ATEXO

Progiciel LOCAL TRUST MPE v3

GUIDE DE GESTION DES BI-CLES DE CHIFFREMENT

IDENTITE DU DOCUMENT	
Client	ATEXO
Affaire	Progiciel LOCAL TRUST MPE v3
Titre	Guide de gestion des bi-clés de chiffrement
Référence	ATEXO – MPE – xxx
Etat	Final
Version	1.0
Du	21 juin 2011
Dernière page	18

Table des matières

1 OBJECTIFS DU PRESENT DOCUMENT

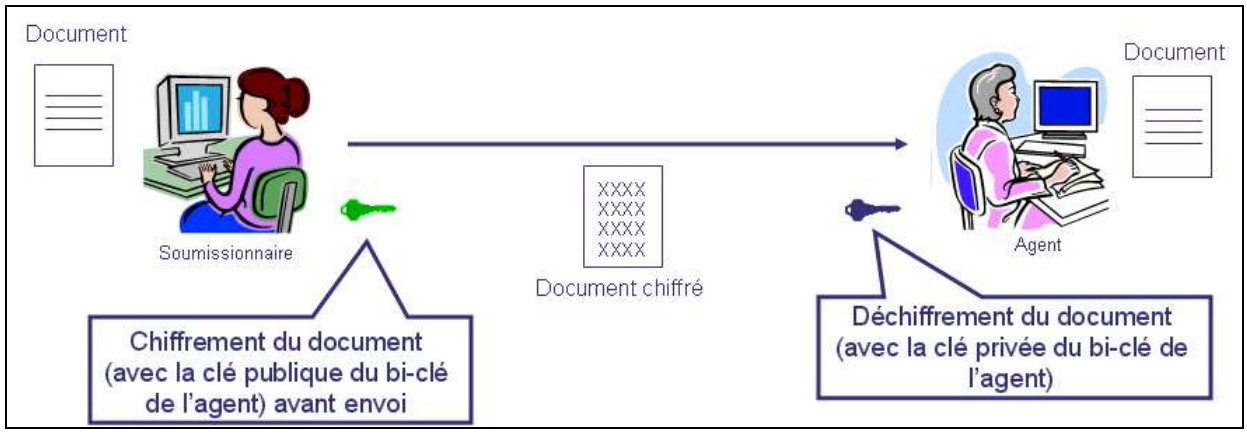
Ce guide a pour but d'assister les agents à :

- la création de bi-clés de chiffrement,
- l'ajout de bi-clés déjà existants,
- l'export de bi-clés de chiffrement,
- l'import des bi-clés de chiffrement.

L'application LOCAL TRUST MPE permet de générer des certificats électroniques afin de pouvoir réaliser des opérations de chiffrement et de déchiffrement des plis électroniques grâce au bi-clé du certificat. Un bi-clé est composé d'une clé publique et d'une clé privée.

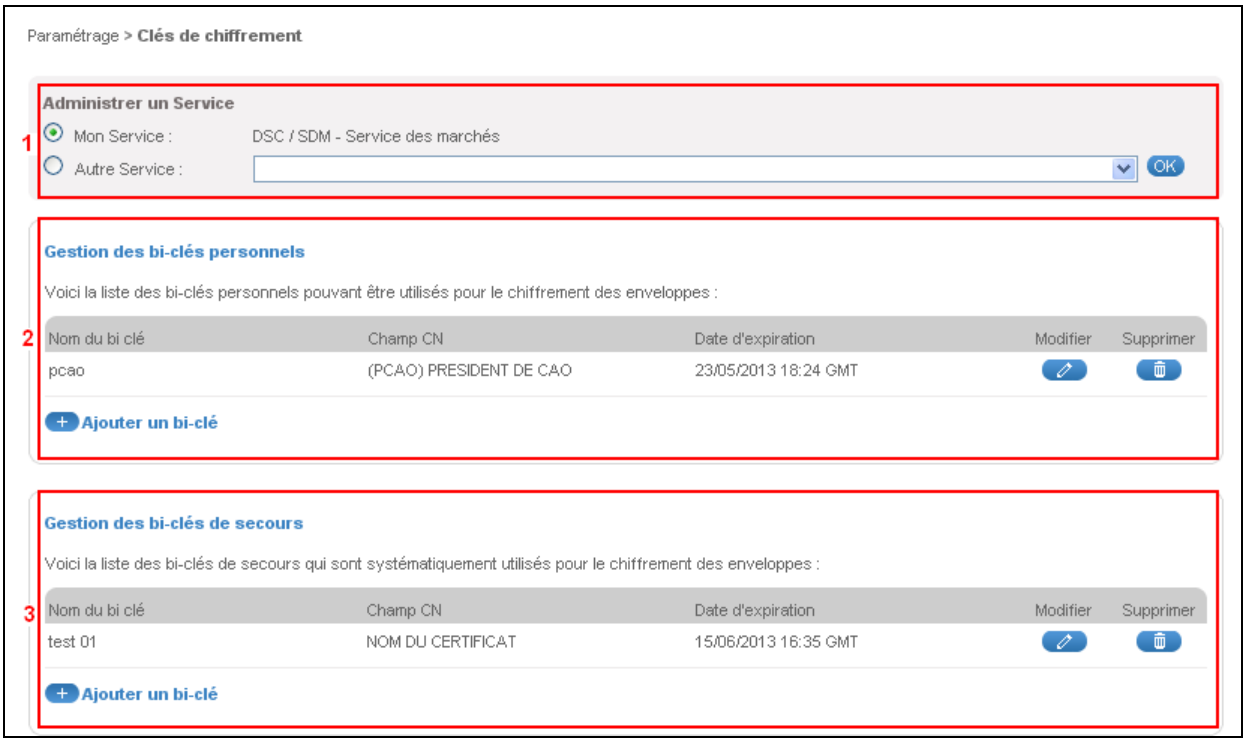
Le chiffrement des données :

