Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Swiss Government PKI

19.07.2024

Guide rapide

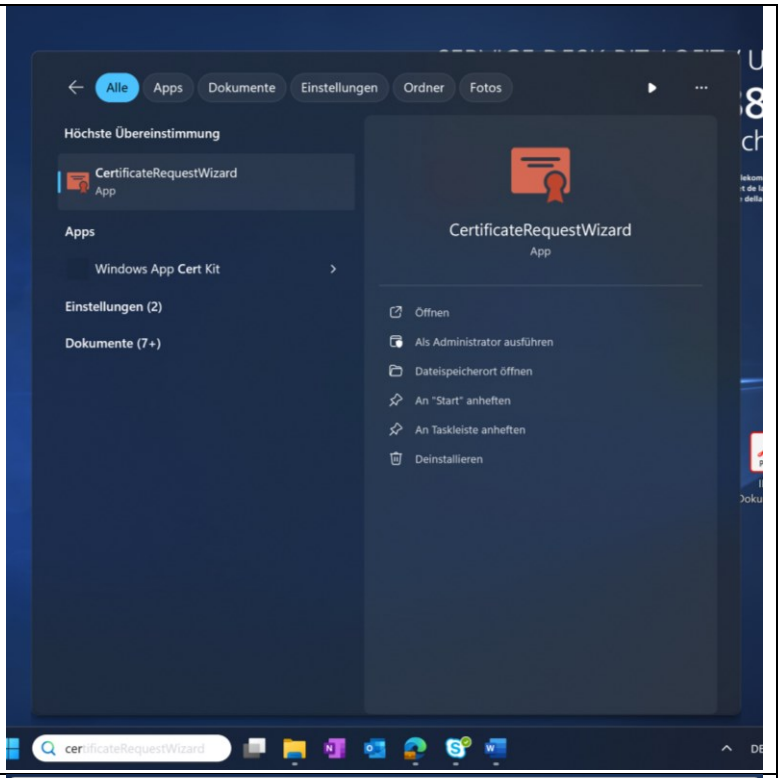
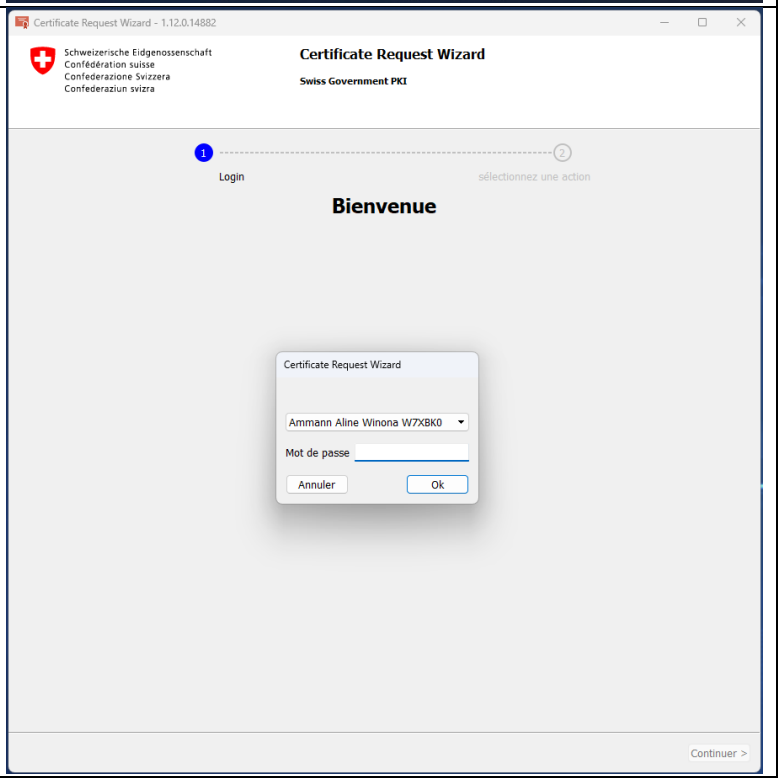
Certificate Request Wizard (CRW)

