Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT
Swiss Government PKI

Salvatore Tomasulo, 25.01.2016

Quick Guide für LRA-Officer der Klasse C

Handbuch für das **Certificate Request Wizard**

Projektname: Schulung LRA-Officer der Klasse C
Projektnummer:
Version: 1.0

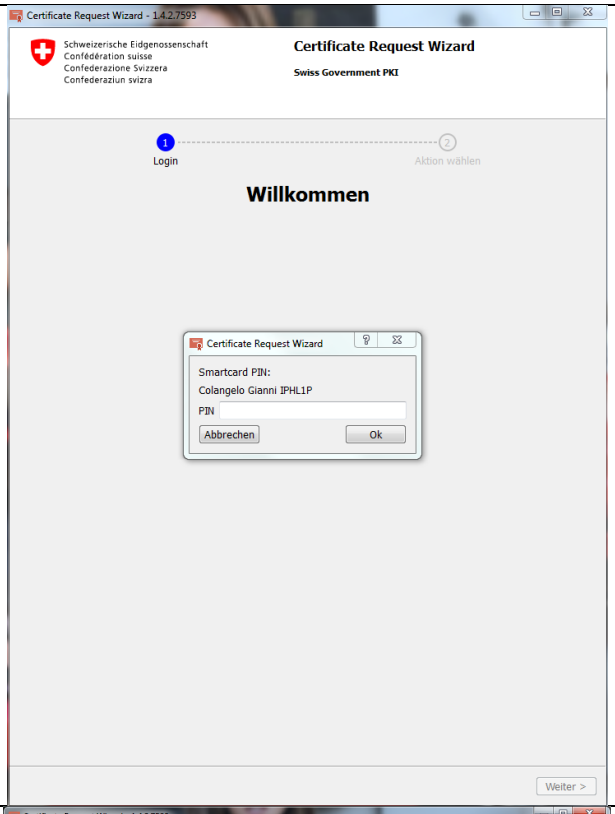
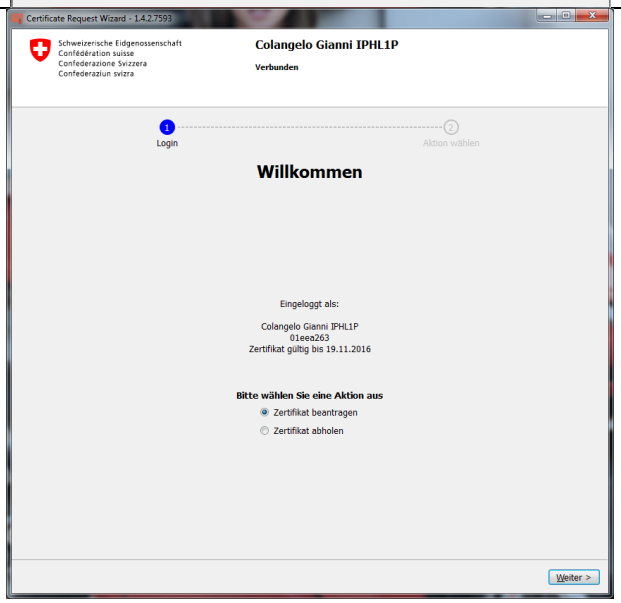
Status: in Arbeit [ ] in Prüfung [ ] genehmigt zur Nutzung [x]

