Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

V2.1 / 11. Décembre 2023

Certificat pour boîte aux lettres de groupe

Guide de travail

Table des matières

1 Introduction

1.1 Objectif du document

L'utilisation de certificats de boîte aux lettres de groupe n'est pas tout à fait triviale et nécessite quelques préparatifs de la part des propriétaires et des utilisateurs. Ce document doit servir de manuel aux propriétaires de certificats de boîte aux lettres de groupe et à tous les autres utilisateurs de la boîte aux lettres de groupe en tant qu'"utilisateurs" de celle-ci.

Ce document a pour but de faciliter le travail avec le certificat de boîte aux lettres de groupe et de fournir des conseils et astuces également à leurs utilisateurs.

1.2 Structure du document

Le document est divisé en deux parties, la première étant destinée aux propriétaires des boîtes aux lettres de groupe et du certificat. Il y sera décrit comment installer le certificat et quelle clé il faut publier pour que le certificat puisse être utilisé par les personnes qui écrivent à la boîte aux lettres et cryptent leurs courriers.

La deuxième partie de ce manuel est destinée aux "clients", c'est-à-dire aux tiers qui souhaitent transmettre un message crypté à un office. Pour ce faire, ils ont besoin de la "clé publique" de la boîte aux lettres de groupe et doivent attribuer ce certificat à l'adresse de messagerie à écrire à leur carnet d'adresses personnel.

2 Généralités sur le certificat de boîte aux lettres de groupe

2.1 Description

Les boîtes aux lettres de groupe soutiennent les unités organisationnelles dans le déroulement de leurs processus commerciaux (administration électronique). Les certificats de boîte aux lettres de groupe servent principalement à l'échange crypté de données dans le trafic administratif entre les citoyens et l'administration. Les certificats de boîte aux lettres de groupe permettent à plusieurs personnes d'accéder aux e-mails cryptés.

Techniquement, il s'agit d'**un** certificat logiciel qui peut être installé sur des clients. Il offre les fonctions de cryptage et de signature. Le certificat logiciel **est** publié par la Swiss Government PKI.

2.2 Validité

Les certificats de boîte aux lettres de groupe ont une validité de 3 ans et doivent être recommandés lors d'un renouvellement par leur propriétaire via Remedy MAC.

2.3 Commande

L'autorité passe une commande de certificats de boîte aux lettres de groupe auprès du MAC-Manager (MAC-Manager@bit.admin.ch) ou saisit directement le MAC via la Remedy Requester Console au moyen de Remedy-MAC. La Swiss Government PKI saisit le certificat au moyen de l'outil CRW et envoie à chaque fois un mail de validation à la boîte aux lettres de groupe. Dès que les données ont été validées par le propriétaire, le certificat de la boîte aux lettres de groupe est émis et envoyé au propriétaire de la boîte aux lettres de groupe.

2.4 Publication

Les certificats pour boîtes aux lettres de groupe sont publiés par la Swiss Government PKI dans le Directory de la Confédération. Si les autorités n'utilisent pas le Directory de la Confédération pour la publication du certificat, elles sont elles-mêmes responsables de sa publication et de son installation.

2.5 Révocation

Les personnes autorisées de l'unité administrative peuvent demander la révocation au moyen de Remedy-MAC.

2.6 Renouvellement

Le processus d'émission initiale s'applique au renouvellement des certificats de boîte aux lettres de groupe.

