Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Ufficio federale dell'informatica e delle telecomunicazioni UFIT
Swiss Government PKI

19.07.2024

Guida rapida

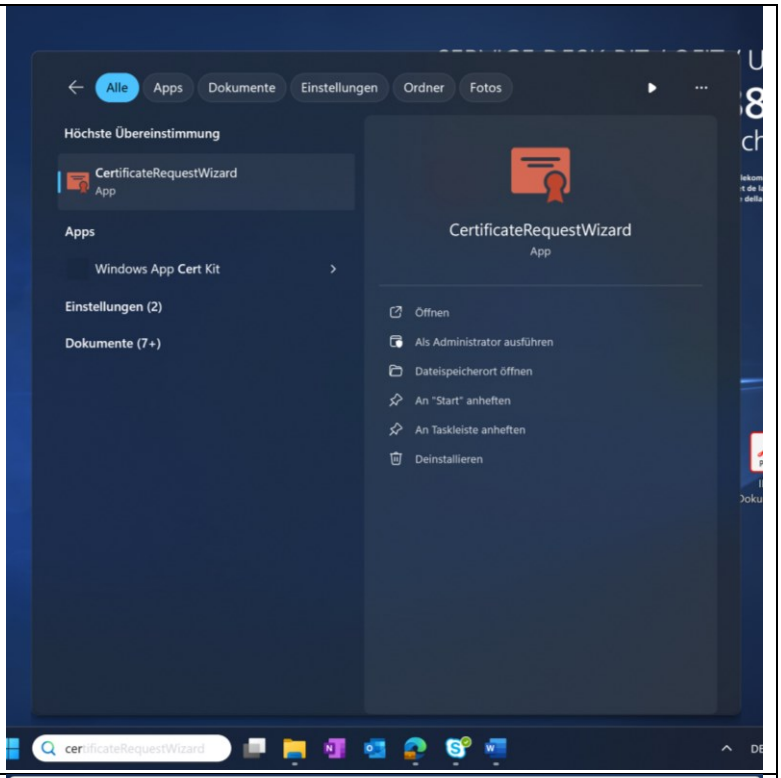
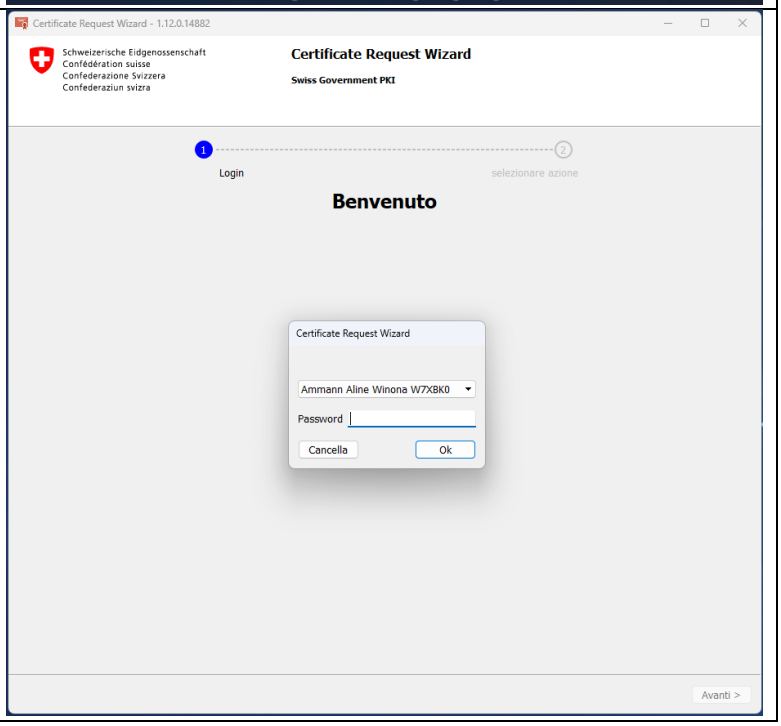
Certificate Request Wizard (CRW)

