Réforme de la demande de logement social

Comment acquérir un certificat ?

Pour tout service enregistreur souhaitant accéder au système d'enregistrement national des demandes de logement social par interface avec son système privatif

Mars 2011

Présent pour l'avenir

Ce document a été réalisé avec l'appui de l'Union Sociale pour l'Habitat

Ministère de l'Écologie, du Développement durable, des Transports et du Logeme

www.developpement-durable.gou

Qu'est-ce qu'un certificat ?

Un certificat est un **document électronique permettant d'identifier une entité et de sécuriser les échanges entre deux systèmes d'information** (ici, le système d'enregistrement national d'une part et le système privatif du service enregistreur d'autre part).

- Les certificats répondent à **trois usages différents** :
  - **Chiffrement** : sécurisation des transferts de données
  - **Signature** : identification de l'entité transmettant les informations dans le cadre d'une connexion par mail (vérification que le transmetteur est autorisé à transférer des données au système d'enregistrement national)
  - **Authentification** : identification des parties qui échangent de l'information dans le cadre d'une connexion en direct sur le Web (usage utile pour les interfaces utilisant le web services, c'est-à-dire le flux synchrone)

- Un certificat **s'achète auprès d'une autorité de certification reconnue par le ministère des finances (MINEFI).** Plusieurs entreprises vendent un tel service/produit. Le certificat exigé coûte environ **80 euros par an**. Les certificats ont une durée de validité de une ou plusieurs années. Ils doivent être renouvelés à l'échéance (1 ou 2 ans en général).

Qui doit acquérir un certificat ?

Qui a besoin d'un certificat pour accéder au système d'enregistrement national ?

- Sont concernés les services enregistreurs ayant choisi de se connecter au système par interface avec leur application privative (en mode asynchrone tout comme par Web services).
  - Ne sont donc pas concernés les services enregistreurs se connectant uniquement via l'application Web.

- Le certificat à acquérir est propre à un numéro de SIREN : il s'agira donc d'acquérir un certificat par service enregistreur (et non pas pour chacun des guichets au sein de ce service enregistreur).
  - Exemple: un certificat pour l'ensemble des guichets enregistreurs d'un même bailleur.

- Les services enregistreurs possédant déjà ce type de certificats pourraient techniquement le réutiliser. Mais d'un point vue juridique, cette réutilisation n'est pas souhaitable.

Quels types de certificats acquérir ?

- Les certificats à acquérir sont des certificats d'entreprise de type client PRISV1.
  - **Certificat d'entreprise de type client** : ce certificat est attribué à un titulaire propre mandaté par l'entreprise. Le certificat de type client s'oppose à la notion de certificat de serveur.
  - **PRISV1** : norme la plus courante. Pour information, la norme PRISV2 n'est aujourd'hui pas reconnue par l'outil national, d'où sa non-utilisation.

- **Pour les connexions en mode asynchrone,** l'usage « Signature » (transmission en différé par échanges de mail) est nécessaire.
- **Pour les connexions en mode synchrone,** l'usage « Authentification » (Echange direct par Web services) est nécessaire.
- Enfin, **quelque soit le mode de connexion,** il est nécessaire d'acquérir un certificat ayant l'usage « chiffrement » (déchiffrement des mails S/MIME).

Comment acquérir concrètement un certificat ?

1 Prendre contact avec le service informatique et l'éditeur de votre logiciel à interfacer

- **Décrivez votre besoin : un certificat entreprise, de type client, de norme PRISV1, ayant l'usage de signature et chiffrement** et aussi, dans certains cas, d'authentification (cf. la rubrique précédente « Quel type de certificat acquérir ? »). Demandez leur s'ils ont pas déjà acquis un certificat de ce type afin de suivre la même démarche.

- **Invitez-les à prendre contact avec l'éditeur de logiciel** qui pourra vous recommander une marque de certificat.

2 S'adresser à une autorité de certification reconnue par le Ministère des finances

- **Les autorités sont recensées au lien suivant :**
http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html

- **Il est important de vérifier,** en particulier, auprès des entités de certification, **si le certificat délivré possède bien l'usage chiffrement.**

- Vous trouverez ci-dessous les entités reconnues et connaissant la problématique propre à l'outil national :

Nom de l'entreprise	Nom du certificat
Chambersign	Fiducio
Crédit Agricole	CA Certificat
Crédit Lyonnais	Crédit Lyonnaire Authentis
Click and Trust Groupe Banque Populaire	Admineo Mercanteo

- **N'hésitez pas à contacter directement ces entreprises pour plus d'information :**
  - Vérifier avec elles que le certificat envisagé est bien adapté (cf. la rubrique précédent « Quel type de certificat acquérir ? »

- Un certificat peut-être délivré dans un support matériel : carte à puce ou clef USB, ou encore fourni sous une forme logicielle. Il est admis que les supports matériels sont non seulement plus sûrs, mais qu'ils ne sont pas plus coûteux à l'usage.

3 Acheter le certificat

- **Constituez un dossier pour l'acquisition du certificats**
  - Signature impérative d'un mandat par le représentant légal de l'entreprise

- **Achetez le certificat** (l'achat peut être se faire en ligne)

- **Déplacez-vous pour un entretien en face à face avec un agent de l'autorité de certification**
  - A l'issue de cet entretien, le certificat sera remis au titulaire, mandaté par l'entreprise.
  - S'il existe, il est recommandé de faire appel au mandataire de certification au sein de l'entreprise.

Comment utiliser le certificat acquis ?

1 Intégrer des données dans votre système privatif

- Il s'agira de paramétrer le certificat et la clé publique de chiffrement sur ordinateur qui assurera l'émission des fichiers vers l'outil national.

- Pour pouvoir utiliser le même certificat sur plusieurs ordinateurs, il faut utiliser un certificat sur support physique et installer sur chaque ordinateur le logiciel de gestion du support du certificat.

2 Transmettre des données au système d'enregistrement national

- **Transmettre** à l'administrateur du système d'enregistrement national **la clé publique de chiffrement** du certificat ayant cet usage, au format PEM ou DER (le format DER correspond à un fichier dont l'extension est .cer)

    - La joindre au questionnaire de collecte avant le 11 mars 2011 (cf. le document « Mode d'emploi pour accéder au système d'enregistrement national », disponible sur www.developpement-durable.gouv.fr)

    - La transmettre de la même façon si vous avez déjà transmis le questionnaire ou si vous le transmettez après le 11 mars 2011.

NB : Il est impératif d'envoyer le questionnaire de collecte au plus tôt. Si jamais vous pensez ne recevoir votre certificat qu'après le 11 mars, nous vous invitons à envoyer d'abord le questionnaire (dans les délais) et à transmettre le certificat ultérieurement. Ce certificat est indispensable pour vous permettre d'échanger avec le système d'enregistrement national, et notamment, pour délivrer le numéro unique d'enregistrement à toute demande de logement social que vous recevez.