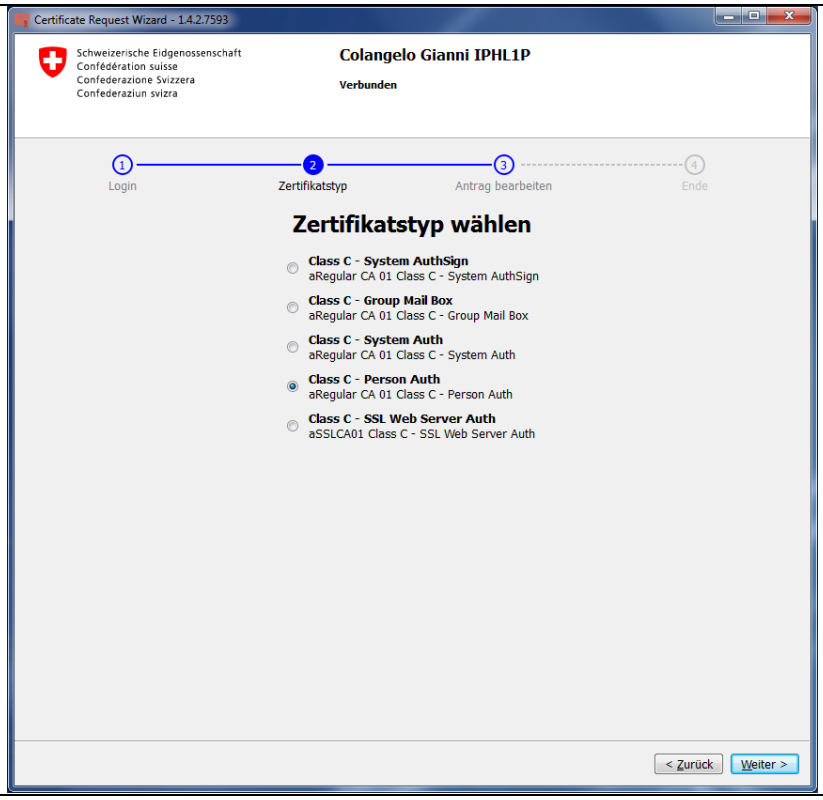
Beteiligter Personenkreis	
Autor:	Beatrice Metaj, Salvatore Tomasulo
Bearbeitung:	Beatrice Metaj / Gianni Colangelo
Prüfung:	Gianni Colangelo
Genehmigung:	Beatrice Metaj
Verteiler:	LRA-Officer der Klasse C

Änderungskontrolle, Prüfung, Genehmigung			
Wann:	**Version**:	**Wer:**	**Beschreibung:**
18.09.2015	0.1	Beatrice Metaj	Initialversion
25.01.2016	1.0	Salvatore Tomasulo	Policy hinzugefügt
09.02.2016	1.0	Beatrice Metaj	Kleinere Korr. und Freigabe

Inhaltsverzeichnis

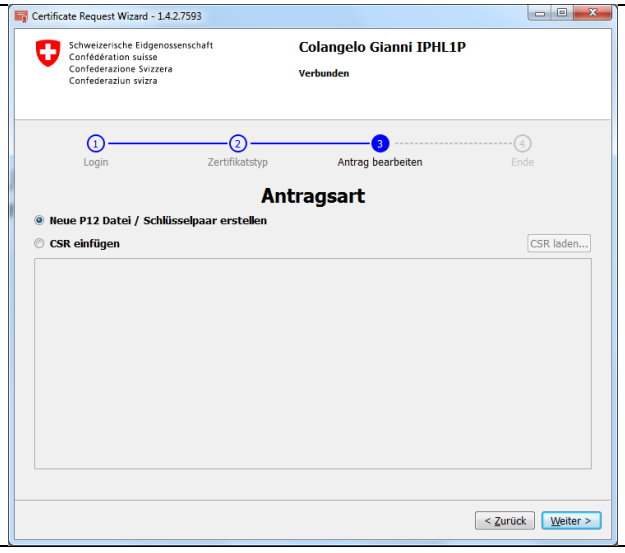
1 Certificate Request Wizard (CRW)

Starten Sie den CRW mittels des **Icons** auf der Taskleiste.	
Nach dem Start kommen Sie zum Willkommensscreen. Geben Sie hier die PIN Ihres berechtigten Zertifikates ein.	
Klicken Sie auf „Zertifikat beantragen“ und fahren Sie mit der „Weiter“-Taste fort	

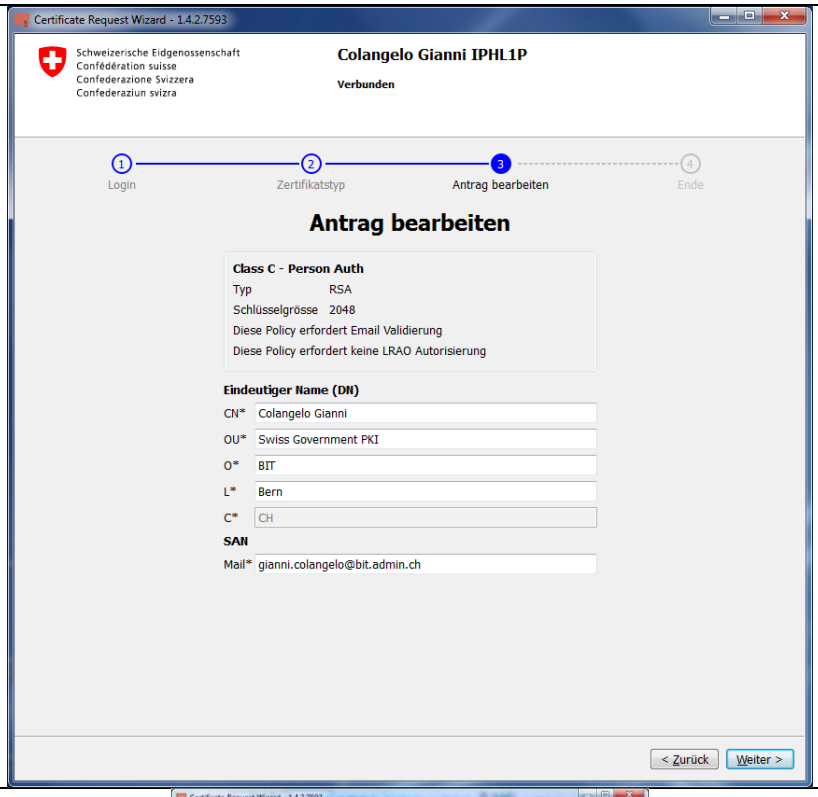
Wählen Sie die gewünschte Policy (je nach Berechtigungen können mehrere zur Auswahl stehen), und klicken Sie auf „Weiter“.	