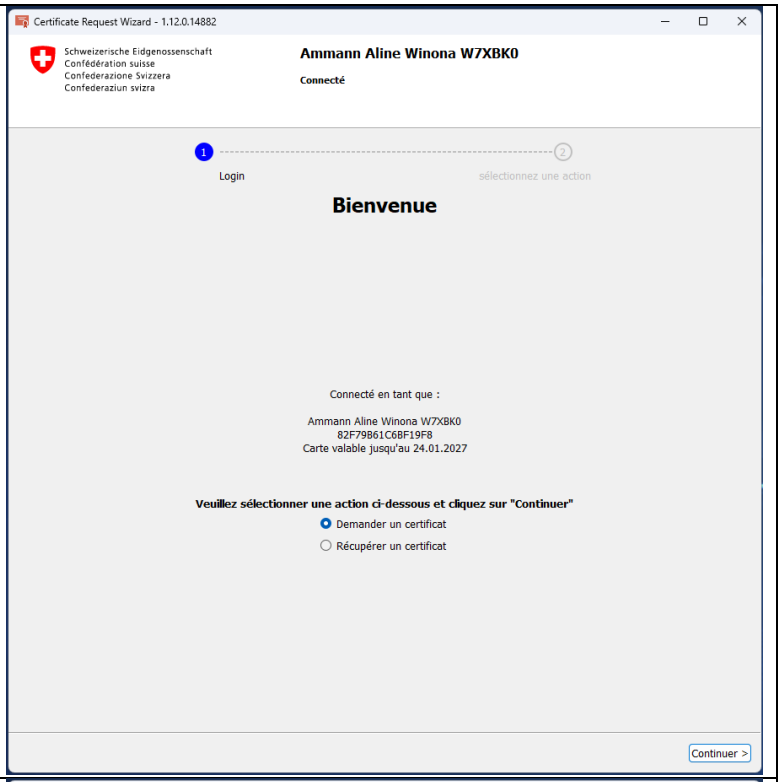
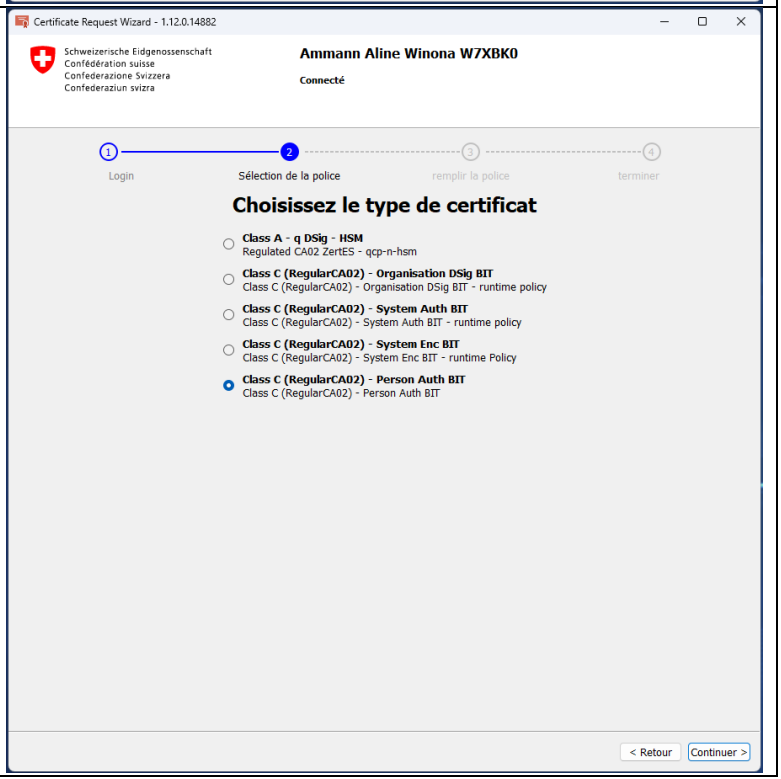
Statut : libéré V1.2

L'assistant de demande de certificats (*certificate request wizard*, CRW) est un logiciel autonome installé sur le poste de travail client de l'administration fédérale. Le CRW permet à une personne de générer localement des Certificate Signing Requests (CSR) pour les certificats pour lesquels elle a été autorisée. Le CRW envoie automatiquement les CSR à la Swiss Government PKI, qui invite la personne destinataire du certificat indiqué dans l'adresse électronique de la demande à valider les données saisies. Le certificat est ensuite émis et peut être récupéré par la personne qui a fait la demande et transmis à la personne destinataire du certificat.

Au lieu de créer un CSR au moyen du CRW, l'utilisateur a la possibilité de copier un CSR existante directement dans le logiciel et d'envoyer la demande.