Le **document ci-après « Utilisation des certificats »** vous présente l'ensemble de la démarche pour **vous aider dans l'installation et l'utilisation du certificat** nécessaire pour communiquer avec le système d'enregistrement national du Numéro unique

Secrétariat Général

Service des Politiques Support et des Systèmes d'Information

Centre de prestations et d'ingénierie Informatiques

Département Opérationnel Normandie Centre

24/02/2011

Utilisation des certificats

Présent pour l'avenir

Ressources, territoires, habitats et logement
Énergies et climat
Développement durable
Prévention des risques
Infrastructures, transports et mer

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère de l'Écologie, du Développement durable, des Transports et du Logement

Ministère de l'Écologie, du Développement durable, des Transports et du Logement

www.developpement-durable.gouv.fr

Sommaire

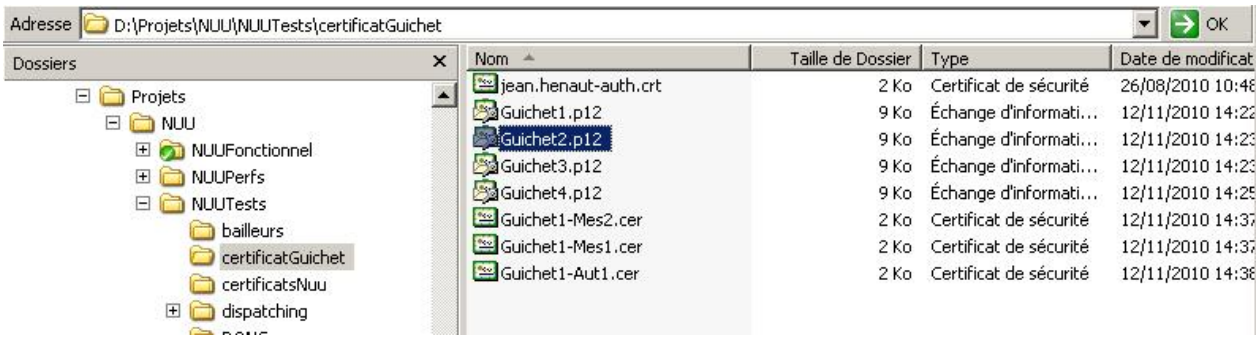
1 - Préambule

Cette note est destinée à vous aider dans l'installation et l'utilisation des différents certificats nécessaires pour communiquer avec le système d'enregistrement national du Numéro unique.

Ces informations ne sont pas exhaustives, et sont illustrées par les copies d'écran de la base « test » du système national, utilisées dans le cadre de l'expérimentation des interfaces, selon le protocole établi à ce sujet. Néanmoins, la démarche est la même lorsque vous voulez utiliser un certificat pour enregistrer directement dans la base de production, avec la mise en service nationale du nouveau système.

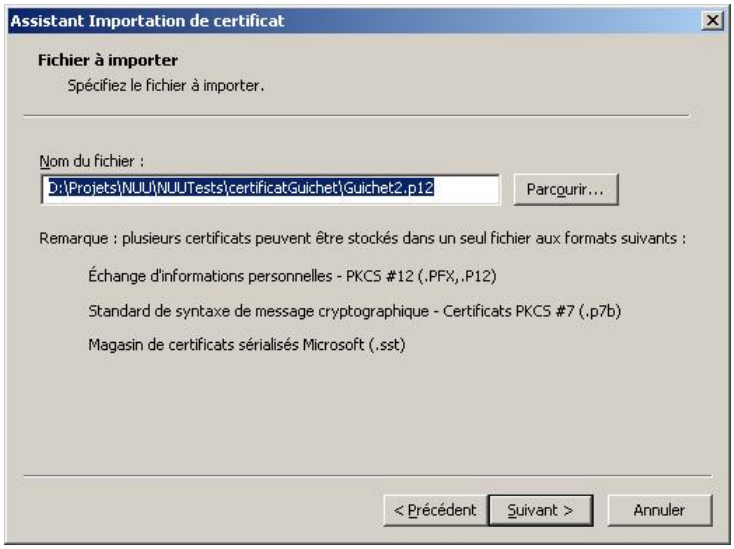
2 - Importer votre certificat dans l'environnement Windows

Depuis l'explorateur de fichier :

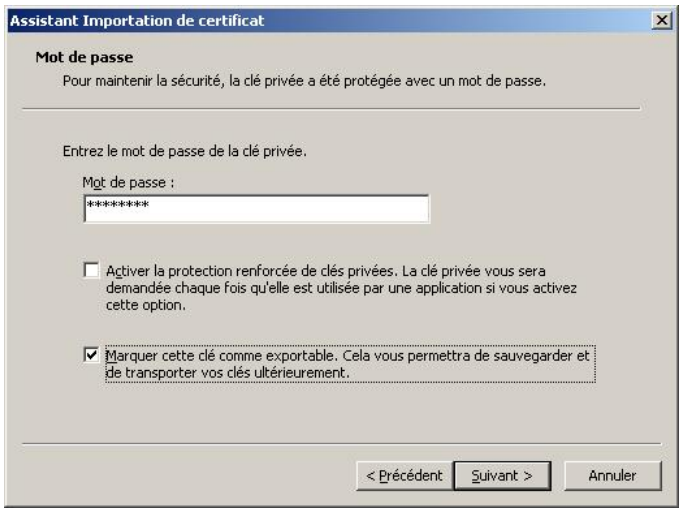


Double cliquer sur le fichier certificat à importer :

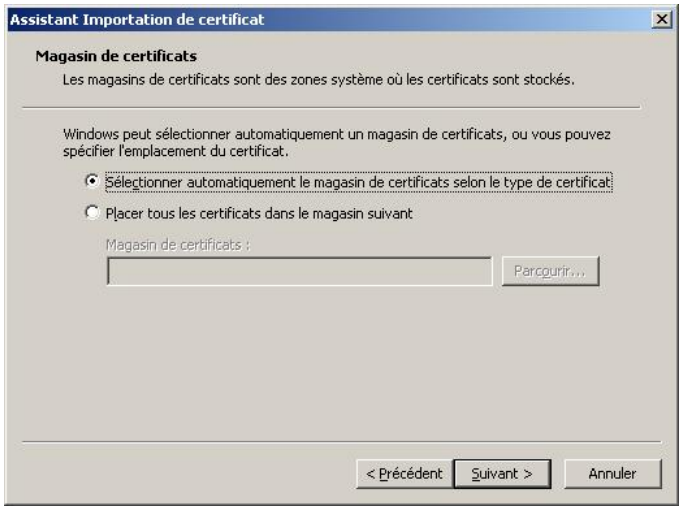
Cliquer sur « Suivant » :



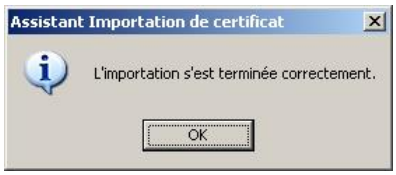
Saisir le mot de passe ET cocher la case « Certificat exportable », puis, cliquer sur « Suivant » :



Cliquer sur « Suivant » :



Cliquer sur « Terminer » :

