

Ebics : Utilisation de Sage direct sur plusieurs postes

Prenons l'exemple d'un client ayant 2 utilisateurs (User 1 et User 2) et qui souhaite installer Sage direct sur 3 postes (Poste 1 et 2 pour l'User 1 et Poste 3 pour l'User 2).

Installation du Poste 1 :

Génération des certificats à partir du menu **Outils/Options/Bancaire**.

Création de la banque sur le poste 1 :

Création de banque

Nom: Banque de test

Code: test Contact: Contact

URL: http://url-de-test.fr

User ID: USER1 Host ID: HOST1

Partner ID: PARTNER1

Certificat authentification (X002) CN=Usage 1/5BDE16F6/My

Certificat chiffrement (E002) CN=Usage 2/6DBD3B74/My

Certificat signature (A005) CN=Usage 3/362ACCDE/My

Certificat banque (E002)

Certificat banque (X002)

Certificat banque SSL

Etat	Phase	Etat
	INI	A faire
	HIA	A faire
	HPB	A faire

Avancé

Ok Annuler

L'utilisateur initialise le contrat auprès de sa banque. Après la récupération des clés de la banque, le bouton "Avancé" permet de connaître le début de la plage d'utilisation des numéros d'ordre.

⚠ L'identification d'une émission se situe dans un premier temps au niveau de l'ordre de transfert (orderId) et de la société (partnerId). Donc ce couple doit être unique pour une banque donnée.

Une bonne plage d'utilisation consiste à donner suffisamment de numéros d'ordre afin que l'utilisateur n'ait pas une plage trop restreinte et qu'il ne rattrape pas trop vite la plage de l'utilisateur suivant.

Exemple :

Sur le poste 1 OrderId Transfert = A003

Sur le poste 2 OrderId Transfert = C003

Sur le poste 3 OrderId Transfert = E003

Options avancées

Paramètres de l'ordre Autres paramètres

Identifiant courant

OrderId INI A001

OrderId HIA A002 ☐ Valider

OrderId HPB A003

OrderId Transfert A01A

Gestion des paramètres supplémentaires des ordres

Nom	Type	Valeur
	String	

Supprimer

Ok Annuler

Le Poste 1 est prêt à l'emploi.

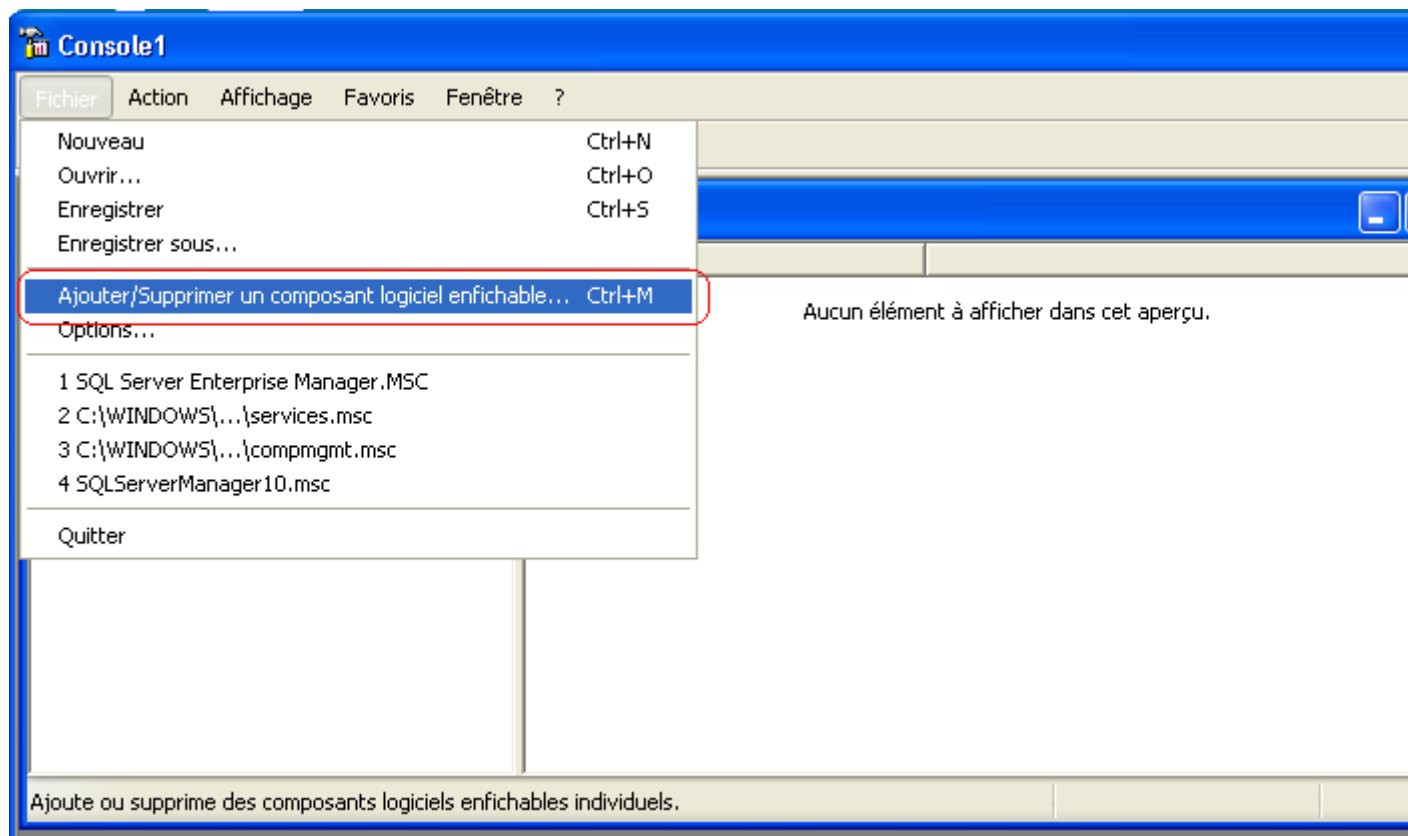
Installation du Poste 2 (même User que sur Poste 1) :

