|  |  |
| --- | --- |
| **IDENTITE DU DOCUMENT** | |
| **Entité** | Trésorerie Générale du Royaume |
| **Objet** | Fourniture, installation et mise en œuvre d'une solution progicielle de dématérialisation de la commande publique ainsi que les prestations de formation, d'assistance technique et de maintenance y afférentes |
| **Titre** | Guide d’utilisation –Administrateur Acheteur |
| **Etat** | Version finale |
| **Version** | 1.7 |
| **Du** | 19 janvier 2012 |
| **Dernière page** | 28 |

|  |  |  |  |
| --- | --- | --- | --- |
| **EVOLUTION DU DOCUMENT** | | | |
| **Date** | **Version** | **Rédacteur** | **Commentaires** |
| 21/01/2010 | 1.0 | TGR | Création du document |
| 18/02/2010 | 1.1 | TGR | Création du document |
| 01/03/2010 | 1.2 | TGR | Mise à jour du document |
| 21/03/2011 | 1.3 | TGR | Mise à jour du document |
| 18/04/2011 | 1.4 | TGR | Mise à jour du document |
| 16/11/2011 | 1.5 | TGR | Séparation des modules selon le profil |
| 12/12/2011 | 1.6 | TGR | Mise à jour du document |
| 19/01/2012 | 1.7 | TGR | Corrections mineures |

Table des matières

[1 Introduction 4](#_Toc312664354)

[1.1 Objet de ce document 4](#_Toc312664355)

[1.2 Connexion à l’application 4](#_Toc312664356)

[1.3 Pré-requis techniques 4](#_Toc312664357)

[1.3.1 Diagnostic du poste de travail de l'Utilisateur Agent 4](#_Toc312664358)

[2 Gestion des agents 6](#_Toc312664359)

[3 Gestion des Clés de chiffrement 7](#_Toc312664360)

[3.1 Génération d'une nouvelle clé de chiffrement 7](#_Toc312664361)

[3.2 Import d’un bi-clé existant 9](#_Toc312664362)

[3.3 Cas des clés de secours 10](#_Toc312664363)

[4 Gestion des fournisseurs de document 11](#_Toc312664364)

[5 Gestion des Journaux d’Annonces Légales (JAL) 12](#_Toc312664365)

[6 Supprimer les plis refusés 13](#_Toc312664366)

[7 Accès aux statistiques 15](#_Toc312664367)

[7.1 Suivi données métier 15](#_Toc312664368)

[7.2 Suivi données entreprise 15](#_Toc312664369)

[7.3 Recherche avancée 15](#_Toc312664370)

[8 Sauvegarde et restauration des cles logicielles 18](#_Toc312664371)

[8.1 Exporter un certificat depuis Internet Explorer 18](#_Toc312664372)

[8.2 Installation d'un certificat logiciel 24](#_Toc312664373)

# Introduction

## Objet de ce document

Ce guide s'adresse aux Agents utilisant la plate-forme de dématérialisation de la commande publique.

Ce document détaille les modes d'utilisation de la plate-forme pour les Agents.

Ce guide doit permettre aux **Agents administrateurs d’un acheteur public**une utilisation simple de la plate-forme. Celle-ci ayant été conçue pour être intuitive et rapidement maîtrisée. Dans la suite du document, les écrans accessibles par les Agents sont décrits en détail ainsi que les différentes fonctionnalités proposées.

## Connexion à l’application

Un Agent Habilité (ci-après dénommé " AH ") accède à la plate-forme comme suit :

* Connexion à l’adresse : [www.marchespublics.gov.ma/agent/](http://www.marchespublics.gov.ma/agent/) ou connexion à l’adresse [www.marchespublics.gov.ma](http://www.marchespublics.gov.ma) puis click sur la bannière ‘’Accès Acheteur Public’’
* Saisie de l’identifiant /mot de passe de l’AH

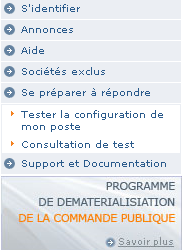
Une fois identifié et connecté, l’AH accède à la page d’accueil, et aux différentes fonctionnalités pour lesquelles il est habilité.