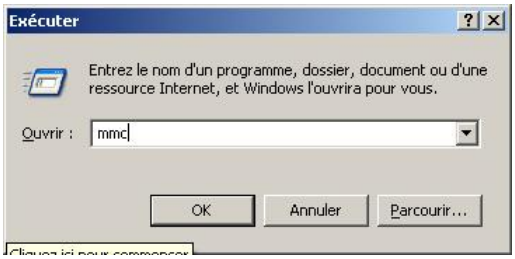


3 - Extraire la clé publique à usage de chiffrement de votre certificat

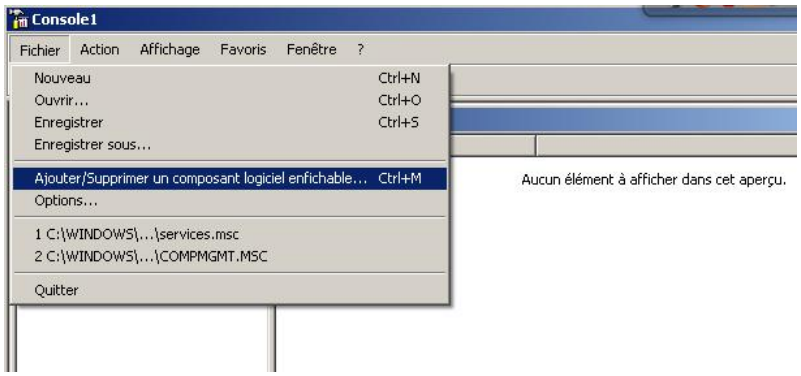
Cette procédure permet d'extraire la clé publique de chiffrement de votre certificat. Le fichier qui en résulte sera à transmettre, avec le questionnaire de collecte des données nécessaires au paramétrage des guichets enregistreurs à l'adresse suivante demande-unique@developpement-durable.gouv.fr ou le cas échéant directement au gestionnaire départemental du Numéro unique.

3.1 - Préparer la console d'administration

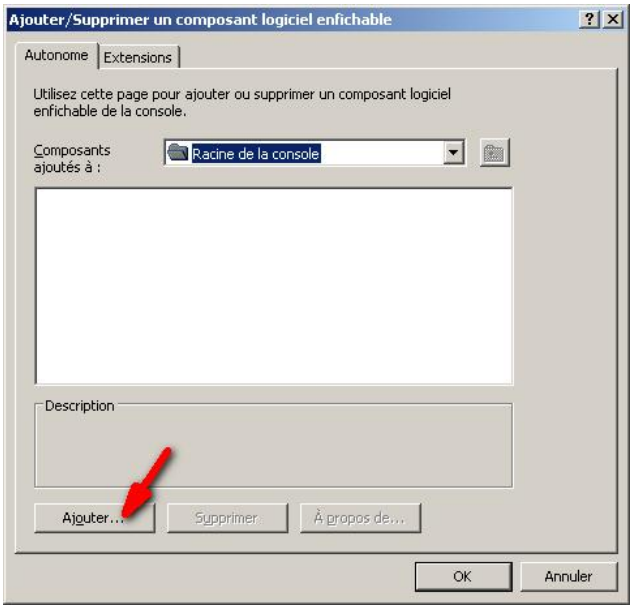
Cliquer sur le menu « Démarrer », puis, sur « Exécuter ».
Dans la fenêtre Exécuter, indiquer « mmc » et cliquer sur « OK » :



Dans « Fichier », sélectionner « Ajouter un composant » :

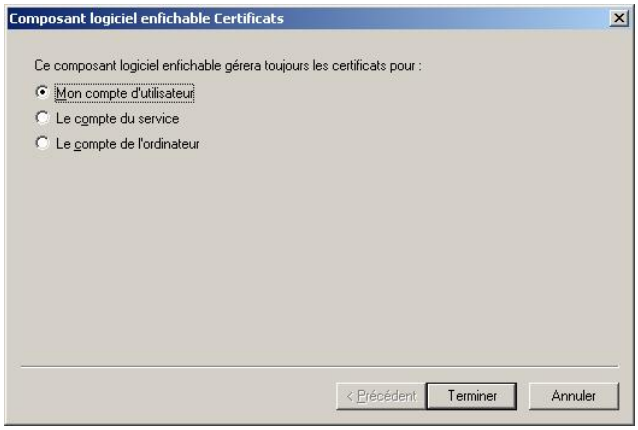


Cliquer sur « Ajouter » :

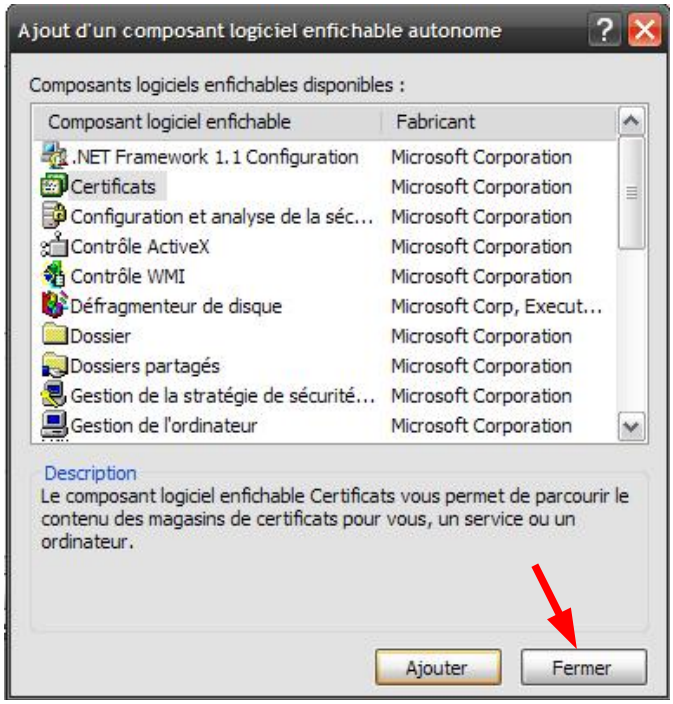


Sélectionner le composant « Certificats » et cliquer sur « Ajouter » :

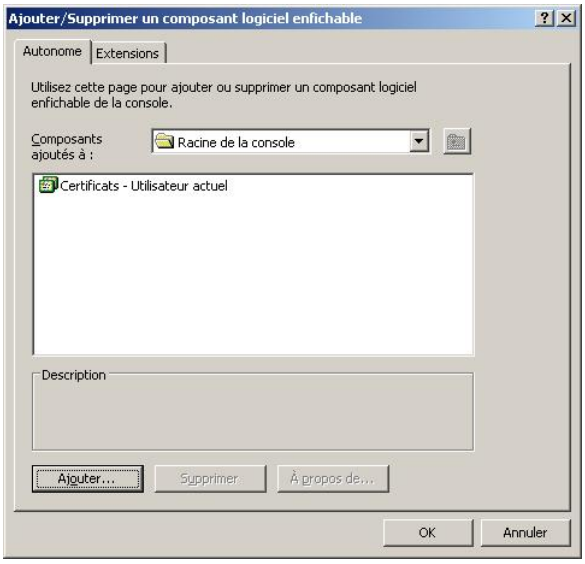
Ajouter le composant pour « Mon compte d'utilisateur », puis cliquer sur Terminer :



Cliquer sur « Fermer » puisqu'il n'y a pas d'autre composant à ajouter.

