O =</b>	O= Organisation: <b>Fixer Eintrag: Admin</b>
<b>OI =</b>	OI= Organisation Identity: UID gemäss <a href="#">UID-Register</a> , Bsp.: <b>CHE-123.456.789</b>
<b>C =</b>	C= Country: <b>Fixer Eintrag: CH</b>
Distinguished Name für Organisationszertifikate*	
<b>CN =</b>	CN= Common Name: Amtsbezeichnung (gemäss UID-Register), oder offizielle Übersetzung davon. Bsp.: <b>Bundesamt für Zukunftsforschung (BFZ)</b>
<b>OU =</b>	OU= Organisationseinheit: <b>Frei wählbar</b> , z.B. Abteilung, Bereich, etc... Bsp.: <b>Büroautomation</b>
<b>O =</b>	O= Organisation: <b>Frei wählbar</b> , Bsp.: <b>Schweizerische Eidgenossenschaft</b> oder <b>BFZ</b>
<b>OI =</b>	OI= Organisation Identity: UID gemäss <a href="#">UID-Register</a> , Bsp.: <b>CHE-123.456.789</b>
<b>C =</b>	C= Country: <b>Fixer Eintrag: CH</b> (offen bei Org Zert. mit Auth/Sign/Enc Funktion, wird aber abgeraten)

## Gültigkeit

Klasse C Standard Zertifikate der Swiss Government PKI sind max. 3 Jahre gültig.