Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports

Armée suisse
Base d'Aide au Commandement BAC

Berne, 31.octobre 2014

Outil de rechiffrement - Guide rapide

1 Quand a-t-on besoin d'un rechiffrement avec la carte à puce (smartcard) ?

Avant le renouvellement d'une carte qui contient d'anciennes clés de chiffrement[1]

Les textes chiffrés X.509 sont générés en utilisant un certificat X.509. Le déchiffrement du texte chiffré X.509 requiert une carte à puce munie de la clé privée correspondante au certificat. Au fil du temps, l'utilisateur possède de nouvelles clés de chiffrement, parce que lors de chaque renouvellement de sa carte, il reçoit une nouvelle clé de chiffrement avec un nouveau certificat X.509. Pour éviter le rechiffrement, il faudrait que la smartcard contienne de plus en plus de clés de chiffrement pour qu'un utilisateur puisse toujours déchiffrer ses documents chiffrés. Cependant, lors du renouvellement de la carte, pour des raisons de place mémoire, on ne peut pas laisser sur la carte autant de clés de chiffrement qu'on voudrait. Et les clés de chiffrement les plus anciennes doivent être supprimées. Il est donc important, avant un renouvellement de la smartcard, de rechiffrer avec la clé de chiffrement actuelle tous les documents qui sont chiffrés avec une ancienne clé de chiffrement. Notons que la clé actuelle de chiffrement sera conservée sur la carte lors du renouvellement. Ainsi, les documents rechiffrés avant le renouvellement, seront toujours accessibles après le renouvellement.

Après la migration vers une autre PKI

Lors de la migration vers une autre PKI, une nouvelle carte à puce sera en principe générée. Pour que les anciens fichiers chiffrés avec un certificat X.509 puissent être déchiffrés avec la nouvelle carte, l'utilisateur doit rechiffrer tous ses fichiers avec l'aide de son ancienne carte et de la nouvelle clé de chiffrement (voir 2.4 „Choix étendu des clés").

2 Comment travailler avec l'outil de rechiffrement?

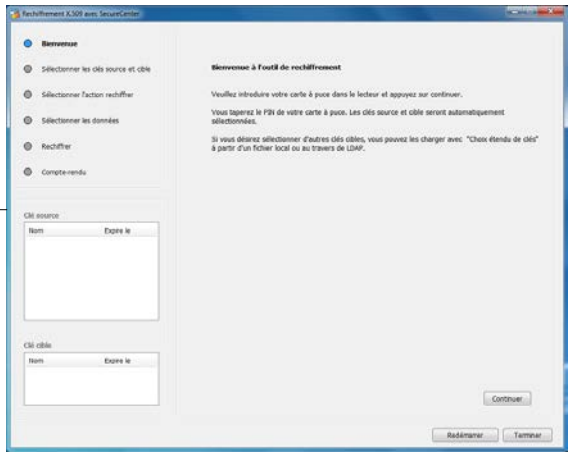
Afin que le rechiffrement fonctionne sans heurt et de manière sûre, veuillez respecter les processus décrits ci-dessous. De plus, il faut prendre en considération les points évoqués au chapitre 3. Si néanmoins des problèmes se présentent, vous êtes priés de vous adresser au helpdesk.

ATTENTION: les fichiers chiffrés contenant des informations classées SECRÈTES ne peuvent être rechiffrés que sur des appareils admis pour le traitement d'informations SECRÈTES. Pour ces documents, il faut absolument enlever la coche à l'étape 6 si l'appareil utilisé n'est pas autorisé au traitement de telles données. Veuillez ensuite effectuer le rechiffrement de ces fichiers sur un appareil autorisé.

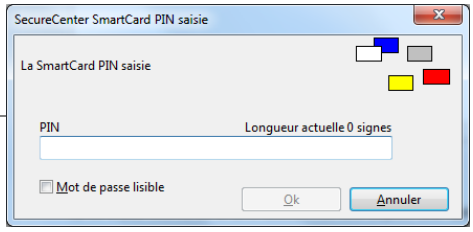
[1] Ce sera le cas à partir du deuxième renouvellement ou si un recouvrement de clé a eu lieu sur la carte à puce.

2.1 Processus de rechiffrement avec choix automatique du lecteur & du répertoire

1. Connexion avec une ancienne Smartcard, affichage de la boîte de dialogue Bienvenue et ouverture de l'outil de rechiffrement, quitter en cliquant sur «Continuer».