Avant l'installation du Poste 2, il faut exporter les certificats d'authentification, de chiffrement et de signature du Poste 1.

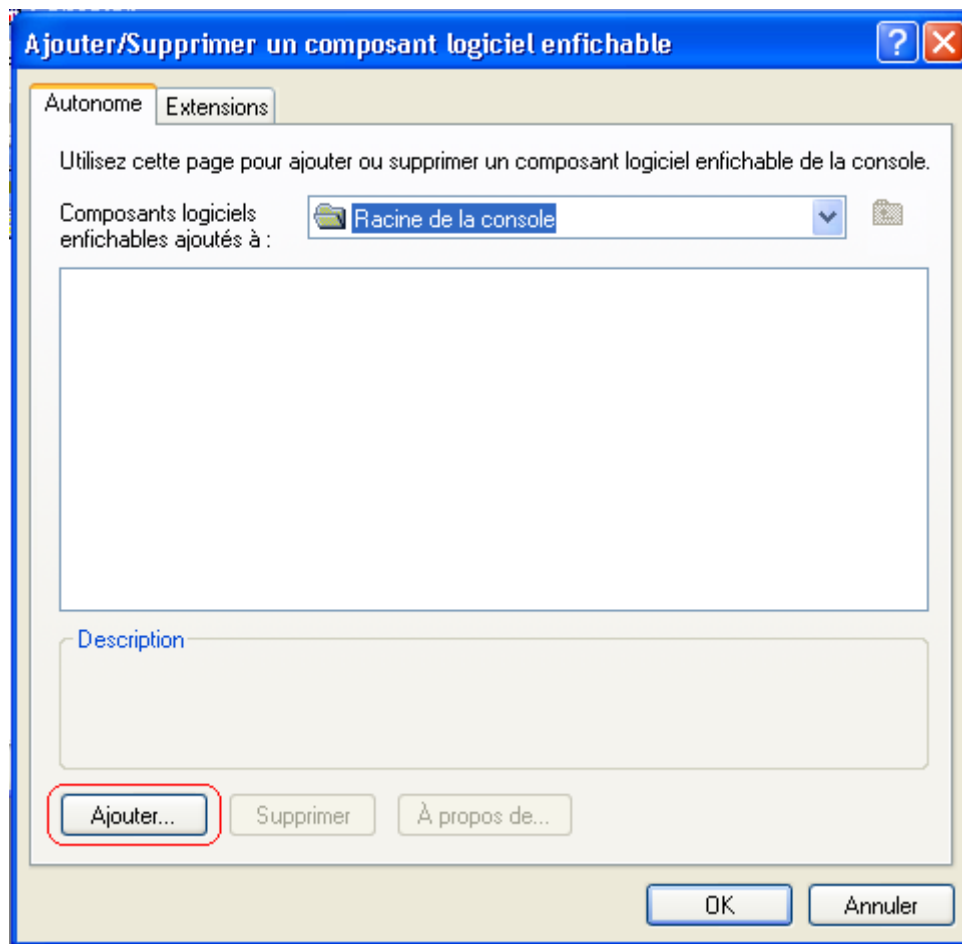
Export des certificats :