2.7 CP/CPS

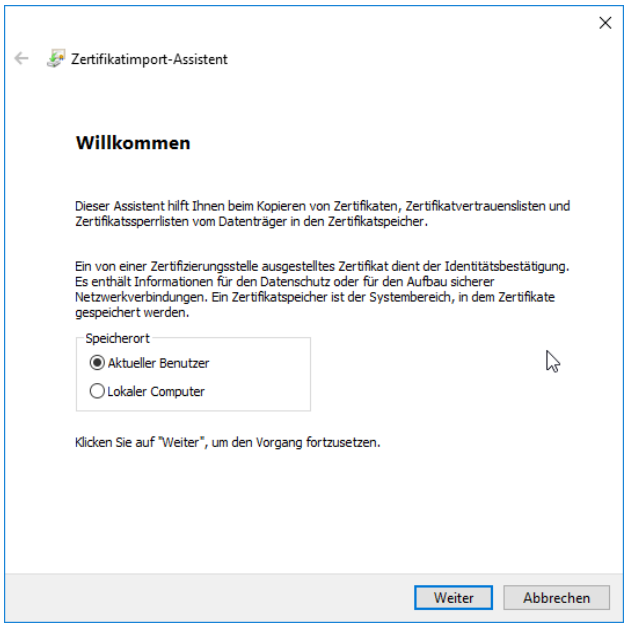
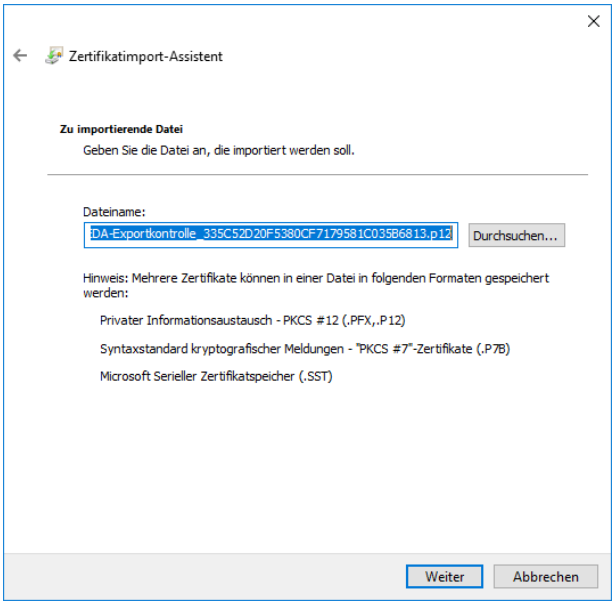
Les droits et obligations liés à l'obtention et à l'utilisation des certificats de boîte aux lettres de groupe sont décrits dans le CP/CPS, ainsi que dans les conditions d'utilisation et les directives des certificats standard de classe C.

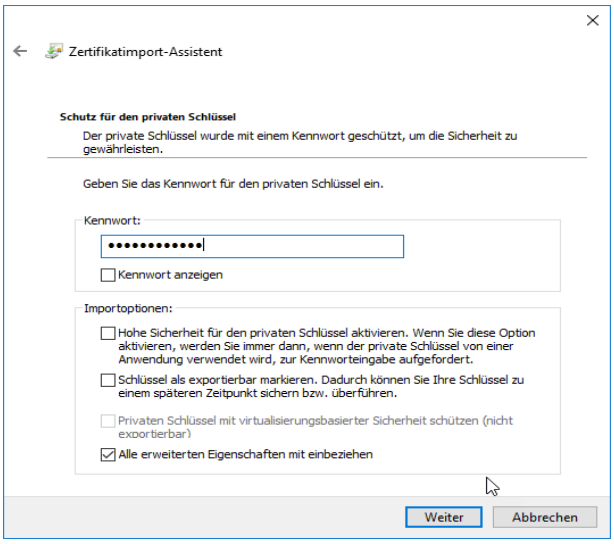
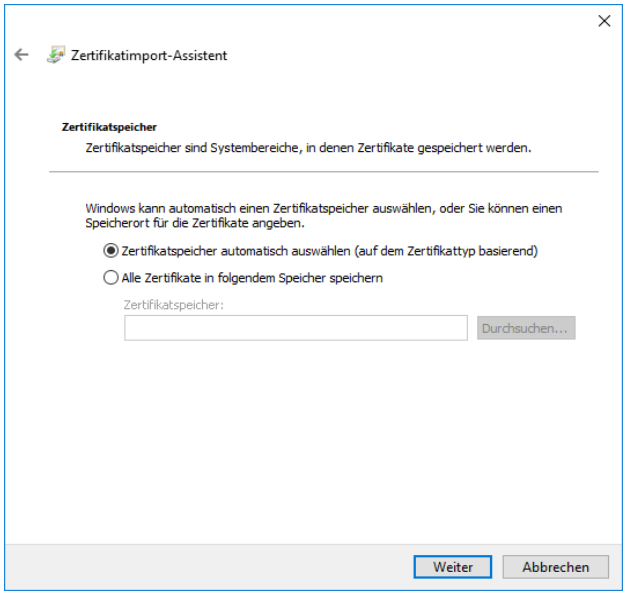
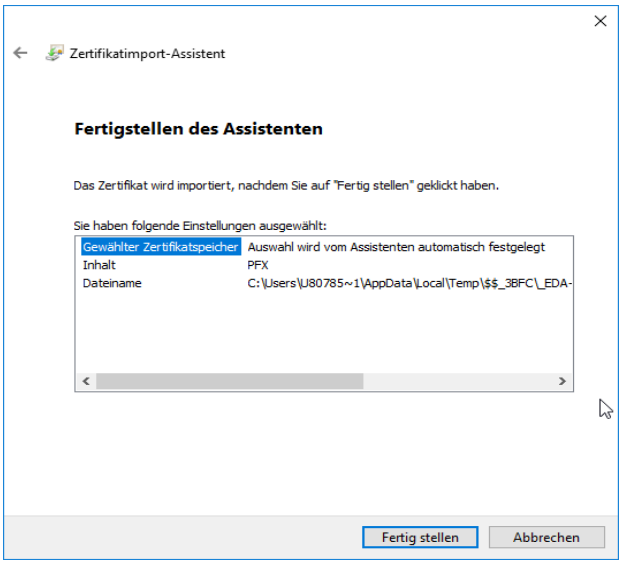
Vous trouverez également des informations, des formulaires et les CP/CPS sur le site :
Boîte aux lettres de groupes **sur notre site** http://www.pki.admin.ch.