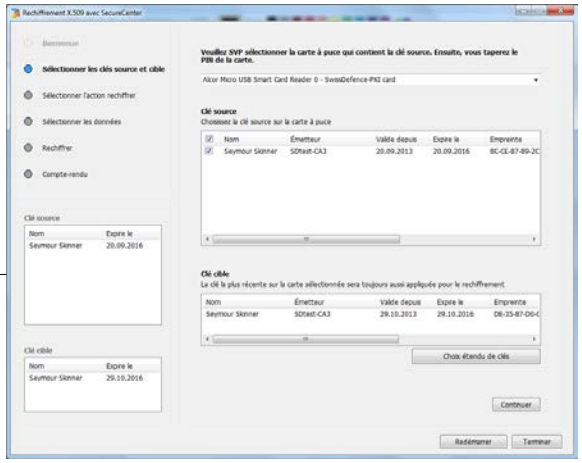
2. Connexion dans l'outil de rechiffrement avec une ancienne Smartcard (saisie du PIN)



3. Dans la boîte de dialogue, sélectionner la Smartcard qui contient la clé source (ancienne clé).

4. Sous Clé source, la boîte de dialogue montre l'ancienne clé enregistrée sur la Smartcard. Cocher si ce n'est pas le cas.

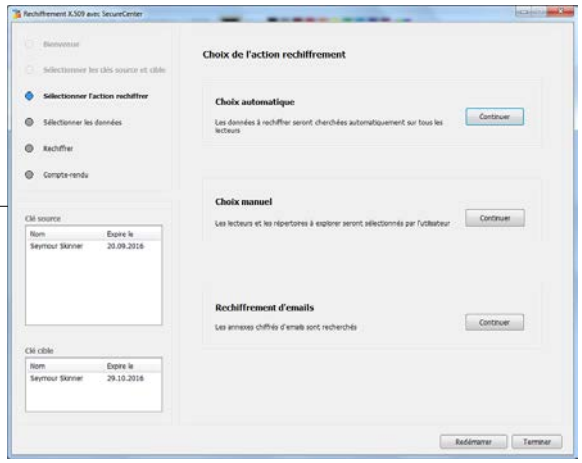
5. Dans la boîte de dialogue, la nouvelle clé enregistrée sur la Smartcard est visible sous Clé cible.
De plus, des clés supplémentaires peuvent être chargées en cliquant sur «Choix étendu de clés» (voir chapitre 2.4).



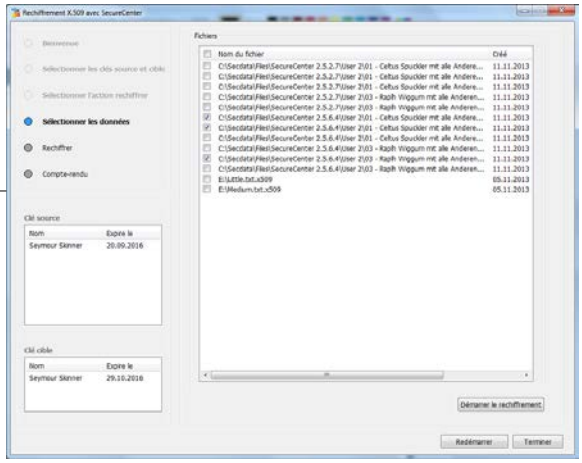
6. Dans la boîte de dialogue «Choix automatique», quitter en sélectionnant «Continuer».

(choix automatique = recherche automatique de fichiers chiffrés dans les lecteurs, y compris sélection des occurrences)

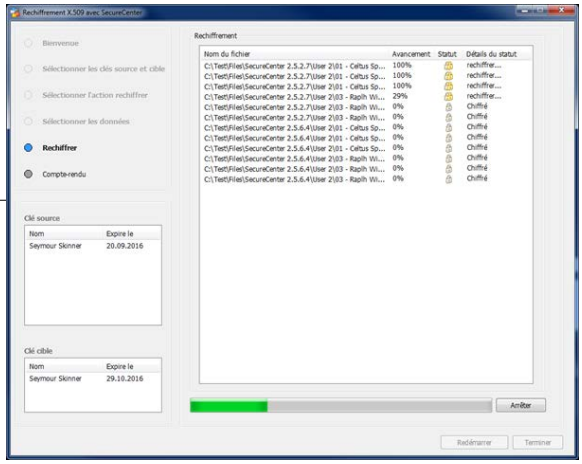
(choix manuel voir chapitre 2.2 et rechiffrement e-mail voir chapitre 2.3)