1.1 Variante 1: P12 ausstellen (Schlüsselpaar und Zertifikat)

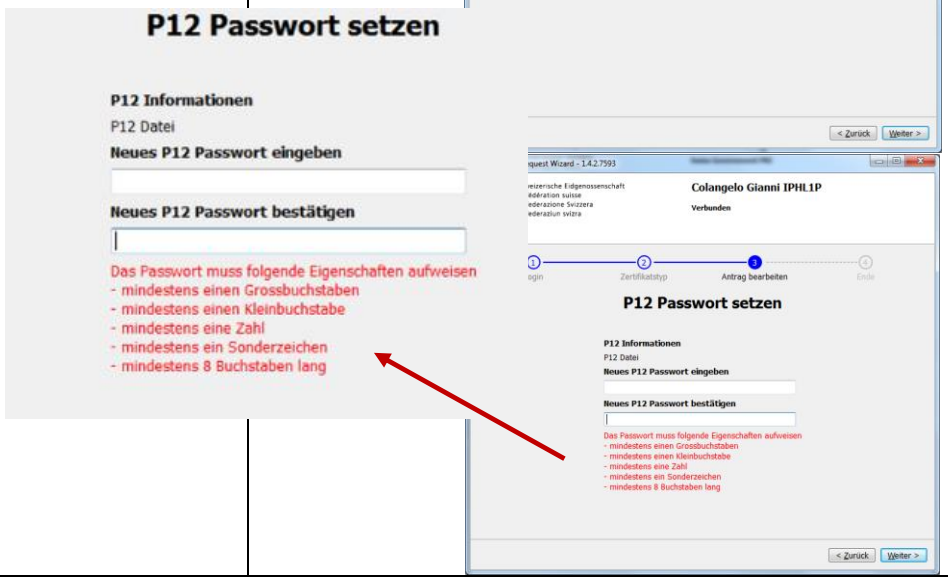
Bei diesem Vorgang erstellt das Tool automatisch ein Certificate Server Request (CSR), das online versendet wird. Das Resultat sind die beiden Schlüssel und das Zertifikate in einem P12 –File.

Klicken Sie auf *Neue P12 Datei/ Schlüsselpaar erstellen.* Und fahren Sie mit „Weiter“ fort.	

Je nach ausgewählter Policy sind verschiedene Felder auszufüllen (**siehe Kapitel 4**) Diese sind jeweils „weiss“. Füllen Sie die nötigen Felder aus und klicken Sie danach auf „Weiter“.



Geben Sie ein Passwort für Ihr P12-File ein. Die Richtlinien für das Passwort werden angezeigt, wenn das Passwort diese nicht erfüllt.

