Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Finance FDF

Federal Office of Information Technology and Telecommunications FOITT
Swiss Government PKI

17.07.2024

Quick Guide

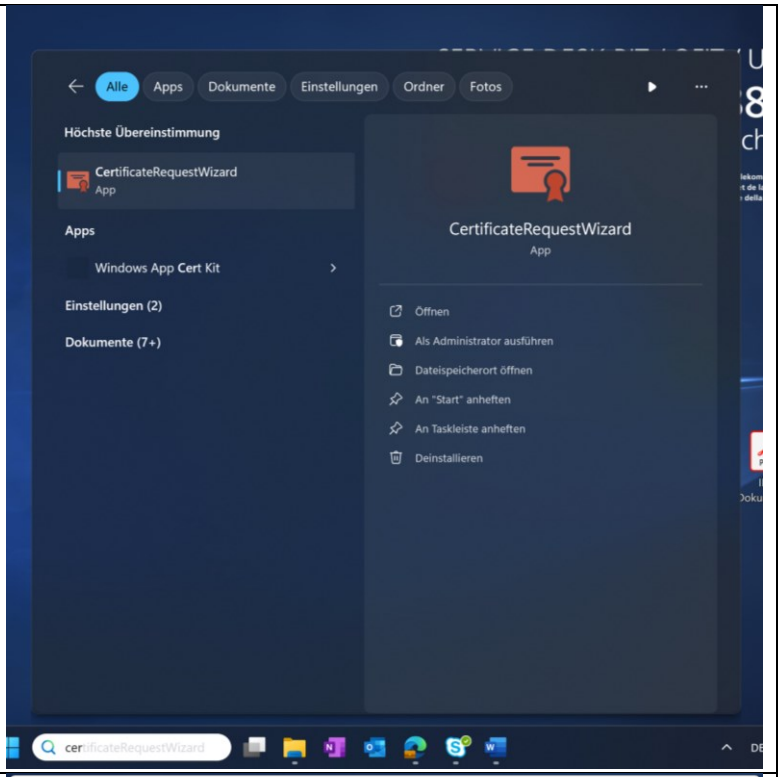
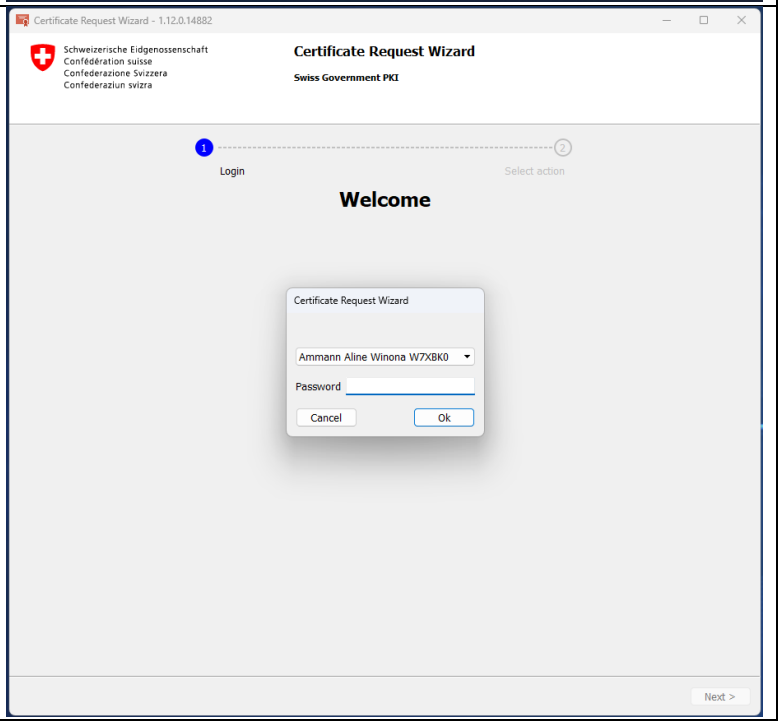
Certificate Request Wizard (CRW)