## Pré-requis techniques

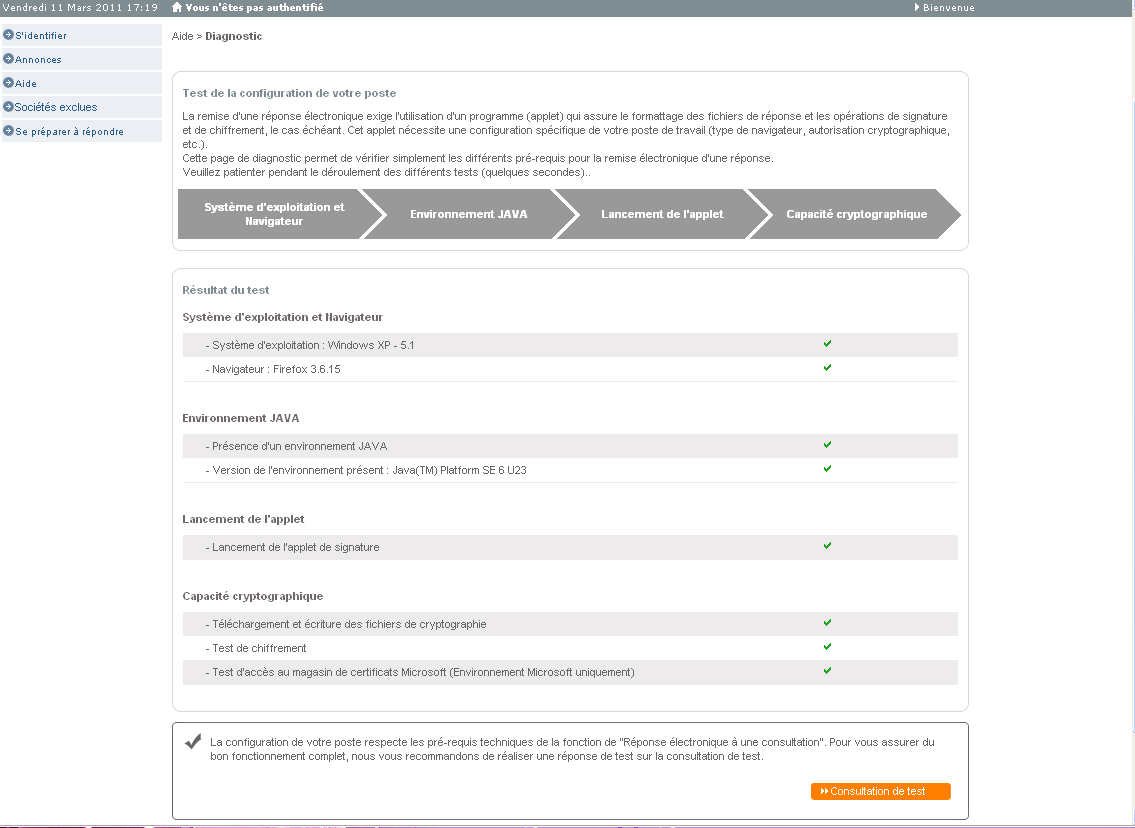
La liste détaillée des pré-requis techniques d'accès à l’application est présentée dans la rubrique "Pré-requis techniques" en pied de page de chaque page de l'application.

### Diagnostic du poste de travail de l'Utilisateur Agent

De plus, un utilisateur agent peut effectuer un diagnostic de la bonne configuration de son poste de travail pour l’utilisation de la plateforme. Ce diagnostic est accessible dans le menu fonctionnel latéral.



Le test de configuration teste successivement le système d’exploitation et le Navigateur, l’environnement Java, le lancement de l’applet et la capacité cryptographique du poste. Il faut que l’ensemble des tests de pré-requis soient validés pour l’utilisation de la plateforme.



L'application propose, le cas échéant, les moyens de remédier aux problèmes rencontrés lors du test.

La rubrique ‘’Consultations de test’’ : renvoie vers des consultations de test pour réaliser des essais de dépôt de réponses électroniques. Ces consultations de tests seront créées à l’initialisation de la plate-forme.

# 

# Gestion des agents

Un administrateur d’un acheteur public n’a pas la main pour la gestion des utilisateurs agents de son entité. Il doit se référer pour cela à l’administrateur central de la plate-forme.

# Gestion des Clés de chiffrement

Les Clés de chiffrement sont des éléments intervenant dans la Validation d’une consultation mettant en œuvre le chiffrement des plis des soumissionnaires

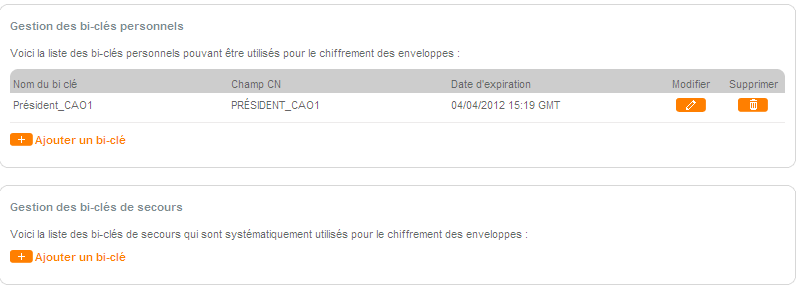
Pour être proposée lors de l'étape de Validation, une clé de chiffrement doit être référencée sur la plate-forme à l'aide de la fonction de Gestion des clés de chiffrement (fonction du menu Administration / Paramétrage).

Pour accéder au menu de gestion des clés de chiffrement, cliquer sur le lien « Clés de chiffrement » dans le menu Paramétrage)





En cliquant sur ce lien, l’écran de gestion des clés apparaît :



Il est possiblede modifier ou supprimer des Clés de chiffrement existantes grâce aux icônes  et .

Il est également possible d’ajouter une nouvelle Clé de chiffrementen cliquant sur 

## Génération d'une nouvelle clé de chiffrement

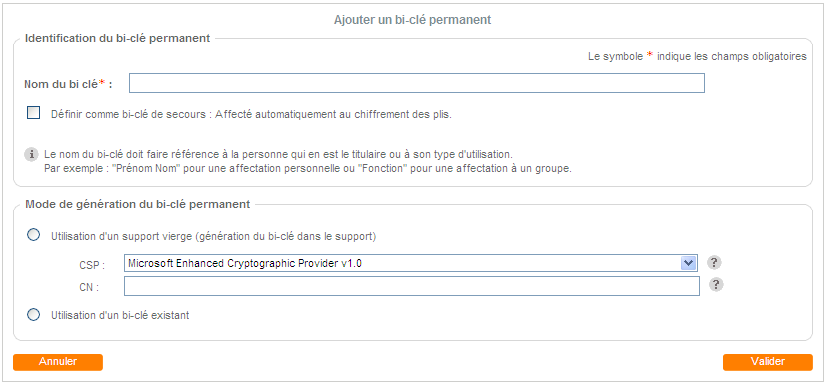
L’application permet de générer des certificats électroniques afin de pouvoir réaliser des opérations de chiffrement et de déchiffrement grâce au bi-clé du certificat. Cette génération est possible sur trois supports différents :

* Clé USB cryptographique
* Carte à puce
* Logiciel : sur le poste de travail de l’utilisateur au niveau du magasin de certificat d’Internet Explorer.