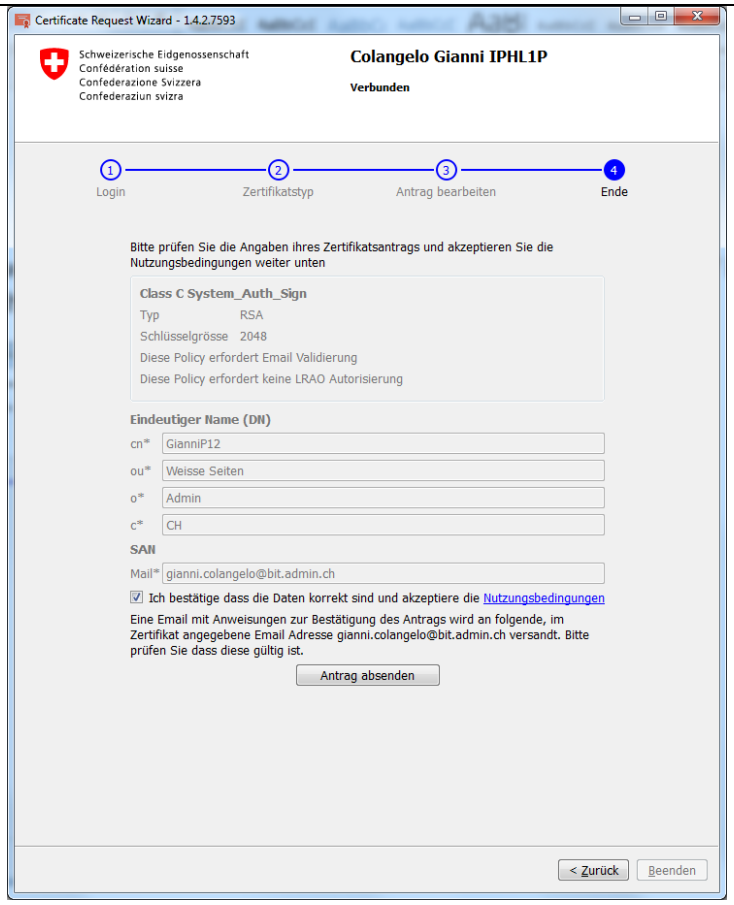


1. Kontrollieren Sie Ihre Angaben.
2. Setzen Sie das Häkchen bei der Bestätigung. (Lesen Sie die Nutzungsbedingungen)
3. Schicken Sie den Antrag ab.

Sie erhalten Ihre P12 Datei per Mail zugestellt.

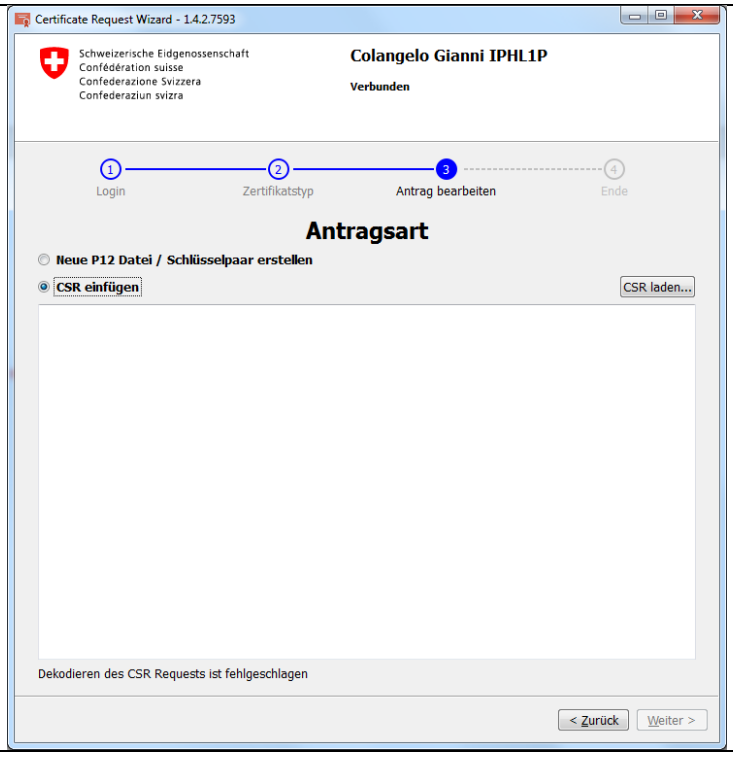
Stellen Sie sicher, dass Sie die Schlüssel an einem sicheren Ort aufbewahren und allenfalls für eine Wiederinstallation des Zertifikates, für die Dauer der Gültigkeit archivieren.