- permet de chiffrer le message du soumissionnaire à l'aide de la partie publique du bi-clé du certificat l'agent (la clé publique)
- permet de rendre le message illisible à toute personne n'ayant pas la clé privée du bi-clé
- permet à l'agent déchiffrer le plis du soumissionnaire à l'aide de la partie privée du bi-clé de son certificat (la clé privée)



2 MENU GESTION DES CLES DE CHIFFREMENT

- **1** Ce bloc permet de sélectionner le service auquel l'on souhaite rattacher le bi-clé.
- **2** Ce bloc permet de créer les bi-clés personnels que les agents du service associé pourront sélectionner lors de la validation des consultations.
- **3** Ce bloc permet de créer des bi-clés de secours qui seront automatiquement rattachées aux consultations créées par les agents du service associé. La clé de secours est une sécurité importante car, si un agent perd son bi-clé personnel, le bi-clé de secours pourra toujours servir à ouvrir les plis.



sert à modifier le bi-clé.

sert à supprimer le bi-clé.

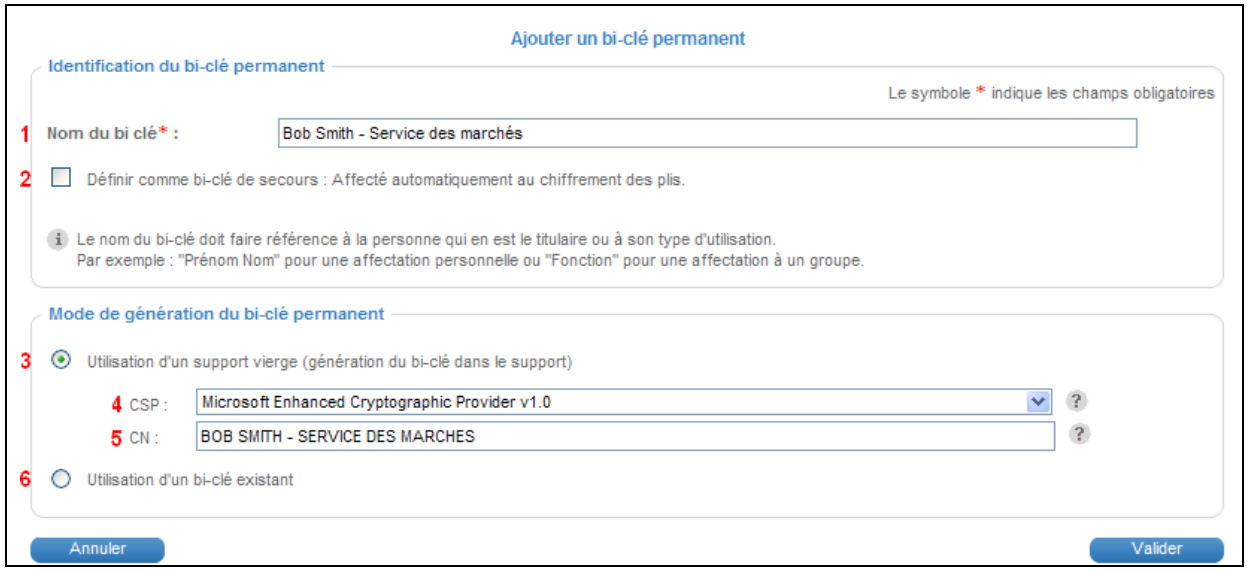
3 DEFINIR UN BI-CLE DANS L'APPLICATION EN CREANT UN BI-CLE CRYPTOGRAPHIQUE

3.1 Création d'un bi-clé sous Windows

Le cas pratique déroulé ci-dessous est celui de la création d'un bi-clé permanent, mais les étapes de création d'un bi-clé de secours sont quasiment les mêmes.

Attention : la création d'un bi-clé ne peut se faire que sous Internet Explorer.

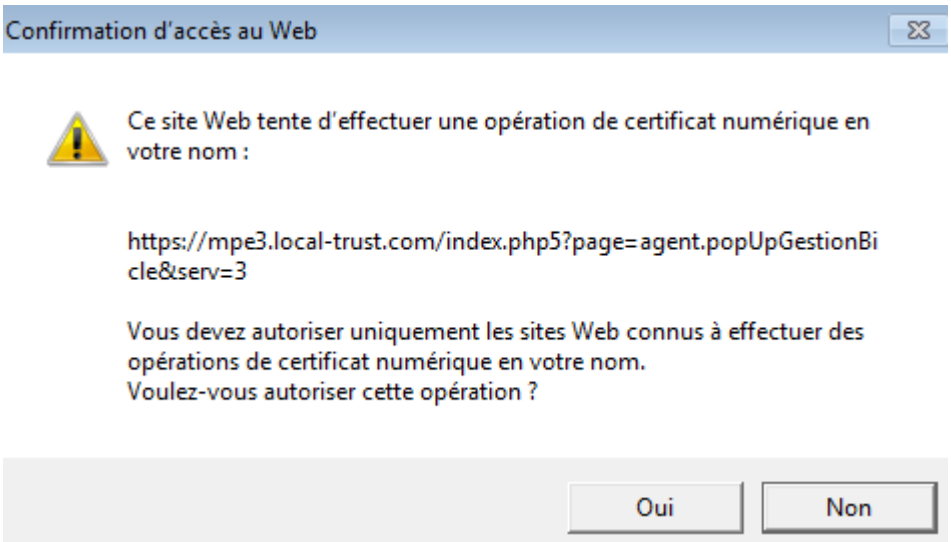
Dans *Gestion des bi-clés personnels*, cliquer sur *Ajouter un bi-clé permanent* ou *de secours.* La fenêtre suivant s'ouvre :



- **1** Choisir le nom que l'on souhaite donner au bi-clé. Ex : Nom-Prénom + Service des marchés. Ce champ est complètement libre mais obligatoire.
- **2** Cette case n'est à cocher que dans le cas où vous souhaiter que le bi-clé crée soit définit comme bi-clé de secours. Auquel cas, après validation, il n'apparaîtra pas dans la liste des bi-clés personnels, mais dans celle des bi-clés de secours.
- **3** Cette case doit être cochée si l'on souhaite créer un nouveau bi-clé cryptographique.
- **4** Ce menu déroulant sert à sélectionner le support physique de la clé cryptographique (CSP : Cryptographic Service Provider. Ex : répertoire protégé de Windows ou carte à puce, etc.).
    - Si vous souhaitez que le bi-clé soit enregistré sur l'ordinateur, vous devez sélectionner la ligne Microsoft Enhanced Cryptographic Provider.
    - Si vous souhaitez que le bi-clé soit stocké sur une carte à puce, il faudra sélectionner la ligne correspondant au fabriquant de votre carte, et ainsi de suite.

