# **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 Ba	anque de test			
Code tes	st	Contact Contac	st	
URL	http://url-de-test.	fr		
User ID	USER1		Host ID	HOST1
Partner ID	PARTNER1			
Certificat a Certificat c Certificat s Certificat b Certificat b Certificat b	uthentification (X002) hiffrement (E002) ignature (A005) anque (E002) anque (X002) anque SSL	CN=Usage 1/5BDE CN=Usage 2/6DBE CN=Usage 3/362A	16F6/My 03B74/My CCDE/My	
😑 Etat	Phase INI HIA HPB	Etat A faire A faire 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 3 OrderId Transfert = E003

Identifiant courant Orderld INI A001 Orderld HIA A002 Valider Orderld HPB A003 Orderld Transfert A01A Gestion des paramètres supplémentaires des ordres Nom Type Valeur String Supprimer	alametres de l'ordre	Autres paramétr	trages
Orderld HIA A002   Orderld HPB A003   Orderld Transfert A01A    Gestion des paramètres supplémentaires des ordres   Nom Type   Valeur Supprimer	dentifiant courant	A001	
Orderld HPB A003 Orderld HPB A003 Orderld Transfert A01A Gestion des paramètres supplémentaires des ordres Nom Type Valeur Supprimer String		A001	
Orderld Transfert A01A Gestion des paramètres supplémentaires des ordres		A002	
Gestion des paramètres supplémentaires des ordres	Orderld Transfert	۵01۵	
	Nom	Type String	Valeur Supprimer
< >>	1-1 <sup>-1</sup> F		

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

🚡 Console1			
Fichier Action Affichage Favoris Fenêtre ?			
Nouveau	Ctrl+N		
Ouvrir	Ctrl+O		
	Ctrl+S		
Enregistrer sous			
Ajouter/Supprimer un composant logiciel enfichable Options	Ctrl+M	Aucun élément à afficher dans cet aperçu.	
1 SQL Server Enterprise Manager.MSC 2 C:\WINDOWS\\services.msc 3 C:\WINDOWS\\compmgmt.msc 4 SQLServerManager10.msc			
Quitter			
Ajoute ou supprime des composants logiciels enfichables i	ndividuels.		_

Appuyez sur le bouton Ajouter :

Ajouter/Supprimer un composant logiciel enfichable 🛛 🔹 🔀
Autonome Extensions
Utilisez cette page pour ajouter ou supprimer un composant logiciel enfichable de la console.
Composants logiciels enfichables ajoutés à :
Description
Ajouter Supprimer A propos de
OK Annuler

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

A	jout d'un composant logiciel enfi	chable autonome 📲	?  >
	Composants logiciels enfichables disponible	s:	
	Composant logiciel enfichable	Fabricant	^
	Antiperation	Microsoft Corporation	
	Certificats	Microsoft Corporation	
	Configuration et analyse de la sécur	Microsoft Corporation	
	🛍 Contrôle ActiveX	Microsoft Corporation	
	🔏 Contrôle WMI	Microsoft Corporation	
	😵 Défragmenteur de disque	Microsoft Corp, Executi	
	Dossier 📃	Microsoft Corporation	
	링 Dossiers partagés	Microsoft Corporation	
	le stion de la stratégie de sécurité	Microsoft Corporation	
	📕 Gestion de l'ordinateur	Microsoft Corporation	~

Le composant logiciel enfichable Certificats vous permet de parcourir le

Composant logiciel enfichable Certificats
Ce composant logiciel enfichable gérera toujours les certificats pour : • Mon compte d'utilisateur
O Le compte du service
C Le compte de l'ordinateur
< Précédent Terminer Annuler

Ajouter/Supprimer un composant logiciel enfichable 🛛 🔹 💽
Autonome Extensions
Utilisez cette page pour ajouter ou supprimer un composant logiciel enfichable de la console.
Composants logiciels aioutés à :
Certificats - Utilisateur actuel
Description Le composant logiciel enfichable Certificats vous permet de parcourir le contenu des
magasins de certificats pour vous, un service ou un ordinateur.
Aiouter Supprimer À propos de