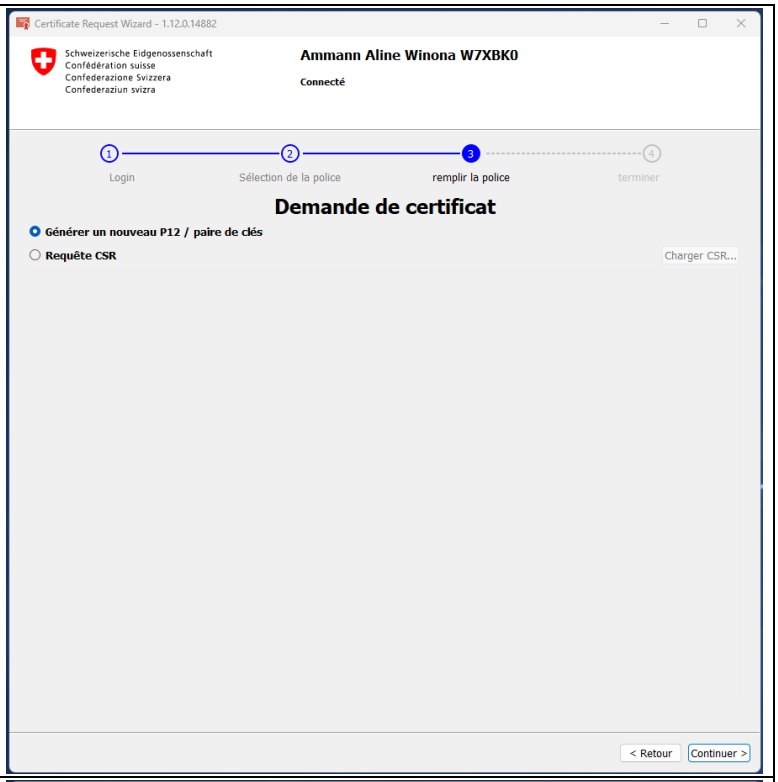
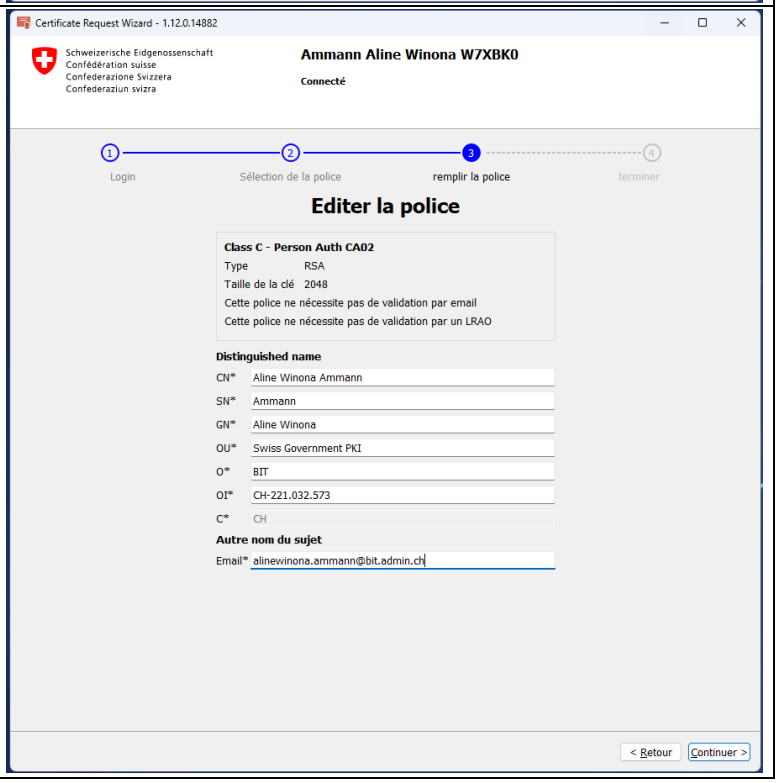
Enregistrer le certificat