7. Sélectionner les fichiers en les cochant et quitter en cliquant sur «Démarrer le rechiffrement».

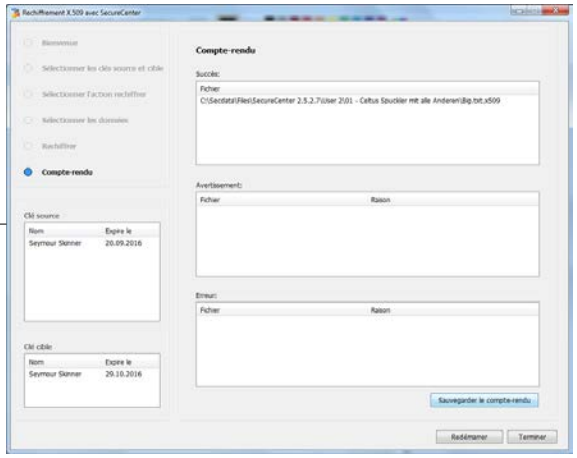


8. La boîte de dialogue avec l'état d'avancement s'affiche. Le processus peut être interrompu à tout moment en cliquant sur «Arrêter».



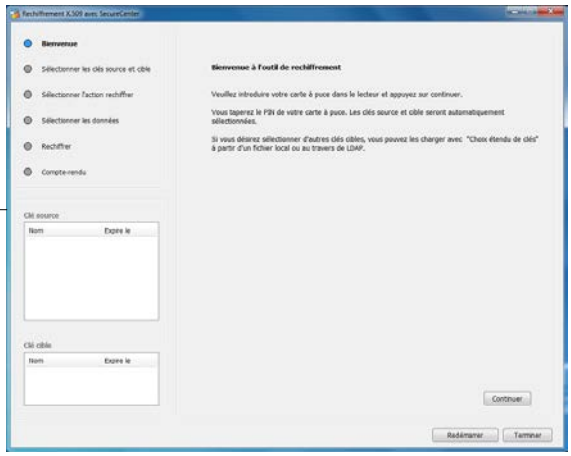
Le rechiffrement est clôturé par l'affichage du compte-rendu. Le compte-rendu dresse la liste de toutes les erreurs éventuelles (pour d'autres informations sur les messages d'erreur voir chapitre 3.1)

Le programme peut alors être redémarré pour un autre rechiffrement (sélectionner «Redémarrer») ou peut être terminé (sélectionner «Terminer»).

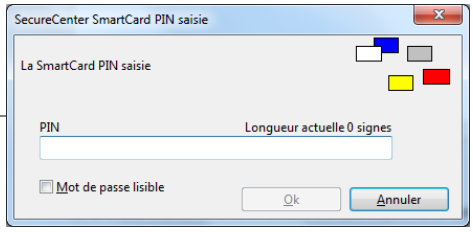


2.2 Processus de rechiffrement avec choix manuel du lecteur & du répertoire

1. Connexion avec une ancienne Smartcard, affichage de la boîte de dialogue Bienvenue et ouverture de l'outil de rechiffrement, quitter en cliquant sur «Continuer».



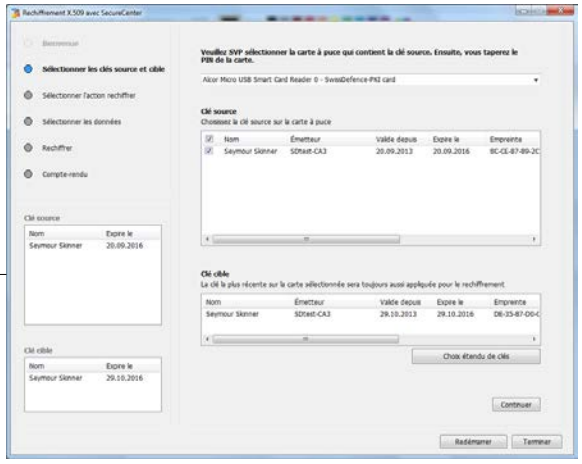
2. Connexion dans l'outil de rechiffrement avec une ancienne Smartcard (saisie du PIN)



3. Dans la boîte de dialogue, sélectionner la Smartcard qui contient la clé source (ancienne clé).

4. Sous Clé source, la boîte de dialogue montre l'ancienne clé enregistrée sur la Smartcard. Cocher si ce n'est pas le cas.