Il faut lancer MMC à partir du menu **Démarrer/Exécuter/MMC** et suivre la procédure suivante afin d'exporter les certificats :

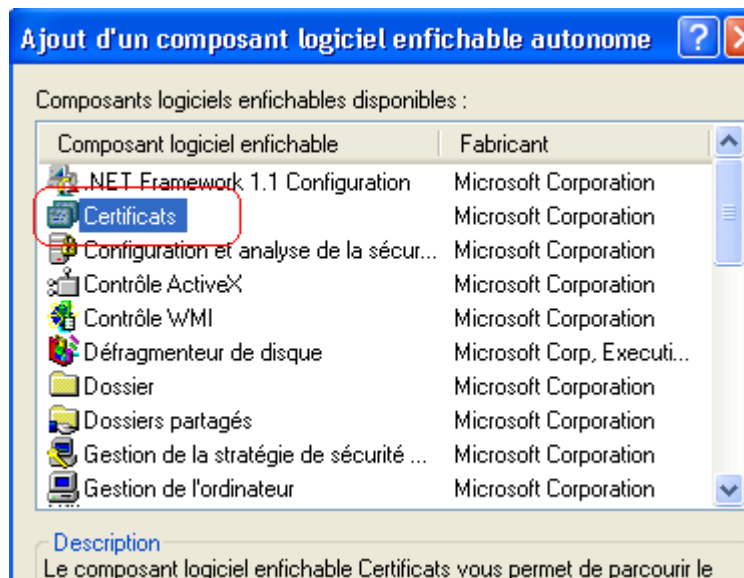
Fichier/Ajouter/Supprimer un composant logiciel enfichable

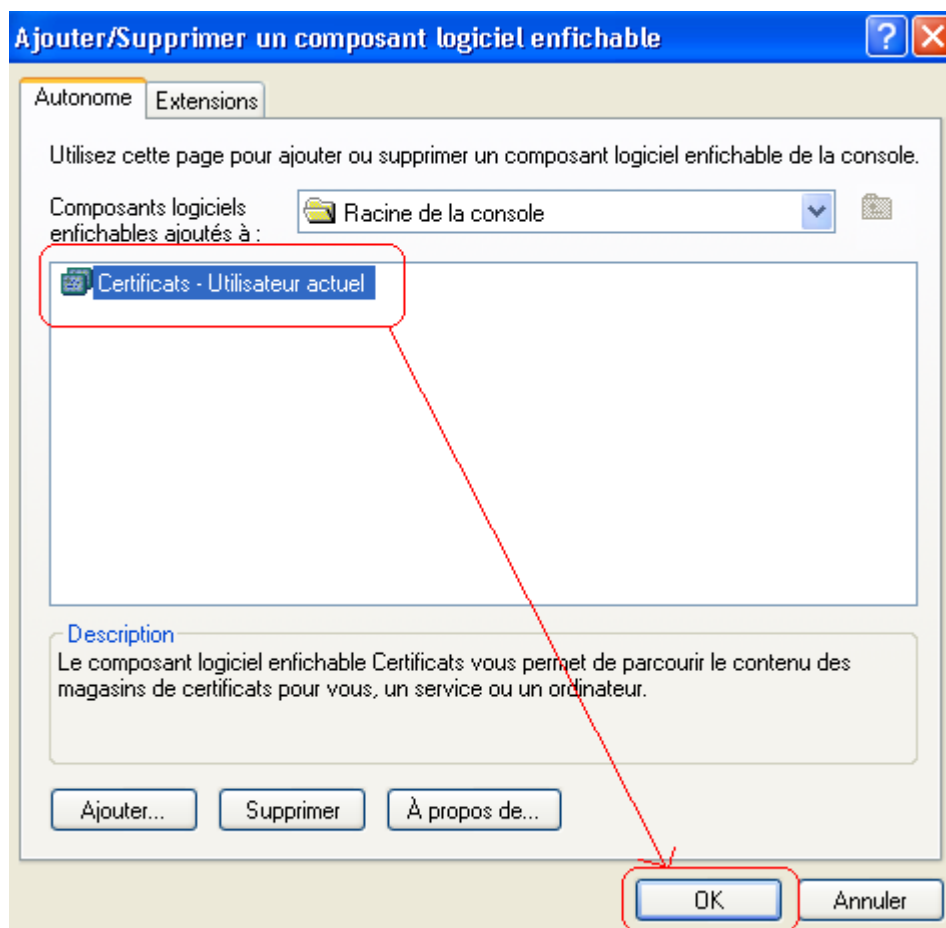


Appuyez sur le bouton **Ajouter** :

