



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

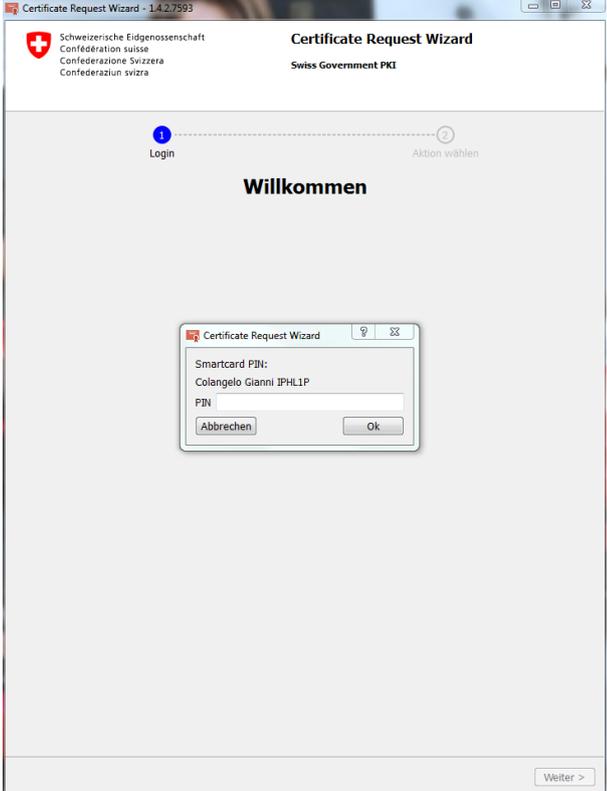
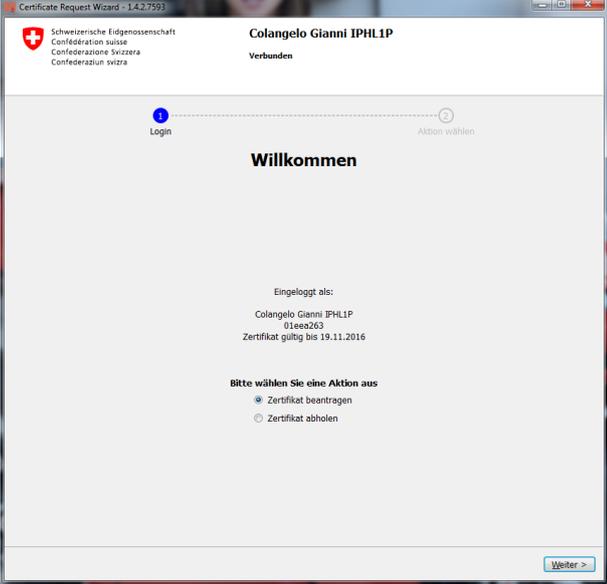
| Beteiligter Personenkreis | |
|---------------------------|------------------------------------|
| Autor: | Beatrice Metaj, Salvatore Tomasulo |
| Bearbeitung: | Beatrice Metaj / Gianni Colangelo |
| Prüfung: | Gianni Colangelo |
| Genehmigung: | Beatrice Metaj |
| Verteiler: | LRA-Officer der Klasse 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) | 3 |
| 1.1 | Variante 1: P12 ausstellen (Schlüsselpaar und Zertifikat)..... | 4 |
| 1.2 | Variante 2: CSR uploaden | 6 |
| 2 | Zertifikate validieren/ablehnen | 8 |
| 3 | Zertifikate abholen | 9 |
| 4 | Policy | 11 |

1 Certificate Request Wizard (CRW)

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

Quick Guide für LRA-Officer der Klasse B

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

The screenshot shows the 'Certificate Request Wizard' window for user 'Colangelo Gianni IPHLIP'. The progress bar indicates the current step is 'Zertifikatstyp' (2). The main content area is titled 'Zertifikatstyp wählen' and lists several certificate classes with radio buttons:

- Class C - System AuthSign
aRegular CA 01 Class C - System AuthSign
- Class C - Group Mail Box
aRegular CA 01 Class C - Group Mail Box
- Class C - System Auth
aRegular CA 01 Class C - System Auth
- Class C - Person Auth
aRegular CA 01 Class C - Person Auth
- Class C - SSL Web Server Auth
aSSLCA01 Class C - SSL Web Server Auth

At the bottom right, there are buttons for '< Zurück' and 'Weiter >'. The window title is 'Certificate Request Wizard - 1.4.2.7593'.