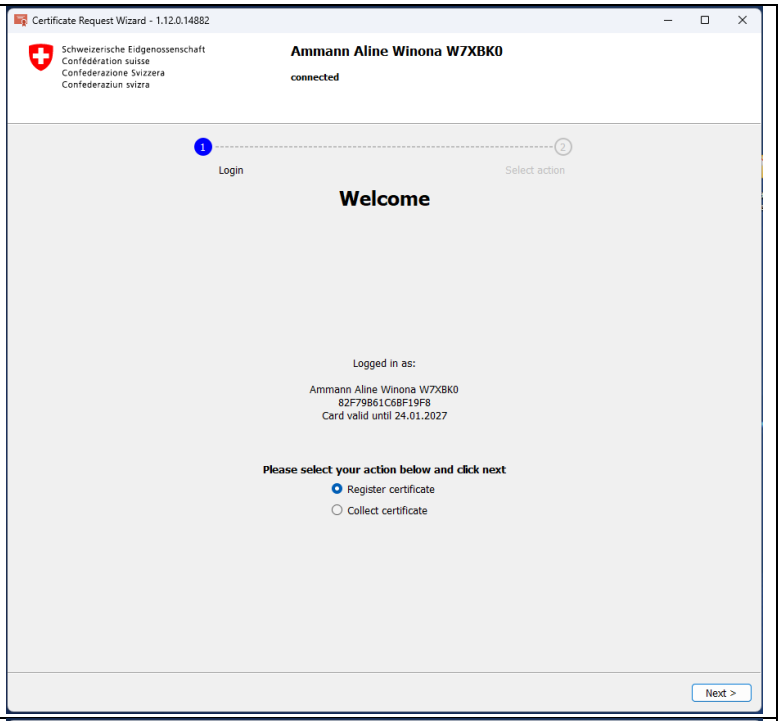
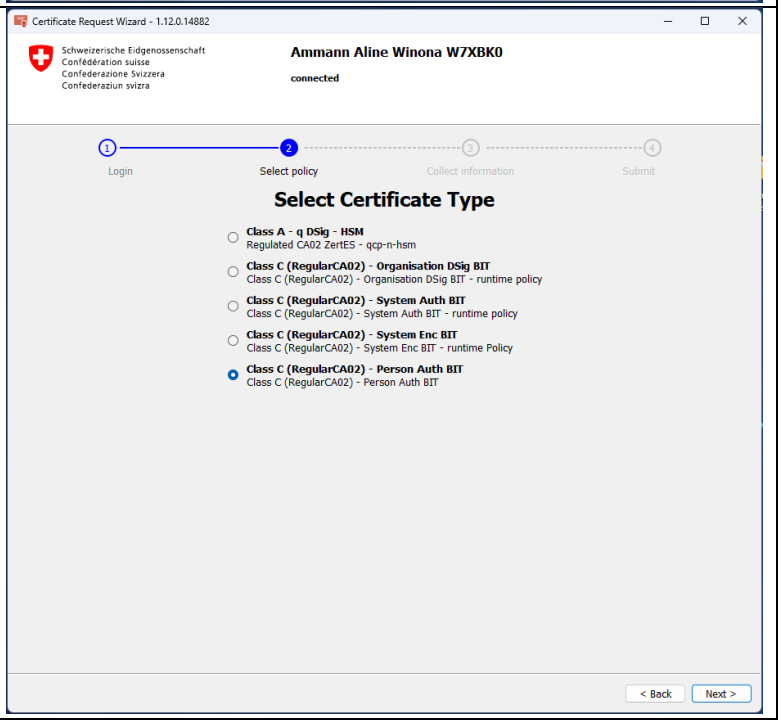
Status: Released V1.2

The Certificate Request Wizard (CRW) is a stand-alone tool that is installed on each federal workstation client. Owners can use the CRW to locally generate certificate signing requests (CSRs) for certificates for which they are authorised. The CRW then automatically sends these CSRs to the Swiss Government PKI. The SG-PKI arranges verification and confirmation of the data entered for the certificate recipient specified in the email address of the request. The certificate is then issued and can be collected by the user and passed on to the certificate recipient.

As an alternative to CSR creation via the wizard, a prepared CSR can also be pasted into the tool and sent off as a request.