Cette fonction n’est possible que depuis le navigateur **Internet Explorer** (à partir de la version 8 d'Internet Explorer, le site doit appartenir aux sites de confiances du navigateur), afin de pouvoir exécuter l’ActiveX nécessaire à la génération.

L’utilisateur devra également être administrateur de son poste de travail afin de pouvoir exécuter la fonction de génération de clé de chiffrement.

Pour générer un nouveau bi-clé, il faut suivre les étapes suivantes : cliquer sur , la fenêtre suivante apparaît :



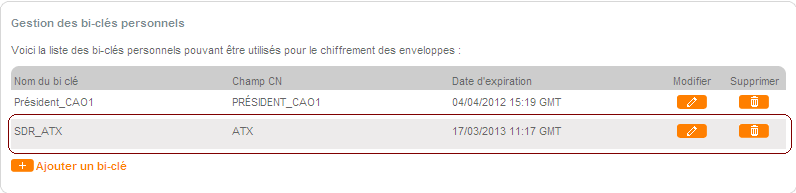
L'utilisateur doit nommer le bi-clé dans le champ « Nom du bi-clé » et cocher « *Utilisation d’un support vierge (génération du cl-clé dans le support)* », puis choisir de générer un certificat en utilisant l’une des CSP proposée :

* "Microsoft Enhanced RSA and AES Cryptographic Provider” pour un certificat logiciel
* "Gemplus GemSAFE Card CSP" pour un certificat sur carte à puce
* "Safenet RSA CSP" pour un certificat sur clé USB cryptographique

L’utilisateur doit également renseigner le champ CN, qui sera le nom du certificat généré sur son poste de travail.

Une fois ces informations complétées et après avoir cliqué surValider, des fenêtres d'alertes d'Internet Explorer vont s'ouvrir demandant des confirmations de création de certificat.

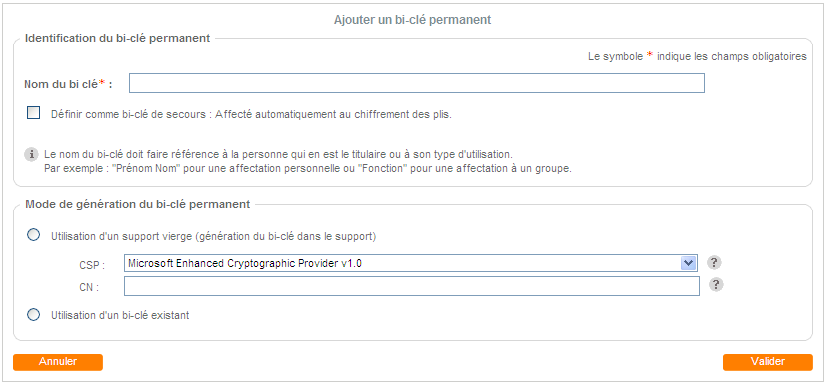
A la fin du cycle de création de certificat, le bi-clé apparaît dans la fenêtre de gestion des bi-clés :



Le certificat est enregistré sur le support spécifié par l'utilisateur.

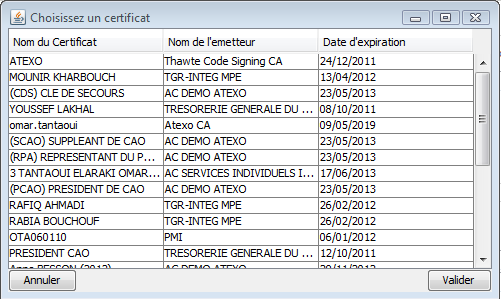
## Import d’un bi-clé existant

Au cas où l’utilisateur dispose déjà d’un bi-clé de chiffrement qu’il souhaite référencer dans l’application, il faut suivre les étapes suivantes : cliquer sur , la fenêtre suivante apparaît :



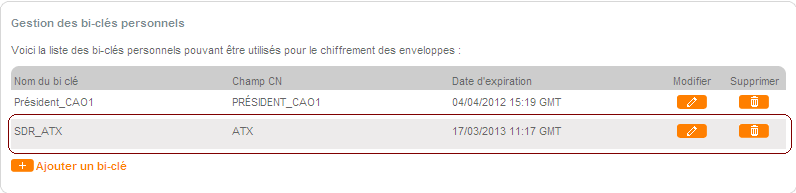
L'utilisateur doit nommer le bi-clé dans le champ « Nom du bi-clé » et cocher « *Utilisation d’un bi-clé existant »*.

En cliquant sur « Valider », une fenêtre s’ouvre permettant de choisir le certificat à importer :



L’utilisateur sélectionne la clé souhaitée puis clique sur valider. Un code PIN peut être demandé à ce moment-là si la clé est protégée par code PIN.

Ensuite la fenêtre se ferme et la clé importé s’ajoute à la liste des bi-clés référencés dans l’application



## Cas des clés de secours

Lors du référencement d’une Clé de chiffrement, celle-ci peut être définie comme étant une Clé de secours (case à cocher).

Lorsqu’une clé est définie comme une clé de secours, celle-ci est automatiquement affectée à toutes les consultations mettant en œuvre le chiffrement.

La clé de secours est ainsi conservée en lieu sûr et est utilisée en cas de perte ou d’indisponibilité de la clé affectée à la consultation.