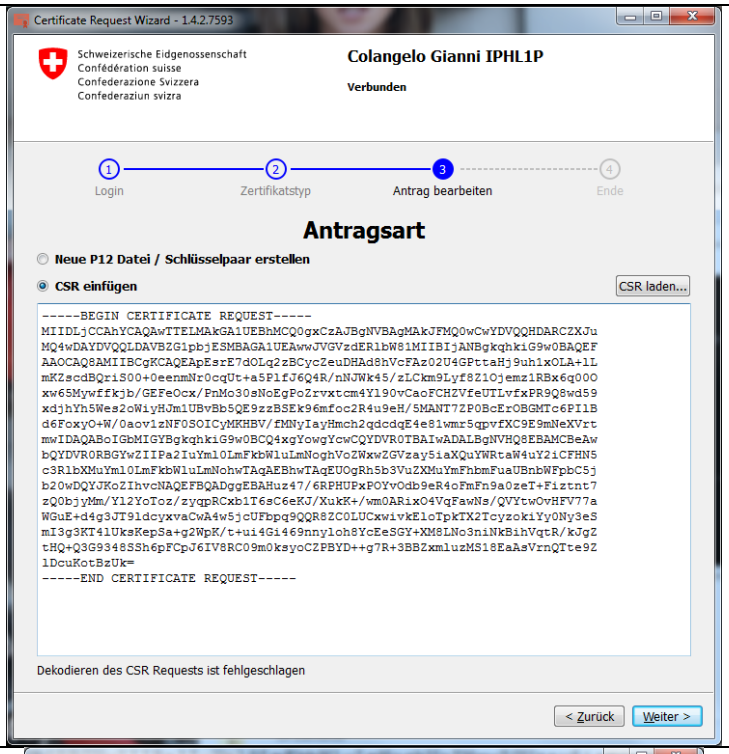
Holen Sie Ihr Zertifikat wie in Kap. 2 beschrieben ab.

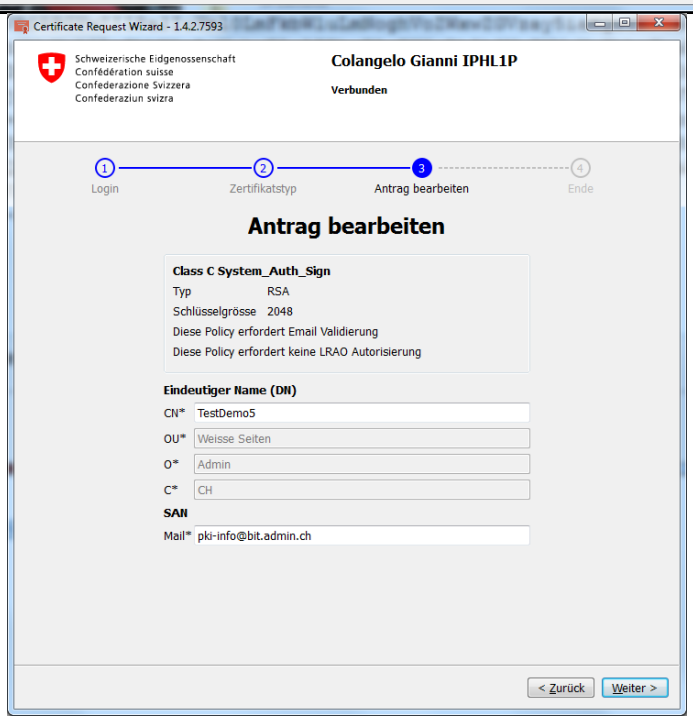


1.2 Variante 2: CSR uploaden

Klicken Sie auf *CSR einfügen.*
Laden Sie das CSR aus einer Datei mit dem Knopf oben rechts, oder kopieren Sie den Text des CSRs direkt in das freie Feld. Fahren Sie mit „Weiter“ fort.



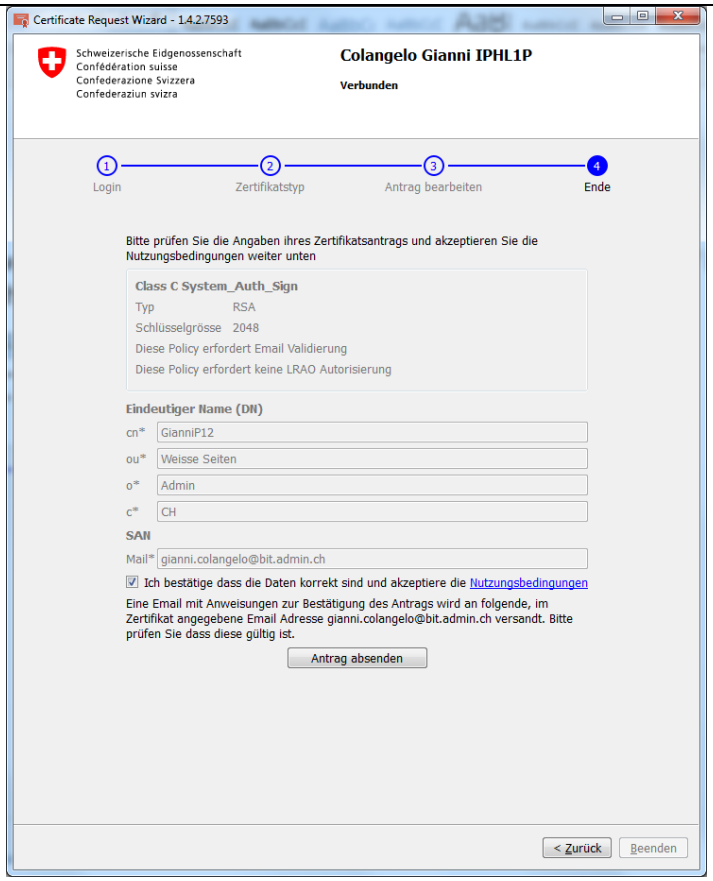
<table>
<tr>
<td></td>
<td> 
</td>
</tr>
<tr>
<td>Überprüfen Sie die Angaben und klicken Sie auf „Weiter“.