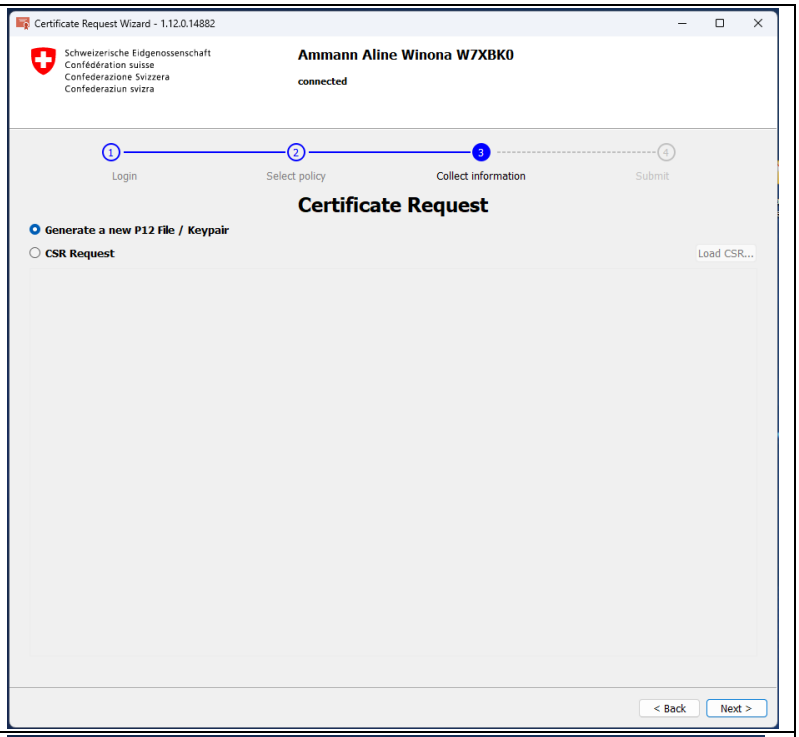
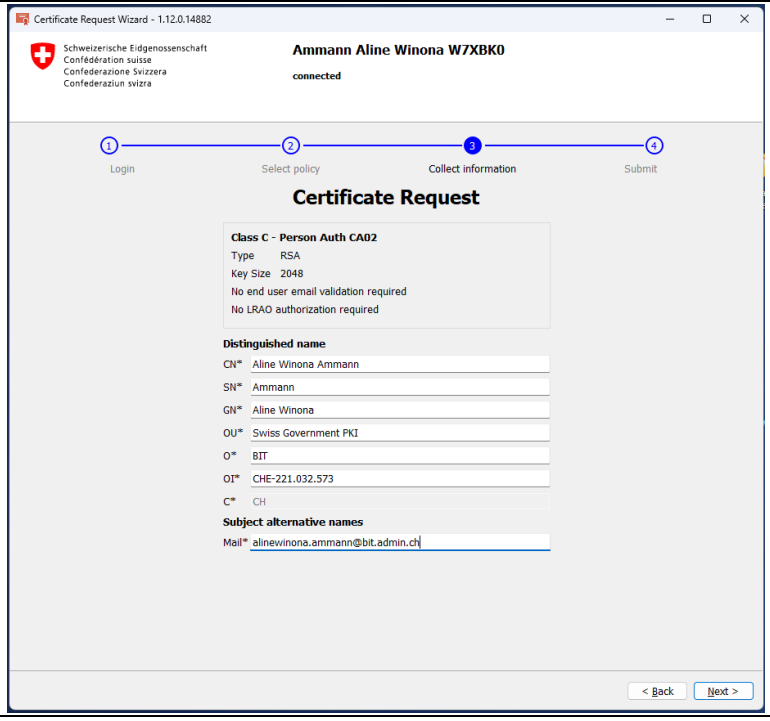
Register certificate