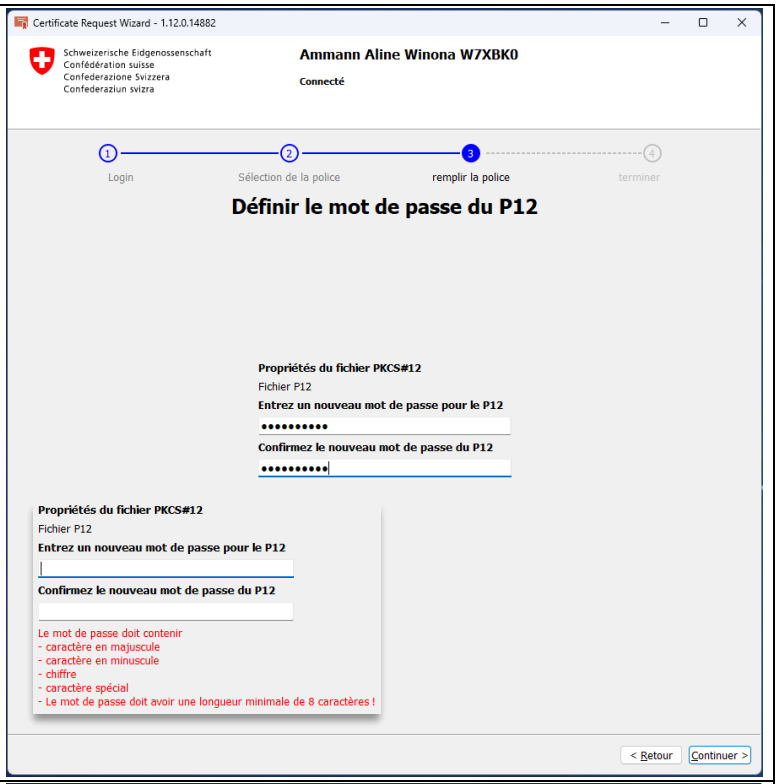
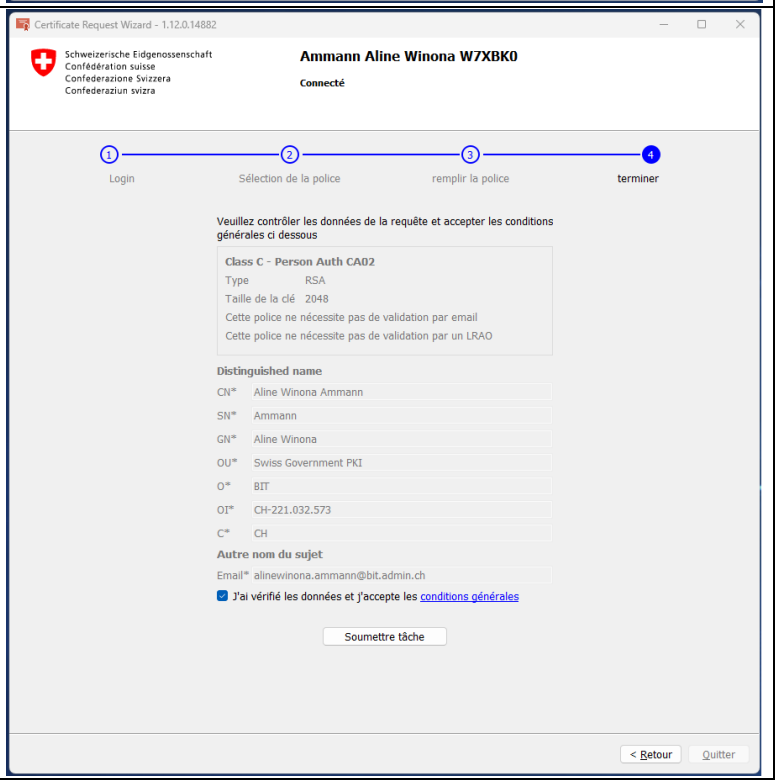
Démarrez l'application CRW.	
Après le lancement de l'application une fenêtre de connexion s'affiche. Saisissez ici le code PIN de votre certificat de classe B autorisé et confirmez en cliquant sur «OK».	

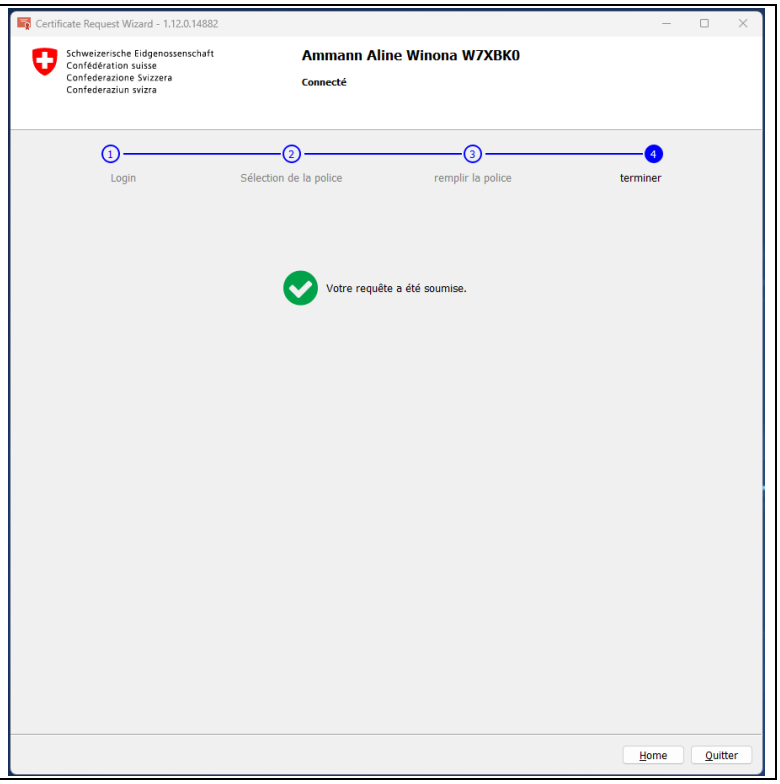
Sélectionnez «Demander un certificat" et cliquez sur le bouton "Continuer".	
Sélectionnez la policy souhaitée (selon les autorisations, il peut y en avoir plusieurs à choisir) et cliquez sur " Continuer".	