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.

The screenshot shows the 'Certificate Request Wizard' window for user 'Colangelo Gianni IPHLIP'. The progress bar indicates the current step is 'Antrag bearbeiten' (3). The main content area is titled 'Antragsart' and has two radio button options:

- Neue P12 Datei / Schlüsselpaar erstellen
- CSR einfügen

Next to the 'CSR einfügen' option is a button labeled 'CSR laden...'. Below the options is a large empty text area. At the bottom right, there are buttons for '< Zurück' and 'Weiter >'. The window title is 'Certificate Request Wizard - 1.4.2.7593'.

Quick Guide für LRA-Officer der Klasse B

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“.

The screenshot shows the 'Antrag bearbeiten' (Edit Request) step of the Certificate Request Wizard. The user is logged in as Colangelo Gianni IPHL1P. The wizard is currently on step 3 of 4. The selected policy is 'Class C - Person Auth' with RSA key size 2048. The unique name (DN) fields are filled as follows: CN* Colangelo Gianni, OU* Swiss Government PKI, O* BIT, L* Bern, C* CH, and SAN Mail* gianni.colangelo@bit.admin.ch. There are '< Zurück' and 'Weiter >' buttons at the bottom.

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

The screenshot shows the 'P12 Passwort setzen' (Set P12 Password) step of the Certificate Request Wizard. The user is logged in as Colangelo Gianni IPHL1P. The wizard is currently on step 3 of 4. The 'P12 Informationen' section shows 'P12 Datei' and two input fields for 'Neues P12 Passwort eingeben' and 'Neues P12 Passwort bestätigen'. A red error message is displayed below the input fields: 'Das Passwort muss folgende Eigenschaften aufweisen: - mindestens einen Grossbuchstaben, - mindestens einen Kleinbuchstabe, - mindestens eine Zahl, - mindestens ein Sonderzeichen, - mindestens 8 Buchstaben lang'. There are '< Zurück' and 'Weiter >' buttons at the bottom.

P12 Passwort setzen

P12 Informationen

P12 Datei

Neues P12 Passwort eingeben

Neues P12 Passwort bestätigen

Das Passwort muss folgende Eigenschaften aufweisen

- mindestens einen Grossbuchstaben
- mindestens einen Kleinbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen
- mindestens 8 Buchstaben lang



Quick Guide für LRA-Officer der Klasse B

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.

Certificate Request Wizard - 1.4.2.7593

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Colangelo Gianni IPHL1P
Verbunden

1 Login 2 Zertifikatstyp 3 **Antrag bearbeiten** 4 Ende

Bitte prüfen Sie die Angaben Ihres Zertifikatsantrags und akzeptieren Sie die Nutzungsbedingungen weiter unten

Class C System_Auth_Sign
Typ RSA
Schlüsselgröße 2048
Diese Policy erfordert Email Validierung
Diese Policy erfordert keine LRAO Autorisierung

Eindeutiger Name (DN)

cn* GianniP12
ou* Weisse Seiten
o* Admin
c* CH

SAN
Mail* gianni.colangelo@bit.admin.ch

Ich bestätige dass die Daten korrekt sind und akzeptiere die [Nutzungsbedingungen](#)

Eine Email mit Anweisungen zur Bestätigung des Antrags wird an folgende, im Zertifikat angegebene Email Adresse gianni.colangelo@bit.admin.ch versandt. Bitte prüfen Sie dass diese gültig ist.

Antrag absenden

< Zurück Beenden

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.