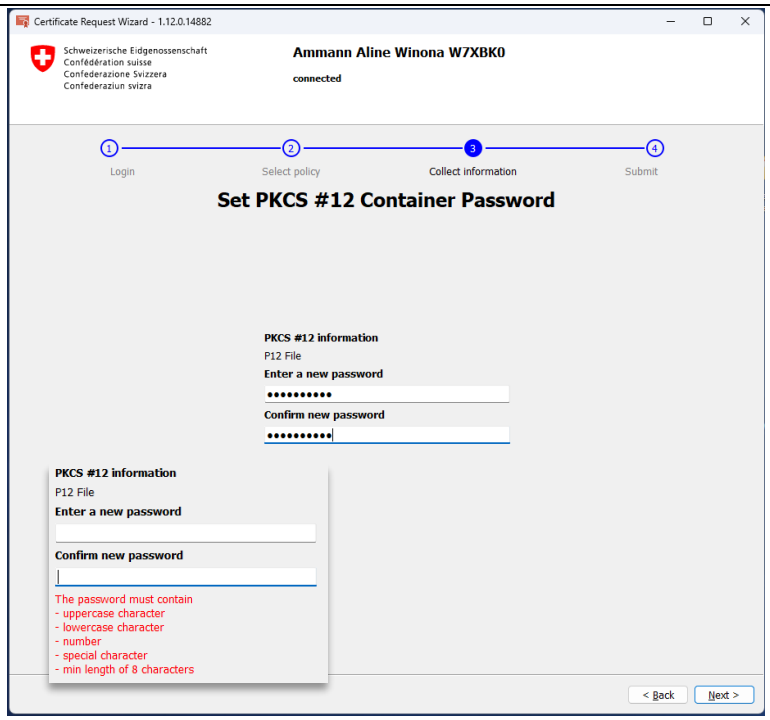
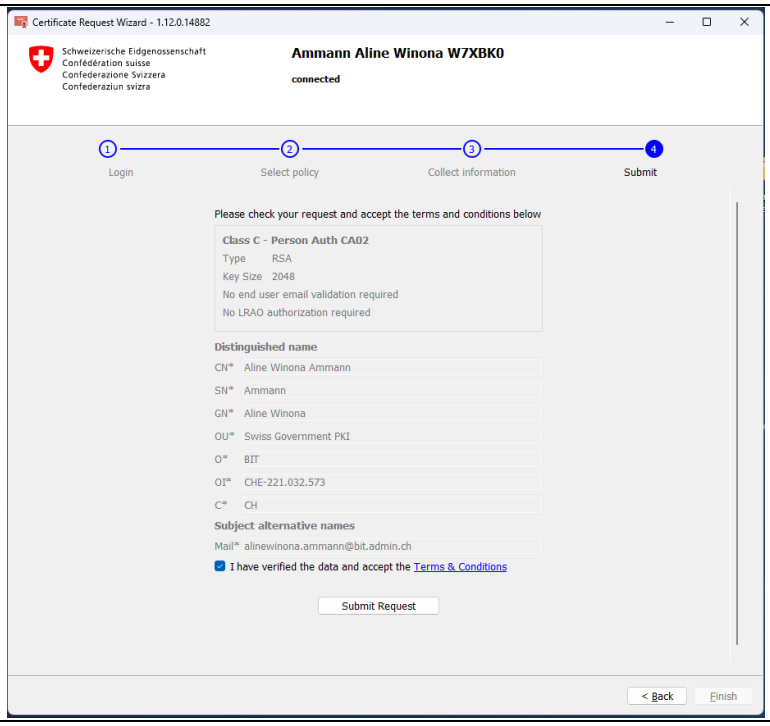
Start the CRW application.	
After starting the application, a login window appears. Enter the PIN of your authorized class B certificate here and confirm with “OK”.	

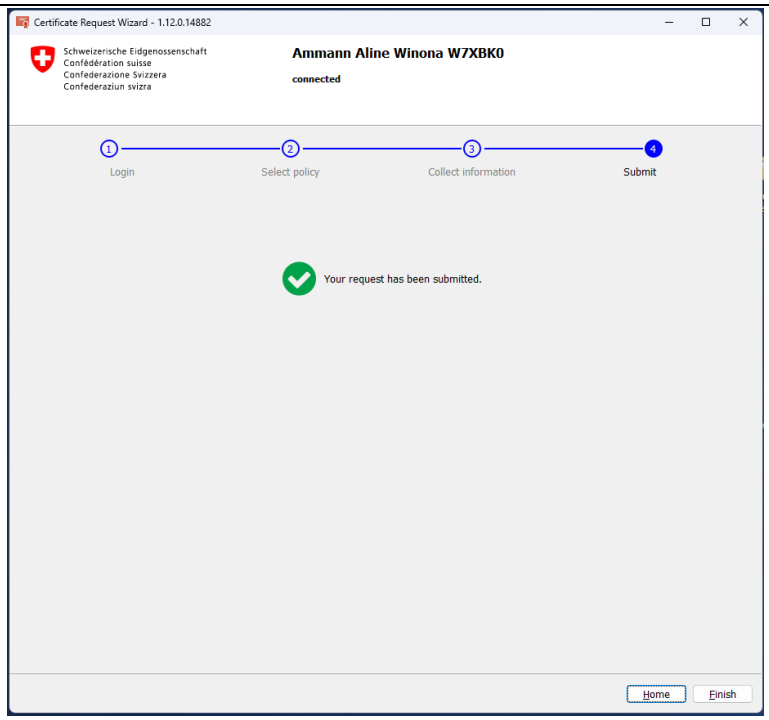
Select "Register certificate" and continue with the "Next" button.	
Select the desired policy (depending on the authorizations, there may be several to choose from) and click on "Next".	

