

# Sage XRT Business Exchange

Version 11.40.500

Gestion des Certificats de Signature :  
Alerte d'expiration et renouvellement





## Sommaire

<b>DESCRIPTION .....</b>	<b>3</b>
<b>GESTION DE L'ALERTE D'EXPIRATION .....</b>	<b>4</b>
Gestionnaire des contrats de signature .....	4
<b>SIGNATURE WEB .....</b>	<b>5</b>
Alerte d'expiration .....	5
Renouvellement de certificat.....	7

## Description

Le présent document décrit les éléments à paramétrer pour permettre de mettre en place une alerte sur l'expiration des certificats de signature ainsi que la procédure à suivre pour renouveler ces certificats avant qu'ils ne soit expirés.

## Gestion de l'alerte d'expiration

### Gestionnaire des contrats de signature

Aller dans la **Liste des signataires**.

Au niveau de chaque Signataire, vérifier les valeurs de la section **Paramètres d'exploitation**.

The screenshot shows the 'Gestionnaire des contrats de signature' application. The left sidebar contains a tree view with 'Liste des signataires' selected. The main window displays the 'Identification' tab for a signatory named 'Sign2012'. The 'Paramètres d'exploitation' section at the bottom is highlighted with a red box, showing the checkbox 'Prévenir en cas d'expiration proche' checked and the 'Seuil de déclenchement' set to 30 jours.

**Prévenir en cas d'expiration proche** : Activé par défaut. Permet d'activer la mise en place du message d'alerte pour le Signataire concerné. L'activation de l'option rend la zone **Seuil de déclenchement** accessible.

**Seuil de déclenchement** : Nombre de jours calendaires précédant l'expiration à partir desquels une alerte est émise. Valeur par défaut initiale = 30.

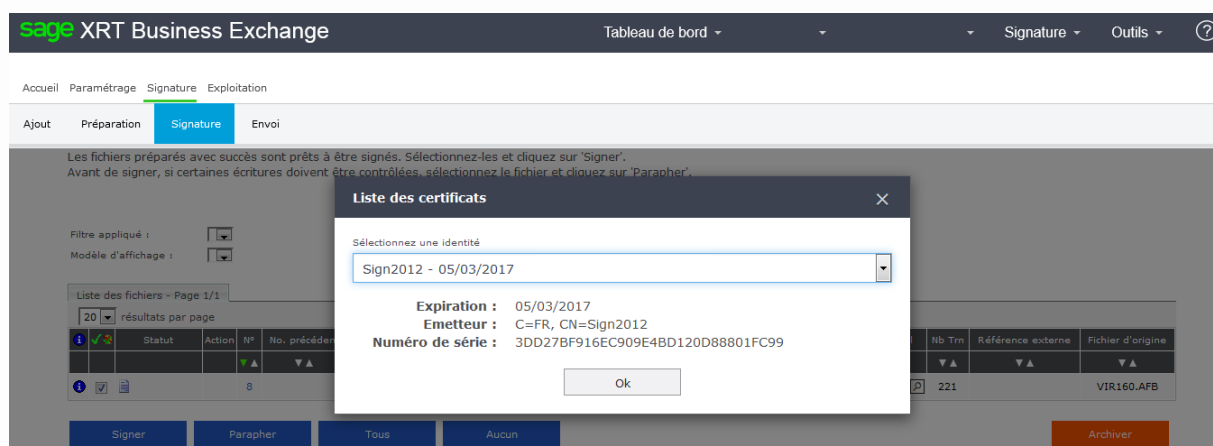


Si la valeur est 30 et un certificat a pour date d'expiration le 05/06/2017, un message d'alerte est émis à partir du 07/05/2017.