Certificate Request Wizard - 1.4.2.7593

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Colangelo Gianni IPHL1P
Verbunden

1 Login 2 Zertifikatstyp 3 **Antrag bearbeiten** 4 Ende

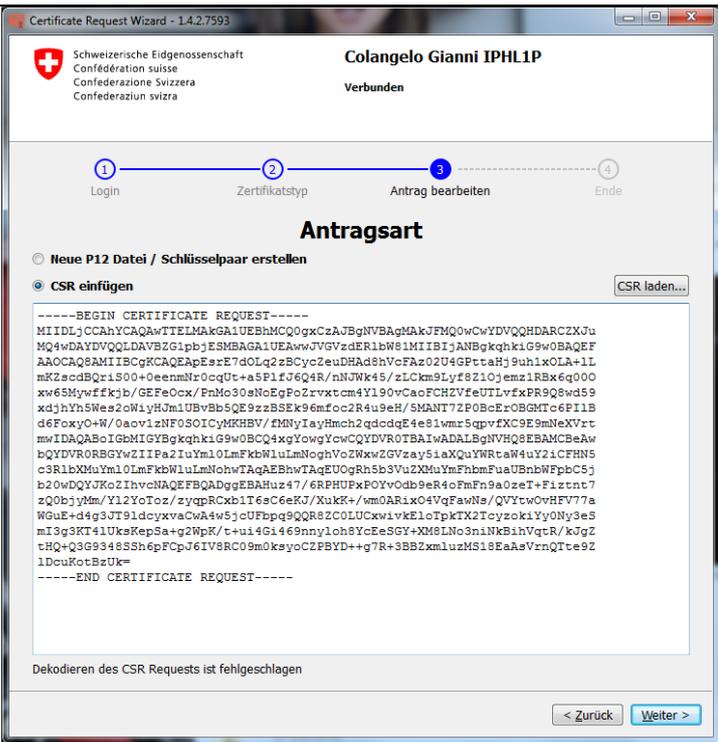
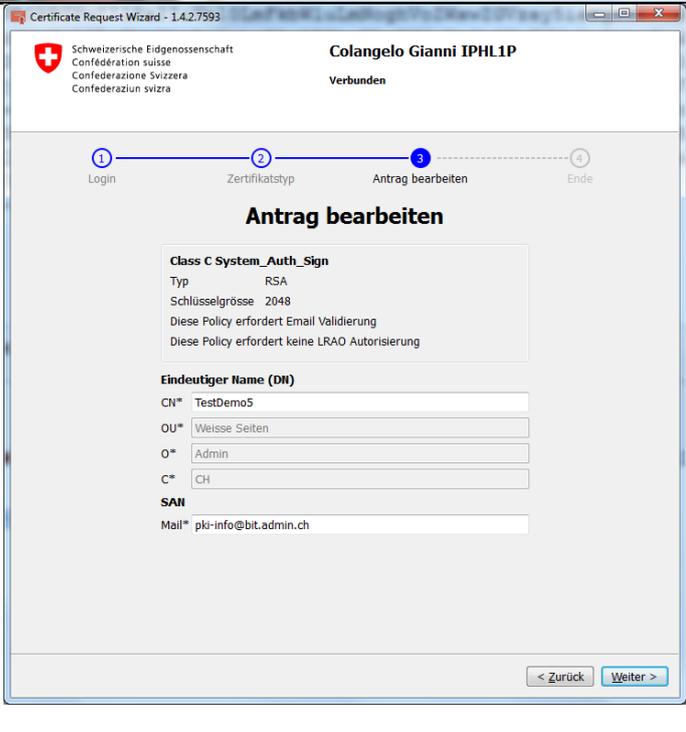
Antragsart

Neue P12 Datei / Schlüsselpaar erstellen
 CSR einfügen

Dekodieren des CSR Requests ist fehlgeschlagen

< Zurück Weiter >

Quick Guide für LRA-Officer der Klasse B

| | |
|--|---|
| |  |
| <p>Überprüfen Sie die Angaben und klicken Sie auf „Weiter“.</p> <p>Sie haben die Möglichkeit hier noch Ihre Angaben zu ändern.</p> |  |

Quick Guide für LRA-Officer der Klasse B

1. Kontrollieren Sie Ihre Eingaben.
2. Setzen Sie das Häkchen bei der Bestätigung.
3. Schicken Sie den Antrag ab.

(Lesen Sie die Nutzungsbedingungen)

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“.