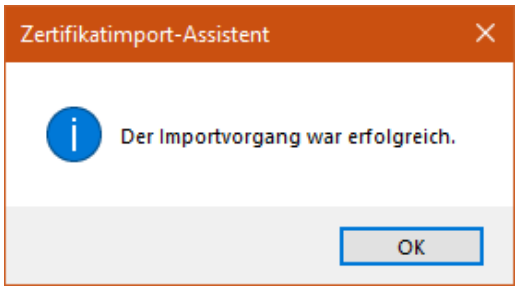
3 Propriétaire d'un certificat de boîte aux lettres de groupe

3.1 Installation du certificat de boîte aux lettres de groupe

L'installation d'un certificat de boîte aux lettres de groupe doit être effectuée sur chaque ordinateur qui travaille avec cette boîte aux lettres de groupe. Le fichier *.P12 obtenu est "importé" dans le magasin de certificats. Voici comment cela fonctionne :

Double-cliquer sur le fichier *.p12 et cliquer sur "Continuer".	
Confirmer le chemin du fichier en cliquant sur "suivant".	

Saisir le mot de passe reçu par e-mail, et **NE PAS** cliquer sur d'autres éléments ! Cliquez sur "continuer" pour passer à la fenêtre suivante.	
Sélectionner "Sélectionner automatiquement le magasin de certificats" et cliquer sur "Continuer".	
„Terminer“.	

„OK“. Le certificat est maintenant importé dans le magasin.	

3.2 Publier la "clé publique" si le directory de la Confédération n'est pas utilisé

En général, le certificat de boîte aux lettres de groupe est publié dans le répertoire de la Confédération (Directory). Si les autorités n'utilisent pas ce répertoire pour la publication du certificat, elles sont responsables de sa publication et de son installation. Pour que des tiers puissent crypter des e-mails pour votre boîte aux lettres de groupe, ils doivent avoir accès à la clé publique ("Public Key") du certificat de boîte aux lettres de groupe. La clé publique a l'extension *.cer et non pas *.p12 comme votre propre certificat importé ! La clé publique est contenue dans le fichier ZIP que vous avez reçu.