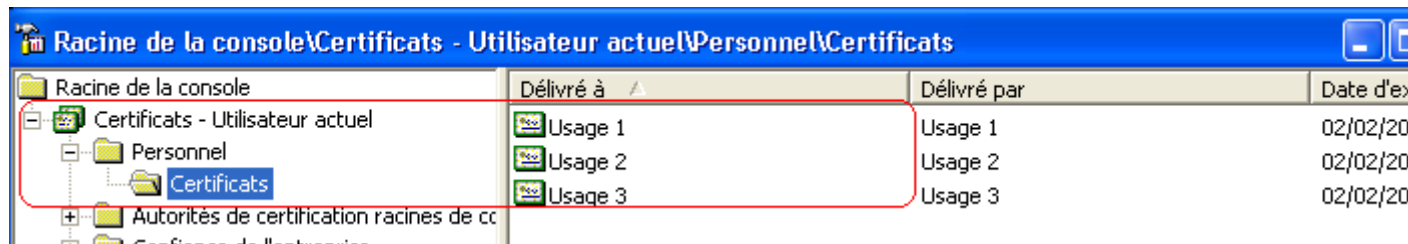


Sélectionnez la ligne **Certificats** et appuyez sur le bouton **Ok** :

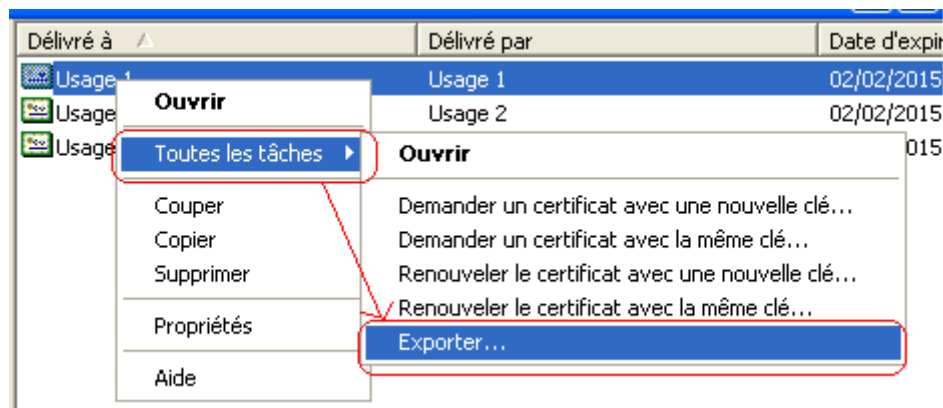




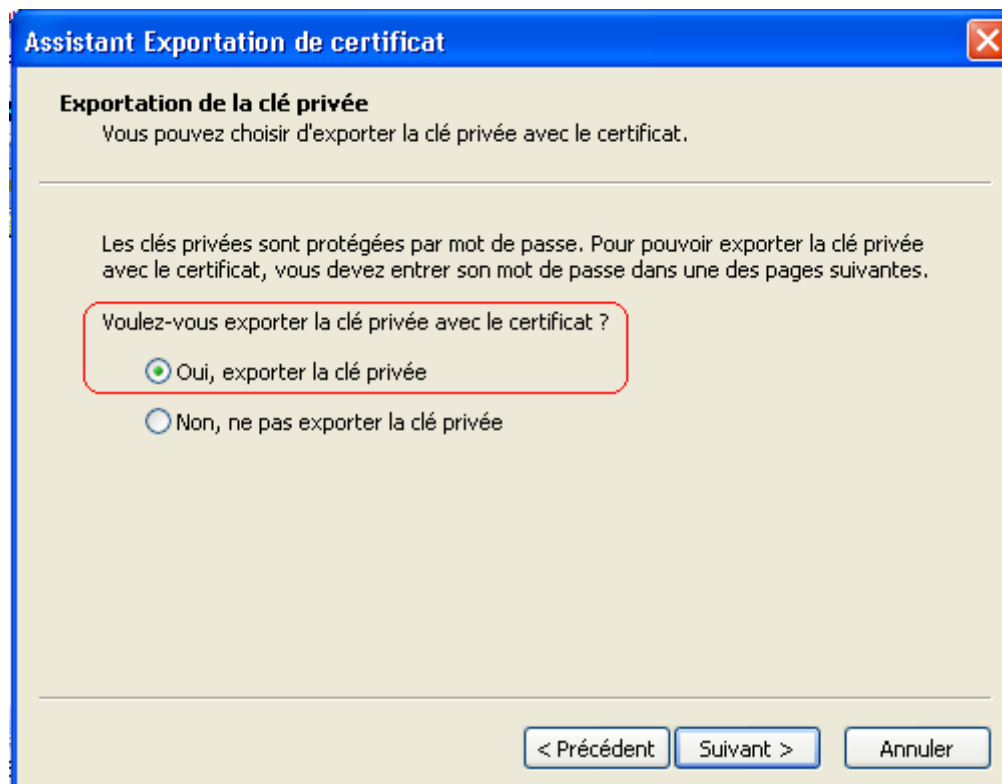
Les certificats apparaissent alors dans la liste :