# Signature Web

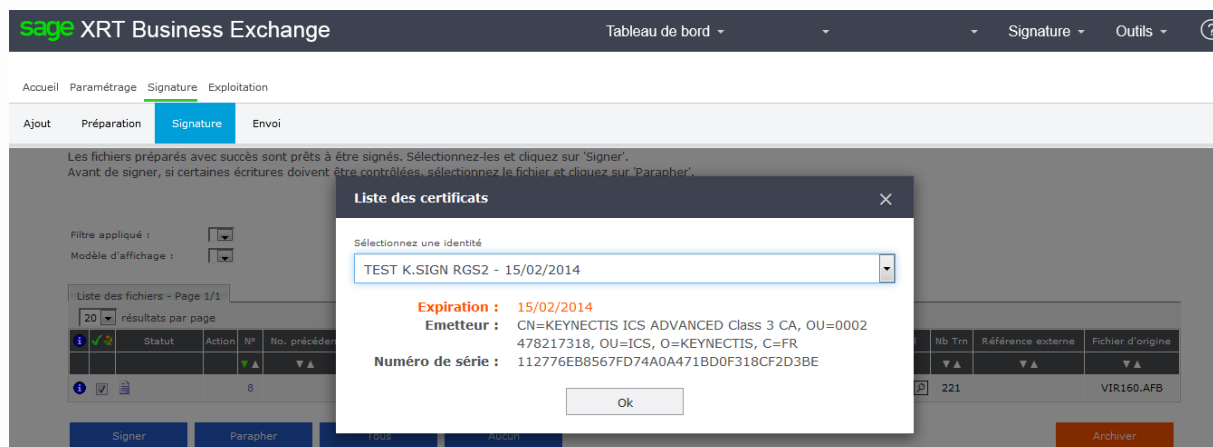
## Alerte d'expiration

Lorsqu'un Signataire signe un fichier avec un certificat, une fenêtre de sélection de certificat parmi ceux qui lui ont été attachés est proposée :

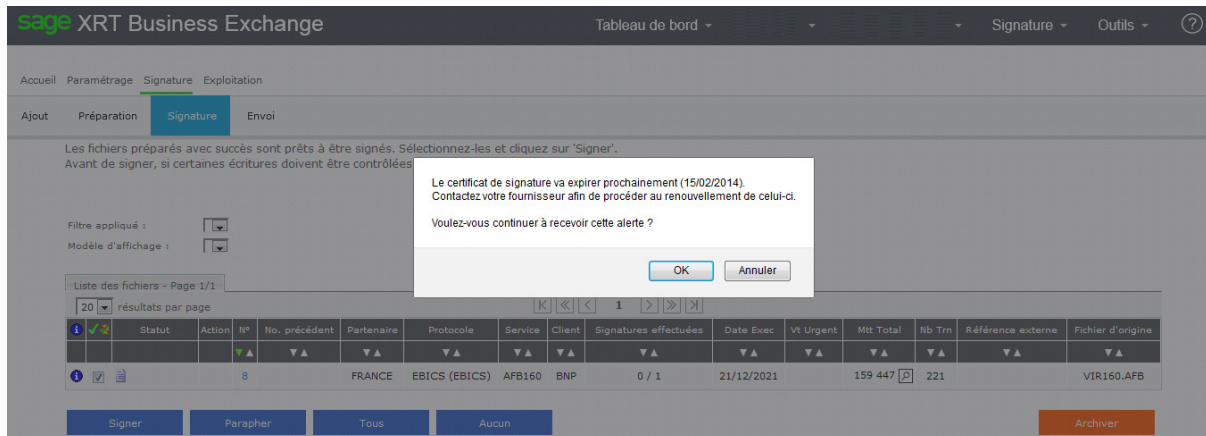


Pour procéder à une signature, le Signataire sélectionne le certificat à utiliser et clique sur OK. Il lui est alors demandé son code d'accès pour procéder à la signature du fichier.