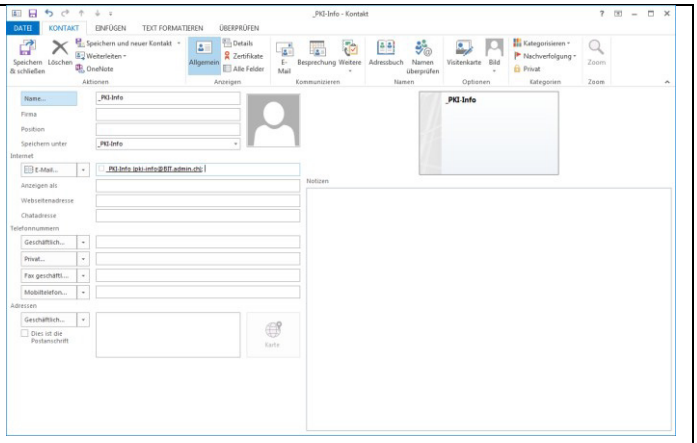
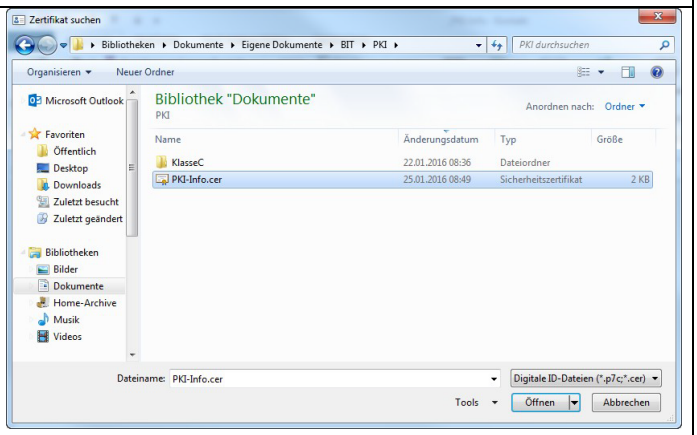
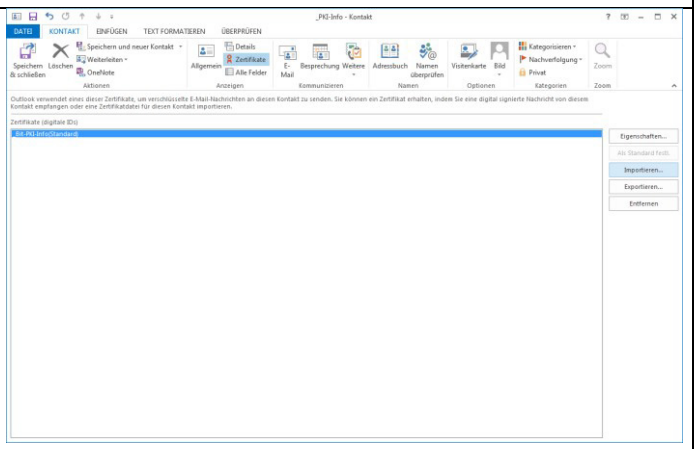
Vous devez mettre ce fichier *.CER à la disposition de tiers afin qu'ils puissent vous envoyer des e-mails cryptés. Si cette procédure n'est pas possible au point 3.2, vous pouvez le faire par exemple en envoyant un e-mail signé depuis cette boîte aux lettres.

4 Utilisateurs d'un certificat de boîte aux lettres de groupe

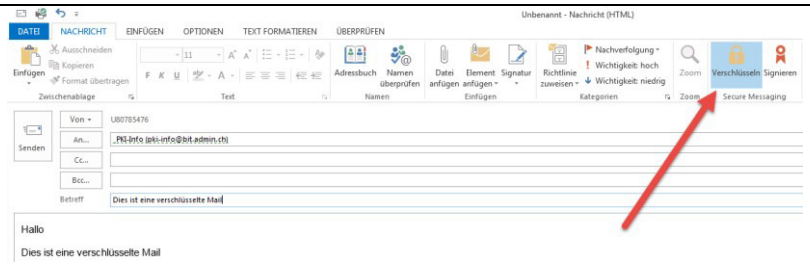
En principe, les e-mails qui doivent être envoyés sous forme cryptée doivent être codés avec la clé publique ("Public Key") du destinataire. La clé publique doit être mise à disposition par le destinataire, que ce soit par e-mail ou sur une page d'accueil à télécharger.

Nous présentons ensuite une proposition pour l'envoi d'un e-mail codé dans MS Outlook à une boîte aux lettres de groupe. Il est important que le "contact" ait été enregistré et que le certificat ait déjà été attribué à l'information de contact. Voici comment procéder dans Outlook :

4.1 Ajouter un contact et associer un certificat

Créer un nouveau "contact" et saisir les exigences minimales : - Nom - E-mail (Le lien avec le certificat est fait avec l'adresse e-mail !)	
Passer au bouton "Certificats" et cliquer sur "importer". Chercher le certificat dans le dossier de stockage, cliquer dessus et cliquer sur "ouvrir".	
Le certificat est maintenant lié au contact. Cliquez sur "Enregistrer » pour sauver le contact.	

4.2 Envoyer un courriel crypté à un contact

Envoyez des e-mails à crypter pour une boîte aux lettres de groupe directement depuis la liste de contacts : Ouvrez votre contact enregistré "contact" du chap. 4.1 et cliquez sur l'icône de mail:	
Rédigez votre e-mail et cliquez sur le symbole de cryptage avant de l'envoyer. Envoyez votre message.	
Le destinataire reçoit le mail avec le même symbole !