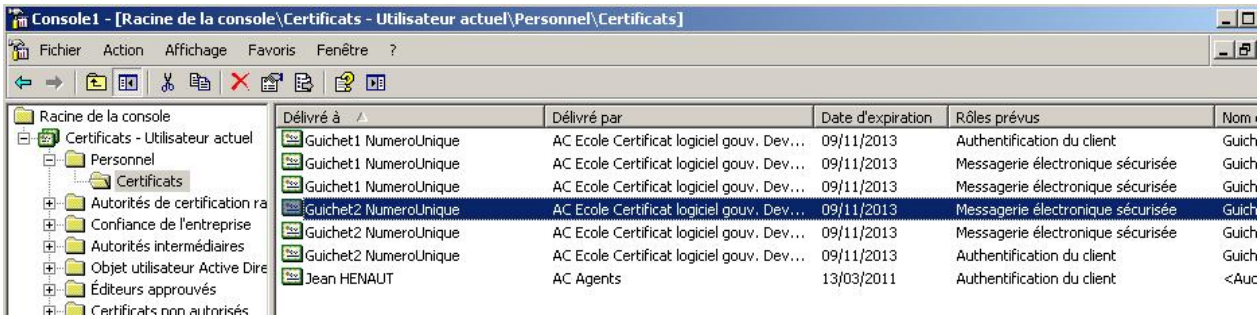


Cliquer sur « OK » :



3.2 - Extraire la clé publique à usage de chiffrement

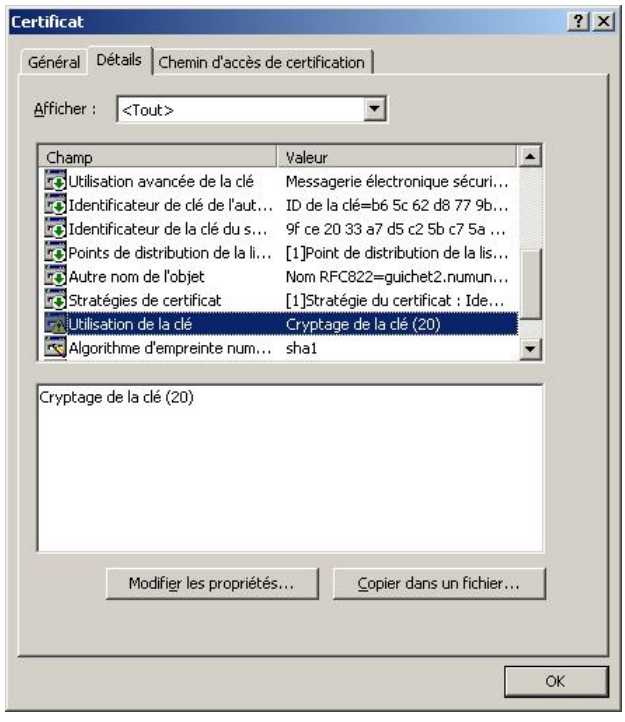
Depuis la console MMC :



Deux possibilités selon votre situation :

- Si vous disposez de plusieurs certificats (1 pour chaque usage par exemple) :
  - recherchez celui qui a le champ « utilisation de la clé » indiquant « Cryptage de la clé (20) »
  - cliquer sur « Copier dans un fichier ».

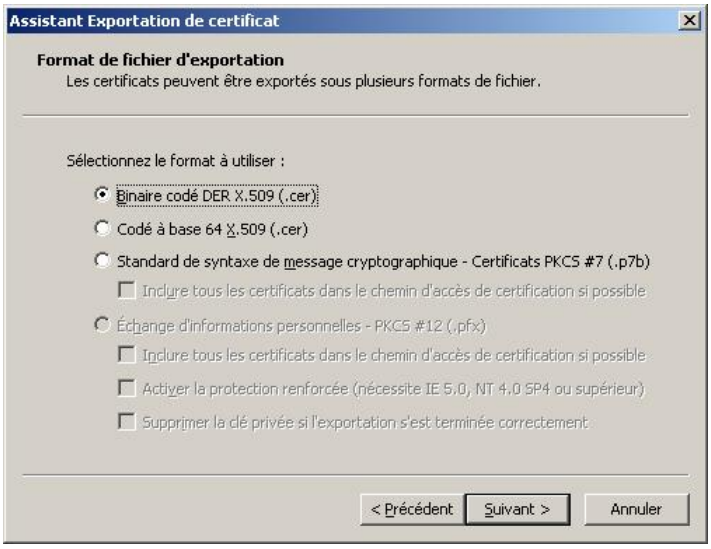
- Si vous disposez d'un certificat contenant plusieurs usages :
  - vérifier que le champ « utilisation de la clé » contient « Cryptage de la clé (20) »
  - cliquer sur « Copier dans un fichier ».



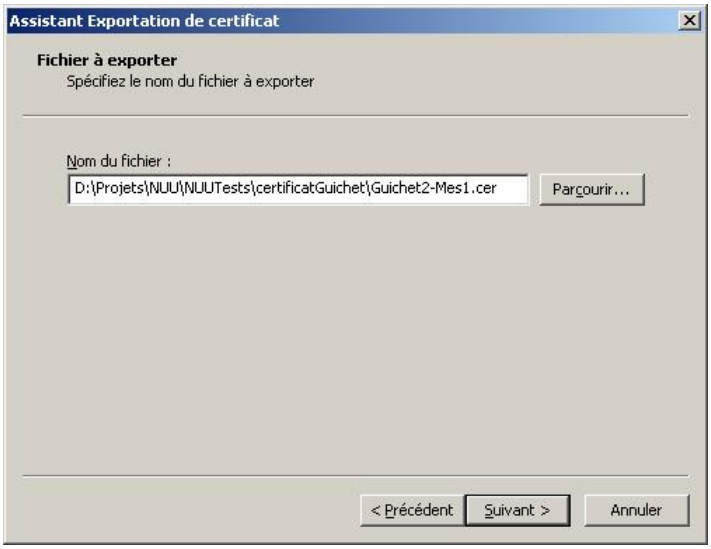
Cliquer sur « Suivant » :

Cocher « Ne pas exporter la clé privée », puis, cliquer sur « Suivant » :

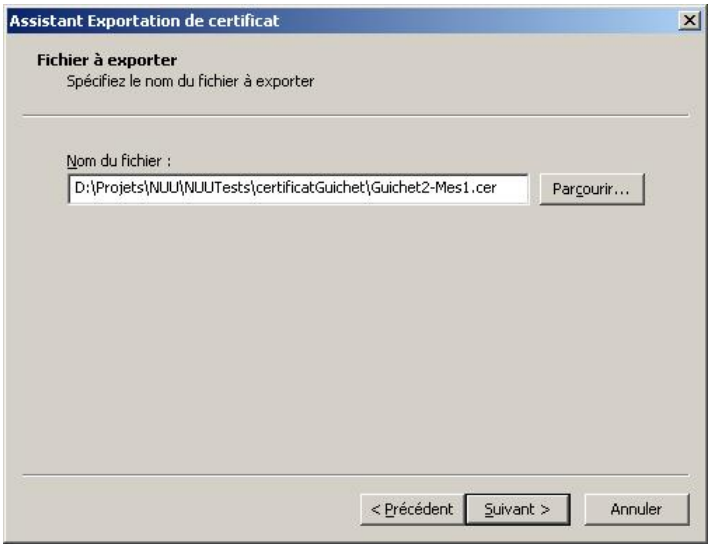
Sélectionner le format d'export nommé « Binaire codé DER X.509 (.cer) », puis, cliquer sur « Suivant » :