Si le certificat sélectionné a une date d'expiration comprise dans le seuil d'alerte défini au niveau du paramétrage, une zone **Expiration**, indiquant la date d'expiration du certificat, apparaît alors en orange :



Si l'utilisateur sélectionne un certificat dans ce cas de figure et clique sur **OK**, un message d'avertissement supplémentaire lui est alors soumis avant de procéder à la demande du code pour la signature du fichier :



Si l'utilisateur clique sur le bouton **OK**, le message apparaîtra à nouveau lors d'une prochaine tentative de signature avec ce certificat.

Si l'utilisateur clique sur le bouton **Annuler**, le message ne sera plus affiché lors des tentatives de signature avec ce certificat (par contre le message apparaîtra toujours avec d'autres certificats qui arriveraient aussi à une date d'expiration proche de leur date d'échéance).



Cliquer sur le bouton **Annuler** n'annule pas le processus de signature lancé. La fenêtre de demande de saisie du code sera proposée quel que soit le choix.

## Renouvellement de certificat

Pour renouveler un certificat, aller dans le module de Signature, puis dans l'onglet **Paramétrage** et choisir dans le bandeau **Certificats**.



Avant de lancer la procédure, assurez vous de disposer du certificat à renouveler et du nouveau certificat.

Sélectionner dans le menu déroulant **Initialisation/Révocation/Mise à jour EBICS** :

Partenaire	Service	Client	Common Name	User ID	Date d'initialisation ou de Mise à jour
BNP	*	*	TEST K.SIGN RGS2	CYRIL	05/03/2016 14:35
FRANCE	*	*	TEST K.SIGN RGS2	CYRIL2	

Partenaire :

Protocole :

Service :

Client :

Buttons: Envoyer, Mettre à jour, Lettre(s) d'initialisation, Révoquer

Sélectionner le certificat que l'on souhaite renouveler, puis cliquer sur le bouton **Mettre à jour**.

**Confirmation**

Vous êtes sur le point de mettre à jour un certificat.

Avant de continuer, assurez-vous que vous disposez bien de l'ancien et du nouveau dispositif contenant les certificats de signature.

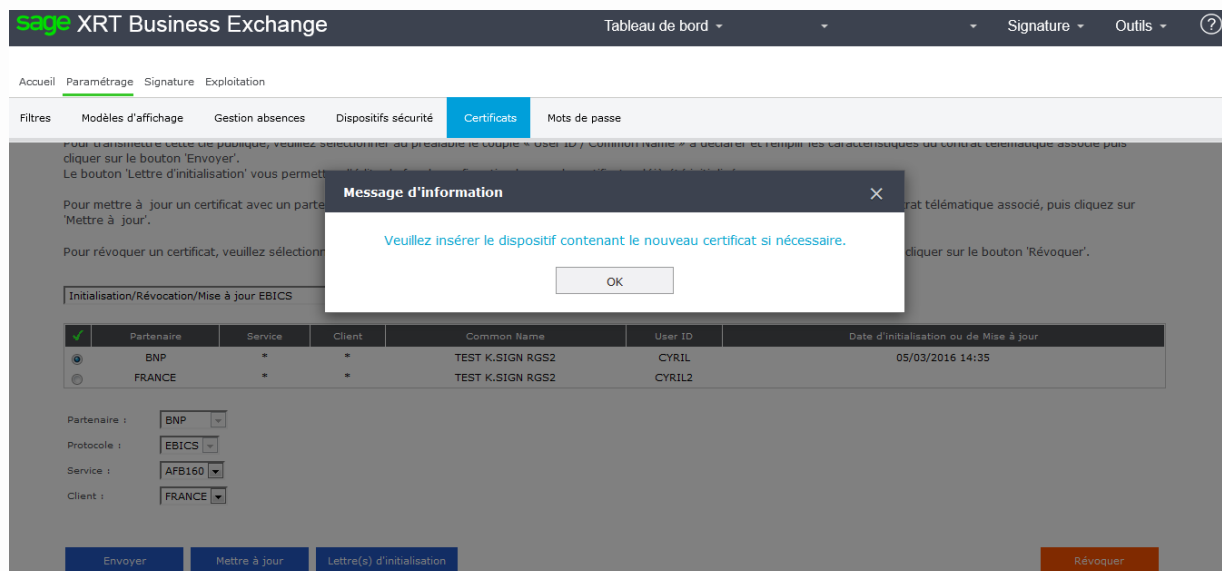
Si vous ne pouvez insérer simultanément les deux dispositifs au niveau du poste, vous devrez d'abord insérer le dispositif contenant le nouveau certificat.