Sie haben die Möglichkeit hier noch Ihre Angaben zu ändern.</td>
<td> 
</td>
</tr>
</table>

1. Kontrollieren Sie Ihre Eingaben.
2. Setzen Sie das Häkchen bei der Bestätigung.

(Lesen Sie die Nutzungsbedingungen)

3. Schicken Sie den Antrag ab.



Sie erhalten Ihre Zertifikats-Datei per Mail zugestellt.

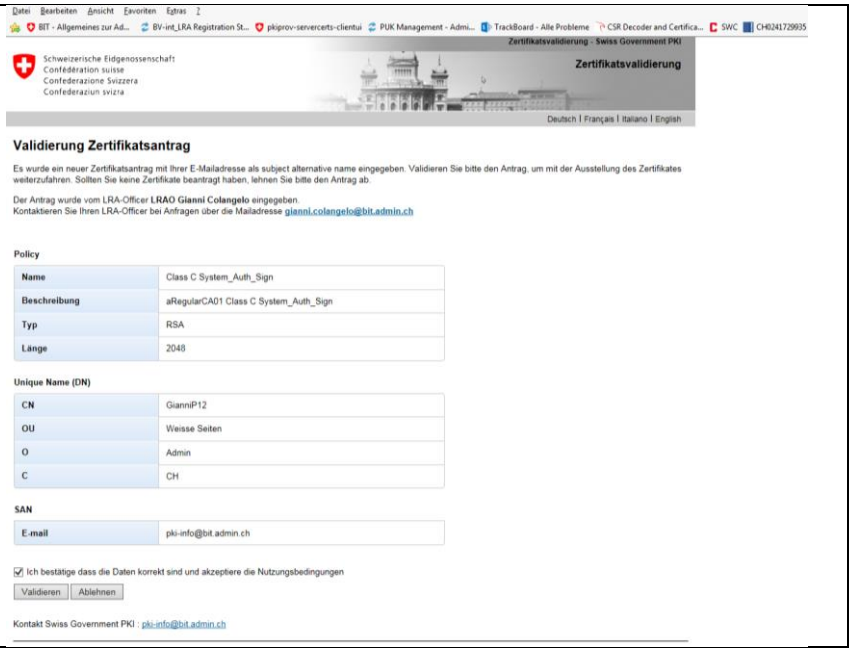
Stellen Sie sicher, dass Sie das Zertifikat an einem sicheren Ort aufbewahren und es allenfalls für eine Wiederinstallation, für die Dauer der Gültigkeit archivieren.
Holen Sie Ihr Zertifikat wie in Kap. 2 beschrieben ab.

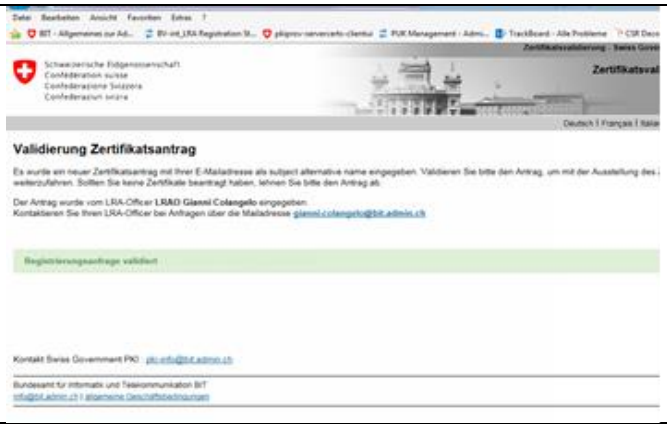
2 Zertifikate validieren/ablehnen

Die eingetragene E-Mail Adresse erhält eine E-Mail mit einem Link. Klicken Sie auf diesen Link um auf folgende Seite zu kommen.