Renseigner le nom du fichier pour l'exportation ainsi qu'un répertoire d'enregistrement :



Cliquer sur « Suivant » :



Cliquer sur « Terminer » et sur « OK » :

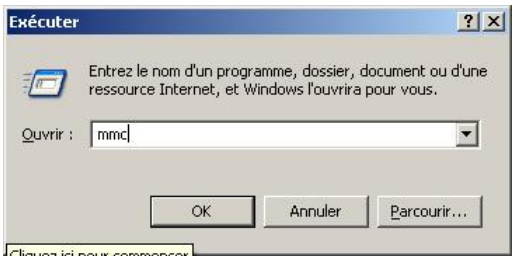
Le fichier obtenu doit être transmis, avec le questionnaire de collecte des données nécessaires à la création, dans le système, des guichets enregistreurs, à l'adresse suivante demande-unique@developpement-durable.gouv.fr ou le cas échéant directement au gestionnaire départemental du Numéro unique.

4 - Importer la chaîne de certification et le certificat de chiffrement de Numéro unique dans l'environnement Windows

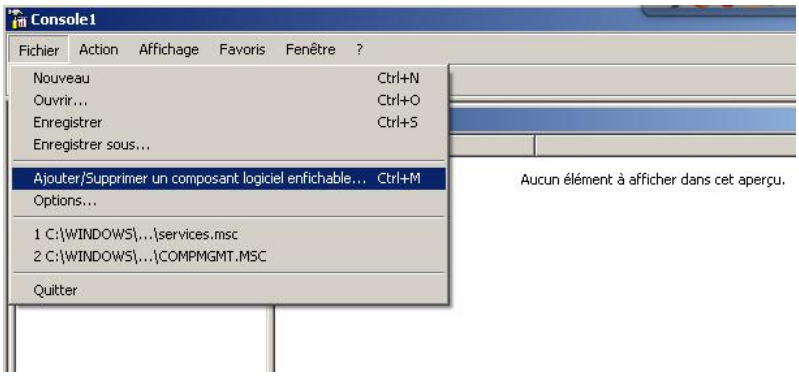
La chaîne de certification, dite également de confiance, est composée des certificats racines servant à reconnaître la validité des certificats.
Ces étapes sont indispensables si le logiciel MS Outlook est utilisé pour émettre les mails vers Numéro unique.

4.1 - Préparer la console d'administration

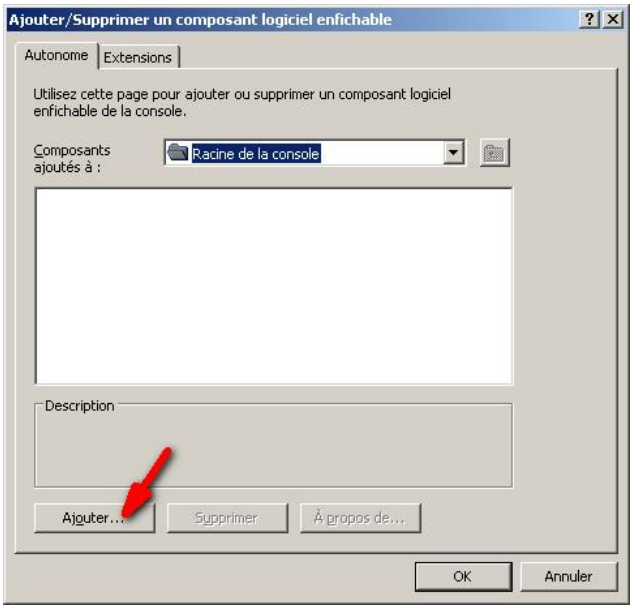
Cliquer sur le menu « Démarrer », puis, sur « Exécuter ».
Dans la fenêtre Exécuter, indiquer « mmc » et cliquer sur « OK » :



Dans « Fichier », sélectionner « Ajouter un composant » :

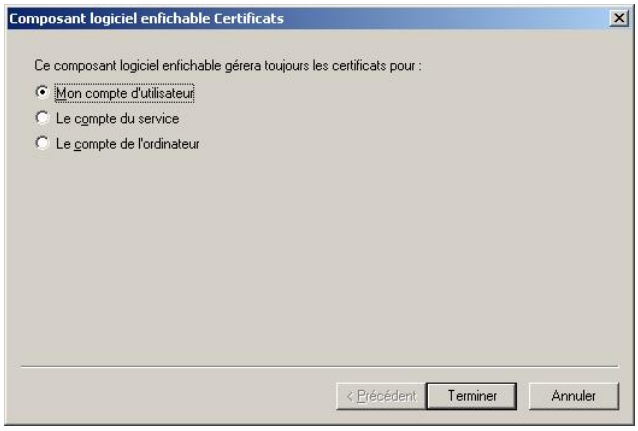


Cliquer sur « Ajouter » :

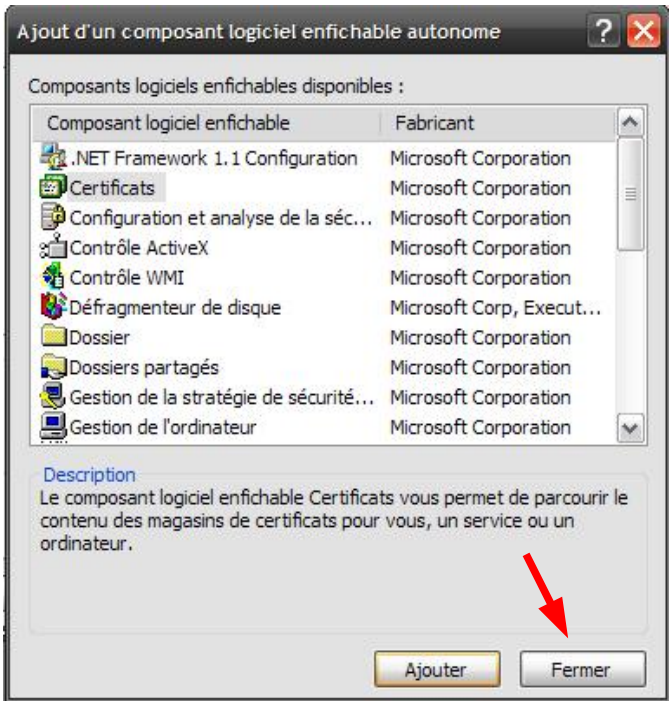


Sélectionner le composant « Certificats » et cliquer sur « Ajouter » :