- Dans le cas présent, nous générons le bi-clé sur l'ordinateur.

- **5** Ce champ permet de choisir le nom courant (CN : Common Name) de votre bi-clé. Une fois le bi-clé généré, c'est son CN qui apparaîtra dans la liste des bi-clés proposé par le navigateur.
- **6** Cette case est à cochée si l'on souhaite utiliser dans l'application un clé déjà existante. Cf. article 4
- Une fois **1** – **3** – **4** – **5** renseignés ou sélectionnés, cliquer sur Valider.
- Plusieurs messages d'autorisation peuvent apparaître. Ex :



Ces messages peuvent différer en fonction de votre système d'exploitation et de votre navigateur. Il suffit de cliquer sur *Oui* ou *OK* à chaque fois.

- La fenêtre d'ajout du bi-clé se referme automatique et le bi-clé apparaît dans la liste des bi-clé personnels.

3.2 Sauvegarde d'un bi-clé logiciel sous Windows

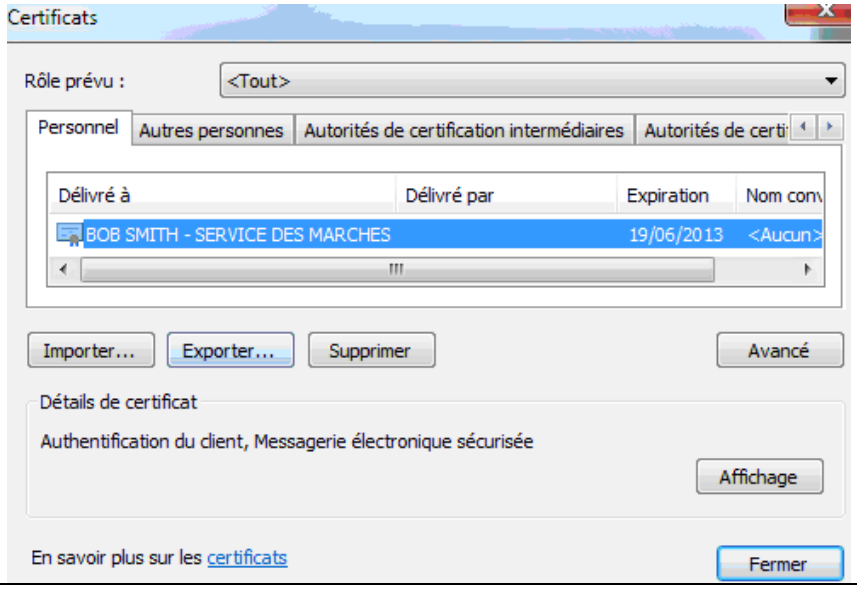
A ce stade, le bi-clé créé se trouve **exclusivement** dans le magasin de certificats d'Internet Explorer. La plateforme, elle, a seulement enregistré l'empreinte du bi-clé. Il est possible de l'associer à une consultation et de l'utiliser pour ouvrir les plus électroniques.

Il est toutefois fortement recommandé de sauvegarder le bi-clé sur un support externe ou sur le réseau, voire les deux :

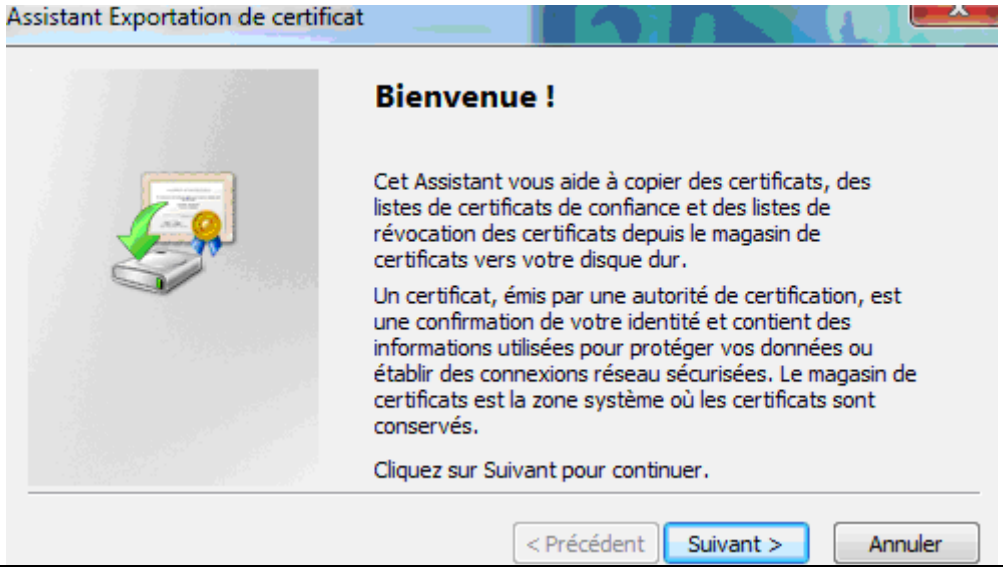
- cela évitera sa perte définitive en cas de dégât matériel,
- cela vous permettra de l'installer sur différents ordinateurs.

Pour ce faire, il faut tout d'abord accéder au magasin de certificats Internet Explorer. Sur Internet Explorer, cliquer sur *Outils, Options Internet, Contenu, Certificats*. Le certificat créé se trouve dans l'onglet *Personnel* du magasin.