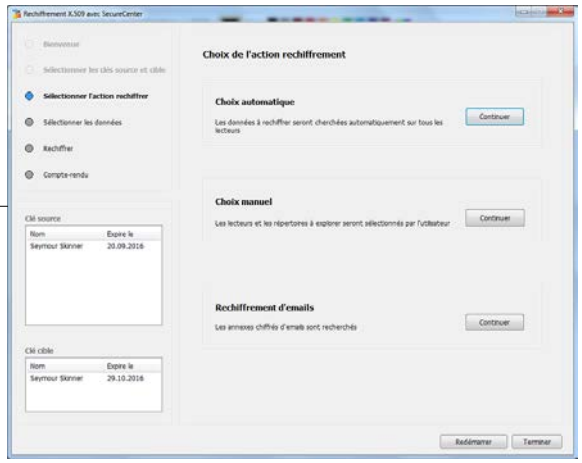
5. Dans la boîte de dialogue, la nouvelle clé enregistrée sur la Smartcard est visible sous Clé cible.
De plus, des clés supplémentaires peuvent être chargées en cliquant sur «Choix étendu de clés» (voir chapitre 2.4).



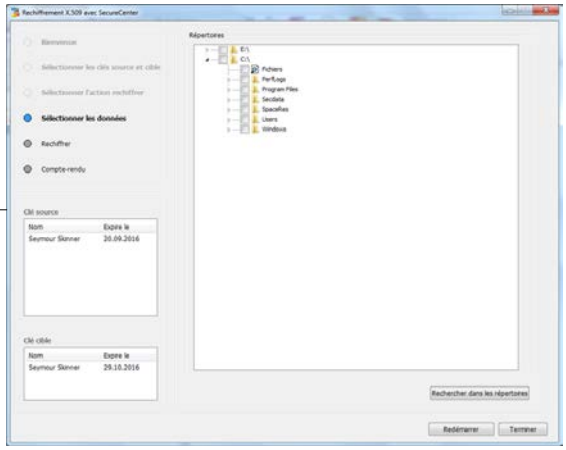
6. Dans la boîte de dialogue «Choix manuel», quitter en sélectionnant «Continuer».

(choix manuel = sélection manuelle des lecteurs et des fichiers chiffrés)

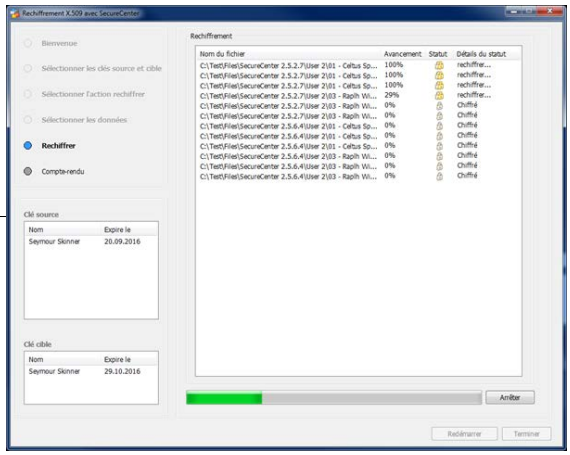
(choix automatique voir chapitre 2.1 et rechiffrement e-mail voir chapitre 2.3)



7. Sélectionner les lecteurs en les cochant, puis cliquer sur «Rechercher dans les répertoires» et sélectionner les répertoires en les cochant, puis quitter la fenêtre en cliquant sur «Démarrer le rechiffrement».

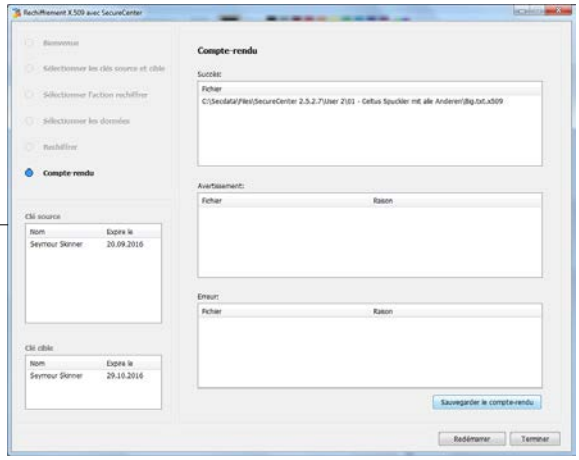


8. La boîte de dialogue avec l'état d'avancement s'affiche. Le processus peut être interrompu à tout moment en cliquant sur «Arrêter».