Variante 1 : établir P12 (paire de clés et certificat)

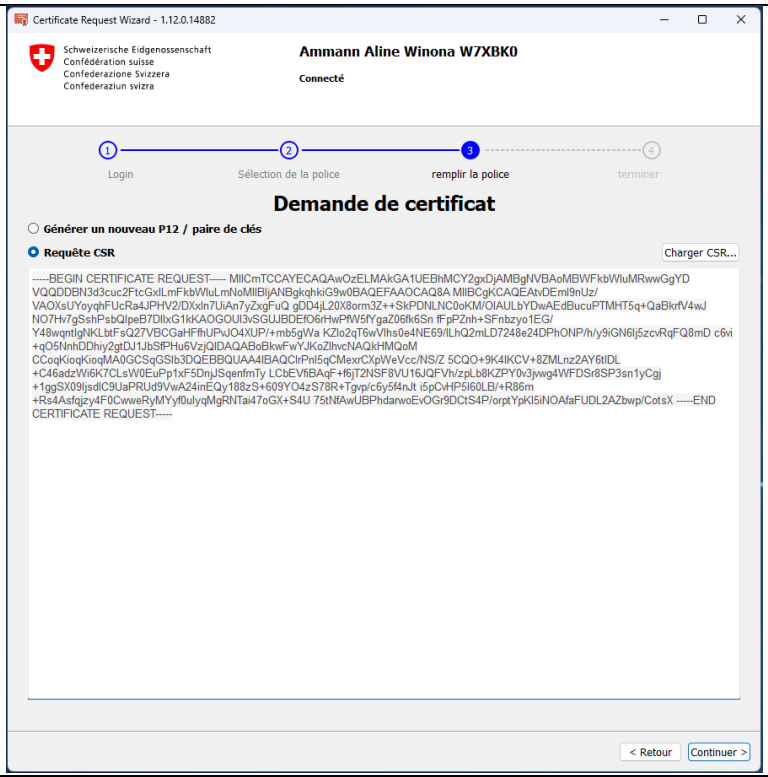
Lors de ce processus, l'outil crée automatiquement un Certificate Signing Request (CSR) qui est envoyée en ligne. Il en résulte les deux clés ainsi que le certificat dans un fichier P12.

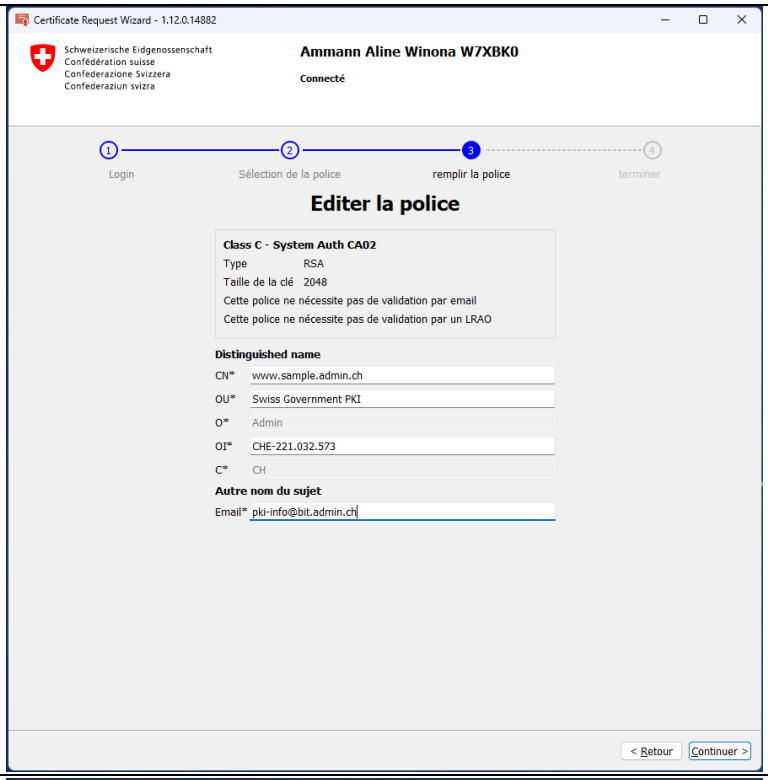
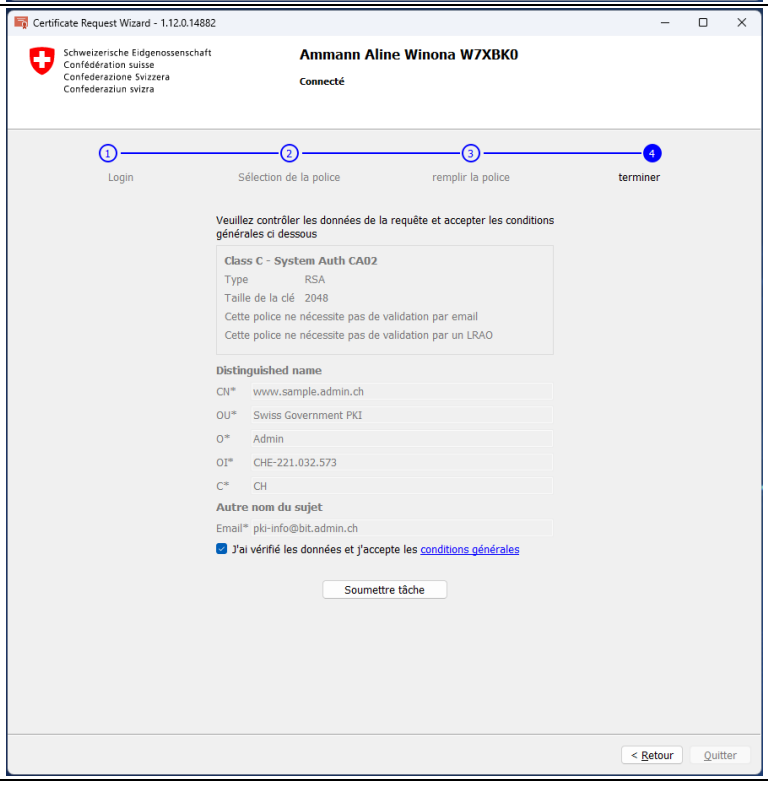
Sélectionnez l'option "Générer un nouveau P12 / paire de clés" et continuez avec " Continuer".	
Selon la policy sélectionnée, les champs du Disdinguished Name (DN) doivent être remplis différemment. Les entrées fixes sont sombres et ne peuvent pas être modifiées. Remplissez les champs nécessaires (voir chapitre Policy) et cliquez ensuite sur "Continuer".	