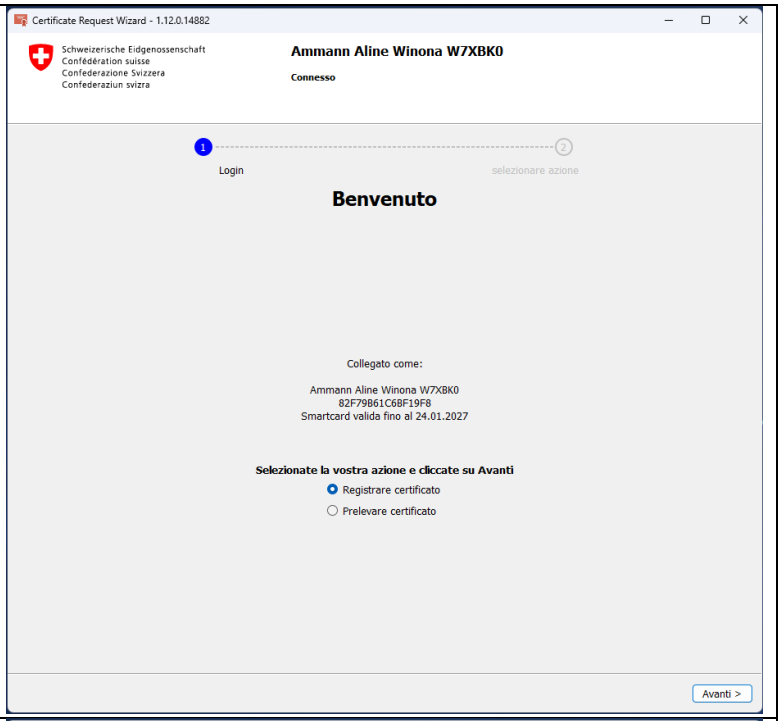
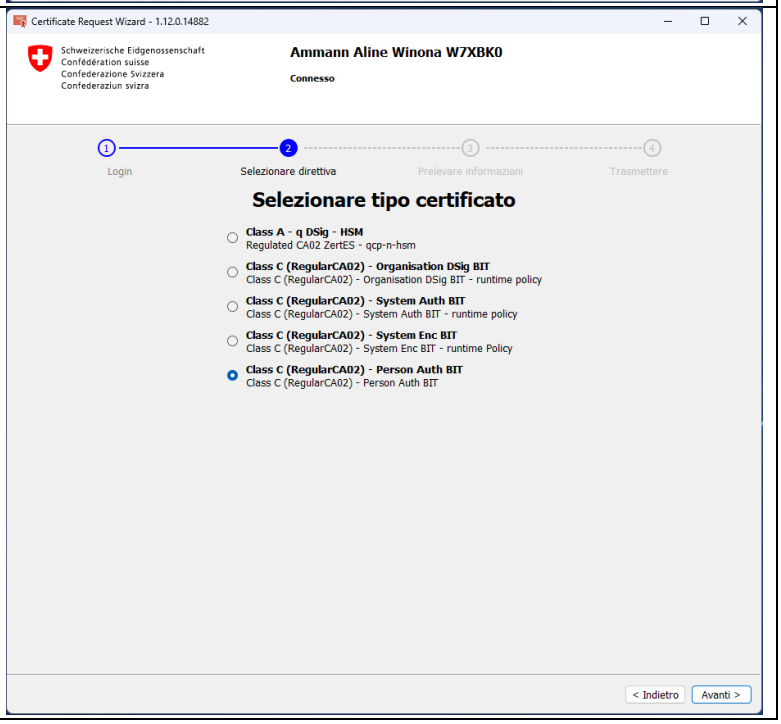
Stato: rilasciato V1.2

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.