Les certificats apparaissent alors dans la liste :

🚡 Racine de la console\Certificats - U	tilisateur actuel\Perso	nnel\Certificats	
📮 Racine de la console	Délivré à 🔺	Délivré par	Date d'ex
🖻 🐻 Certificats - Utilisateur actuel	🔛 Usage 1	Usage 1	02/02/20
	🔛 Usage 2	Usage 2	02/02/20
Certificats	🔛 Usage 3	Usage 3	02/02/20
Autorites de certification racines de co	c		

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

Délivré à	Δ	Délivré par	Date d'expi
Usage 🔛	1	Usage 1	02/02/2015
🔛 Usage	Ouvrir	Usage 2	02/02/2015
See Usage	Toutes les tâches 🔸	Ouvrir	015
	Couper	Demander un certificat avec une nouvelle c	lé
	Copier	Demander un certificat avec la même clé	
	Supprimer	Renouveler le certificat avec une nouvelle (	:lé
	Bropriétés	Renouveler le certificat avec la même clé	
	Frophetes	Exporter	
	Aide	<u></u>	
L '			

L'assistant d'exportation suivant s'ouvre :

As	sistant Exportation de certificat	K
	<b>Exportation de la clé privée</b> Vous pouvez choisir d'exporter la clé privée avec le certificat.	
	Les clés privées sont protégées par mot de passe. Pour pouvoir exporter la clé privée avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.	
	Voulez-vous exporter la clé privée avec le certificat ?	
	⊙ Oui, exporter la clé privée	
	🚫 Non, ne pas exporter la clé privée	
	< Précédent Suivant > Annuler	)

Assistant Exportation de certificat
Format de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.
Sélectionnez le format à utiliser :
O 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
<ul> <li>Échange d'informations personnelles - PKCS #12 (.pfx)</li> <li>Inclure tous les certificats dans le chemin d'accès de certification si possible</li> </ul>
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

<u>Attention</u> : Suivant les environnements, il conviendra également de cocher la case ''Exporter toutes les propriétés étendues'' (exemple:Vista)

Assistant Exportation de certificat
<b>Mot de passe</b> 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

Assistant Exportation de certificat	×
Fichier à exporter Spécifiez le nom du fichier à exporter	
(Nom du fichier :	
C:\Documents and Settings\Mes documents\Ebics\certificats.pfx Parcourir	
< 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	×
<b>Mot de passe</b> 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	

<u>Attention</u> : 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	
<ul> <li>Placer tous les certificats dans le magasin suivant</li> <li>Magasin de certificats :</li> </ul>	
Personnel Parcourir	
< Précédent Suivant > Annuler	

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

Création	de banque							X
Nom Ba	inque de test							
Code test		Con	tact Conta	ct				
								_
URL	http://url-de	-test.fr						
User ID	USER1			Host ID	HC	DST1		
Partner ID	PARTNER1			]				
				1				_
Certificat authentification (X002) CN=Usage 1/5BDE16F6/My								
Certificat c	Certificat chiffrement (E002) CN=Usage 2/6DBD3B74/My							
Certificat signature (A005) CN=Usage 3/362ACCDE/My								
Certificat b	Certificat banque (E002)							
Certificat b	Certificat banque (X002)						3	
Certificat b	anque SSL							
<b>— — —</b> • •			<b>F</b>					
U Etat	Phase		E tat				Avance	
			A raire					
	HPB		A faire					
					(	Ok	Annuk	er

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.

ptions avancées		
Paramètres de l'ordre	Autres paramétr	ages
Identifiant courant		
OrderId INI	C001	
Orderld HIA	C002	Valider
Orderld HPB	C003	
Orderld Transfert	C004	
Sestion des naramètr	es supplémentaire	se des ordres
	co ouppionion dare	
Nom	Туре	Valeur Supprimer
<u>}</u>	String	
<	111	
		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''.

'aramètres de l'ordre	Autres paramé	itrages				
Orderld INI	E001					
Orderld HIA	E002	Valider				
Orderld HPB	E003					
Orderld Transfert	E004					
Nom	Type String	Valeur	Supprimer			

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.