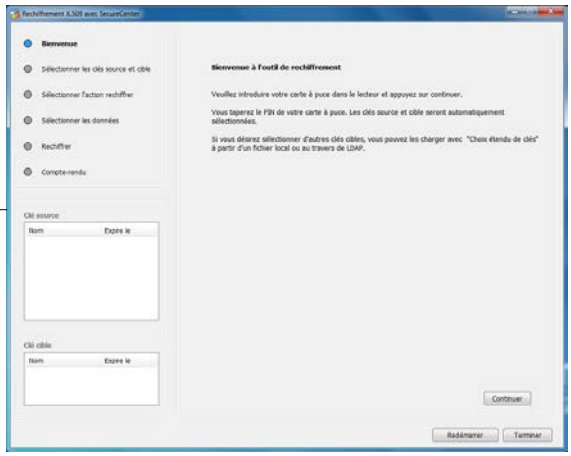
Le rechiffrement est clôturé par l'affichage du compte-rendu. Le compte-rendu dresse la liste de toutes les erreurs éventuelles (pour d'autres informations sur les messages d'erreur voir chapitre 3.1)

Le programme peut alors être redémarré pour un autre rechiffrement (sélectionner «Redémarrer») ou peut être terminé (sélectionner «Terminer»).

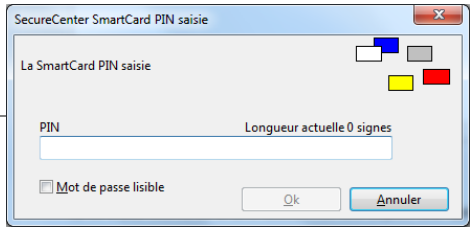


2.3 Processus de rechiffrement pour annexes e-mail

1. Connexion avec une ancienne Smartcard, affichage de la boîte de dialogue Bienvenue et ouverture de l'outil de rechiffrement, quitter en cliquant sur «Continuer».



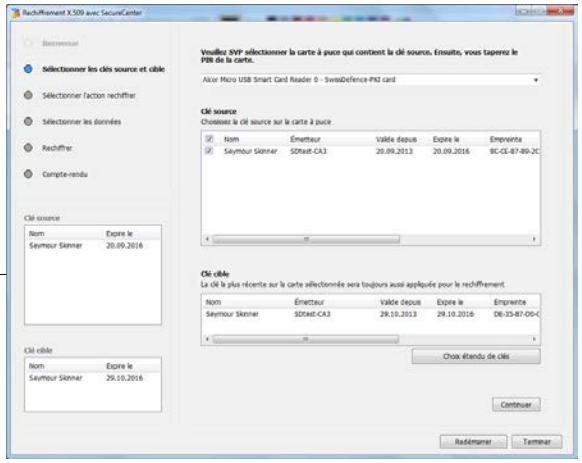
2. Connexion dans l'outil de rechiffrement avec une ancienne Smartcard (saisie du PIN)



3. Dans la boîte de dialogue, sélectionner la Smartcard qui contient la clé source (ancienne clé).

4. Sous Clé source, la boîte de dialogue montre l'ancienne clé enregistrée sur la Smartcard. Cocher si ce n'est pas le cas.

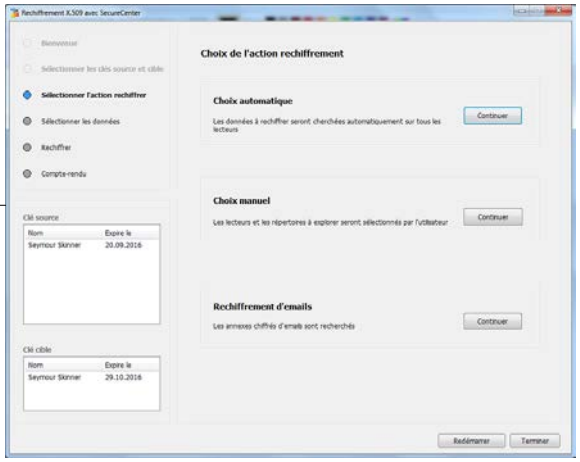
5. Dans la boîte de dialogue, la nouvelle clé enregistrée sur la Smartcard est visible sous Clé cible.
De plus, des clés supplémentaires peuvent être chargées en cliquant sur «Choix étendu de clés» (voir chapitre 2.4).