Variant 1: Issue P12 (key pair and certificate)

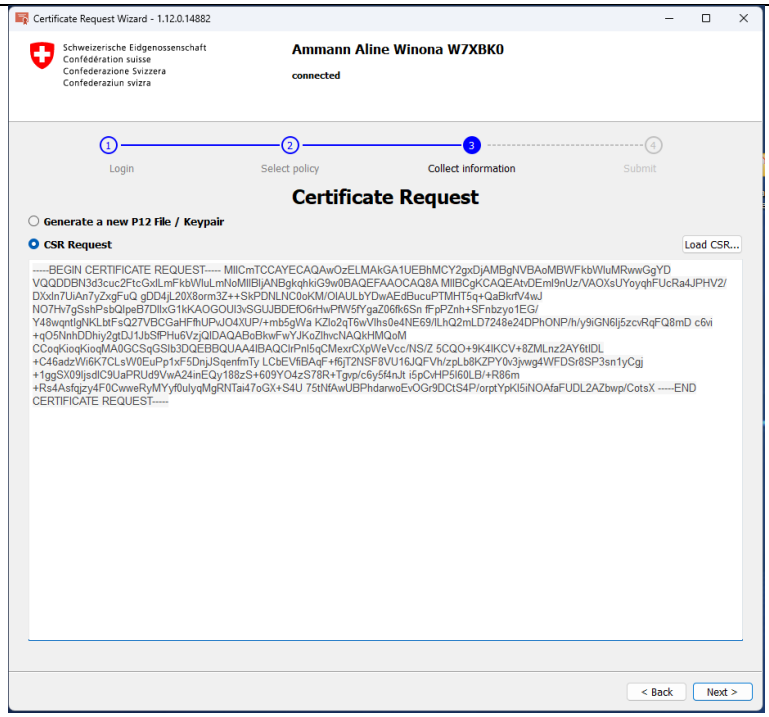
During this process, the tool automatically creates a Certificate Signing Request (CSR), which is sent online. The result is the two keys and the certificate in a P12 file

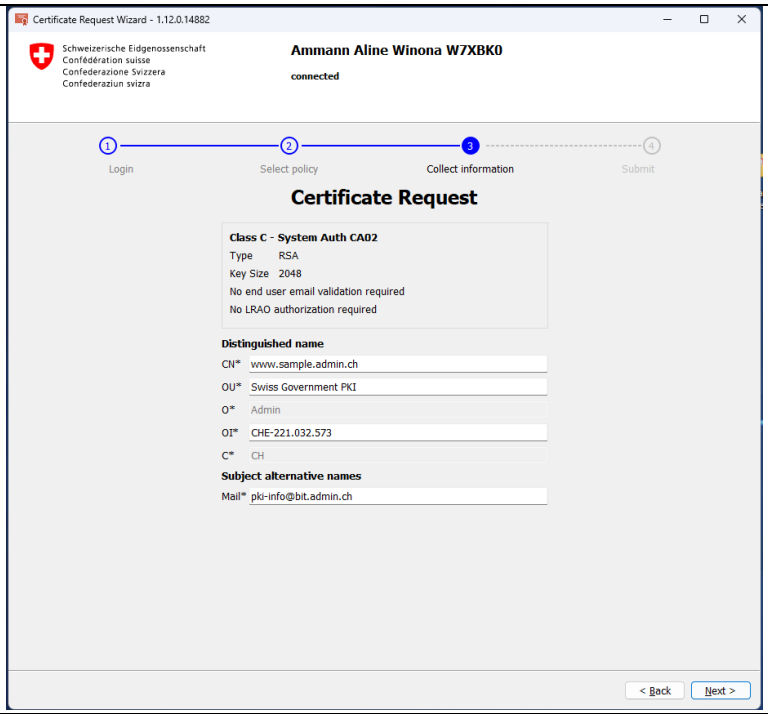
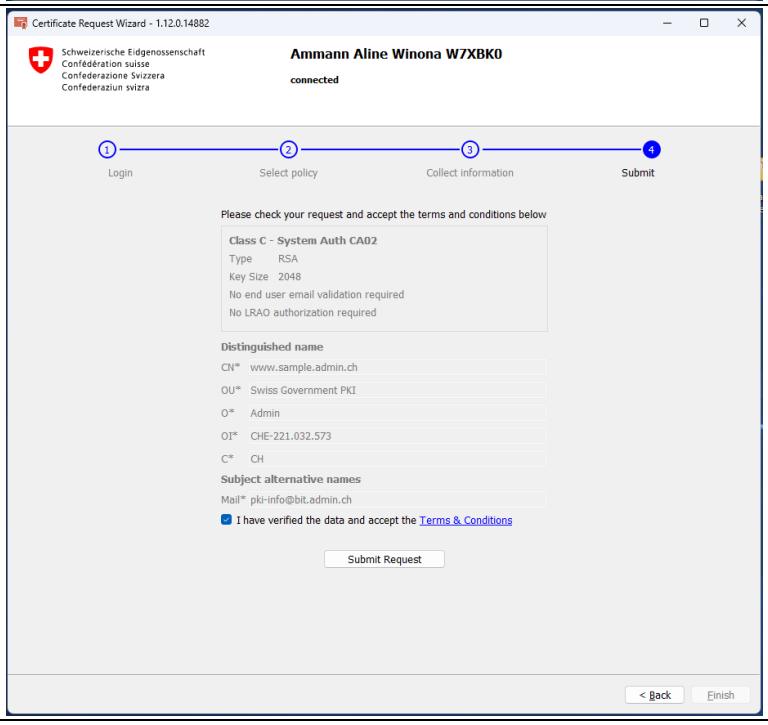
Select the option "Generate a new P12 file / Keypair" and continue with "Next".	
Depending on the selected policy, the fields of the Disdinguished name (DN) must be filled in differently. Fixed entries are shaded and cannot be edited. Fill in the required fields (see Policy chapter) and then click on "Next".	