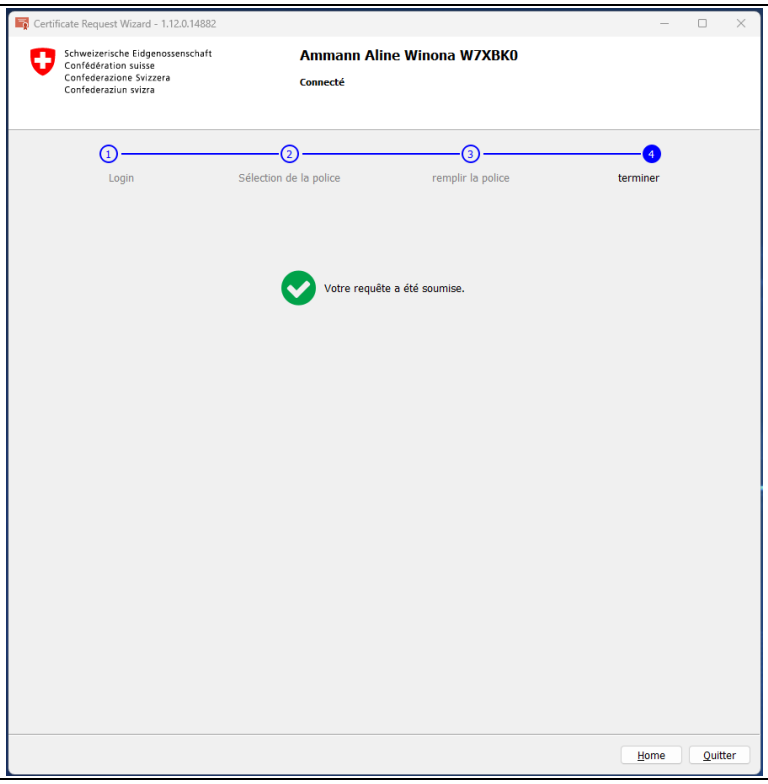
Saisissez un mot de passe pour votre fichier P12. Les directives pour le mot de passe s'affichent si la saisie ne les respecte pas. Appuyez ensuite sur «Continuer».	
Vérifiez les données. Cochez ensuite la case de confirmation (Lisez les conditions d'utilisation). Soumettez la demande et appuyez sur le bouton «Quitter». La personne qui fait la demande peut alors procéder à la validation du courriel, si la politique l'exige.	

Le processus est maintenant terminé. En cliquant sur le bouton «Home», vous revenez directement à la page d'accueil. Sinon, vous pouvez fermer l'application en cliquant sur le bouton «Quitter».	