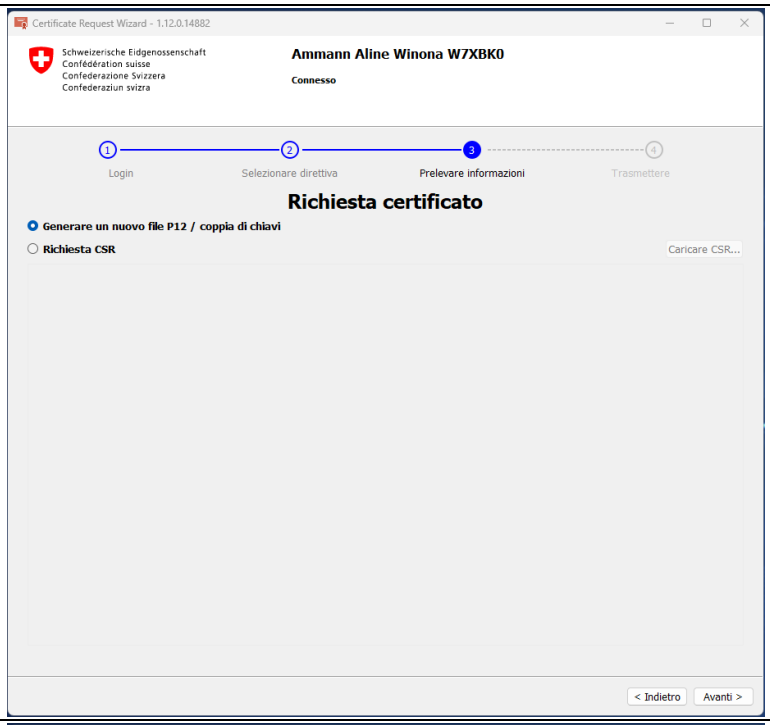
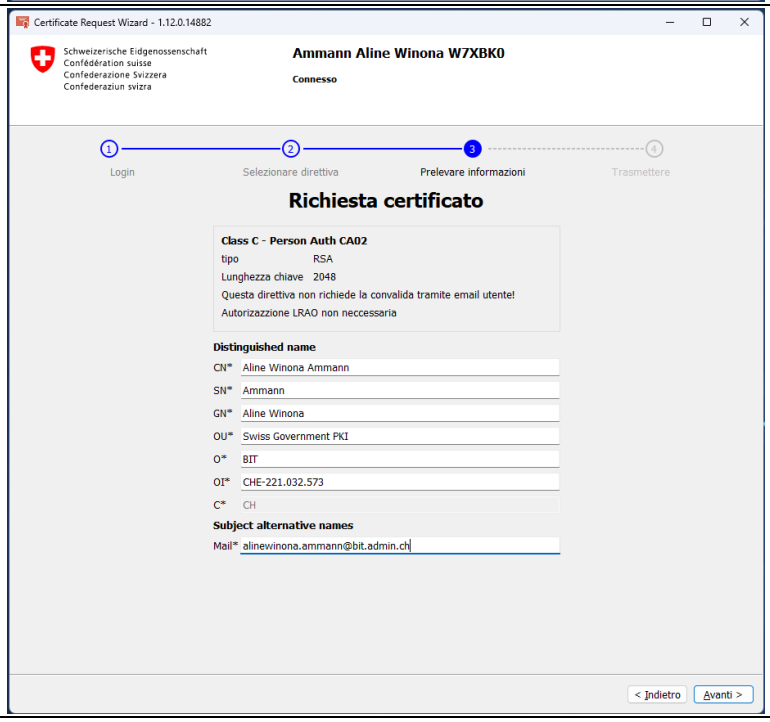
Certificato di registrazione