Confirmez-vous le lancement de la mise à jour ?

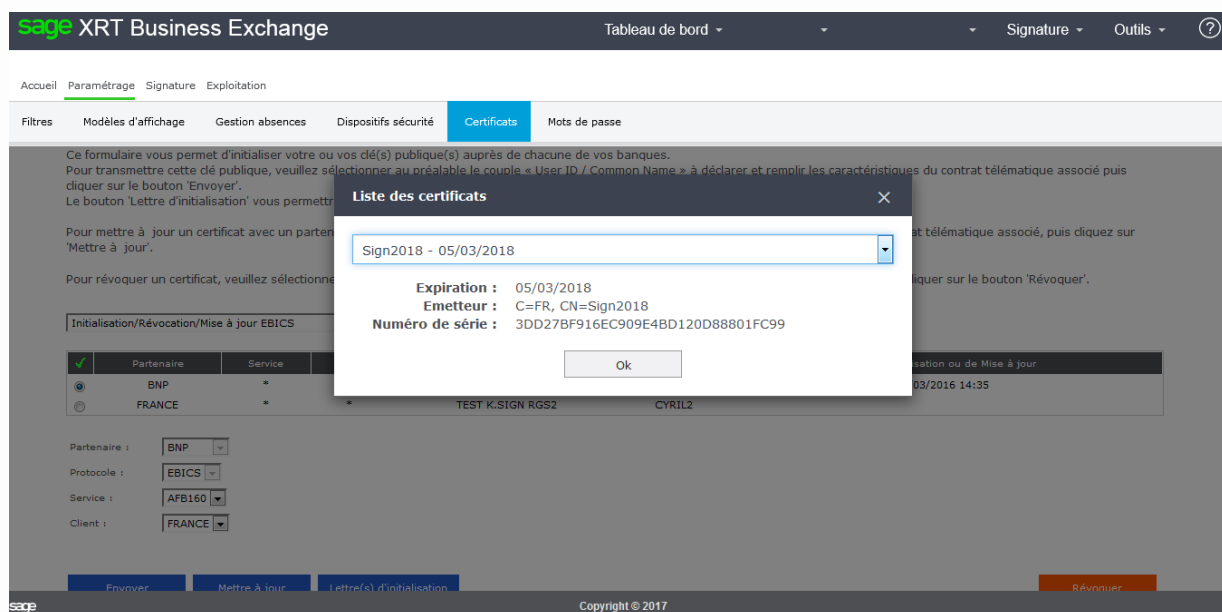
Buttons: Ok, Annuler

Après avoir lu les instructions cliquer sur OK.

Un message indique d'insérer le **nouveau** certificat.