# Gestion des fournisseurs de document

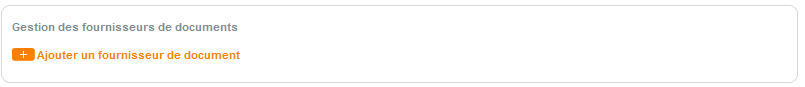
Cette fonctionnalité permet de paramétrer les fournisseurs externes de documents. Ces fournisseurs de document sont les organismes définis par les acheteurs publics et paramétrés par consultation, et qui peuvent délivrer les plans ou autres documents aux fournisseurs qui en font la demande.

Pour accéder à la gestion des fournisseurs de documents, cliquer sur le menu suivant :

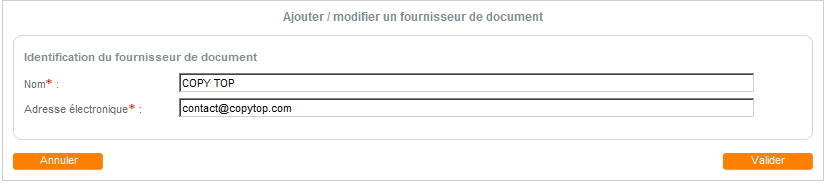




En cliquant sur ce lien, l’écran de gestion des fournisseurs de document apparaît :



En cliquant sur « Ajouter un fournisseur de document », l’utilisateur accède à l’écran de saisie d’un fournisseur de document :



En cliquant sur « Valider », le tableau des fournisseurs de document se met à jour



# Gestion des Journaux d’Annonces Légales (JAL)

Cette fonctionnalité permet de gérer les informations relatives aux Journaux d’Annonces Légales auxquels peuvent être envoyées des données sur les consultations publiées sur la plate-forme.

Pour accéder à la gestion des JAL, cliquer sur le menu suivant :

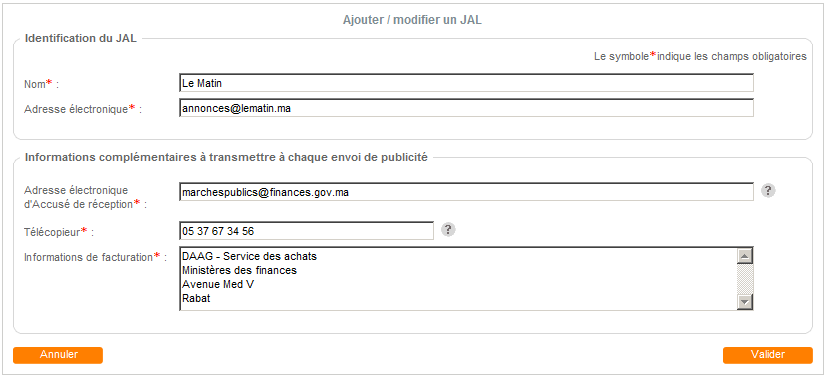




En cliquant sur ce lien, l’écran de gestion des JAL apparaît :



En cliquant sur « Ajouter un JAL », l’utilisateur accède à l’écran de saisie d’un JAL :



En cliquant sur Valider, le tableau des JAL se met à jour :



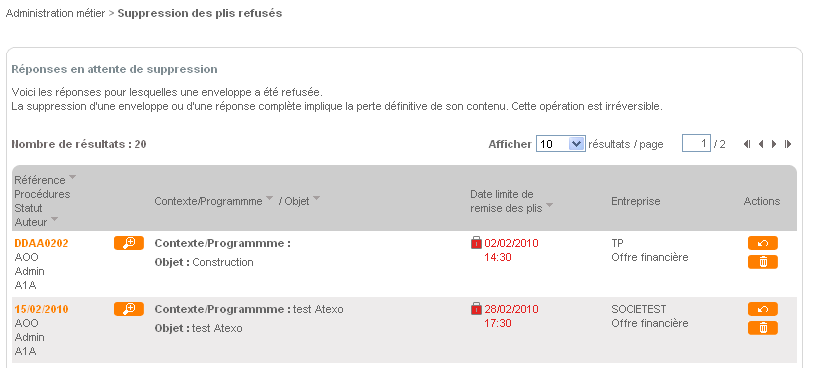
# Supprimer les plis refusés

Les plis refusés lors de l'ouverture sont stockés dans un espace de quarantaine. Les administrateurs acheteurs peuvent ensuite les supprimer définitivement ou décider de les restaurer pour les rendre à nouveau visibles dans les écrans de dépouillement.

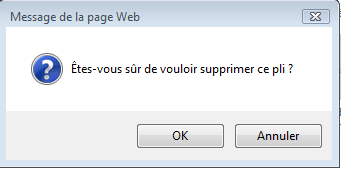
Pour accéder à la gestion des plis refusés, cliquer sur le menu suivant :



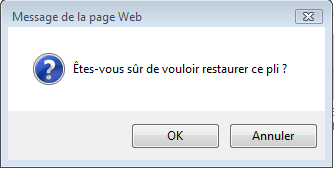
En cliquant sur ce lien, le tableau des réponses en attente de suppression définitive apparaît :



En cliquant sur , l’enveloppe et son contenu sont définitivement supprimés de l’application. Cette opération est irreversible. Avant cela, un message de confirmation apparaît à l’écran :



En cliquant sur , l’enveloppe et son contenu sont remis à disposition dans le tableau de dépouillement pour être ouverte. Avant cela, un message de confirmation apparaît à l’écran :



# Accès aux statistiques

Un Administrateur acheteur peut accéder aux statistiques relatives à son entité publique en cliquant sur le menu suivant :



En cliquant sur ce lien, un sous menu-apparaît :



Lorsque le tableau présente des résultats agrégés (appels d'offre ouverts et restreints agrégés par exemple), un export complémentaire permet d'obtenir la même synthèse présentant tous les types de procédure.