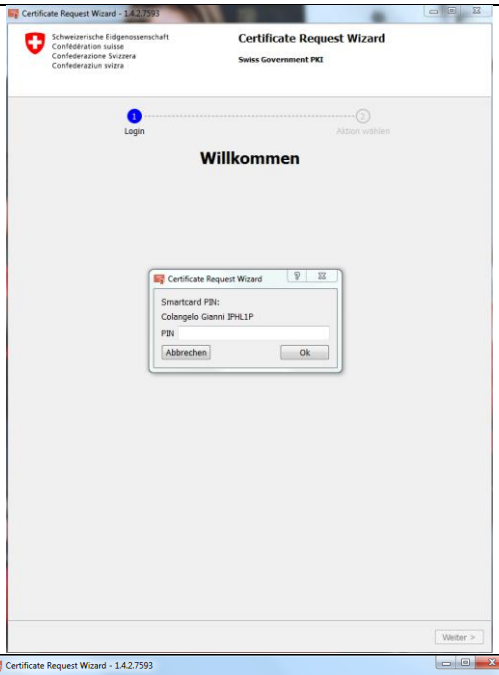
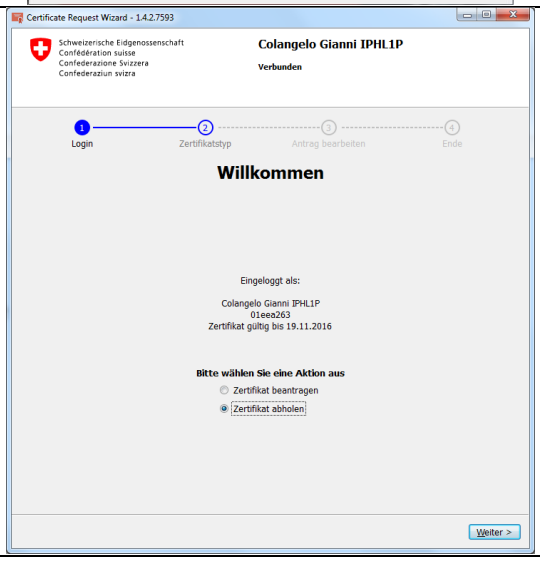
Kontrollieren Sie alle Angaben und setzen Sie das Häkchen beim Bestätigungstext.

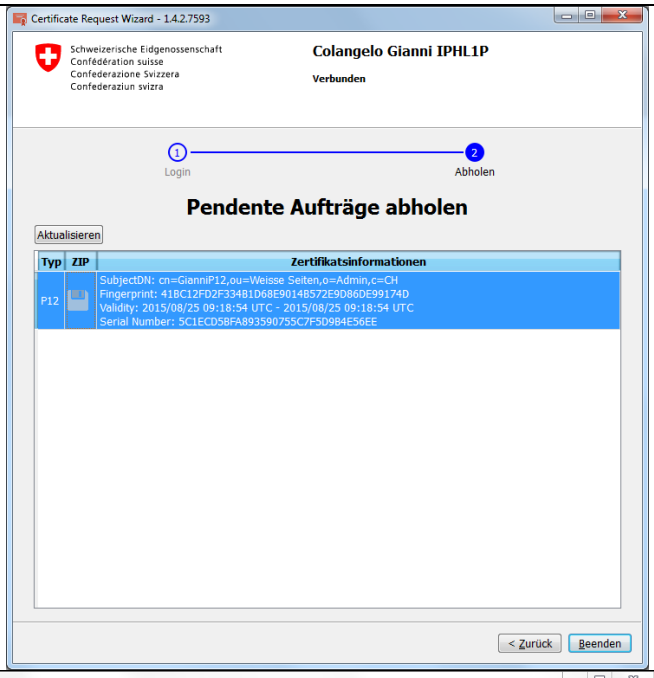
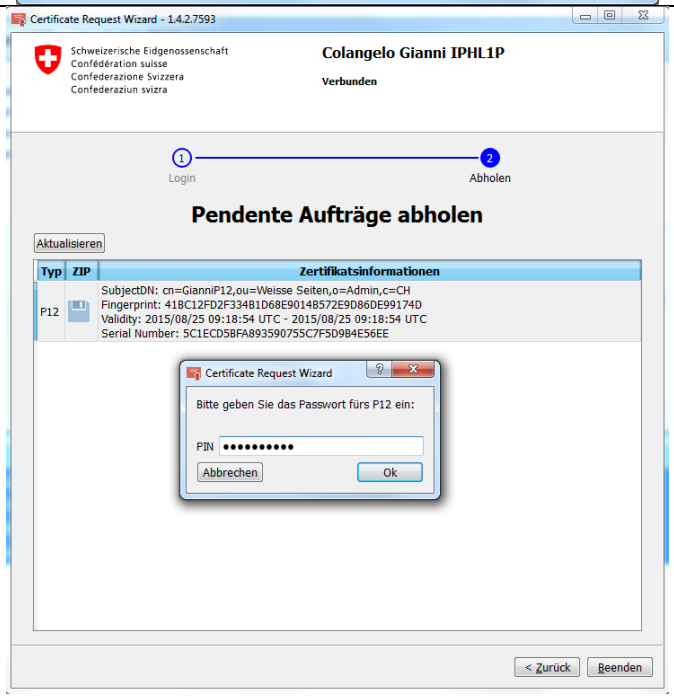
Klicken Sie bei korrekten Angaben auf „Validieren“; andernfalls auf „Ablehnen.