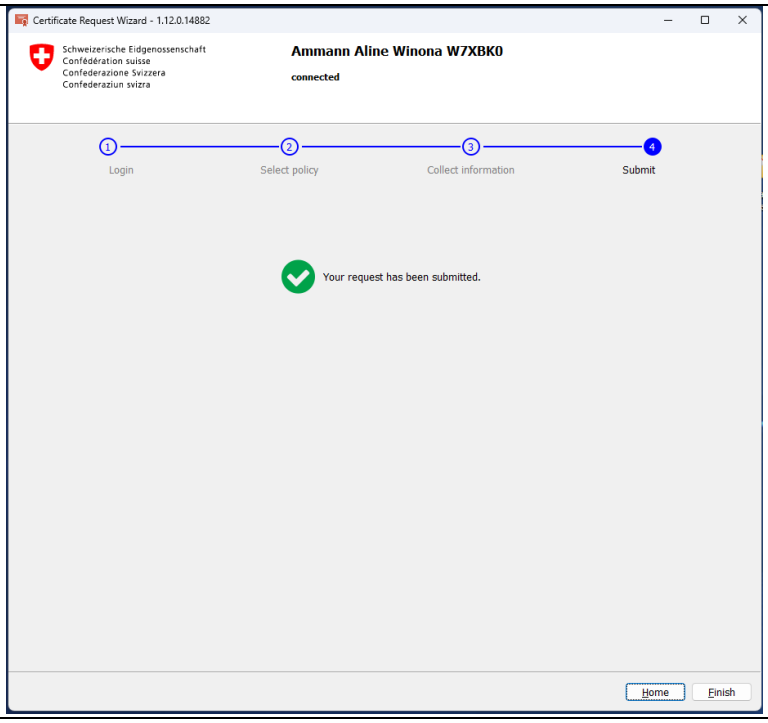
Enter a password for your P12 file. The requirements for the password are displayed if the entry does not meet them. After doing so, click “Next”.	
Verify the details. Then check the box next to the confirmation (read the terms of use). Send the application and press the “Finish” button. The applicant can now carry out the e-mail validation, if required by the policy.	

The process is now complete. The “Home” button takes you directly back to the start page. Otherwise, you can close the application with the “Exit” button.	