## Suivi données métier

Ce lien permet de visualiser une synthèse de l'activité d'une entité.

Le moteur de recherche permet d'accéder aux résultats d'autres Services.

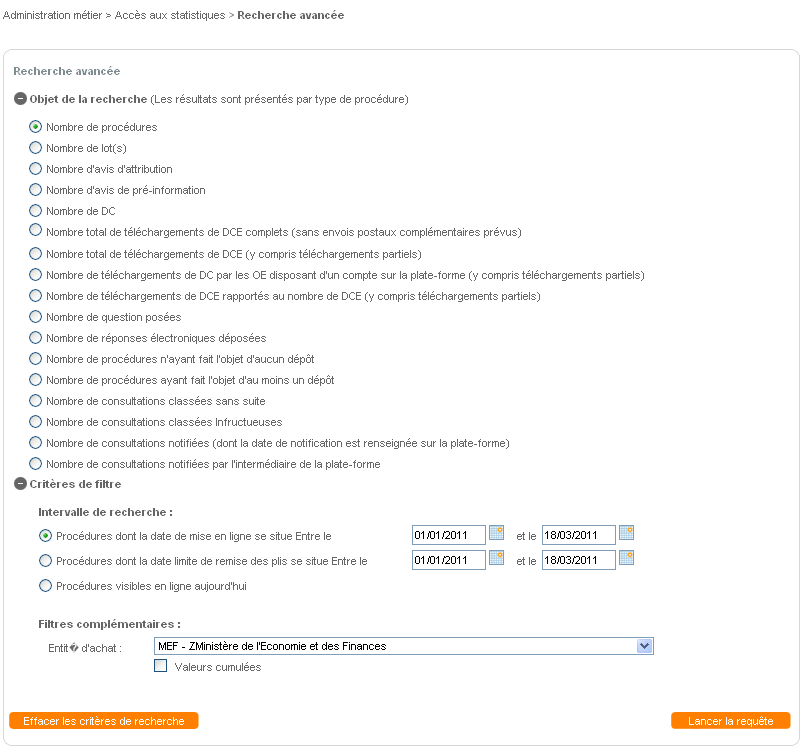
## Suivi données entreprise

Ce lien permet de visualiser une synthèse de l'activité de la plate-forme en proposant notamment une synthèse des comptes créés par les opérateurs économiques.

## Recherche avancée

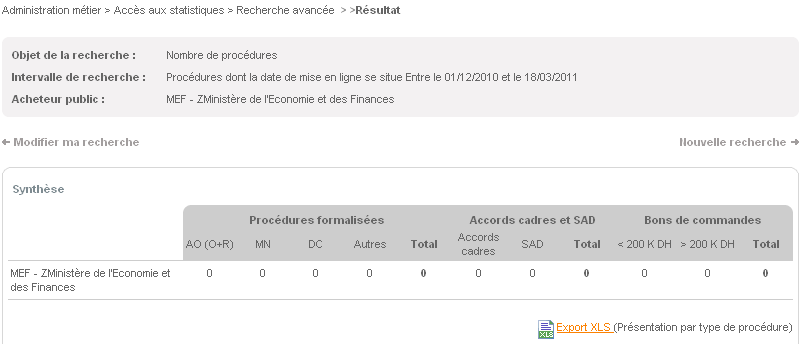
Ce lien permet à l'utilisateur de personnaliser l'analyse de la plate-forme en choisissant :

* Une requête parmi les requêtes proposées



* Un filtre associé :
  + Période de recherche
  + Entité concernée

Le résultat est présenté dans un tableau obtenu en cliquant sur "Lancer la requête".



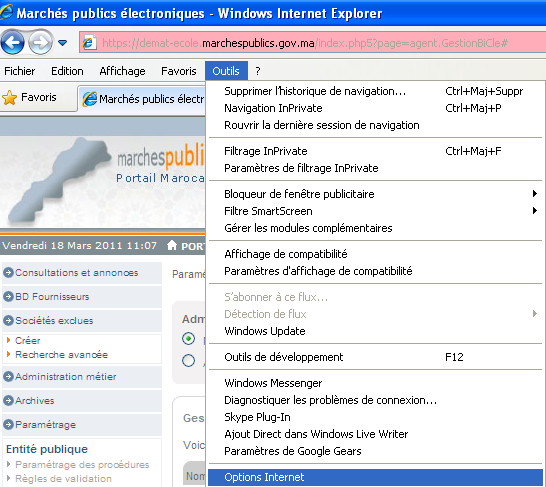
# Sauvegarde et restauration des cles logicielles

## Exporter un certificat depuis Internet Explorer

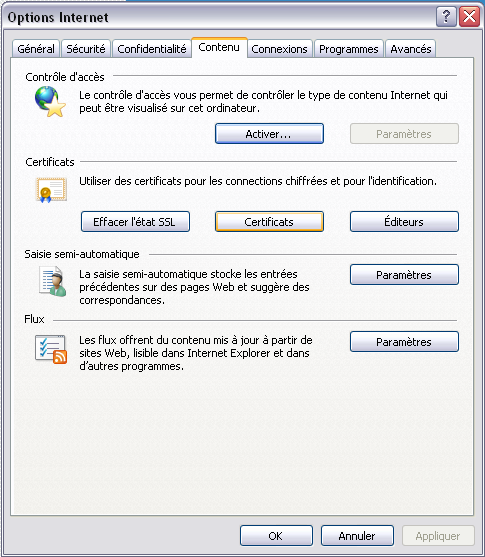
Les fonctions explicitées ci-après sont uniquement valables pour des certificats de "type logiciel". C'est-à-dire des certificats générés à partir de la CSP " Microsoft Enhanced RSA and AES Cryptographic Provider".