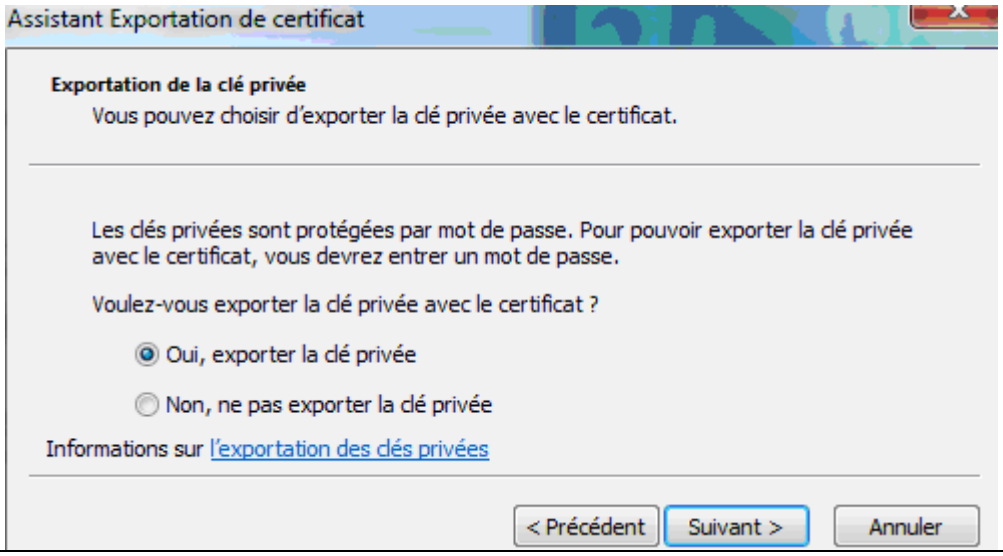
1 - Cliquer sur le nom du bi-clé pour le sélectionner, puis cliquer sur exporter.



