



19.07.2024

## Guida rapida

# Certificate Request Wizard (CRW)

**Stato:** rilasciato

V1.2

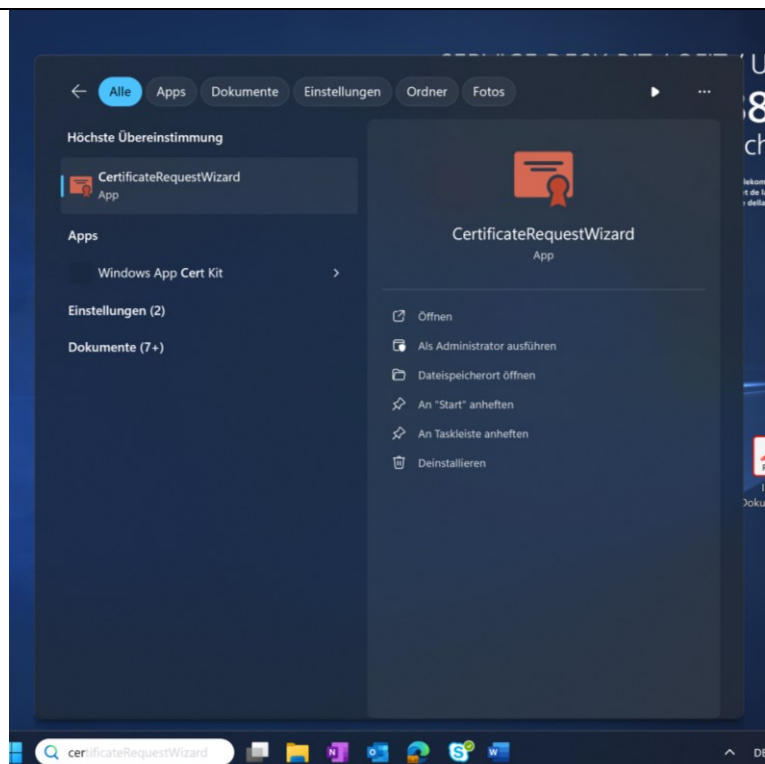


Il CRW è uno strumento autonomo che viene installato su un client BAB. Con il CRW, una persona può generare localmente richieste di firma di certificati (CSR) per i certificati per i quali è stata autorizzata. Il CRW invia quindi i file CSR automaticamente alla Swiss Government PKI (SG-PKI). Quest'ultima fa verificare e confermare i dati registrati dalla persona destinataria del certificato indicato nell'indirizzo e-mail della richiesta. Il certificato viene quindi emesso e può essere ritirato dalla persona richiedente e inoltrato alla persona destinataria del certificato.

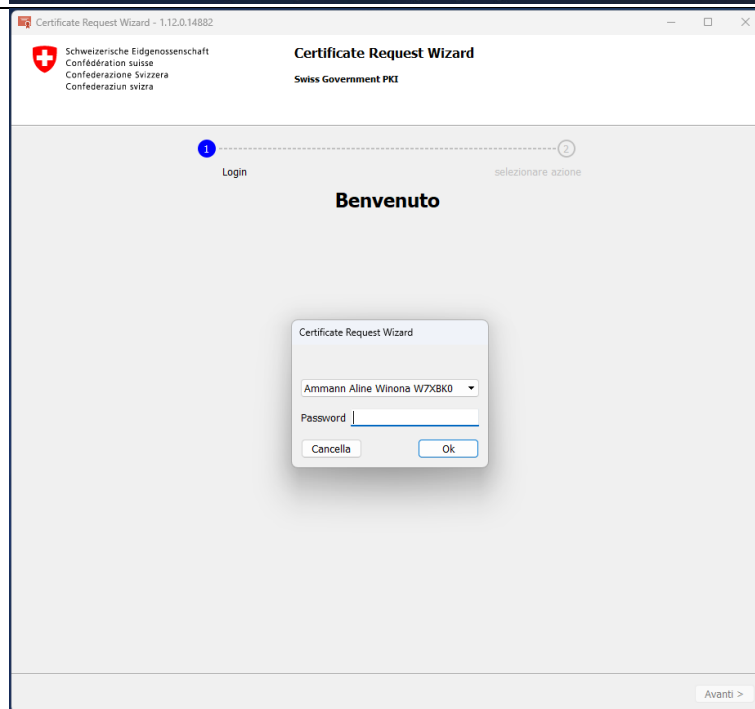
In alternativa alla creazione di un CRS mediante il wizard, è possibile copiare un file CSR già pronto nello strumento (CRW) e inviarlo come richiesta.