Afin de se prémunir des risques de perte du certificat généré, qui devra absolument être présent sur le poste de travail lors d'une ouverture de plis électroniques, il est recommandé d'exporter le certificat afin de le sauvegarder de manière sécurisée (sur une clé USB par exemple).

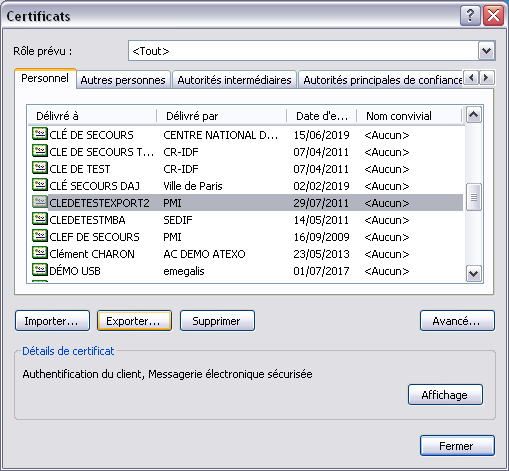
Pour accéder au magasin de certificat d'Internet Explorer, l'AH doit cliquer sur Outils, puis sur Options Internet :



Dans la fenêtre ci-dessous, l'AH clique sur le bouton Certificats au niveau de l'onglet Contenu :



Dans la fenêtre " Certificats ", l'AH sélectionne le certificat qu'il souhaite exporter dans la liste des certificats " Personnel ". Il clique ensuite sur le bouton " Exporter "



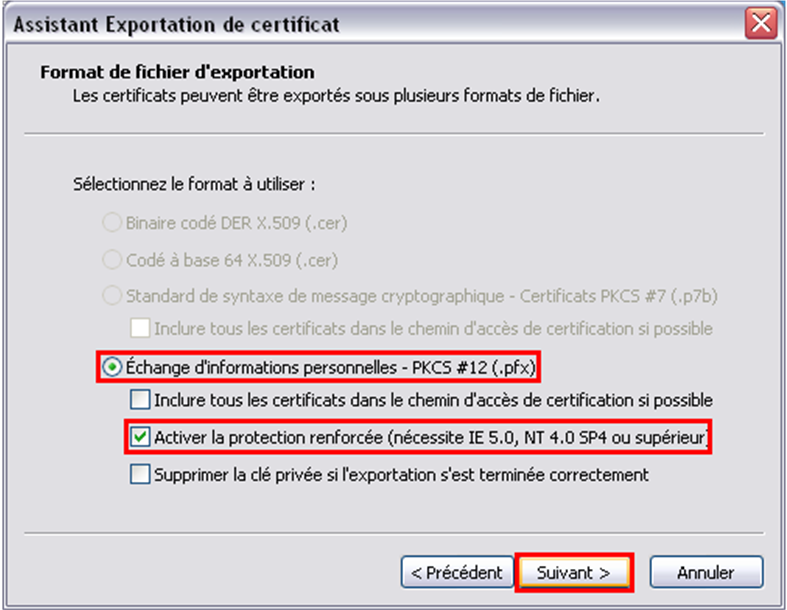
L’assistant d’exportation de certificat démarre. Dans la fenêtre proposée, l'AH doit cliquer sur "Suivant".



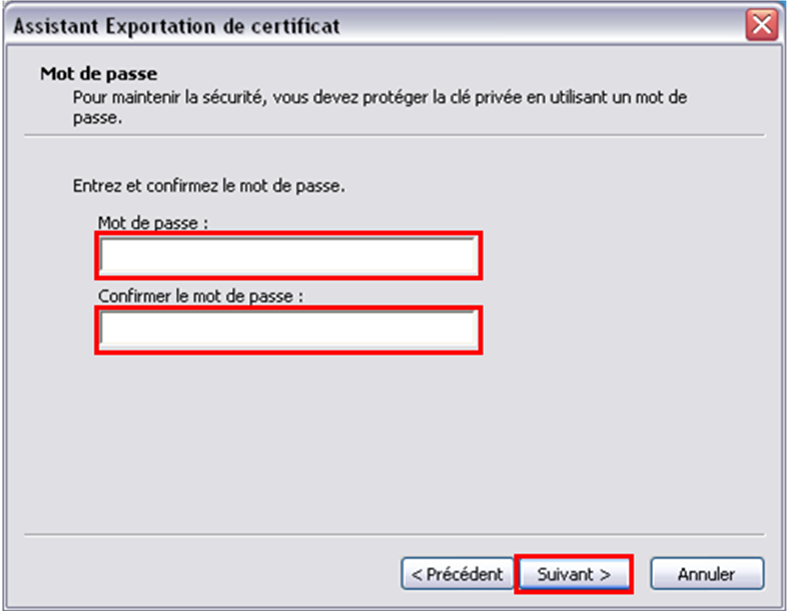
Dans l'écran suivant, l'AH sélectionne " Oui, exporter la clé privée " (obligatoire pour le déchiffrement), puis clique sur le bouton " Suivant ".