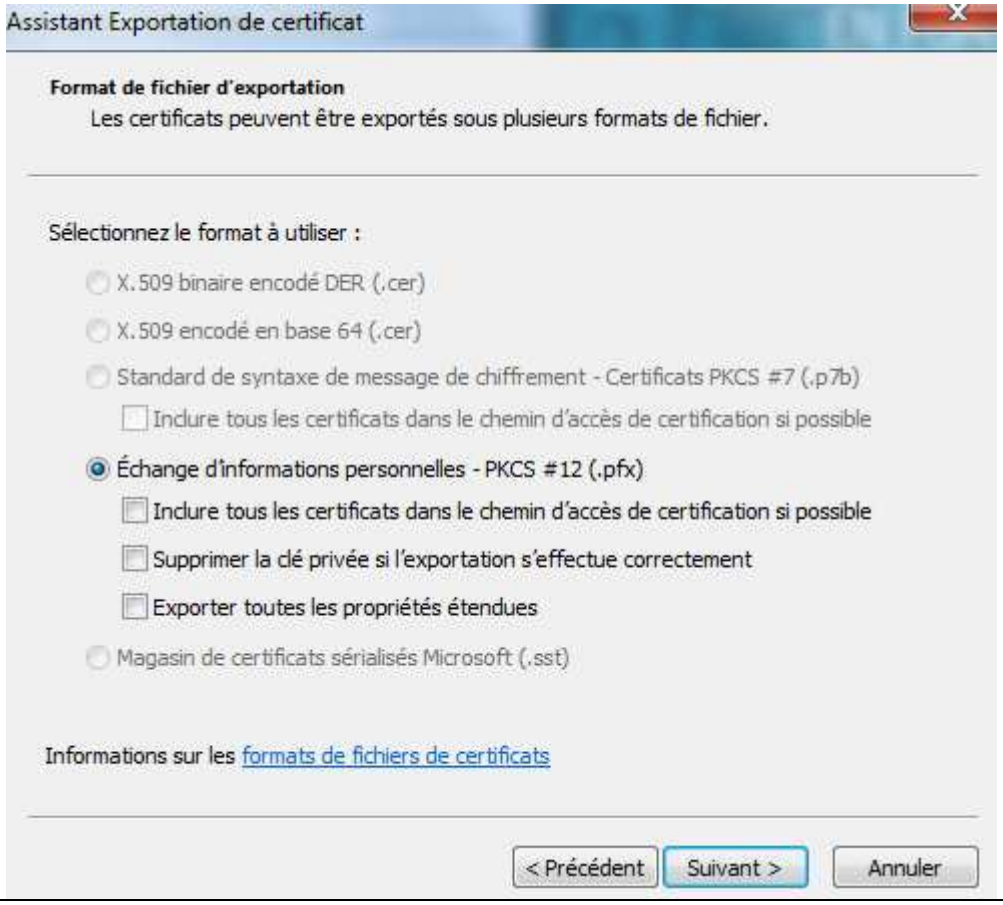
2 – Cliquer sur *Suivant*



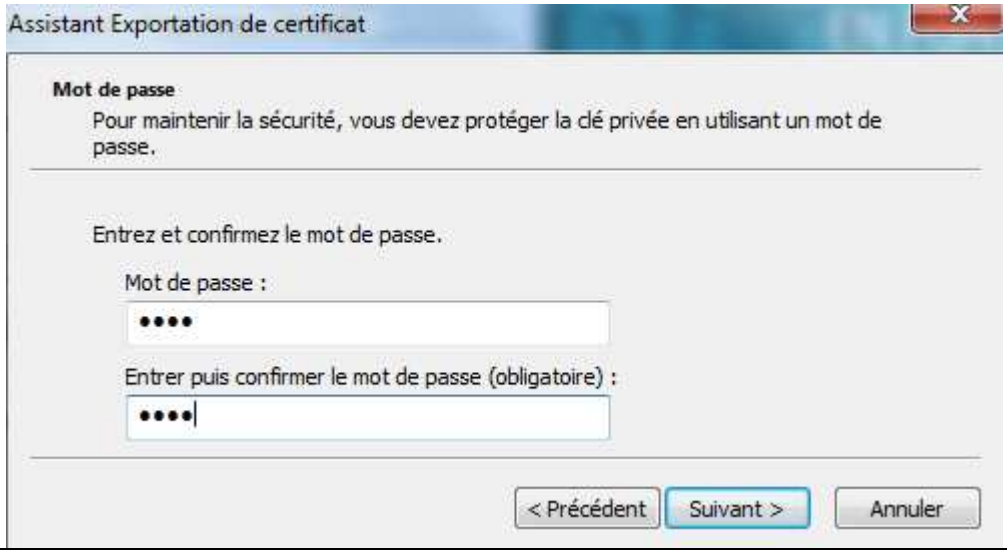
3 - Cocher *Oui, exporter la clé privée* puis cliquer sur *Suivant*. Il est impératif d'exporter cette clé. C'est celle qui vous permettra d'ouvrir les plis électroniques.



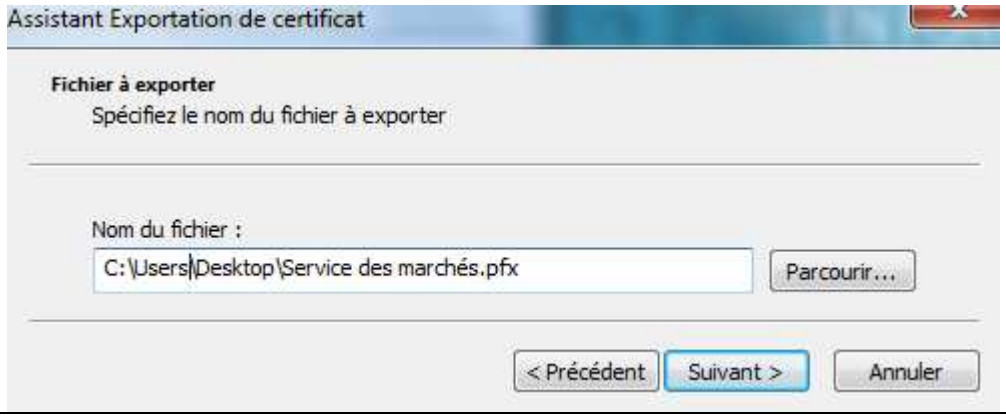
4 - Cliquer sur *Suivant*



5 - Entrer et confirmer un mot de passe ou laisser les champs vierges si l'on ne souhaite pas en mettre un.

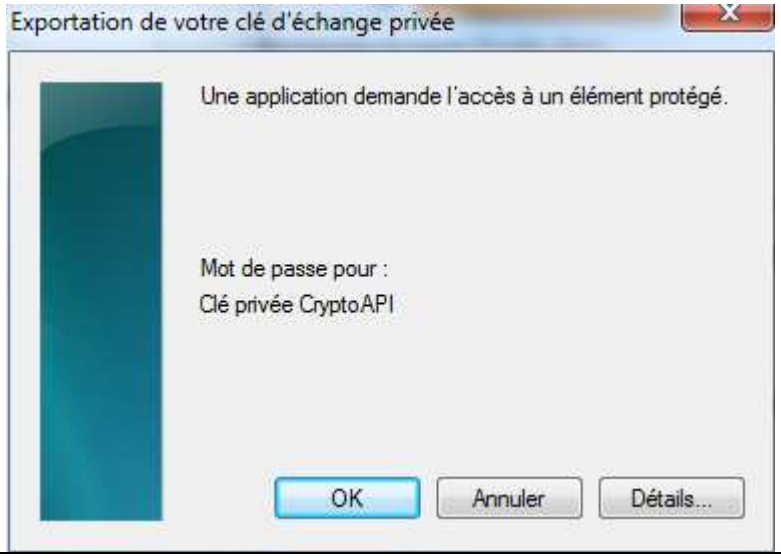


6 – Cliquer sur *Parcourir* et indiquer dans quel répertoire le bi-clé doit être exporté (ici, il sera sauvegardé sur le bureau, mais il est possible de l'enregistrer sur une clé USB, un réseau etc. Il est d'ailleurs fortement conseillé d'exporter le bi-clé sur un support externe qui sera toujours disponible si l'ordinateur ne fonctionne plus). Il faudra également lui donner un nom. Ex : bi-clé service des marchés.

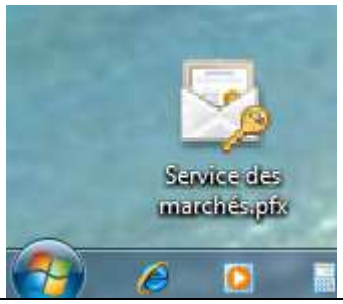


7 – Cliquer sur *Terminer* pour fermer l'assistant d'exportation.

8 - Plusieurs messages d'autorisation peuvent apparaître. Ces messages peuvent différer en fonction de votre système d'exploitation et de votre navigateur. Il suffit de cliquer sur *Oui* ou *OK* à chaque fois. Ex :



9 – L'assistant d'exportation se referme automatiquement, et le bi-clé apparaît dans le répertoire de destination, ici le bureau.



L'exportation se fait toujours de cette façon et ce, quel que soit le répertoire de destination (bureau, support externe, réseau etc.).