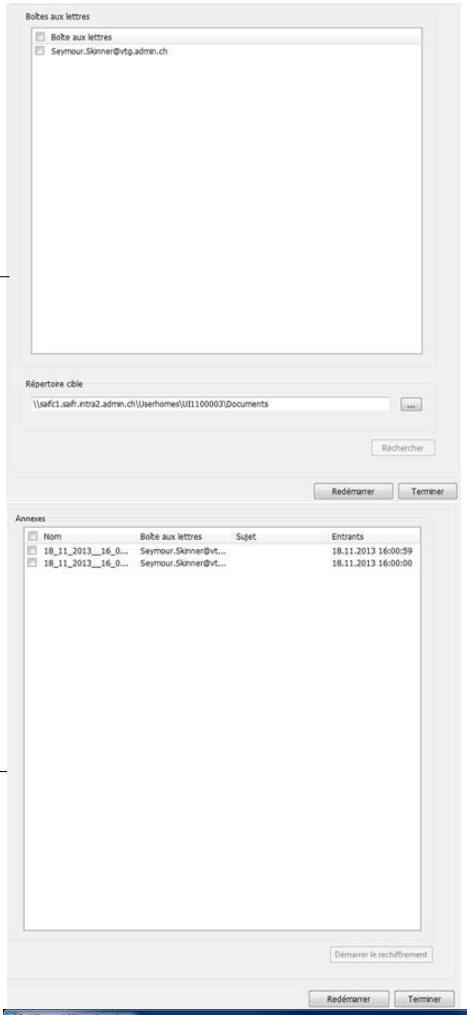
6. Dans la boîte de dialogue «Rechiffrement d'emails», quitter en sélectionnant «Continuer».

(rechiffrement d'e-mails = recherche d'annexes e-mail dans les boîtes à lettres sélectionnées)

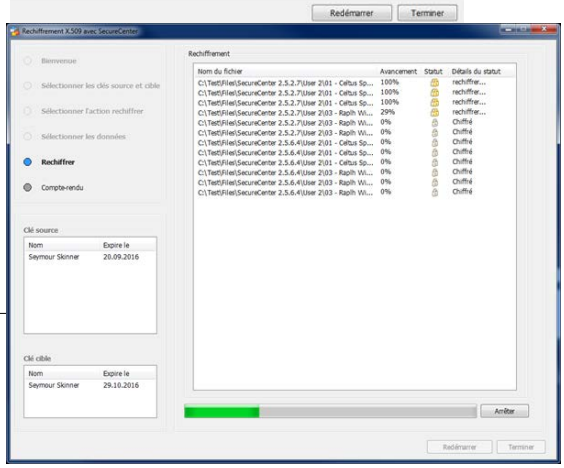
(choix automatique voir chapitre 2.1 et choix manuel voir chapitre 2.2)



7. Sélectionner les boîtes aux lettres en les cochant, puis cliquer sur «Rechercher» et sélectionner les répertoires en les cochant. Puis quitter la fenêtre en cliquant sur «Démarrer le rechiffrement», Indiquer ensuite le répertoire cible et sélectionner «Enregistrer».

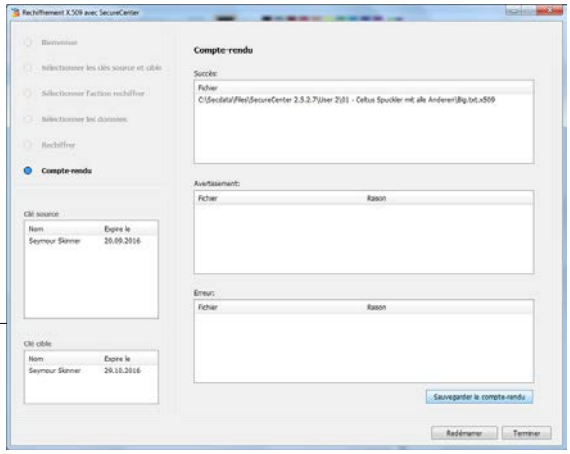


8. La boîte de dialogue avec l'état d'avancement s'affiche. Le processus peut être interrompu à tout moment en cliquant sur «Arrêter».



Le rechiffrement est clôturé par l'affichage du compte-rendu. Le compte-rendu dresse la liste de toutes les erreurs éventuelles (pour d'autres informations sur les messages d'erreur voir chapitre 3.1)

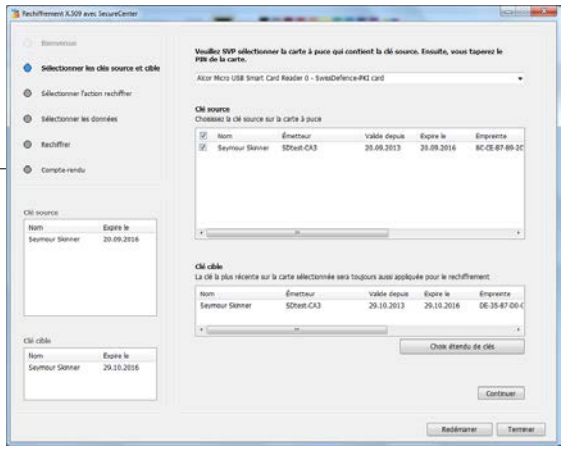
Le programme peut alors être redémarré pour un autre rechiffrement (sélectionner «Redémarrer») ou peut être terminé (sélectionner «Terminer»).