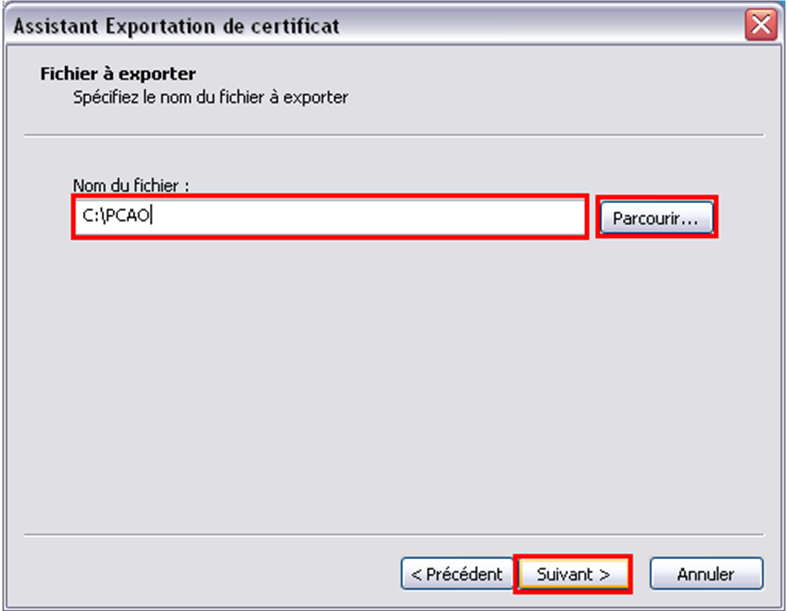
Ensuite, l'AH sélectionne " Echange d’informations personnelles – PKCS #12 (.pfx) ", puis coche " Activer la protection renforcée " et enfin clique sur " Suivant ".



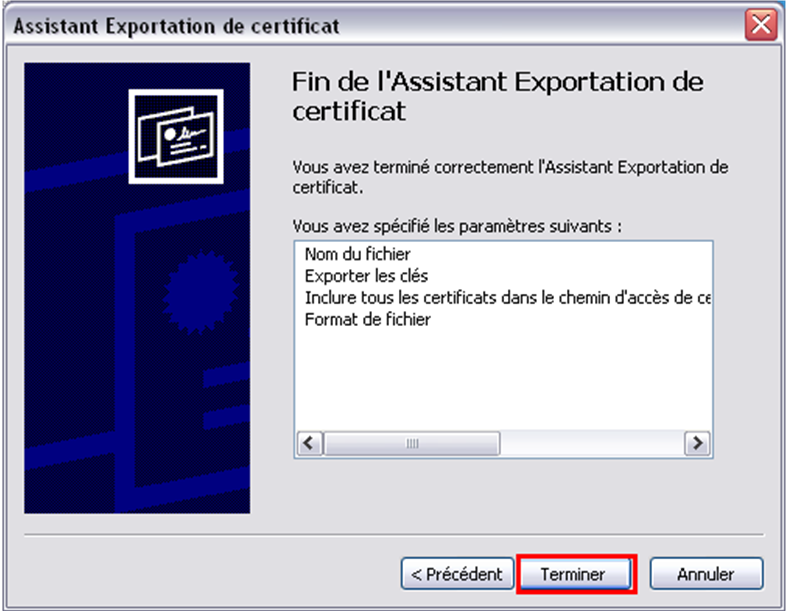
Il est possible de protéger le certificat par un mot de passe. Ce mot de passe sera nécessaire lors de l’installation du certificat ou de l’accès à la clé privée de celui-ci (ouverture des plis chiffrés par exemple). L'AH peut donc saisir un mot de passe et cliquer sur " Suivant ".



Dans l'écran suivant, l'AH doit saisir le nom sous lequel le certificat sera exporter, ou par l’intermédiaire du bouton " Parcourir… ". Une fois le nom saisi, l'AH clique sur " Suivant ".



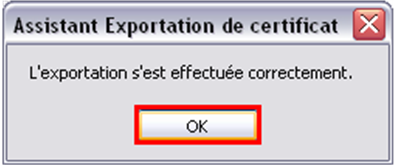
Dans cet écran, l’assistant rappelle les paramètres saisis pour l’export. Il suffit à l'AH de cliquer sur " Terminer " pour lancer l’export du certificat.



Internet Explorer propose une fenêtre de confirmation pour l’export de la clé privée. L'AH doit cliquer sur " OK ".



Une fois l’export terminé, une fenêtre confirme l’export du certificat. Il suffit à l'AH de cliquer sur " OK " pour fermer l'écran.



Le certificat est maintenant créer, il peut être stocké sur une clé USB ou gravé sur un CD, ou tout autre média de stockage.



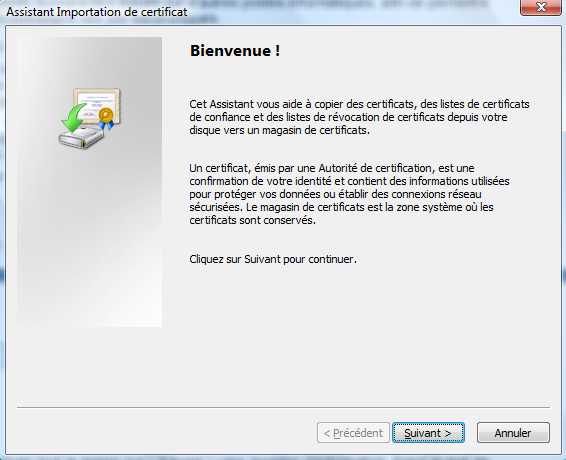
Si besoin, il pourra être installé sur d’autres postes informatiques, afin de permettre le déchiffrement des plis électroniques.