Variante 2 : Demande de CSR

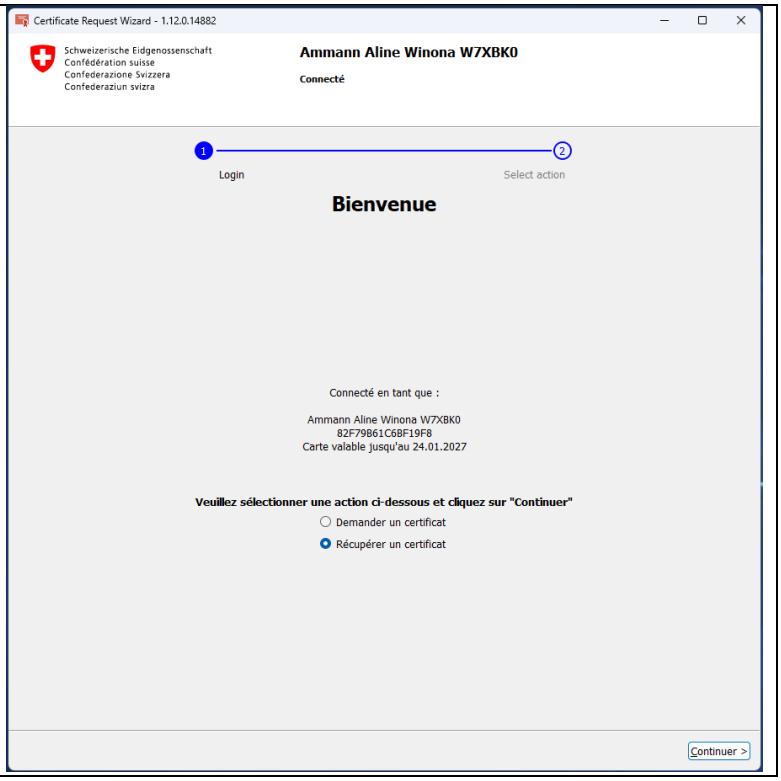
Sélectionnez l'option "Requête CSR". Soit, vous chargez le CSR à partir d'un fichier en cliquant sur le bouton "Charger CSR", soit vous copiez le texte de le CSR directement dans le champ libre comme indiqué dans l'exemple. Appuyez ensuite sur "Continuer".	

Avec le CSR, les champs du Distingushed Name sont déjà remplis. Vérifiez les données à l'aide des directives de la policy et procédez aux adaptations nécessaires. Les entrées fixes sont ombrées et ne peuvent pas être modifiées. Poursuivez ensuite en cliquant sur «Continuer».	
Vérifiez les données. Cochez ensuite la case de confirmation (Lisez les conditions d'utilisation). Envoyez la demande et appuyez sur le bouton «Quitter». La personne qui fait la demande peut alors procéder à la validation de l'e-mail, si la politique l'exige.	

Le processus est maintenant terminé. En cliquant sur le bouton «Home», vous revenez directement à la page d'accueil. Sinon, vous pouvez fermer l'application en cliquant sur le bouton «Quitter».	

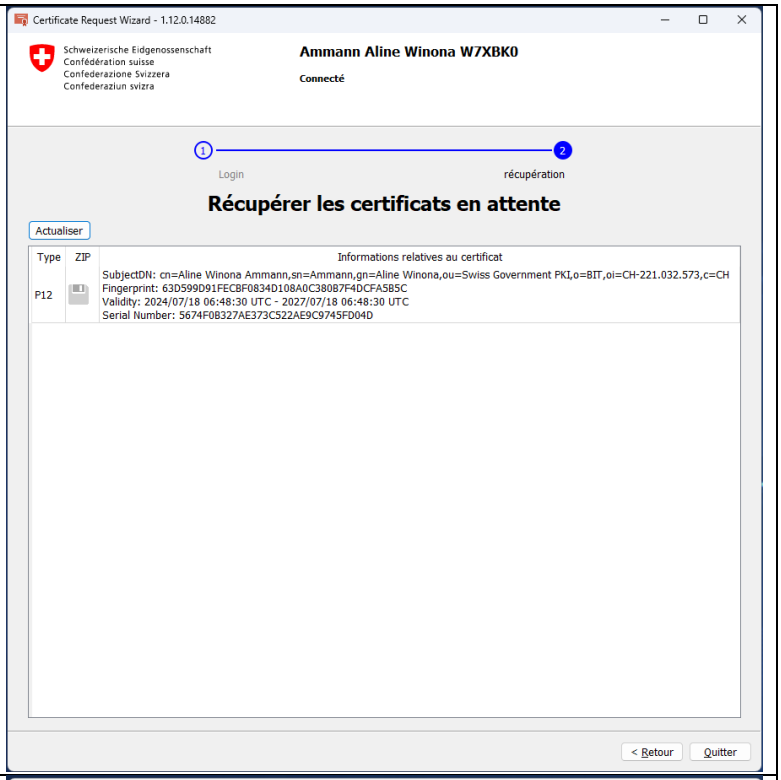
Récupérer le certificat

Vous pouvez obtenir un certificat soit directement après l'enregistrement, soit, si la politique l'exige, après la validation de l'e-mail de la personne qui fait la demande.

Si nécessaire, connectez-vous à l'application selon la description du chapitre 1. Sélectionnez ensuite l'option "Récupérer un certificat" et appuyez sur "Continuer".	