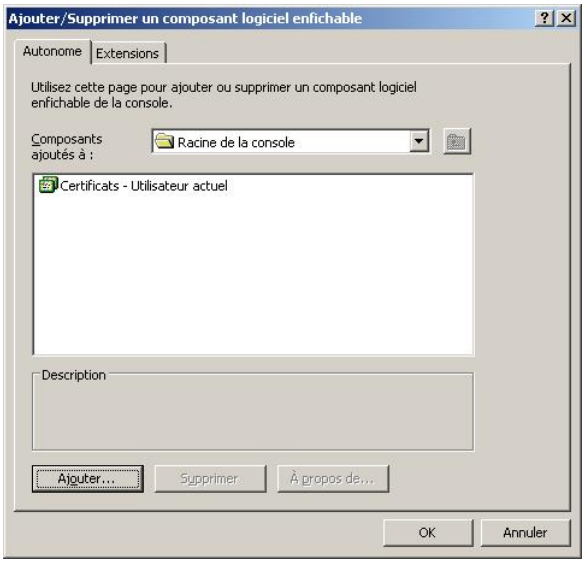
Ajouter le composant pour « Mon compte d'utilisateur », puis cliquer sur Terminer :



Cliquer sur « Fermer » puisqu'il n'y a pas d'autre composant à ajouter.



Cliquer sur « OK » :

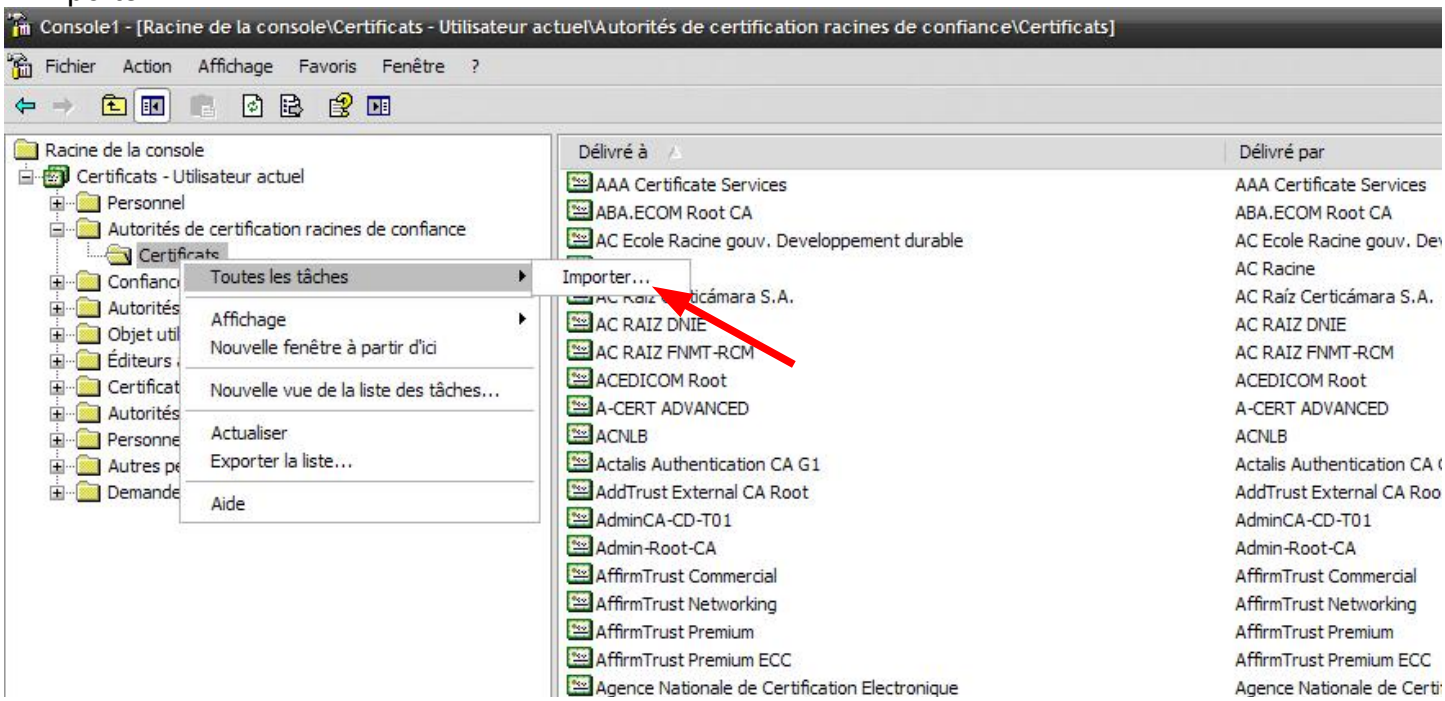


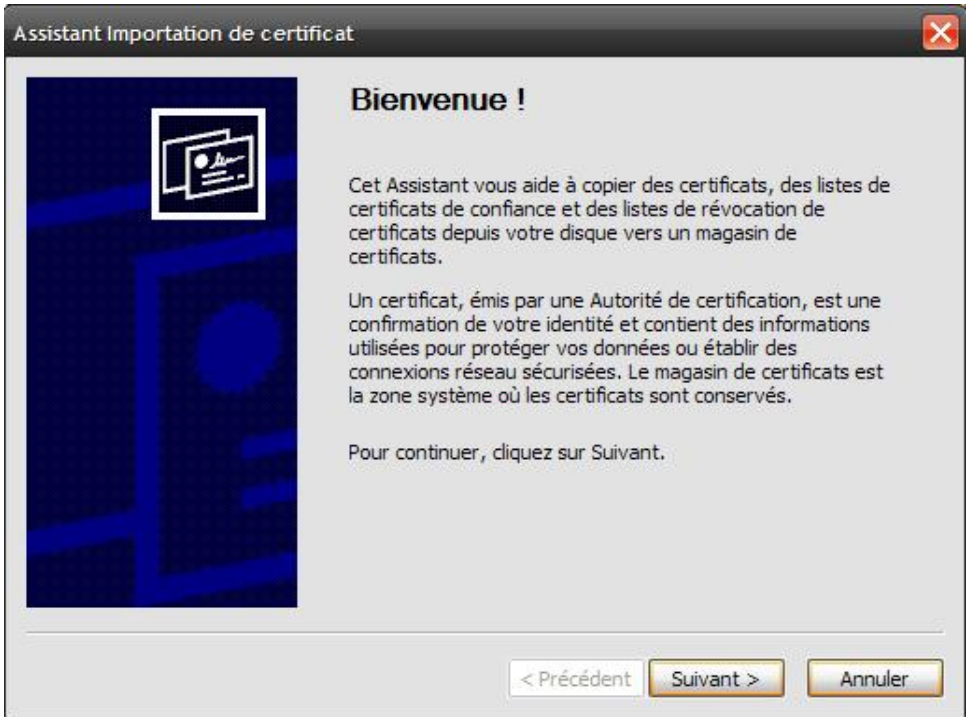
4.2 - Importer les certificats racines

Information : cette procédure vaut pour les certificats racines liés à vos certificats personnels ainsi que pour pour les certificats racines de la chaîne des autorités de certifications du ministère.
Cependant, seule la procédure d'importation des 4 certificats racines composant la chaîne de certification du ministère sera présentée ici.
Pour ce qui concerne l'importation des certificats racines de vos certificats, nous vous proposons de vous rapprocher des autorités de certification qui vous les ont délivrés.