## Installation d'un certificat logiciel

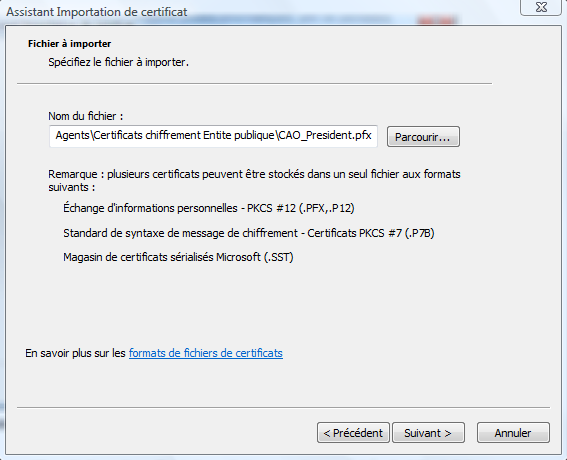
Les fonctions explicitées ci-après sont uniquement valables pour des certificats de "type logiciel". C'est-à-dire des certificats générés à partir de la CSP " Microsoft Enhanced RSA and AES Cryptographic Provider".

Les fichiers .pfx peuvent être installés sur un poste de travail afin de pouvoir procéder à l'ouverture de plis électroniques. L'installation d'un certificat est présentée pour une ouverture sur un poste équipé de l'OS Windows.

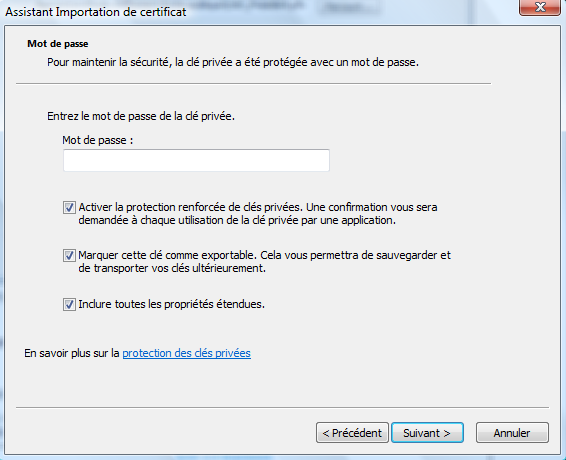
Pour l’installation, double-cliquer sur le certificat



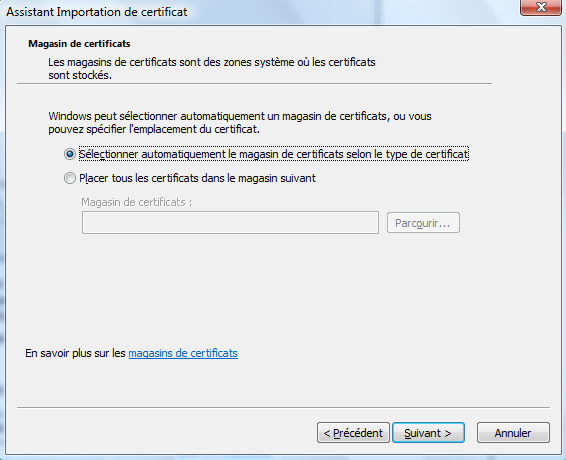
Un assistant d'installation démarre. L'AH doit cliquer sur " Suivant ".



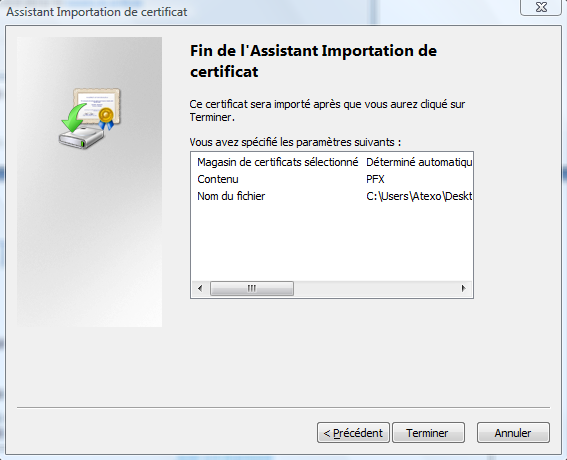
L'AH clique sur "Suivant" sans modifier d’information.



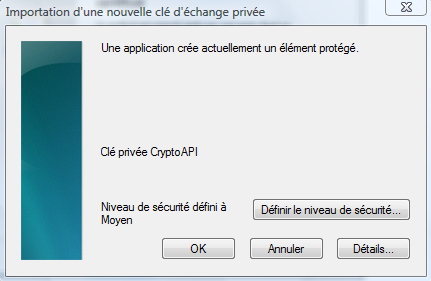
L'AH doit entrer son mot de passe le cas échéant et sélectionner "Activer la protection renforcée des clés privées…", "Marquer cette clé comme exportable…" et "Inclure toutes les propriétés étendues". L'AH clique ensuite sur "Suivant".



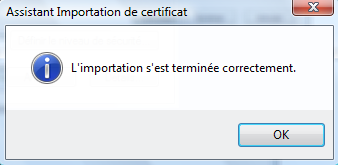
L'AH clique sur "Suivant" sans rien modifier.



L'AH clique sur "Terminer" afin de lancer le processus d'installation du certificat.



Une fenêtre apparaît. L'AH clique sur "OK".



Une fois l'installation terminée, un message de confirmation apparait. L'AH clique sur "OK". Le certificat est maintenant installé sur le poste de travail et la clé privée peut être utilisée pour l'ouverture éventuelle de plis électroniques.