Cliquez sur "Actualiser" pour lister les tâches en attente. Dans la colonne ZIP, cliquez sur l'icône de la disquette pour télécharger le certificat correspondant.

Attention : une commande ne peut être retirée qu'une seule fois. Ensuite, elle ne sera plus listée.



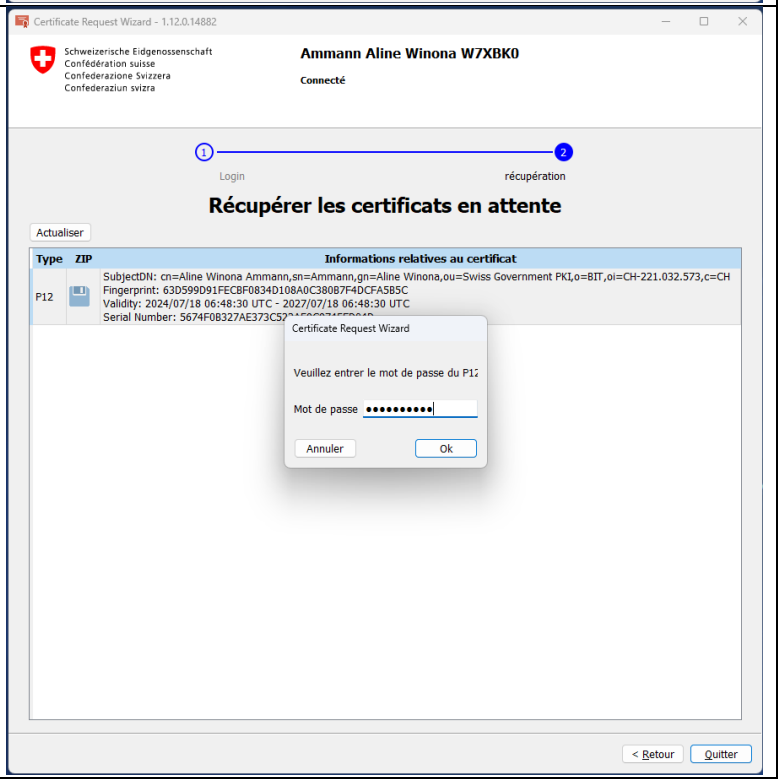
Dans la variante P12, le mot de passe de la clé privée vous est demandé. Saisissez-le dans la fenêtre (il ne s'agit pas ici du code PIN de la carte à puce).

Déterminez ensuite l'emplacement de votre fichier.

Si la variante CSR a été choisie, aucun mot de passe n'est demandé lors du téléchargement. En outre, le fichier ZIP de la commande CSR ne contient pas non plus de fichier P12.

Quittez ensuite le CRW.

Notez que les certificats ne peuvent être archivés que **par la personne qui les détient !**



Policy

Les certificats standard de classe C se distinguent par les DN applicables comme suit :

Distinguished Name pour les certificats de personnes*.	
CN =	*CN= Nom commun : nom(s) de famille prénom(s), ex : **Mustermeier Hanspeter***
SN =	*SN = Surnom : Nom(s) de famille*
GN =	*GN= nom d'usage : prénom(s)*
OU =	*OU= unité organisationnelle : libre choix, p.ex. département, secteur, etc... Ex : **Office fédéral de la recherche (OFR) - Bureautique***
O =	*O= Organisation : sélectionnable, entre unité administrative Ex : **BFZ***
OI =	*OI= Organisation Identity : UID selon le registre UID, ex. : **CHE-123.456.789***
C =	*C= Country : Entrée fixe : **CH***
Distinguished Name pour les certificats système	
CN =	*CN= Nom commun : nom du système, ex. : **TUSER-SYSP-SCPP123***
OU =	*OU= unité organisationnelle : libre choix, p.ex. département, secteur, etc... Ex : **Office fédéral de la prospective (OFP) - Bureautique***
O =	*O= Organisation : Entrée fixe : **Admin***
OI =	*OI= Organisation Identity : UID selon le registre UID, ex. : **CHE-123.456.789***
C =	*C= Country : Entrée fixe : **CH***
Distinguished Name pour les certificats d'organisation*.	
CN =	*CN= Common Name : désignation officielle (selon le registre IDE), ou traduction officielle de celle-ci. Ex : **Office fédéral de la prospective (OFP)***
OU =	*OU= unité organisationnelle : libre choix, p.ex. département, domaine, etc... Ex : **Bureautique***
O =	*O= Organisation : libre choix, ex. : **Confédération suisse** ou **BFZ***
OI =	*OI= Organisation Identity : UID selon le registre UID, ex. : **CHE-123.456.789***
C =	*C= Country : Fixer l'entrée : **CH** (ouvert en cas de certificat d'org. avec fonction Auth/Sign/Enc, mais déconseillé)*

Validité

Les certificats standard de classe C de la Swiss Government PKI sont valables au maximum 3 ans.