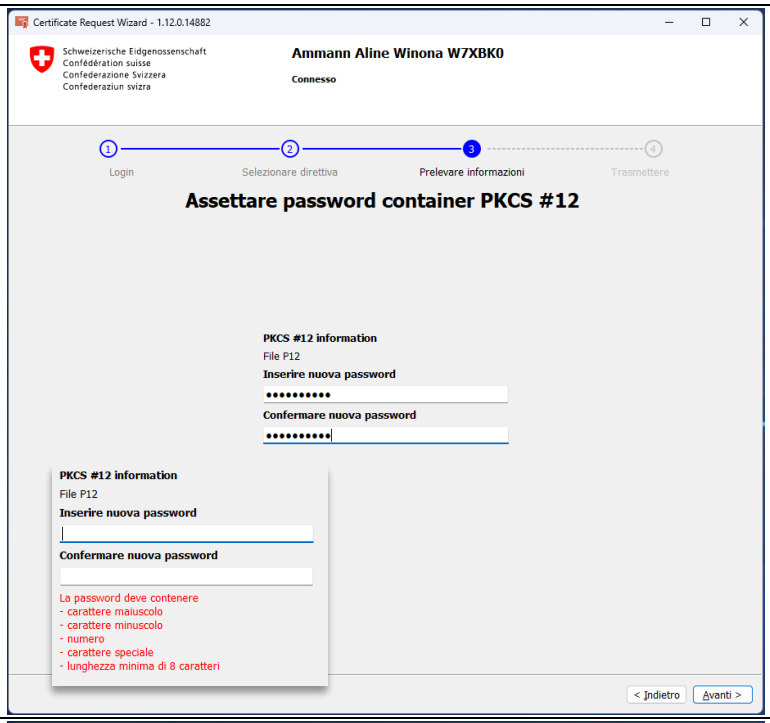
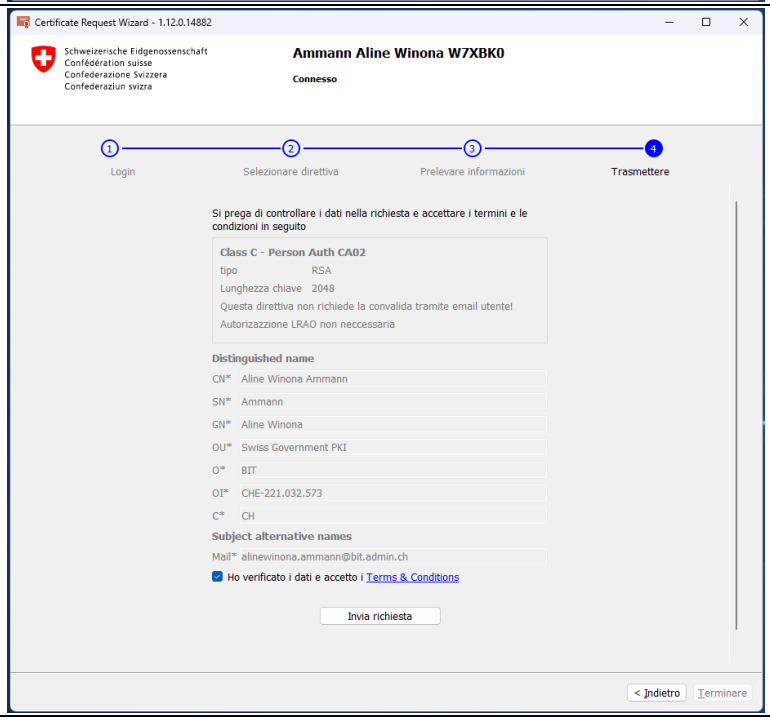
Avviare l'applicazione CRW.	
Dopo aver avviato l'applicazione, appare una finestra di login. Inserire qui il PIN del proprio certificato autorizzato di classe B e confermare con “OK”.	

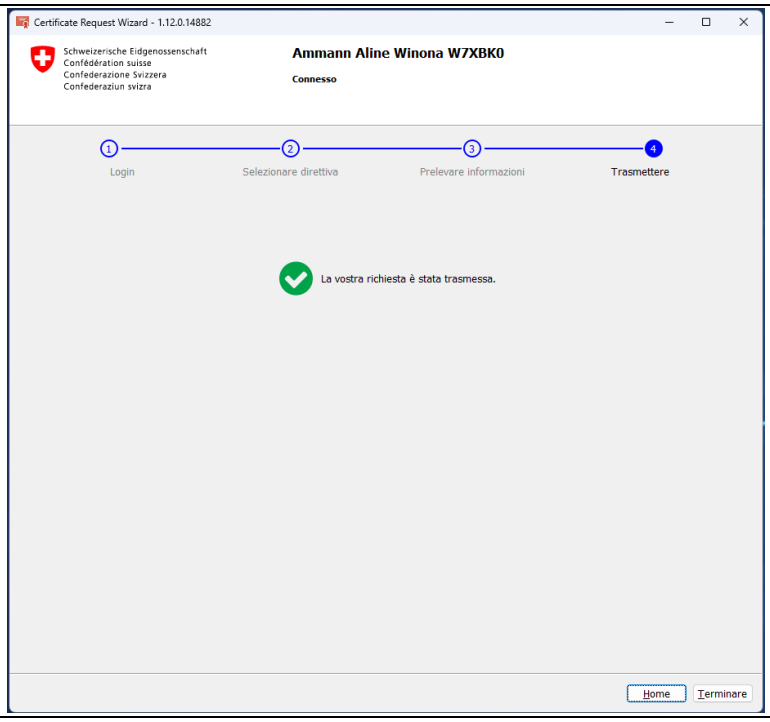
Fare clic su "Registrare certificato" e continuare con il pulsante "Avanti".	
Selezionare la politica desiderata (a seconda delle autorizzazioni, possono essercene diverse tra cui scegliere) e fare clic su "Avanti".	