Ihre Entscheidung wird in beiden Fällen bestätigt. (Hier Bsp. Mit Validierung).	

3 Zertifikate abholen

Starten Sie das CRW und loggen Sie sich gemäss Kap.1 ein.	
Klicken Sie auf *Zertifikat abholen* und danach auf „Weiter“.	

Klicken Sie auf „aktualisieren“. Wählen Sie das gewünschte Zertifikat aus und klicken Sie danach auf das Diskettensymbol um das Zertifikate herunter zu laden.	
Sie werden nach dem Passwort des privaten Schlüssels gefragt, falls Sie die Variante P12 gewählt haben. Fügen Sie den in die Zeile ein. (Achtung: Hier ist NICHT der Smartcard-PIN gemeint!). Bestimmen Sie danach den Speicherort Ihrer Datei. Falls die „CSR-einfügen“-Variante gewählt wurde, wird beim herunterlanden kein Passwort verlangt. In der ZIP-Datei ist auch keine P12-Datei des Zertifikats vorhanden. Beenden Sie danach den CRW.	

4 Policy

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

Distinguished Name für Personenzertifikate	
CN =	*CN= Common Name: Nachname(n) Vorname(n), Bsp.:* ***Mustermeier Hanspeter***
OU =	*OU= Organisationseinheit: Frei wählbar, z.B. Amt, Abteilung, Bereich, etc…* *Bsp.:* ***Bundesamt für Zukunftsforschung (BFZ)-Büroautomation***
O =	*O= Organisation: Auswählbar, zw. Administrative Einheit oder „Swiss Government PKI“* *Bsp.:* ***BFZ – Büroautomation*** *oder* ***Swiss Government PKI***
L =	*L= Location: Ort der Organisation, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH***
Distinguished Name für Systemzertifikate	
CN =	*CN= Common Name: System Name, Bsp.:* ***TUSER-SYSP-SCPP123***
OU =	*OU= Systemplattformname: Bsp.:* ***Systemplattform eDokumente***
O =	*O= Organisation: Fixer Eintrag:* ***Admin***
C =	*C= Country: Fixer Eintrag:* ***CH***
Distinguished Name für Organisationszertifikate	
CN =	*CN= Common Name: Amtsbezeichnung gemäss UID-Register, oder offizielle Übersetzung davon.* *Bsp.:* ***Bundesamt für Zukunftsforschung (BFZ)***
OU =	*OU= Organisationseinheit: Frei wählbar, z.B. UID gemäss UID-Register, Abteilung, Bereich, etc…* *Bsp.:* ***CHE-123.456.789*** *oder* ***Büroautomation***
O =	*O= Organisation: Frei wählbar, Bsp.:* ***Schweizerische Eidgenossenschaft*** *oder* ***BFZ – Büroautomation***
L =	*L= Location: Ort der Organisation, gegebenenfalls gemäss UID-Register, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH***
Distinguished Name für Gruppenmailboxzertifikate	
CN =	*CN= Common Name: Displayname der Gruppenmailbox: Bsp.:* ***_BIT-PKI-Info***
OU =	*OU= Organisationseinheit: Fixer Eintrag:* ***Group Mailboxes***
OU =	*OU= Organisationseinheit: Fixer Eintrag:* ***eGov-Services***
O =	*O= Organisation: Frei wählbar, Bsp.:* ***Schweizerische Eidgenossenschaft*** *oder* ***BFZ – Büroautomation***
L =	*L= Location: Ort der Organisation, Bsp.:* ***Bern (BE)***
C =	*C= Country: Fixer Eintrag:* ***CH***

Gültigkeit

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