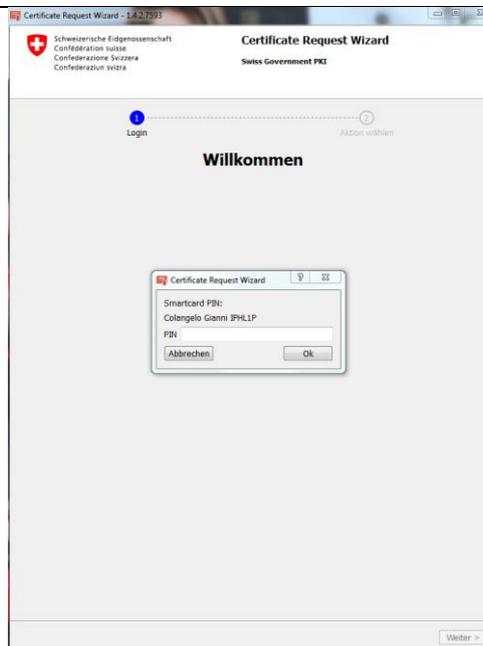
Quick Guide für LRA-Officer der Klasse B

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

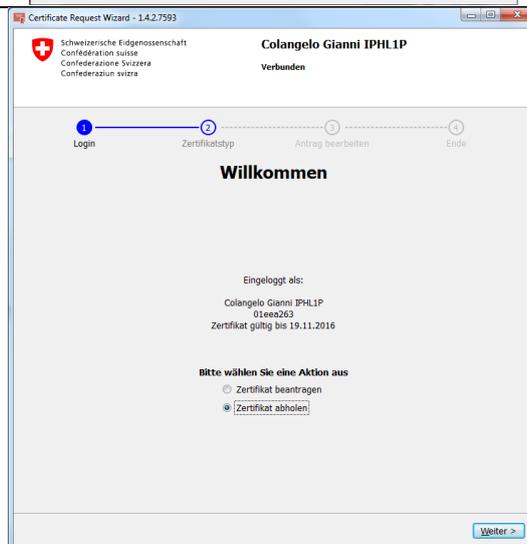


3 Zertifikate abholen

Starten Sie das CRW und loggen Sie sich gemäss Kap.1 ein.



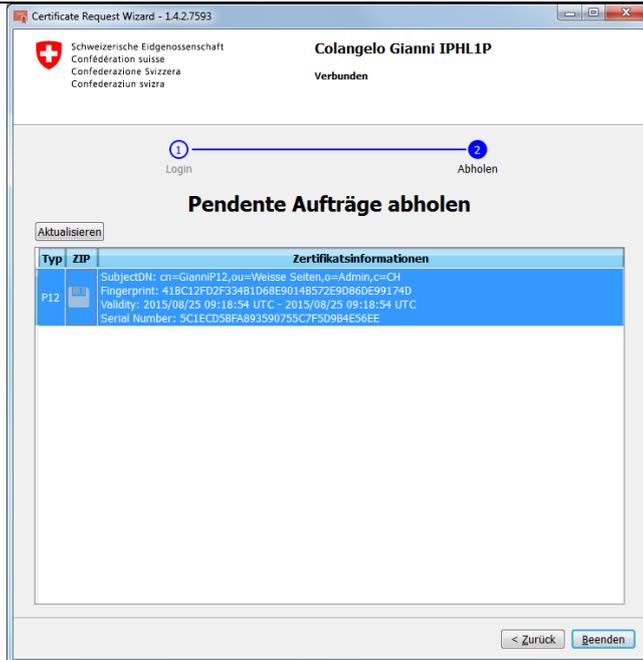
Klicken Sie auf *Zertifikat abholen* und danach auf „Weiter“.



Quick Guide für LRA-Officer der Klasse B

Klicken Sie auf „aktualisieren“.