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

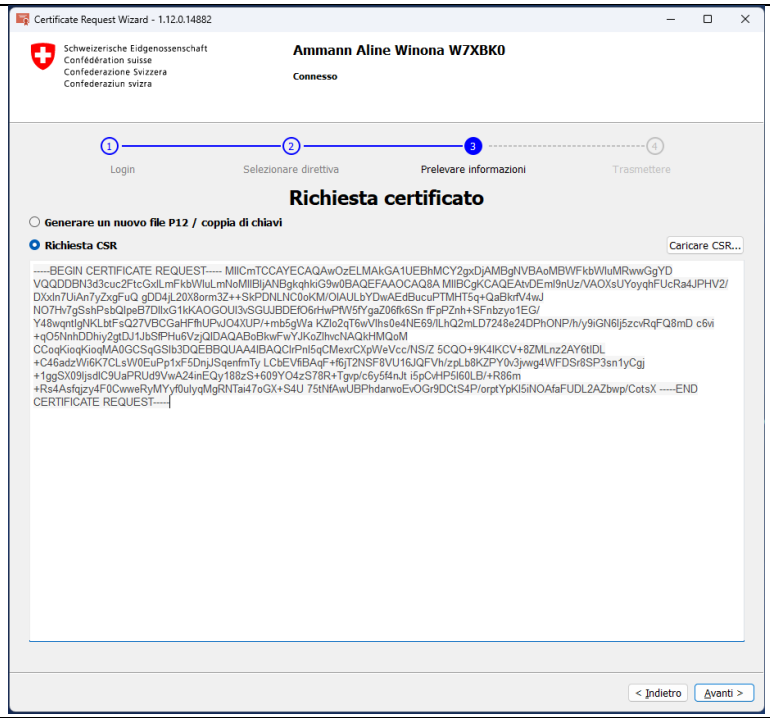
Durante questo processo, lo strumento crea automaticamente una Certificate Signing Request (CSR), che viene inviata online. Il risultato è costituito dalle due chiavi e dal certificato in un file P12.