## Certificato di registrazione

Avviare l'applicazione CRW.



Dopo aver avviato l'applicazione, appare una finestra di login. Inserire qui il PIN del proprio certificato autorizzato di classe B e confermare con "OK".



Fare clic su "Registrare certificato" e continuare con il pulsante "Avanti".

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Ammann Aline Winona W7XBK0  
Connesso

1 Login 2 selezionare azione

**Benvenuto**

Collegato come:  
Ammann Aline Winona W7XBK0  
82F79B61C6BF19F8  
Smartcard valida fino al 24.01.2027

Selezionate la vostra azione e cliccate su Avanti

☒ Registrare certificato  
☐ Prelevare certificato

Avanti >

Selezionare la politica desiderata (a seconda delle autorizzazioni, possono essercene diverse tra cui scegliere) e fare clic su "Avanti".

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Ammann Aline Winona W7XBK0  
Connesso

1 Login 2 Selezionare direttiva 3 Prelevare informazioni 4 Trasmettere

**Selezionare tipo certificato**

☐ Class A - q DSig - HSM  
Regulated CA02 ZertES - qcp-n-hsm

☐ Class C (RegularCA02) - Organisation DSig BIT  
Class C (RegularCA02) - Organisation DSig BIT - runtime policy

☐ Class C (RegularCA02) - System Auth BIT  
Class C (RegularCA02) - System Auth BIT - runtime policy

☐ Class C (RegularCA02) - System Enc BIT  
Class C (RegularCA02) - System Enc BIT - runtime Policy

☒ Class C (RegularCA02) - Person Auth BIT  
Class C (RegularCA02) - Person Auth BIT

< Indietro Avanti >

**Variante 1: emissione di P12 (coppia di chiavi e certificato)**

Durante questo processo, lo strumento crea automaticamente una Certificate Signing Request (CSR), che viene inviata online. Il risultato è costituito dalle due chiavi e dal certificato in un file P12.

Selezionare l'opzione "Generare un nuovo file P12 / coppia di chiavi" e proseguire con "Avanti".

A seconda della policy selezionata, i campi del Distinguished Name (DN) devono essere compilati in modo diverso. Le voci fisse sono ombreggiate e non possono essere modificate. Compilare i campi richiesti (vedere la sezione policy) e fare clic su "Avanti".

Inserire una password per il file P12. Le linee guida per la password vengono visualizzate se l'immissione non le soddisfa. Quindi premere "Avanti".

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Ammann Aline Winona W7XBK0**  
Connesso

1 Login 2 Selezionare direttiva 3 **Assegnare password container PKCS #12** 4 Trasmettere

**Assegnare password container PKCS #12**

PKCS #12 information  
File P12  
Inserire nuova password  
.....  
Confermare nuova password  
.....

PKCS #12 information  
File P12  
Inserire nuova password  
.....  
Confermare nuova password  
.....

La password deve contenere

- carattere maiuscolo
- carattere minuscolo
- numero
- carattere speciale
- lunghezza minima di 8 caratteri

< Indietro Avanti >

Controllare i dettagli. Spuntare la casella di conferma (leggere le condizioni d'uso).

Inviare la domanda e premere il pulsante "Terminare".

La persona che ha inviato la richiesta può ora eseguire la convalida dell'e-mail, se richiesto dalla politica.

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Ammann Aline Winona W7XBK0**  
Connesso

1 Login 2 Selezionare direttiva 3 Prelevare informazioni 4 **Trasmettere**

Si prega di controllare i dati nella richiesta e accettare i termini e le condizioni in seguito

Class C - Person Auth CA02  
tipo RSA  
Lunghezza chiave 2048  
Questa direttiva non richiede la convalida tramite email utente  
Autorizzazione LRAO non necessaria

Distinguished name  
CN\* Aline Winona Ammann  
SN\* Ammann  
GN\* Aline Winona  
OU\* Swiss Government PKI  
O\* BIT  
OT\* CHE-221.032.573  
C\* CH