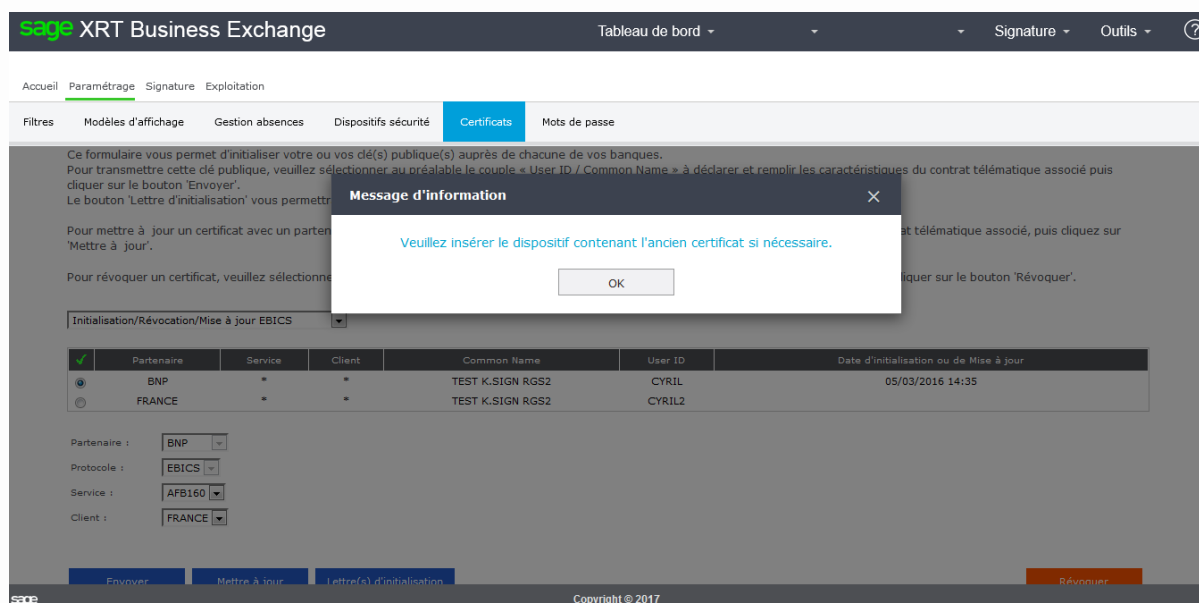
Cliquer sur **OK**.



Sélectionner le **nouveau** certificat, puis cliquer sur **OK**.



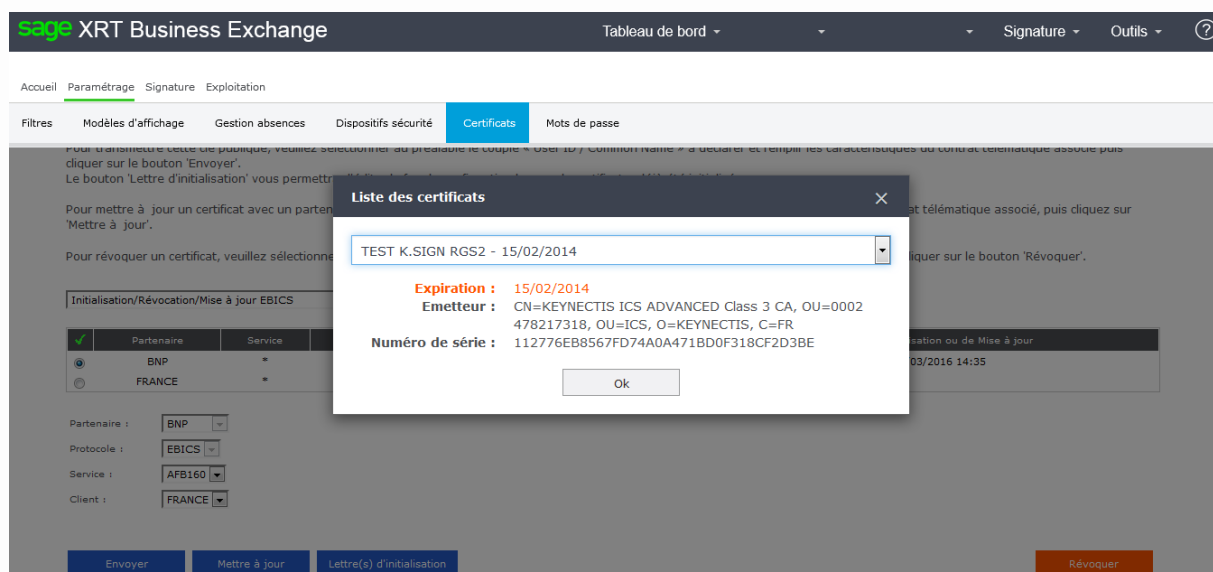
Un message indique d'insérer l' **ancien** certificat.