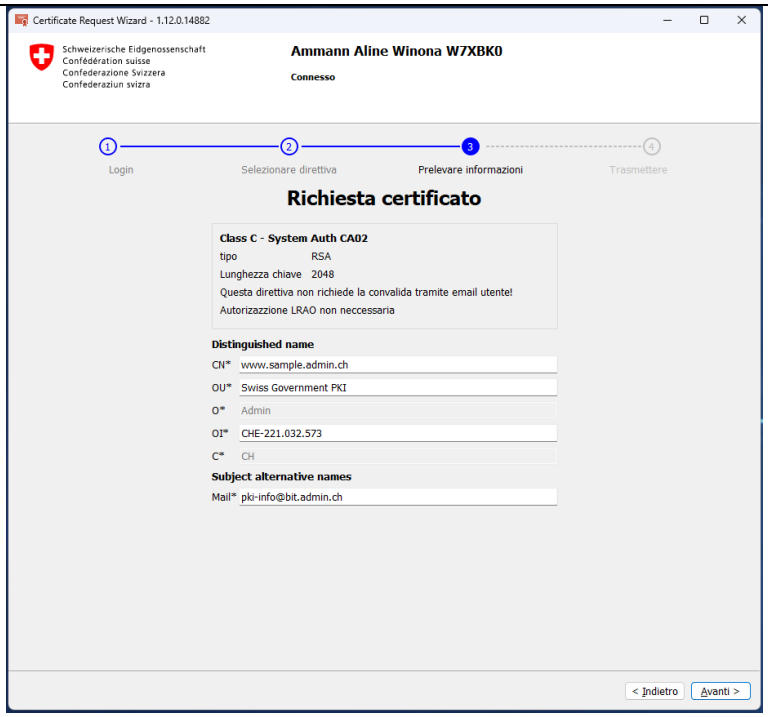
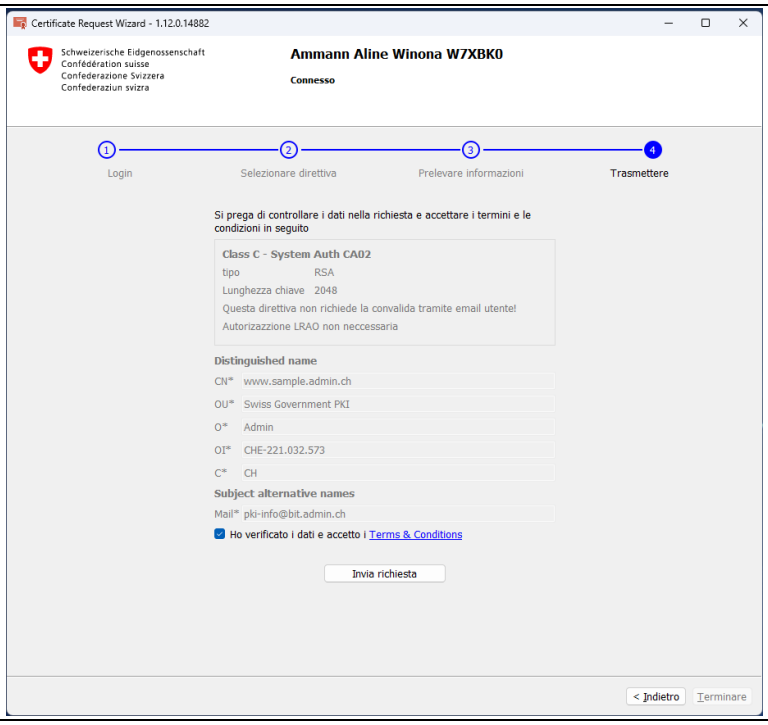
Selezionare l'opzione "Generare un nuovo file P12 / coppia di chiavi" e proseguire con "Avanti".	
A seconda della policy selezionata, i campi del Distinguished Name (DN) devono essere compilati in modo diverso. Le voci fisse sono ombreggiate e non possono essere modificate. Compilare i campi richiesti (vedere la sezione policy) e fare clic su "Avanti".	

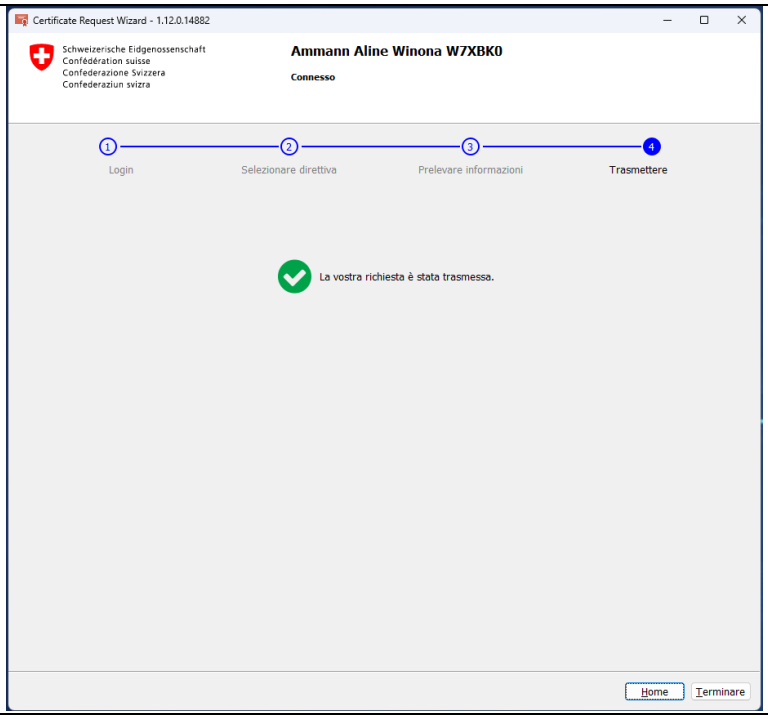
Inserire una password per il file P12. Le linee guida per la password vengono visualizzate se l'immissione non le soddisfa. Quindi premere “Avanti”.	
Controllare i dettagli. Spuntare la casella di conferma (leggere le condizioni d'uso). Inviare la domanda e premere il pulsante “Terminare”. La persona che ha inviato la richiesta può ora eseguire la convalida dell'e-mail, se richiesto dalla politica.	