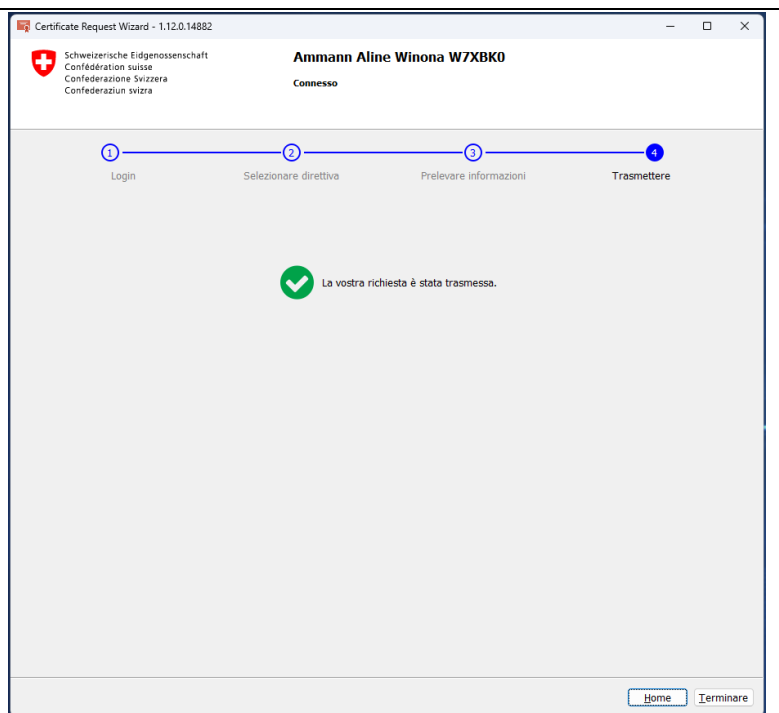
Subject alternative names  
Mail\* alinewinona.ammann@bit.admin.ch

☒ Ho verificato i dati e accetto i [Terms & Conditions](#)

Invia richiesta

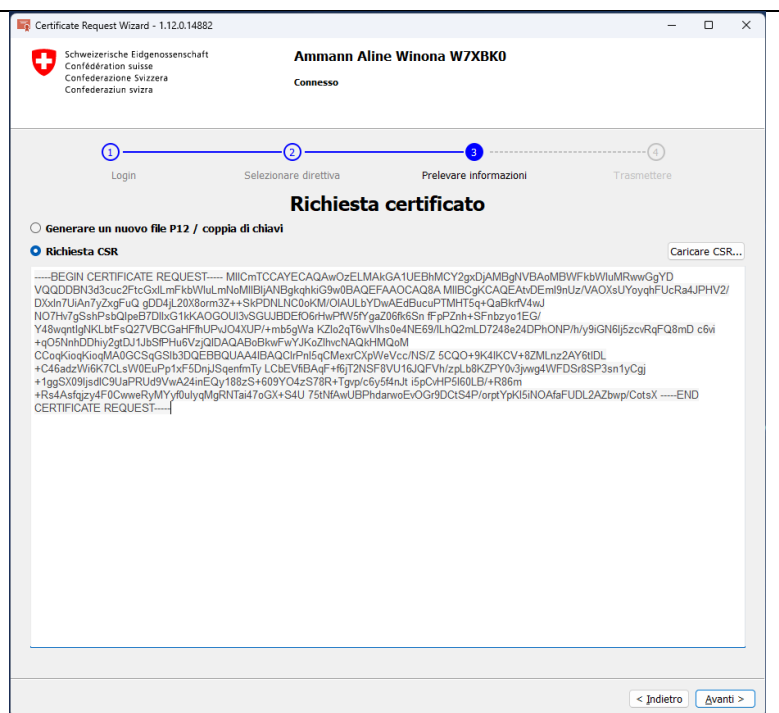
< Indietro Terminare

Il processo è ora completato. Il pulsante "Home" riporta direttamente alla pagina iniziale. Altrimenti, è possibile chiudere l'applicazione con il pulsante "Terminare".



## Variente 2: applicazione CSR

Selezionare l'opzione "Richiesta CSR". Caricare il CSR da un file utilizzando il pulsante "Carica CSR" oppure copiare il testo del CSR direttamente nel campo vuoto, come mostrato nell'esempio. Quindi fare clic su "Avanti".



I campi del Distinguished Name sono già compilati con il CSR. Verificare i dettagli rispetto alle specifiche della politica e apportare le modifiche necessarie. Le voci fisse sono ombreggiate e non possono essere modificate. Continuare quindi con “Avanti”.