The screenshot shows the Sage XRT Business Exchange interface. A modal dialog titled "Message d'information" is displayed in the center, with the text: "Veuillez insérer le dispositif contenant l'ancien certificat si nécessaire." and an "OK" button. The background interface shows the "Certificats" tab selected, with a table of certificates and various configuration options.

Partenaire	Service	Client	Common Name	User ID	Date d'initialisation ou de Mise à jour
BNP	*	*	TEST K.SIGN RGS2	CYRIL	05/03/2016 14:35
FRANCE	*	*	TEST K.SIGN RGS2	CYRIL2	

Cliquer sur **OK**.



The screenshot shows the Sage XRT Business Exchange interface. A modal dialog titled "Liste des certificats" is displayed in the center. It contains a dropdown menu with the selected item "TEST K.SIGN RGS2 - 15/02/2014". Below the dropdown, the following information is displayed:

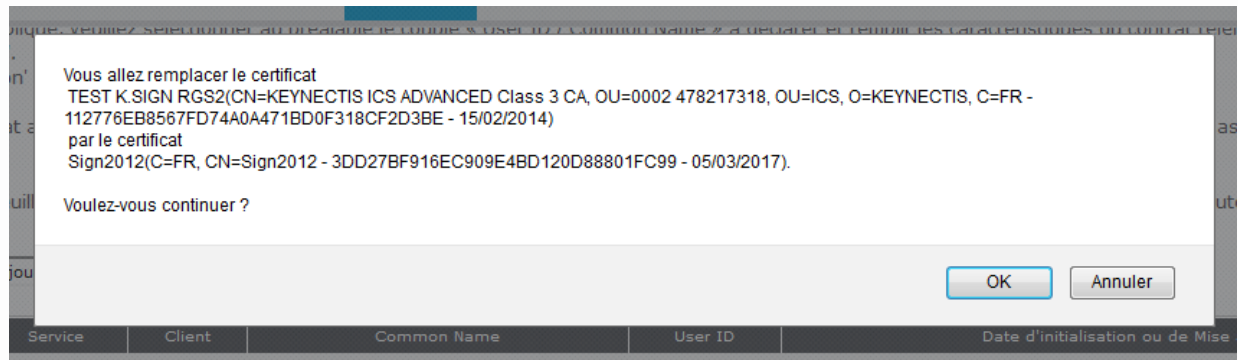
- Expiration :** 15/02/2014
- Emetteur :** CN=KEYNECTIS ICS ADVANCED Class 3 CA, OU=0002 478217318, OU=ICS, O=KEYNECTIS, C=FR
- Numéro de série :** 112776EB8567FD74A0A471BD0F318CF2D3BE

An "Ok" button is at the bottom of the dialog. The background interface shows the "Certificats" tab selected, with a table of certificates and various configuration options.

Partenaire	Service	Client	Common Name	User ID	Date d'initialisation ou de Mise à jour
BNP	*	*	TEST K.SIGN RGS2	CYRIL	05/03/2016 14:35
FRANCE	*	*	TEST K.SIGN RGS2	CYRIL2	

Sélectionner l'**ancien** certificat (si sa date d'expiration est proche, on retrouve la date d'expiration indiquée en orange), puis cliquer sur **OK**.

Un message récapitule les informations du nouveau et de l'ancien certificat.



Vérifier avec soin que les certificats sélectionnés sont bien ceux voulus et, si c'est le cas, cliquer sur **OK**.

En cas de détection d'une erreur de sélection de certificat à ce niveau, cliquer sur **Annuler** et recommencer l'opération de renouvellement depuis le début.

Après avoir cliqué sur **OK**, le code d'accès de l' ancien certificat est demandé afin de sécuriser l'envoi de la commande de mise à jour au serveur de la banque.

Une fois cette opération effectuée, l'ancien certificat n'est plus utilisable et le nouveau certificat est opérationnel.