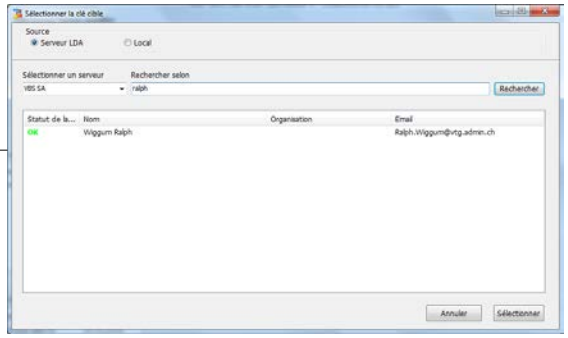
2.4 Choix étendu de clés

Si un rechiffrement avec une clé supplémentaire est nécessaire, la clé souhaitée peut être ajoutée par «Choix étendu de clés». Vous trouverez des informations sur le statut de clé au chapitre 3.2.

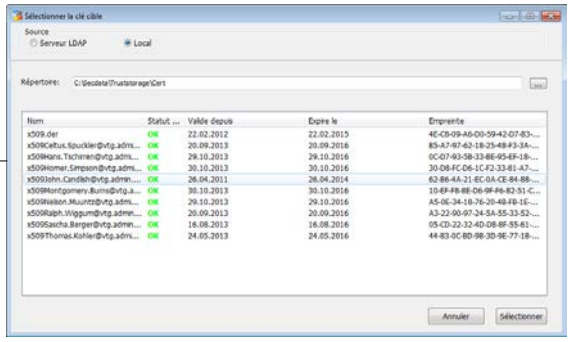
1. Sélectionner «Choix étendu de clés» pour ajouter d'autres clés.



2. Sélectionner la source «Serveur LDA» ou «Local», puis marquer les clés souhaitées et les reprendre avec «Sélectionner».



Les clés ont été reprises et sont visibles dans la boîte de dialogue «Sélectionner les clés source et cible».



3 Notes importantes

3.1 Compte-rendu de fermeture

Le compte-rendu renseigne sur le déroulement du rechiffrement: le rechiffrement est-il réussi, des erreurs se sont-elles produites, quelles erreurs se sont produites et quelle clé a échoué au rechiffrement?

Voici la liste des erreurs possibles:

Message d'erreur	Signification	Mesures
La clé demandée n'est pas disponible.	Les clés requises ne peuvent pas être chargées à partir de la Smartcard.	Retirer la Smartcard du lecteur, la remettre en place et redémarrer le rechiffrement.
Erreur générale.	Une erreur non prévisible s'est produite. Ceci peut être déclenché par des erreurs du système de fichier, des fichiers endommagés, des erreurs de cryptage, etc.	Redémarrer le rechiffrement et rechiffrer à nouveau les données non rechiffrées.
Pas de carte à puce disponible.	La Smartcard n'a pas pu être lue parce qu'elle a été retirée ou parce qu'une erreur a empêché l'accès.	Insérer la Smartcard dans le lecteur et redémarrer le rechiffrement.
Le fichier original est défectueux.	Le fichier source n'a pas pu être déchiffré, car il a déclenché une erreur dans l'unité de cryptage. Cela se produit lorsque le fichier source est endommagé.	Vérifier le fichier original et redémarrer le rechiffrement.
Erreur inconnue.	Une erreur inconnue s'est produite.	Redémarrer le chiffrement.
Erreur sur les listes de clés.	La liste de clés du fichier rechiffré ne correspond pas au résultat attendu.	Redémarrer le rechiffrement et rechiffrer à nouveau le(s) fichier(s) concerné(s).
Erreur de statut du fichier.	Le fichier rechiffré n'est pas un fichier rechiffré X.509 valide.	Redémarrer le rechiffrement et rechiffrer à nouveau le(s) fichier(s) concerné(s).

L'avertissement «Clés manquantes: utilisateur X» si le fichier correspondant ne peut plus être déchiffré par cet utilisateur après le rechiffrement. Cette situation apparaît lorsqu'aucun certificat n'a pu être trouvé pour cet utilisateur ou que le certificat n'est pas clairement identifiable. Dans ce cas, vous trouverez dans le répertoire donné aussi bien le fichier original que le nouveau fichier rechiffré que vous reconnaitrez par un nom commençant par « Votre_Nom_ », suivi du nom du fichier original. Si ce fichier doit rester accessible à l'utilisateur X et éventuellement à d'autres utilisateurs donnés, veuillez d'abord enregistrez le compte-rendu (« Sauvegarder le compte-rendu »).