Les points importants sont :

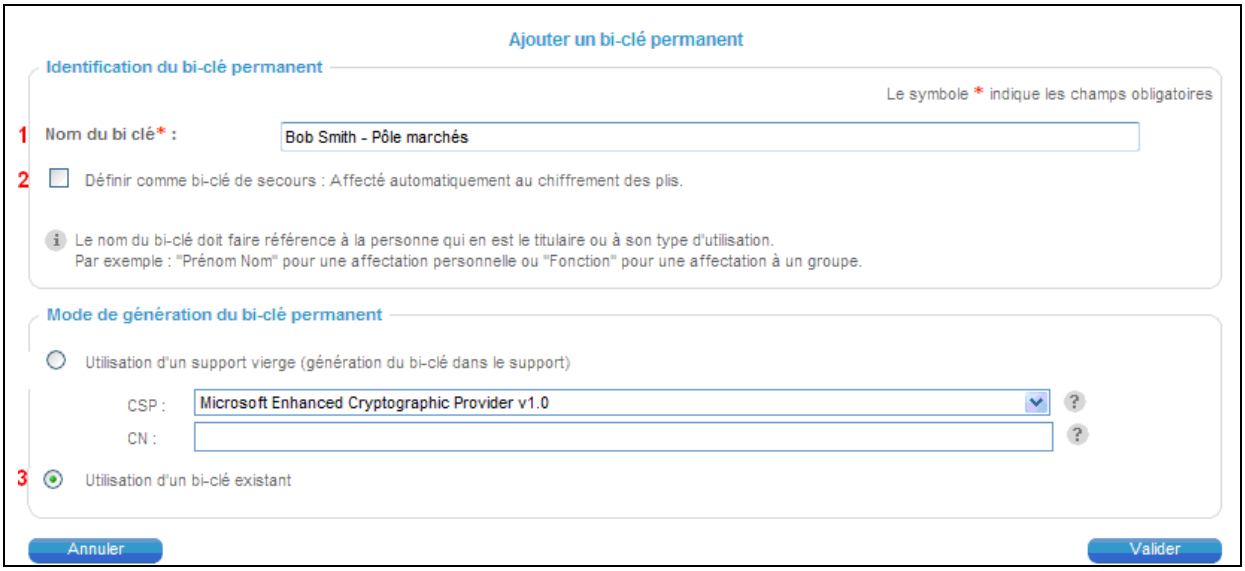
- bien cocher « Oui, exporter la clé privée ». Si la clé privée n'est pas exportée, il sera **impossible** d'ouvrir les plis.
- si l'on décide de mettre un mot de passe, le noter quelque part. Si le mot de passe est perdu, il sera **impossible** d'ouvrir les plis.
- dans la mesure du possible, exporter le bi-clé sur au moins deux supports différents comme l'ordinateur et une clé USB. En effet, si le bi-clé n'est pas dupliqué et qu'il est perdu, il sera **impossible** d'ouvrir les plis.

4 DEFINIR UN BI-CLE DANS L'APPLICATION EN UTILISANT UN BI-CLE CRYPTOGRAPHIQUE DEJA EXISTANT

Ce cas concerne un Agent qui dispose déjà d'un bi-clé cryptographique (logiciel ou sur support physique).

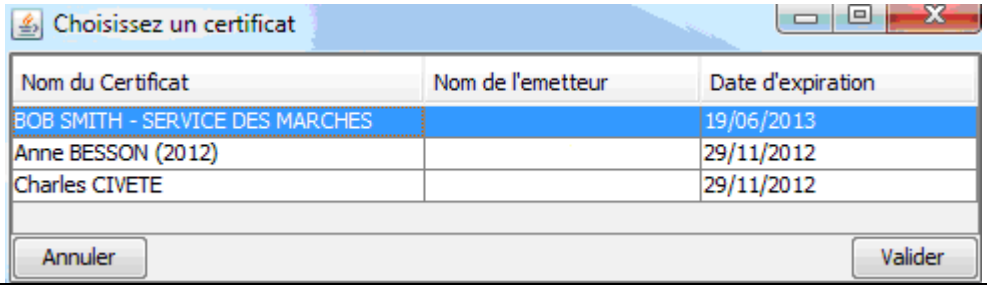
Ce chapitre décrit la manière de renseigner ce bi-clé existant dans l'application, de manière à permettre le chiffrement / déchiffrement des plis à l'aide de celui-ci.

L'Agent utilise la fonction Gestion des clés de chiffrements. Il choisit le Service auquel le bi-clé doit être associé et clique sur *Ajouter un bi-clé personnel* ou *de secours*.



- **1** Choisir le nom que l'on souhaite donner au bi-clé. Ex : Nom-Prénom + Service des marchés. Ce champ est complètement libre mais obligatoire. C'est le nom choisi à cet endroit qui apparaîtra ensuite dans la liste des bi-clés.
- **2** Cette case n'est à cocher que dans le cas où l'on souhaite que le bi-clé créé soit défini comme bi-clé de secours. Auquel cas, après validation, il n'apparaîtra pas dans la liste des bi-clés personnels, mais dans celle des bi-clés de secours.
- **3** Cette case est à cocher si l'on souhaite associer un bi-clé déjà existant à un service. Ex : le bi-clé A est associé au Service 1, mais je souhaite également le rattacher au service B. Nous la cochons donc.
- Une fois **1** – **2** – **3** renseignés ou sélectionnés, cliquer sur Valider.
- Une fenêtre de choix de certificat s'ouvre.

1 – Sélectionner le certificat qui convient puis cliquer sur *Valider*.



2 – Plusieurs messages d'autorisation peuvent apparaître. Ex :

Ces messages peuvent différer en fonction de votre système d'exploitation et de votre navigateur. Il suffit de cliquer sur *Oui* ou *OK* à chaque fois.