Sur chacun des certificats à exporter, faire un **Clic droit/toutes les tâches/Exporter** :



L'assistant d'exportation suivant s'ouvre :



Assistant Exportation de certificat

Format de fichier d'exportation
Les certificats peuvent être exportés sous plusieurs formats de fichier.

Sélectionnez le format à utiliser :

- ☐ Binaire codé DER X.509 (.cer)
- ☐ Codé à base 64 X.509 (.cer)
- ☐ Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)
 - ☐ Inclure tous les certificats dans le chemin d'accès de certification si possible
- ☒ Échange d'informations personnelles - PKCS #12 (.pfx)
 - ☒ Inclure tous les certificats dans le chemin d'accès de certification si possible
 - ☐ Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)
 - ☐ Supprimer la clé privée si l'exportation s'est terminée correctement

< Précédent Suivant > Annuler

Attention : *Suivant les environnements, il conviendra également de cocher la case "Exporter toutes les propriétés étendues" (exemple: Vista)*

Assistant Exportation de certificat

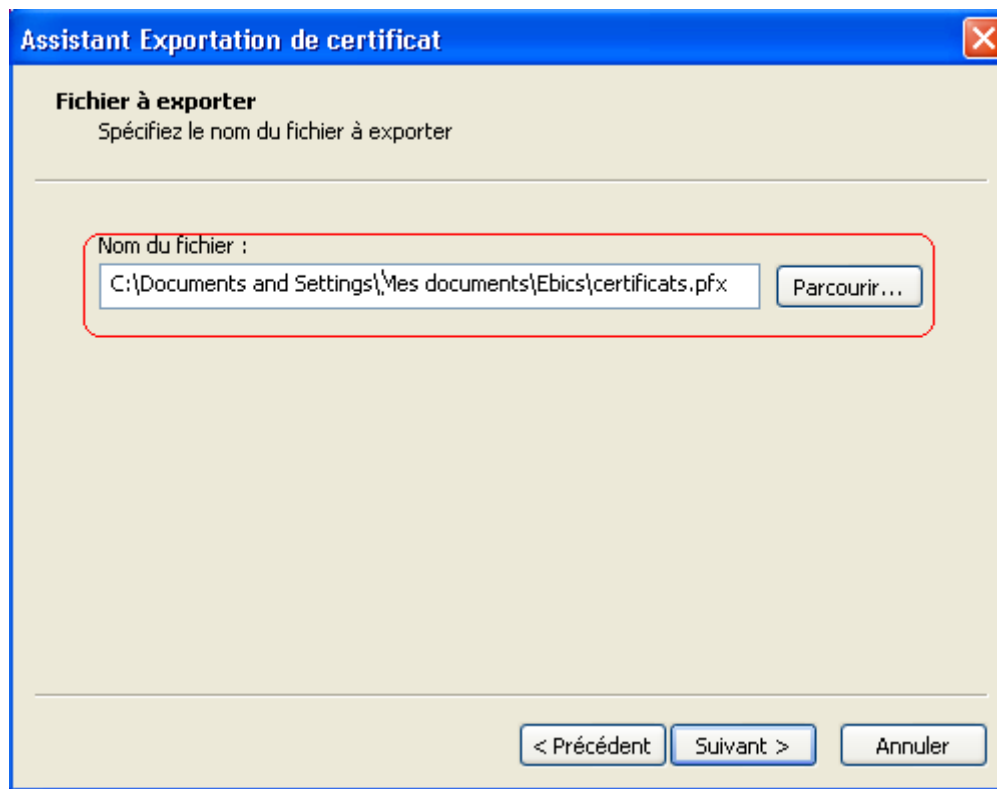
Mot de passe
Pour maintenir la sécurité, vous devez protéger la clé privée en utilisant un mot de passe.