S'il manque seulement quelques utilisateurs, vous pouvez les ajouter l'un après l'autre en rechiffrant le fichier à nouveau. Pour cela, redémarrez l'outil de rechiffrement et sélectionnez à la 5ème étape du processus "Choix étendu de clés". Choisissez alors la clé de chiffrement de l'utilisateur X que vous souhaitez ajouter comme clé cible. A le 6ème étape, sélectionnez «Choix manuel» et le fichier « Votre_Nom_fichier_original ». Effectuez alors le rechiffrement. Pour ajouter un autre utilisateur, il suffit de répéter ce processus. Lorsque vous avez terminé, vous pouvez supprimer le fichier d'origine et éventuellement renommer le fichier « Votre_Nom_fichier_original » avec le nom du fichier d'origine.

S'il manque de nombreux utilisateurs, veuillez consulter la FAQ (www.securecenter.ch). Vous y trouverez une autre solution qui est plus efficace dans ce cas.

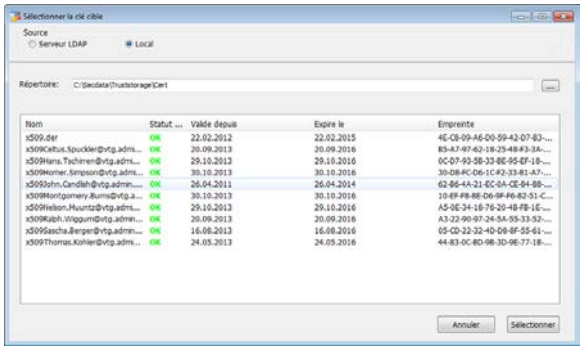
L'avertissement «Ancien format de chiffrement ou information incomplète sur la/les clé(s) » apparaît si le fichier était initialement aussi chiffré pour d'autres utilisateurs que vous, mais dont leurs noms sont inconnus. Les fichiers avec cet avertissement sont rechiffrés et sont enregistrés avec le nom « Votre_Nom_fichier_original ». Vous pouvez dans tous les cas déchiffrer un tel fichier, mais par contre les autres utilisateurs, dont les noms sont inconnus,

ne peuvent pas le déchiffrer. C'est pourquoi, il est recommandé de ne pas effacer le fichier d'origine s'il est enregistré à un endroit partagé avec d'autres utilisateurs.

3.2 Explication des statuts de clés

Vous trouverez ci-dessous les explications de statut valables pour le choix de clés étendu du serveur LDAP tout comme pour un lecteur local. Veuillez noter qu'il faut systématiquement utiliser des clés avec le marquage vert «OK». L'ajout de clés avec le choix de clés étendu est expliqué au chapitre 2.4.

Statut	Description
OK	La clé est valide et ne figure pas sur la liste des certificats révoqués (CRL).
WARN	La clé est valide, mais on ne sait pas si la clé figure sur la CRL, car: a) pas de CRL disponible, ou b) la CRL elle-même n'est plus valide
CRL	La clé figure sur la CRL, qu'elle soit valide ou périmée.



3.3 Méthodologie de travail

3.3.1 Annexes e-mail

Lors du rechiffrement, les annexes e-mail sont copiées dans un répertoire cible (déterminé par l'utilisateur) où elles sont rechiffrées. Ensuite, elles sont disponibles dans ce répertoire. Il faut noter que dans la boîte aux lettres se trouve toujours le fichier original chiffré qui n'a pas subi de modifications.
Il est donc recommandé de déposer les annexes e-mail dans un répertoire conforme aux directives de l'unité administrative concernée et de ne pas les laisser dans le programme d'e-mail. Le rechiffrement d'annexes e-mail est expliqué au chapitre 2.3.

3.3.2 Comportement après le rechiffrement

Après le rechiffrement, le poste de travail doit obligatoirement être nettoyé avec SecureCenter. La réalisation de cette opération est expliquée dans le manuel SecureCenter au chapitre 7.4 «Nettoyage du poste de travail».

3.4 Note de sécurité

Veuillez noter que les documents classés CONFIDENTIEL ne doivent être rechiffrés que sur des appareils autorisés pour le traitement de telles informations.

4 FAQ

Vous trouverez la FAQ et d'autres informations sur le rechiffrement ou sur SecureCenter sur le site www.securecenter.ch.