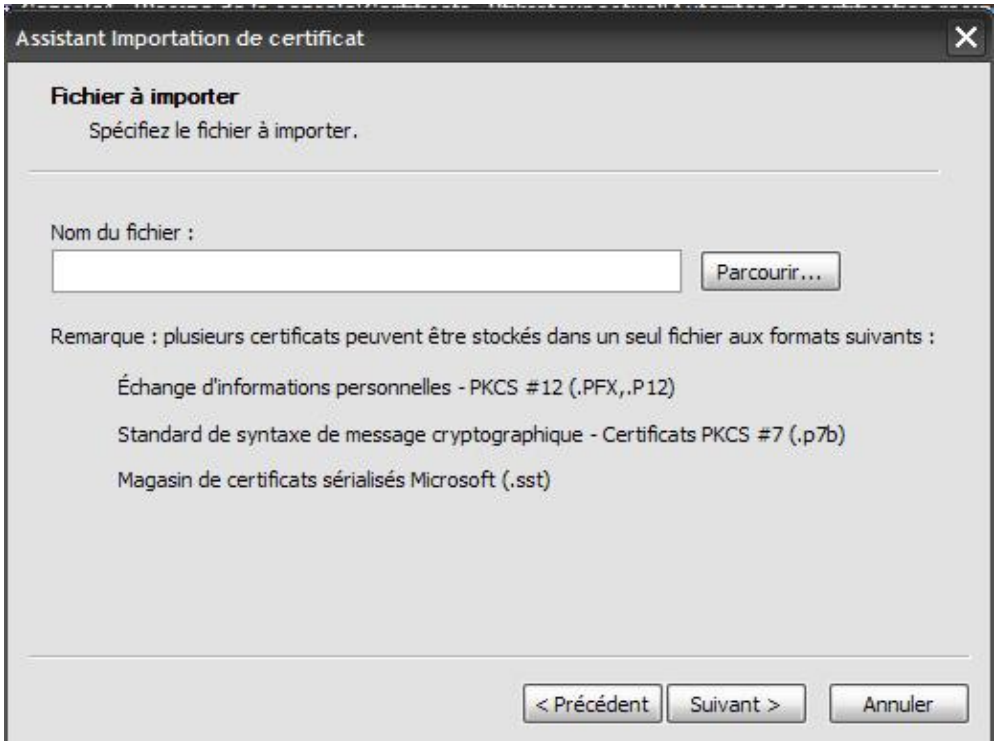
Pré-requis : disposer des 4 certificats de la chaîne de certification du ministère et du fichier LisezMoi.txt
Dans le fichier LisezMoi.txt, un ordre d'importation est spécifié selon une hiérarchie qu'il vous faut respecter.

Depuis la console qui s'est affichée, déployer l'arborescence de la racine de la console proposée à gauche sur l'écran selon le cheminement suivant : « Certificats – Utilisateur actuel », puis, « Autorités de certification racine de confiance », puis, « Certificats ».
Effectuer un clic droit sur le dossier « Certificats », puis, sélectionner « Toutes les tâches », et « Importer ».

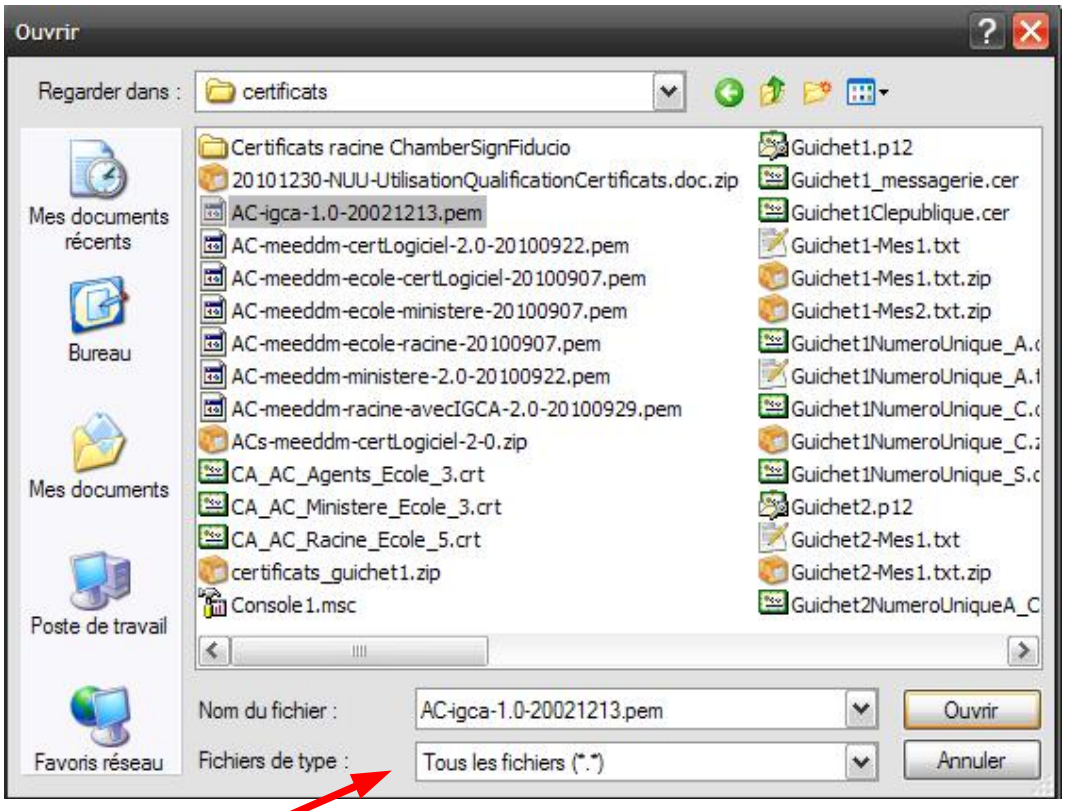




Cliquer sur « Suivant ».