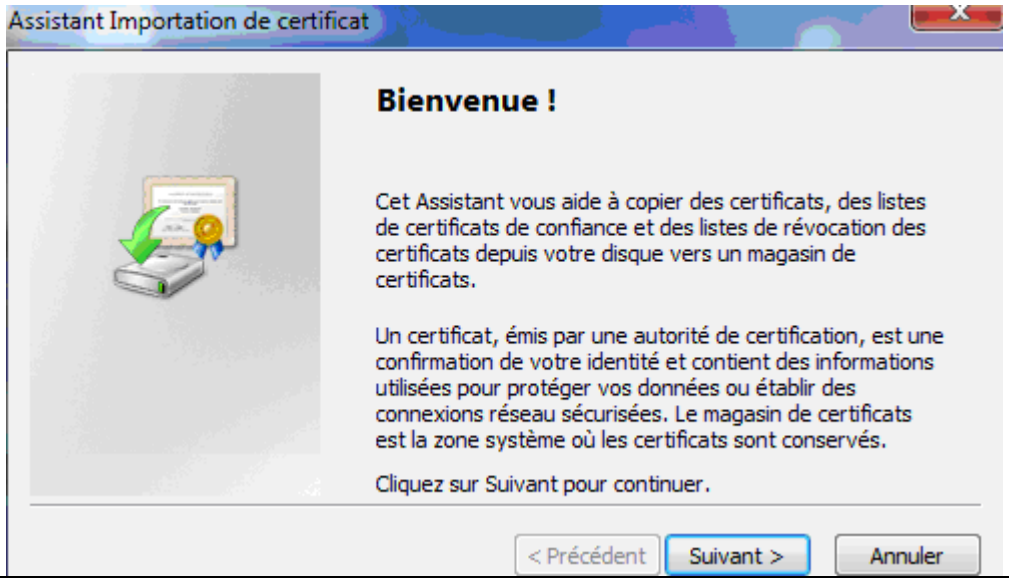
3 – Le certificat apparaît dans la liste des bi-clés.

Ajouter un bi-clé déjà existant enregistre son empreinte sur la plateforme de manière à pouvoir le sélectionner à la validation des consultations. Ce bi-clé n'est en aucun cas installé sur l'ordinateur. Pour pouvoir s'en servir pour ouvrir les plis, il faut l'installer sur le poste, qu'il apparaisse dans le magasin de certificat.

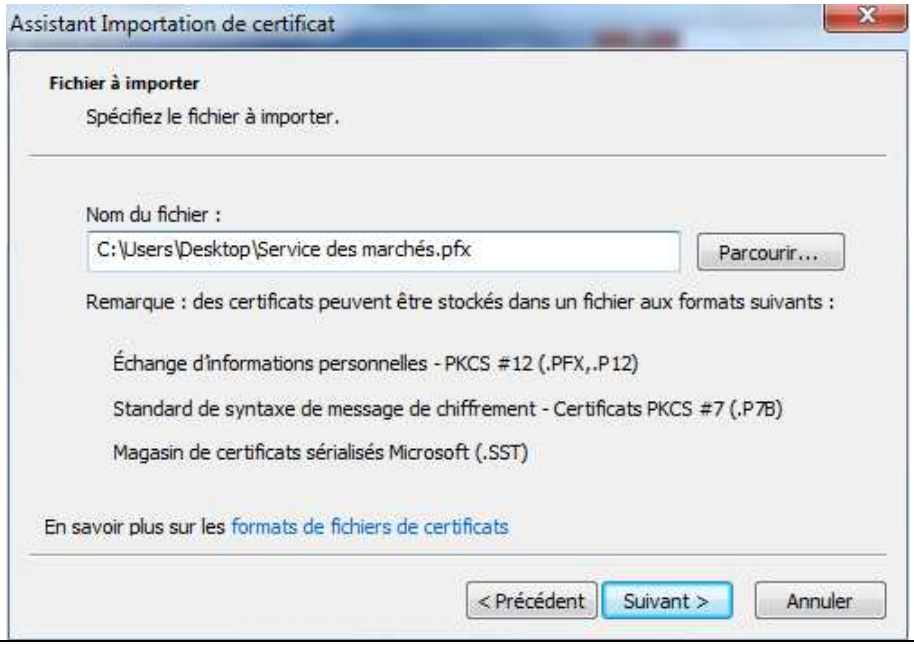
5 IMPORTATION D'UN BI-CLE

Si le bi-clé a été créé ou exporté sur le réseau ou un support externe, une clé USB par exemple, et que l'on souhaite l'installer sur un autre ordinateur, il faudra effectuer une importation. Pour ce faire, il suffit de se rendre dans le répertoire dans lequel est enregistré le bi-clé et de double cliquer sur son icône. La fenêtre d'assistant d'importation s'ouvre.