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Ammann Aline Winona W7XBK0**  
Connesso

1 Login 2 Selezionare direttiva 3 Prelevare informazioni 4 Trasmettere

### Richiesta certificato

**Class C - System Auth CA02**  
tipo RSA  
Lunghezza chiave 2048  
Questa direttiva non richiede la convalida tramite email utente!  
Autorizzazione LRAO non necessaria

**Distinguished name**  
CN\* www.sample.admin.ch  
OU\* Swiss Government PKI  
O\* Admin  
OI\* CHE-221.032.573  
C\* CH

**Subject alternative names**  
Mail\* pkc-info@bit.admin.ch

< Indietro Avanti >

Controllare i dettagli. Spuntare la casella di conferma (leggere le condizioni d'uso).

Inviare la domanda e premere il pulsante “Terminare”.

La persona che ha inviato la richiesta può ora eseguire la convalida dell'e-mail, se richiesto dalla politica.

Certificate Request Wizard - 1.12.0.14882

Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Ammann Aline Winona W7XBK0**  
Connesso

1 Login 2 Selezionare direttiva 3 Prelevare informazioni 4 Trasmettere

Si prega di controllare i dati nella richiesta e accettare i termini e le condizioni in seguito

**Class C - System Auth CA02**  
tipo RSA  
Lunghezza chiave 2048  
Questa direttiva non richiede la convalida tramite email utente!  
Autorizzazione LRAO non necessaria

**Distinguished name**  
CN\* www.sample.admin.ch  
OU\* Swiss Government PKI  
O\* Admin  
OI\* CHE-221.032.573  
C\* CH

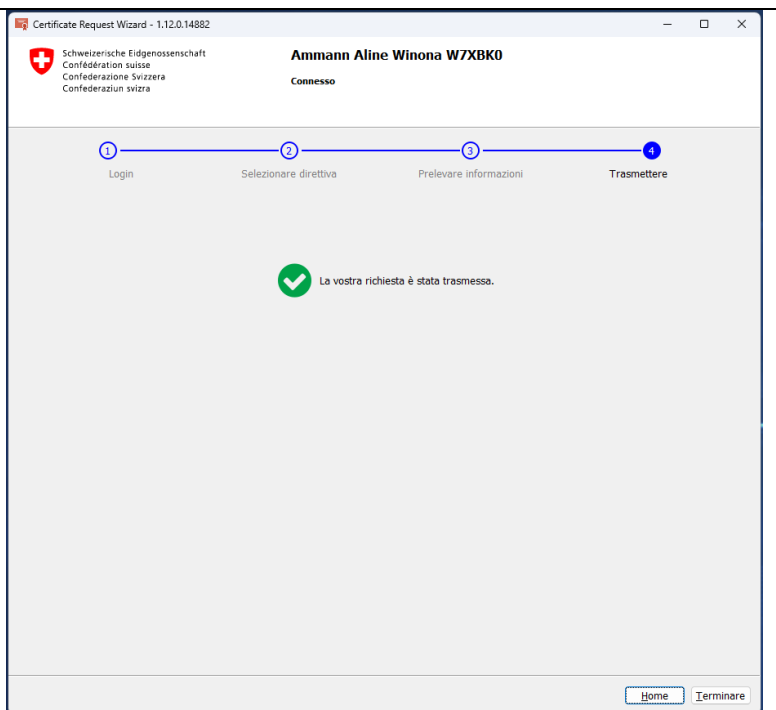
**Subject alternative names**  
Mail\* pkc-info@bit.admin.ch

☒ Ho verificato i dati e accetto i [Terms & Conditions](#)

Invia richiesta

< Indietro Terminare

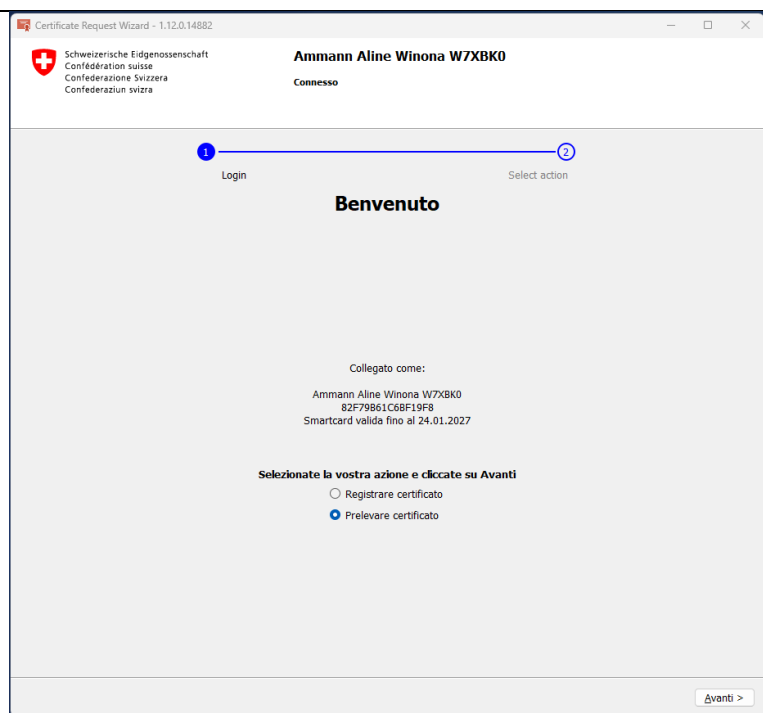
Il processo è ora completato. Il pulsante "Home" riporta direttamente alla pagina iniziale. Altrimenti, è possibile chiudere l'applicazione con il pulsante "Esci".