Entrez et confirmez le mot de passe.

Mot de passe :

Confirmer le mot de passe :

< Précédent Suivant > Annuler



Import des certificats :

Une fois les certificats exportés du Poste 1, copiez les fichiers pfx contenant les certificats X509 exportés du Poste 1 sur le Poste 2.

Double-cliquez sur chaque fichier pfx pour importer le certificat X509, l'assistant d'importation apparaît :

Renseignez le fichier pfx à importer puis sur la fenêtre suivante saisissez le mot de passe en indiquant que la clé est exportable.

Assistant Importation de certificat

Mot de passe

Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.

Entrez le mot de passe de la clé privée.

Mot de passe :

☐ Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

☒ Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.

< Précédent Suivant > Annuler

Attention : *Suivant les environnements, il conviendra également de cocher la case "Inclure toutes les propriétés étendues" (Vista)*

Sélectionnez le magasin Personnel :

Assistant Importation de certificat

Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont stockés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.

☐ Sélectionner automatiquement le magasin de certificats selon le type de certificat

☒ Placer tous les certificats dans le magasin suivant

Magasin de certificats :
Personnel Parcourir...

< Précédent Suivant > Annuler

Dans Sage direct, paramétrez la banque en sélectionnant les certificats importés :

Création de banque

Nom: Banque de test

Code: test Contact: Contact

URL: http://url-de-test.fr

User ID: USER1 Host ID: HOST1

Partner ID: PARTNER1

Certificat authentification (X002) CN=Usage 1/5BDE16F6/My ...

Certificat chiffrement (E002) CN=Usage 2/6DBD3B74/My ...

Certificat signature (A005) CN=Usage 3/362ACCDE/My ...

Certificat banque (E002)

Certificat banque (X002)

Certificat banque SSL

Etat

Phase	Etat
INI	A faire
HIA	A faire
HPB	A faire

Avancé

Ok Annuler

Paramétrez les options avancées de la banque en indiquant des plages d'identifiant pour INI, HIA, HPB et Transfert et en cochant "Valider". **La banque doit passer à l'état HIA initialisé.**

Options avancées

Paramètres de l'ordre Autres paramétrages

Identifiant courant

OrderId INI	C001	
OrderId HIA	C002	<input checked="" type="checkbox"/> Valider
OrderId HPB	C003	
OrderId Transfert	C004	

Gestion des paramètres supplémentaires des ordres

Nom	Type	Valeur
	String	

Supprimer

Ok Annuler

Initialisez la banque (les certificats de la banque sont ainsi récupérés). **La banque doit passer à l'état initialisé** et les transferts peuvent commencer sur ce poste.

Installation du Poste 3 (User différent du Poste 1) :

Avant l'installation du Poste 3, **il faut exporter les certificats d'authentification et de chiffrement uniquement pas celui de signature** du Poste 1 (car l'User du Poste 3 est différent de l'User du Poste 1) (*voir procédure précédente pour l'export et l'import des certificats.*)

Une fois les certificats d'authenticité et de chiffrement importés, générez les certificats sur le Poste 3 pour créer un certificat X509 de signature par le menu **Outils/Options/Bancaire**.

Paramétrez la banque en sélectionnant les certificats X509 importés pour l'authentification et le chiffrement puis utilisez le certificat de signature généré sur ce poste précédemment.

Paramétrez les options avancées de la banque en indiquant des plages d'identifiant pour INI HIA, HPB et Transfert et **ne cochant pas "Valider"**. **La banque doit rester à l'état "à faire"**.

Options avancées

Paramètres de l'ordre Autres paramétrages

Identifiant courant

OrderId INI	E001	
OrderId HIA	E002	<input type="checkbox"/> Valider
OrderId HPB	E003	
OrderId Transfert	E004	

Gestion des paramètres supplémentaires des ordres

Nom	Type	Valeur
	String	

Supprimer

Ok Annuler

Initialisez la banque avec les deux phases habituelles INI/HIA puis HPB (les certificats de la banque sont ainsi récupérés). **La banque doit passer à l'état initialisé** et les transferts peuvent commencer sur ce poste.