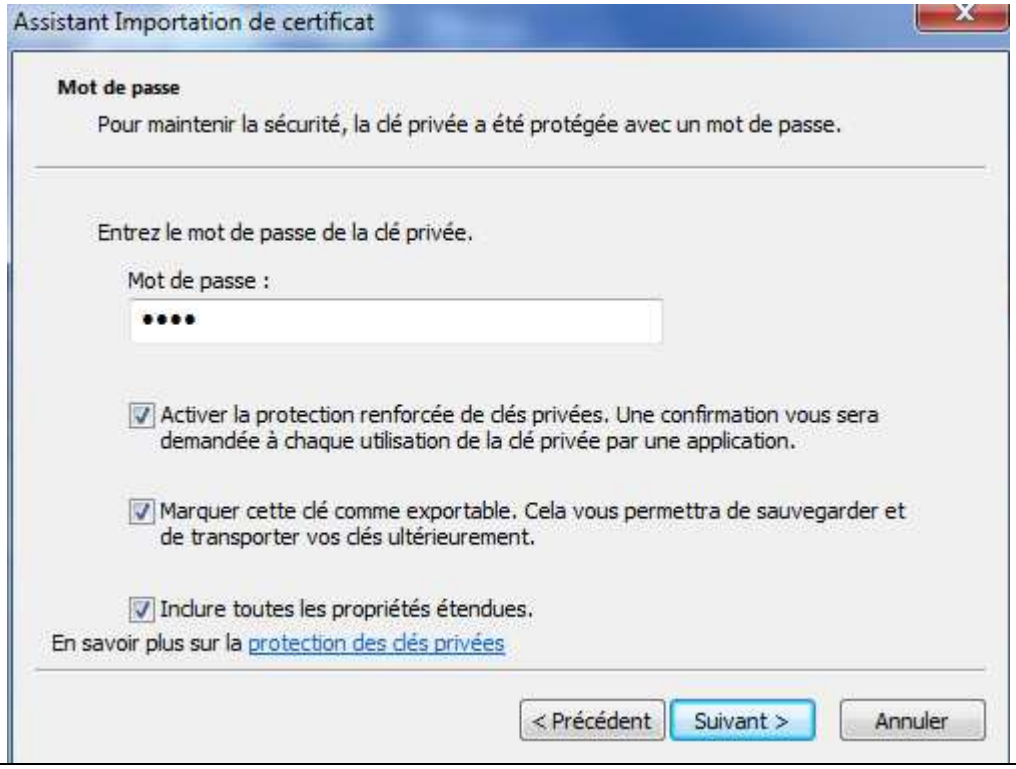
1 - Cliquer sur *Suivant.*



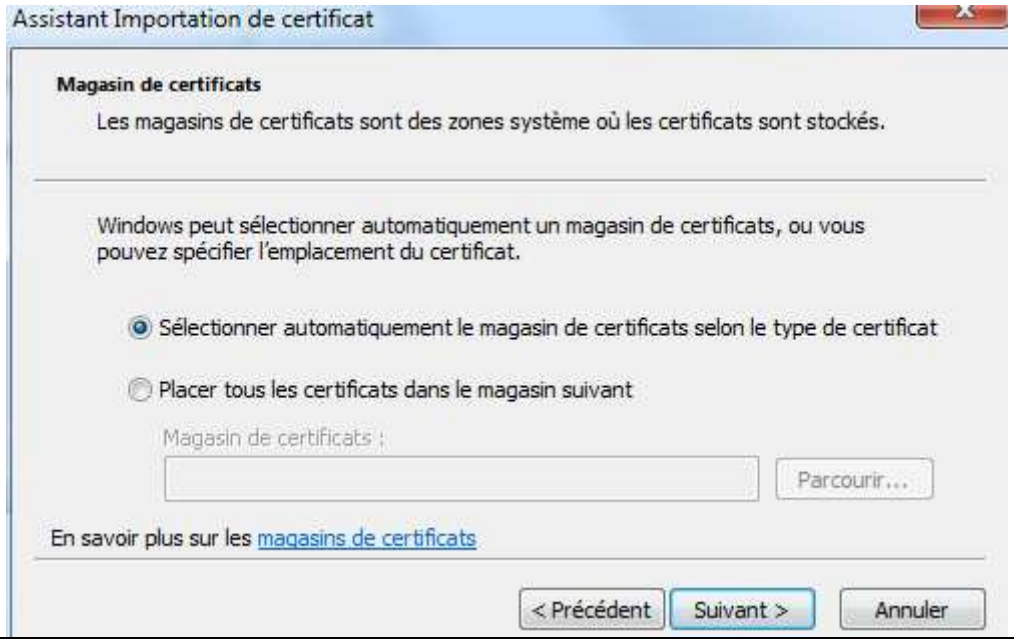
2 – Cliquer sur *Parcourir* et sélectionner le bi-clé dans le répertoire qui le contient.



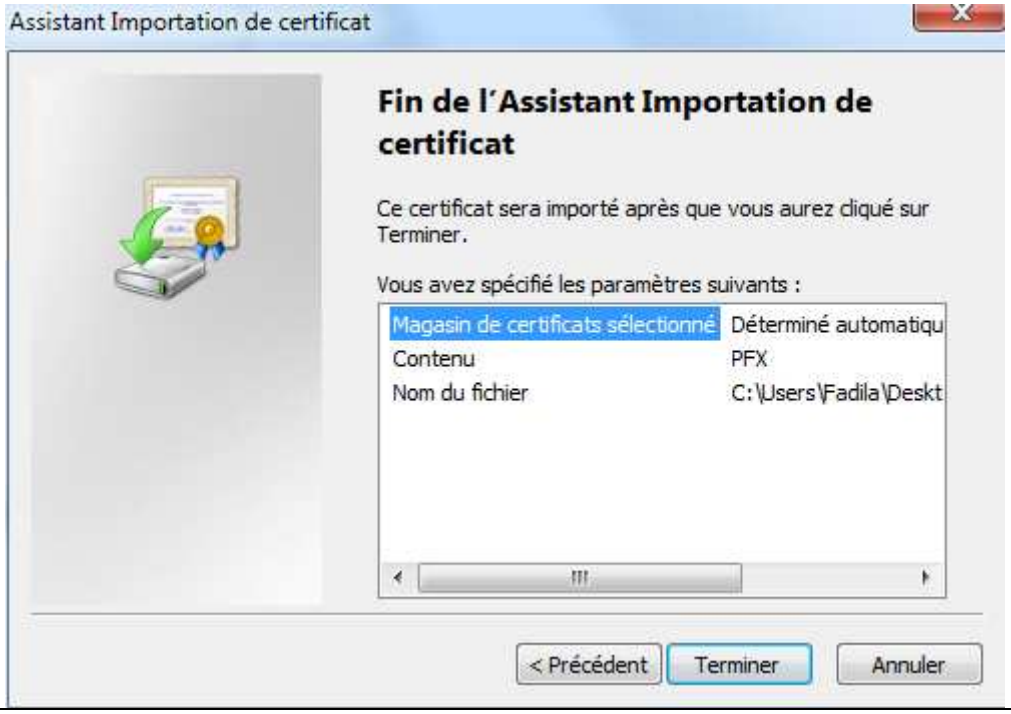
3 – Renseigner le mot de passe s'il y en a un et cocher les cases *Activer la protection renforcée* […] et *Marquer cette clé comme exportable* […]



4 – Cliquer sur *Suivant*. Le bi-clé sera automatiquement installé dans le bon répertoire.



5 – Cliquer sur *Terminer* pour terminer l'installation. L'assistant d'importation se referme automatiquement.



Si l'installation s'est correctement déroulée, on doit retrouver le bi-clé dans l'onglet *Personnel* du magasin de certificats d'Internet Explorer.

Une fois le bi-clé installé sur l'ordinateur, il n'est pas nécessaire d'insérer la clé USB ou la carte à puce pour pouvoir ouvrir les plis.