## Ritirare il certificato

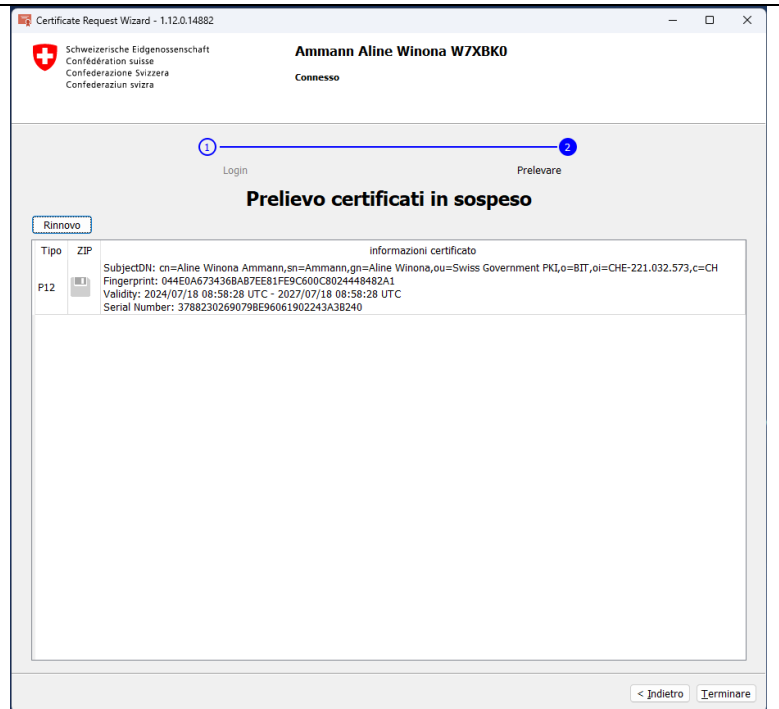
Il certificato può essere ritirato direttamente dopo la registrazione o, se richiesto dalla politica, dopo la convalida dell'e-mail del richiedente.

Se necessario, effettuare l'accesso all'applicazione come descritto nel capitolo 1. Selezionare quindi l'opzione "Prelevare certificato" e premere "Avanti".



Fare clic su "Rinnovo" per elencare gli ordini in sospeso. Cliccare sul simbolo del disco nella colonna ZIP per scaricare il rispettivo certificato.

**Nota bene: un ordine può essere ritirato solo una volta. Dopodiché non sarà più elencato.**



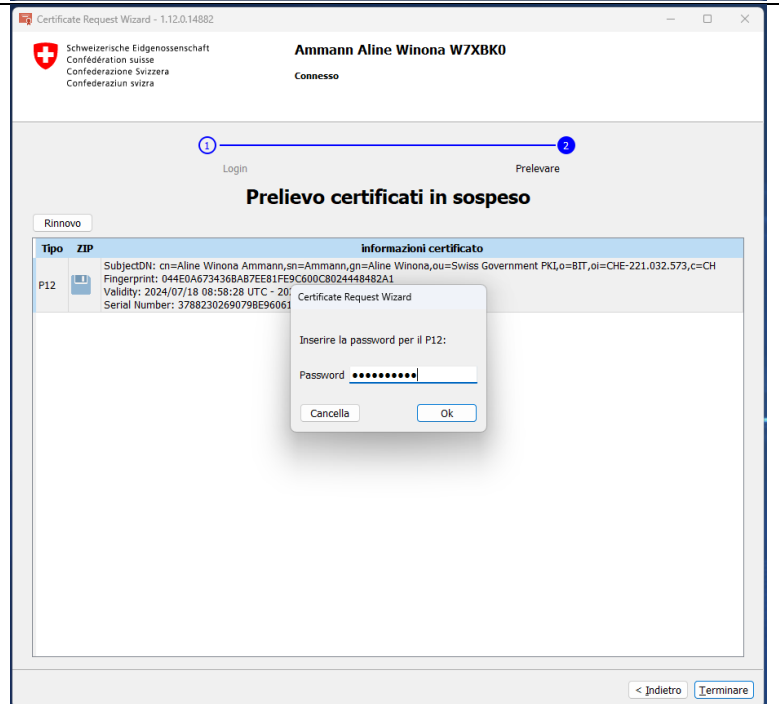
Nella variante P12 viene richiesta la password per la chiave privata. Inserirla nella finestra (NON si tratta del PIN della smartcard).