Wählen Sie das gewünschte Zertifikat aus und klicken Sie danach auf das Diskettensymbol um das Zertifikate herunter zu laden.

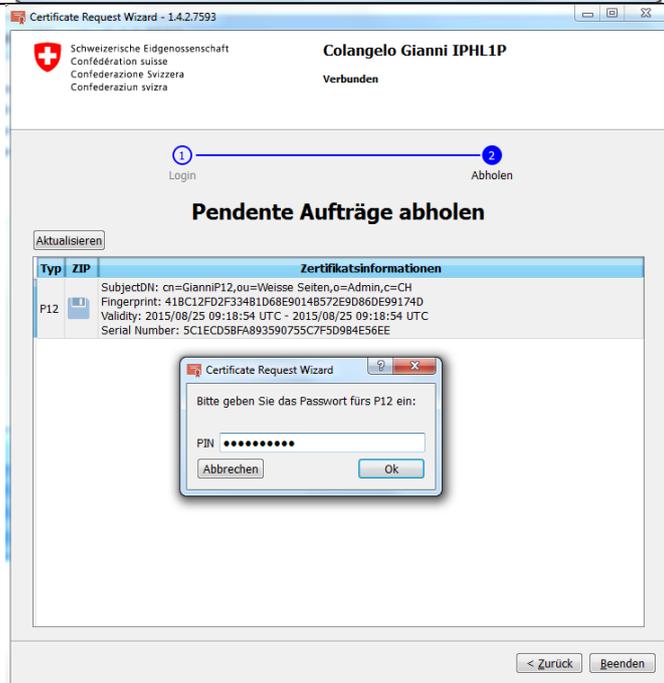


Sie werden nach dem Passwort des privaten Schlüssels gefragt, falls Sie die Variante P12 gewählt haben. Fügen Sie den in die Zeile ein. (Achtung: Hier ist NICHT der Smartcard-PIN gemeint!).

Bestimmen Sie danach den Speicherort Ihrer Datei.

Falls die „CSR-einfügen“-Variante gewählt wurde, wird beim herunterladen 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: <i>Frei wählbar</i> , z.B. Amt, Abteilung, Bereich, etc... Bsp.: Bundesamt für Zukunftsforschung (BFZ)-Büroautomation |
| o = | O= Organisation: <i>Auswählbar</i> , 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: <i>Fixer Eintrag</i> : CH |
| Distinguished Name für Systemzertifikate | |
| cn = | CN= Common Name: System Name, Bsp.: TUSER-SYSP-SCPP123 |
| ou = | OU= Systemplattformname: Bsp.: Systemplattform eDokumente |
| o = | O= Organisation: <i>Fixer Eintrag</i> : Admin |
| c = | C= Country: <i>Fixer Eintrag</i> : 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: <i>Frei wählbar</i> , z.B. UID gemäss UID-Register, Abteilung, Bereich, etc... Bsp.: CHE-123.456.789 oder Büroautomation |
| o = | O= Organisation: <i>Frei wählbar</i> , Bsp.: Schweizerische Eidgenossenschaft oder BFZ – Büroautomation |
| l = | L= Location: Ort der Organisation, gegebenenfalls gemäss UID-Register, Bsp.: Bern (BE) |
| c = | C= Country: <i>Fixer Eintrag</i> : CH |
| Distinguished Name für Gruppenmailboxzertifikate | |
| cn = | CN= Common Name: Displayname der Gruppenmailbox: Bsp.: _BIT-PKI-Info |
| ou = | OU= Organisationseinheit: <i>Fixer Eintrag</i> : Group Mailboxes |
| ou = | OU= Organisationseinheit: <i>Fixer Eintrag</i> : eGov-Services |
| o = | O= Organisation: <i>Frei wählbar</i> , Bsp.: Schweizerische Eidgenossenschaft oder BFZ – Büroautomation |
| l = | L= Location: Ort der Organisation, Bsp.: Bern (BE) |
| c = | C= Country: <i>Fixer Eintrag</i> : CH |

Gültigkeit

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