Variant 2: CSR application

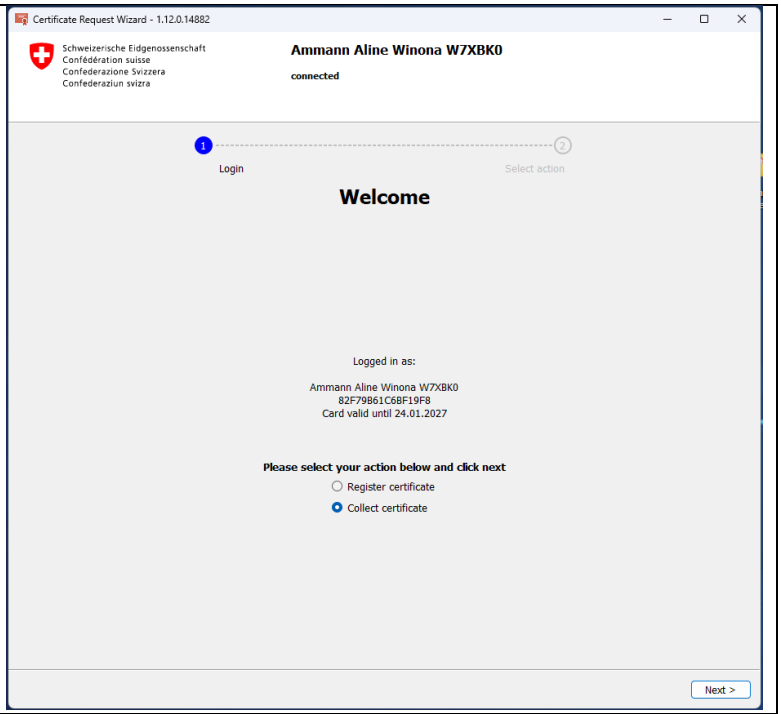
Select the "CSR Request" option. Either load the CSR from a file using the "Load CSR" button or copy the text of the CSR directly into the empty field as shown in the example. Then click on "Next".	

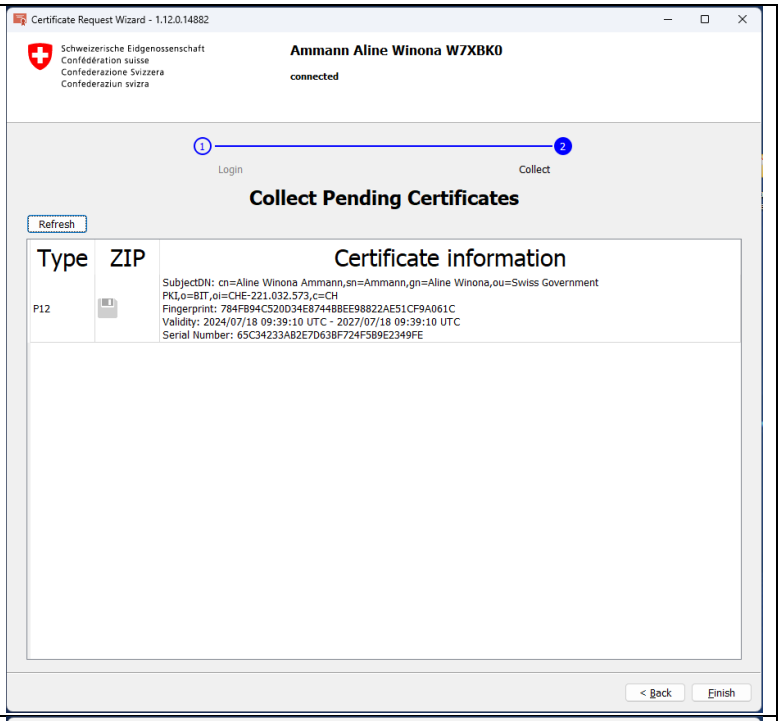
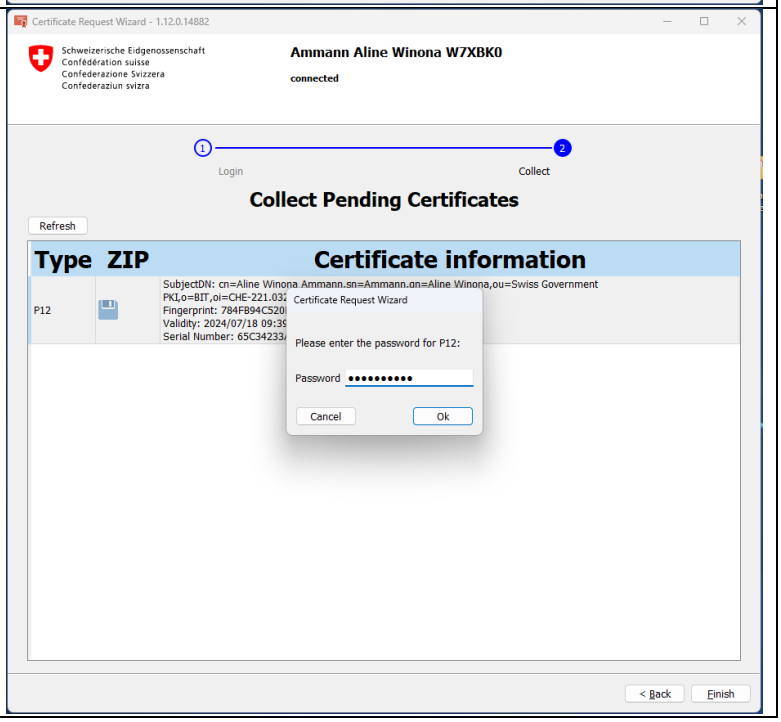
The fields of the Distingushed Name are already filled in with the CSR. Check the details against the policy specifications and adjust if necessary. Fixed entries are shaded and cannot be edited. Then click on «Next».	
Verify the details. Then check the box next to the confirmation (read the terms of use). Send the application and press the “Finish” button. The applicant can now carry out the e-mail validation, if required by the policy.	