Quindi determinare la posizione di memorizzazione del file.

Se è stata selezionata la variante CSR, al momento del download non viene richiesta alcuna password. Inoltre, nel file ZIP dell'ordine CSR non è presente alcun file P12.

Quindi uscire dal CRW.

Si noti che i certificati possono essere archiviati solo dalla **persona che li detiene!**



## Policy

I certificati standard di Classe C si differenziano per i DN applicabili come segue:

| Nome distinto per i certificati personali*           |   |
|--|---|
| <b>CN =</b>  | CN= Nome comune: Cognome/i Nome/i, ad esempio: <b>Mustermeier Hanspeter</b>   |
| <b>SN =</b>  | SN = Cognome: Cognome/i   |
| <b>GN =</b>  | GN= Nome: Nome(i) di battesimo  |
| <b>OU =</b>  | OU= Unità organizzativa: <i>liberamente selezionabile</i> , ad esempio dipartimento, divisione, ecc...<br>Esempio: <b>Ufficio federale per gli studi sul futuro (BFZ) - Automazione d'ufficio</b> |
| <b>O =</b>   | O= Organizzazione: <i>selezionabile</i> , tra unità amministrative<br>Esempio: <b>BFZ</b>   |
| <b>OI =</b>  | OI= Identità dell'organizzazione: UID secondo il <a href="#">registro UID</a> , ad esempio: <b>CHE-123.456.789</b>  |
| <b>C =</b>   | C= Paese: <i>Voce fissa</i> : <b>CH</b>   |
| Nome distinto per i certificati di sistema           |   |
| <b>CN =</b>  | CN= Nome comune: nome del sistema, ad esempio: <b>TUSER-SYSP-SCPP123</b>  |
| <b>OU =</b>  | OU= Unità organizzativa: <i>liberamente selezionabile</i> , ad esempio dipartimento, divisione, ecc...<br>Esempio: <b>Ufficio federale per gli studi sul futuro (BFZ)-Automazione d'ufficio</b>   |
| <b>O =</b>   | O= Organizzazione: <i>Voce fissa</i> : <b>Admin</b>   |
| <b>OI =</b>  | OI= Identità dell'organizzazione: UID secondo il <a href="#">registro UID</a> , ad esempio: <b>CHE-123.456.789</b>  |
| <b>C =</b>   | C= Paese: <i>Voce fissa</i> : <b>CH</b>   |
| Nome distinto per i certificati dell'organizzazione* |   |
| <b>CN =</b>  | CN= Nome comune: denominazione ufficiale (secondo il registro UID), o traduzione ufficiale della stessa.<br>Esempio: <b>Ufficio Federale di Futurologia (BFZ)</b>                                 |
| <b>OU =</b>  | OU= Unità organizzativa: <i>liberamente selezionabile</i> , ad esempio dipartimento, divisione, ecc...<br>Esempio: <b>automazione d'ufficio</b>   |
| <b>O =</b>   | O= Organizzazione: <i>selezionabile liberamente</i> , ad esempio <b>Confederazione Svizzera</b> o <b>BFZ</b> .  |
| <b>OI =</b>  | OI= Identità dell'organizzazione: UID secondo il <a href="#">registro UID</a> , ad esempio: <b>CHE-123.456.789</b>  |
| <b>C =</b>   | C= Paese: <i>Voce fissa</i> : <b>CH</b> (aperta per Org Cert. con funzione Auth/Sign/Enc, ma non raccomandata)  |

## Validità

I certificati di classe C Standard della Swiss Government PKI sono validi per un massimo di 3 anni.