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

Variante 2: applicazione CSR

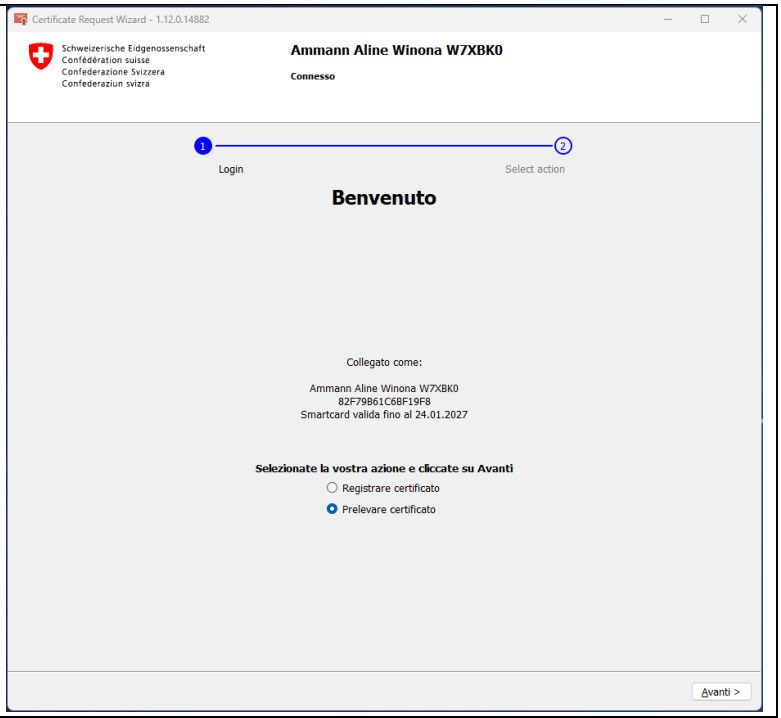
Selezionare l'opzione "Richiesta CSR". Caricare il CSR da un file utilizzando il pulsante "Carica CSR" oppure copiare il testo del CSR direttamente nel campo vuoto, come mostrato nell'esempio. Quindi fare clic su "Avanti".	