The process is now complete. The “Home” button takes you directly back to the start page. Otherwise, you can close the application with the “Exit” button.	

Collect a certificate

You can pick up a certificate either directly after registration or, if required by the policy, after the applicant's e-mail validation.

If necessary, log in to the application as described in chapter 1. Then select the "Collect certificate" option and press "Next".	

Click on "Refresh" to list the pending orders. Click on the floppy disk symbol in the ZIP column to download the respective certificate. **Please note**: An order can only be collected once. After that, it will no longer be listed.	
With the P12 variant, you will be asked for the password for the private key. Enter it into the designated field (this does NOT refer to the smartcard PIN). Then determine the storage location of your file. If the CSR variant was selected, no password is requested when downloading. There is also no P12 file in the ZIP file of the CSR order. Exit the CRW when you're done. Please note that the certificates may only be archived by the **owner**!	

Policy

Class C standard certificates differ in the applicable DNs as follows:

Distinguished Name for personal certificates*	
CN =	*CN= Common Name: Last name(s) First name(s), e.g.:* ***Mustermeier Hanspeter***
SN =	*SN = Surname: Surname(s)*
GN =	*GN= Givenname: First name(s)*
OU =	*OU= Organizational unit: Freely selectable, e.g. department, division, etc...* *Example:* ***Federal Office for Future Studies (BFZ) - Office automation***
O =	*O= Organization: Selectable, between Administrative unit* *Example:* ***BFZ***
OI =	*OI= Organization Identity: UID according to UID register, e.g.:* ***CHE-123.456.789***
C =	*C= Country: Fixed entry:* ***CH***
Distinguished name for system certificates	
CN =	*CN= Common Name: System Name, e.g.:* ***TUSER-SYSP-SCPP123***
OU =	*OU= Organizational unit: Freely selectable, e.g. department, division, etc...* *Example:* ***Federal Office for Future Studies (BFZ)-Office Automation***
O =	*O= Organization: Fixed entry:* ***Admin***
OI =	*OI= Organization Identity: UID according to UID register, e.g.:* ***CHE-123.456.789***
C =	*C= Country: Fixed entry:* ***CH***
Distinguished Name for organization certificates*	
CN =	*CN= Common Name: official designation (according to the UID register), or official translation thereof.* *Example:* ***Federal Office for Futurology (BFZ)***
OU =	*OU= Organizational unit: Freely selectable, e.g. department, division, etc...* *Example:* ***Office automation***
O =	*O= Organization: freely selectable, e.g.* ***Swiss Confederation*** *or* ***BFZ***
OI =	*OI= Organization Identity: UID according to UID register, e.g.:* ***CHE-123.456.789***
C =	*C= Country: Fixed entry:* ***CH*** *(open for Org Cert. with Auth/Sign/Enc function, but not recommended)*

Validity

Class C Standard Certificates of the Swiss Government PKI are valid for a maximum of 3 years.