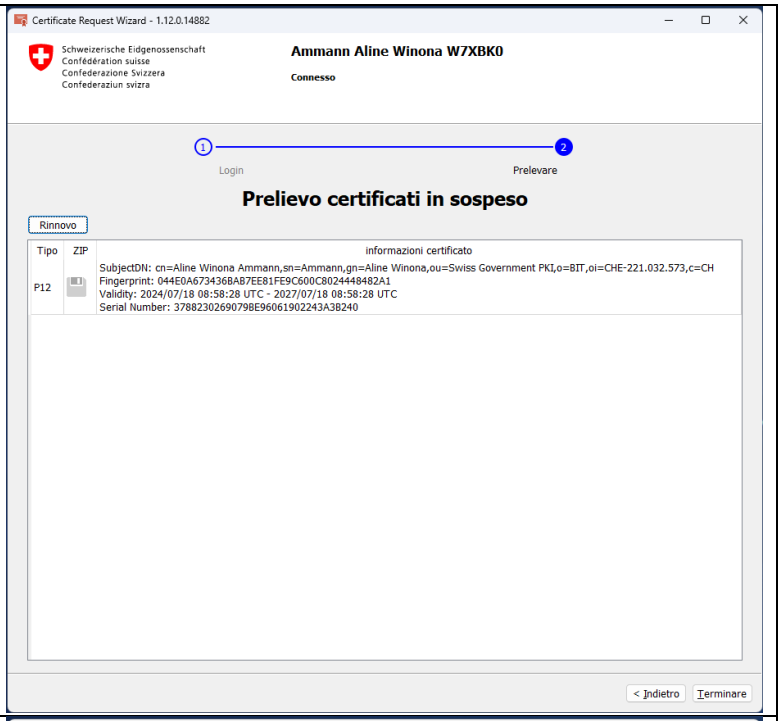
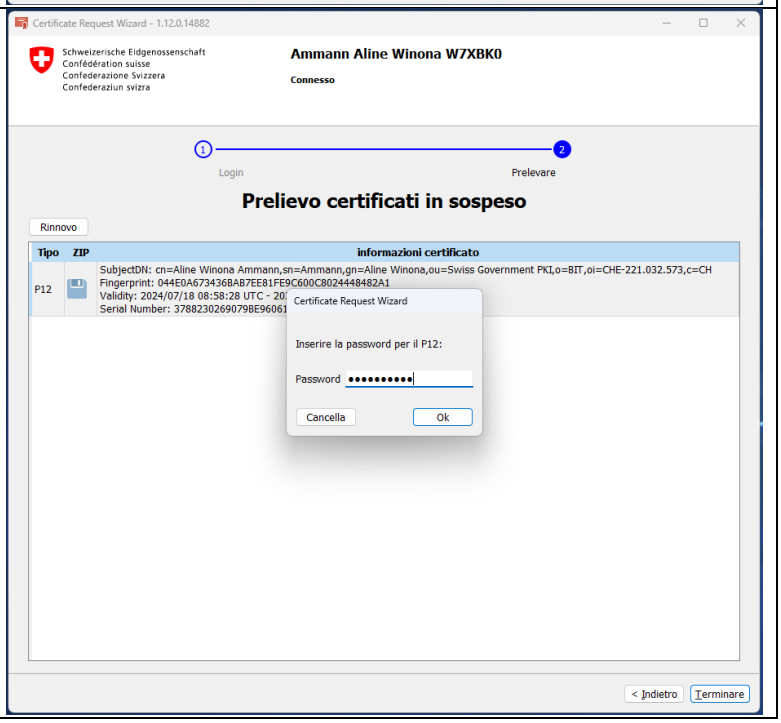
I campi del Ditinguished Name sono già compilati con il CSR. Verificare i dettagli rispetto alle specifiche della politica e apportare le modifiche necessarie. Le voci fisse sono ombreggiate e non possono essere modificate. Continuare quindi con “Avanti”.	
Controllare i dettagli. Spuntare la casella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

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*	
CN =	*CN= Nome comune: Cognome/i Nome/i, ad esempio:* ***Mustermeier Hanspeter***
SN =	*SN = Cognome: Cognome/i*
GN =	*GN= Nome: Nome(i) di battesimo*
OU =	*OU= Unità organizzativa: liberamente selezionabile, ad esempio dipartimento, divisione, ecc...* *Esempio:* ***Ufficio federale per gli studi sul futuro (BFZ) - Automazione d'ufficio***
O =	*O= Organizzazione: selezionabile, tra unità amministrative* *Esempio:* ***BFZ***
OI =	*OI= Identità dell'organizzazione: UID secondo il registro UID, ad esempio:* ***CHE-123.456.789***
C =	*C= Paese: Voce fissa:* ***CH***
Nome distinto per i certificati di sistema	
CN =	*CN= Nome comune: nome del sistema, ad esempio:* ***TUSER-SYSP-SCPP123***
OU =	*OU= Unità organizzativa: liberamente selezionabile, ad esempio dipartimento, divisione, ecc...* *Esempio:* ***Ufficio federale per gli studi sul futuro (BFZ)-Automazione d'ufficio***
O =	*O= Organizzazione: Voce fissa:* ***Admin***
OI =	*OI= Identità dell'organizzazione: UID secondo il registro UID, ad esempio:* ***CHE-123.456.789***
C =	*C= Paese: Voce fissa:* ***CH***
Nome distinto per i certificati dell'organizzazione*	
CN =	*CN= Nome comune: denominazione ufficiale (secondo il registro UID), o traduzione ufficiale della stessa.* *Esempio:* ***Ufficio Federale di Futurologia (BFZ)***
OU =	*OU= Unità organizzativa: liberamente selezionabile, ad esempio dipartimento, divisione, ecc...* *Esempio:* ***automazione d'ufficio***
O =	*O= Organizzazione: selezionabile liberamente, ad esempio* ***Confederazione Svizzera*** *o* ***BFZ.***
OI =	*OI= Identità dell'organizzazione: UID secondo il registro UID, ad esempio:* ***CHE-123.456.789***
C =	*C= Paese: Voce fissa:* ***CH*** *(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.