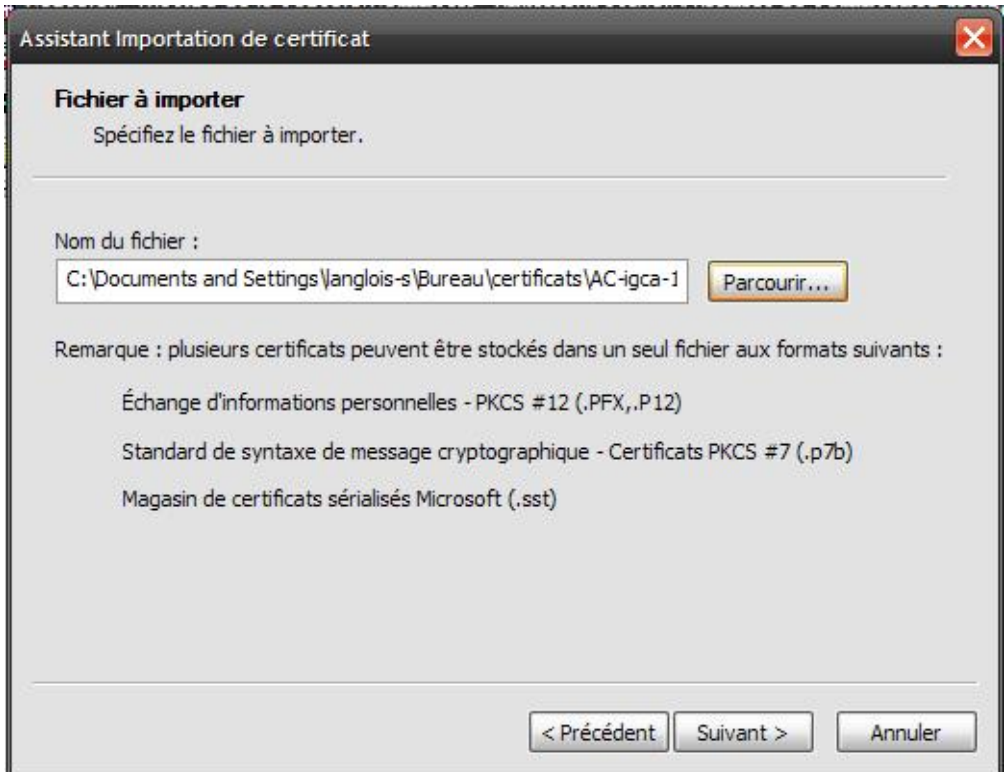


Cliquer sur « Parcourir ». Puis, dans la liste « Fichiers de type », sélectionner « Tous les fichiers » afin de voir apparaître les certificats dont l'extension est .pem. Sélectionner « AC-igca-1.0-20021213.pem ».

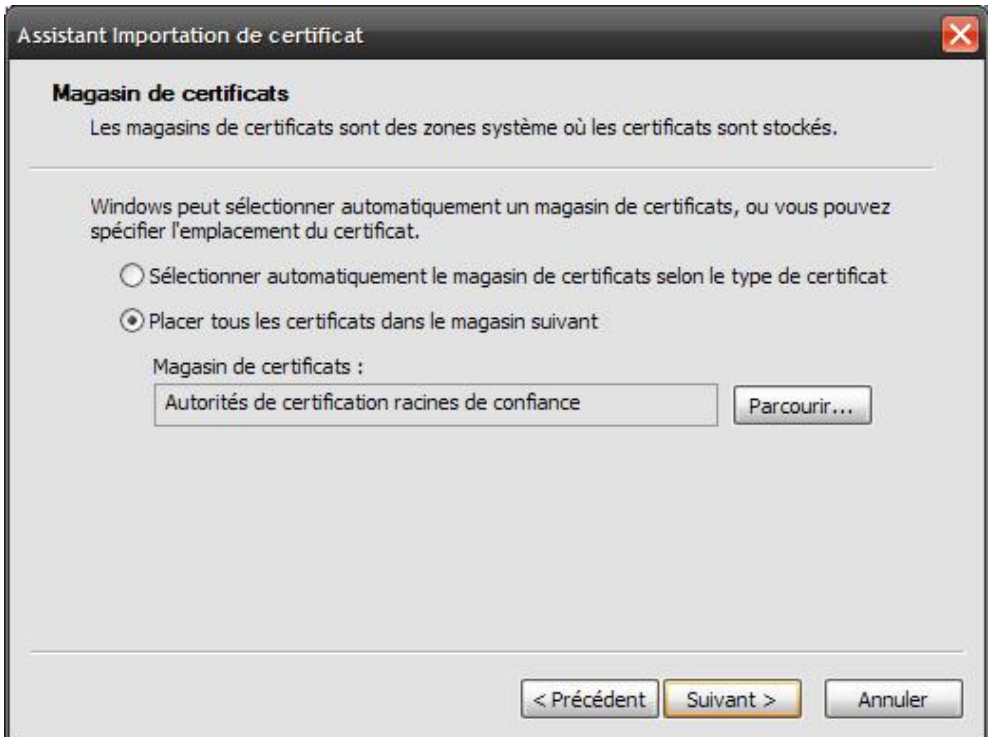


Cliquer sur « Ouvrir ».

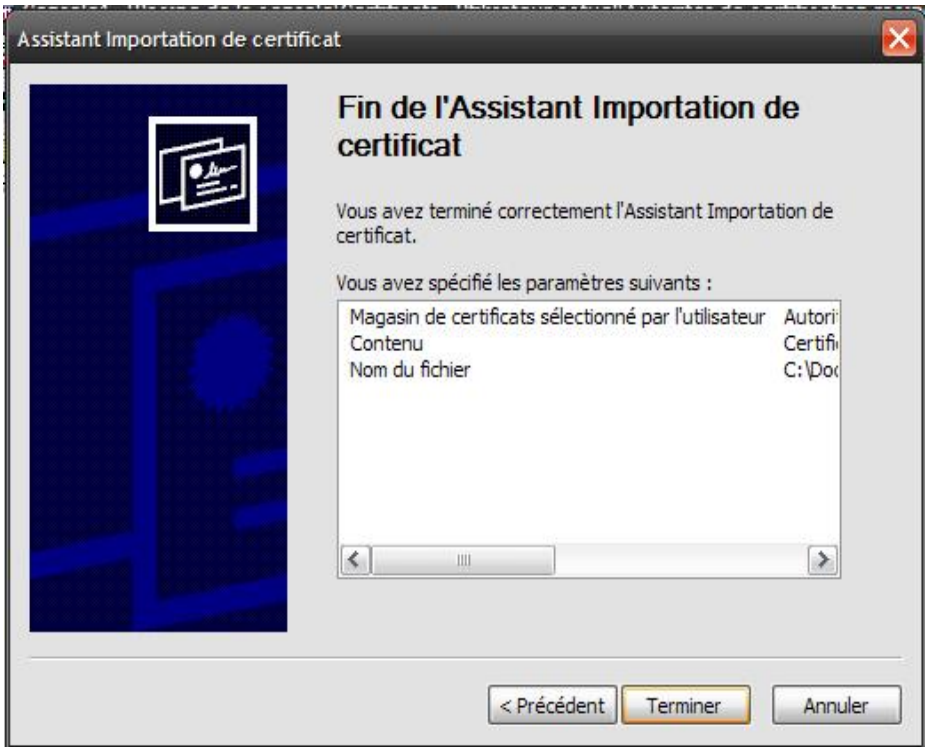
Cliquer sur « Suivant ».



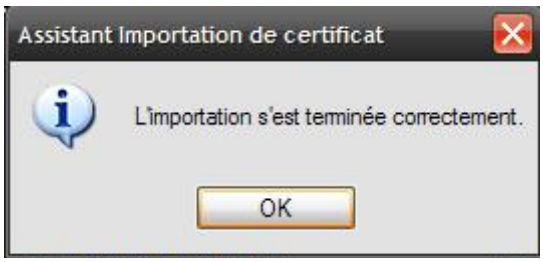
Vérifier que « Placer tous les certificats dans le magasin suivant : Autorités de certification racines de confiance » est coché. Puis, cliquer sur « Suivant ».



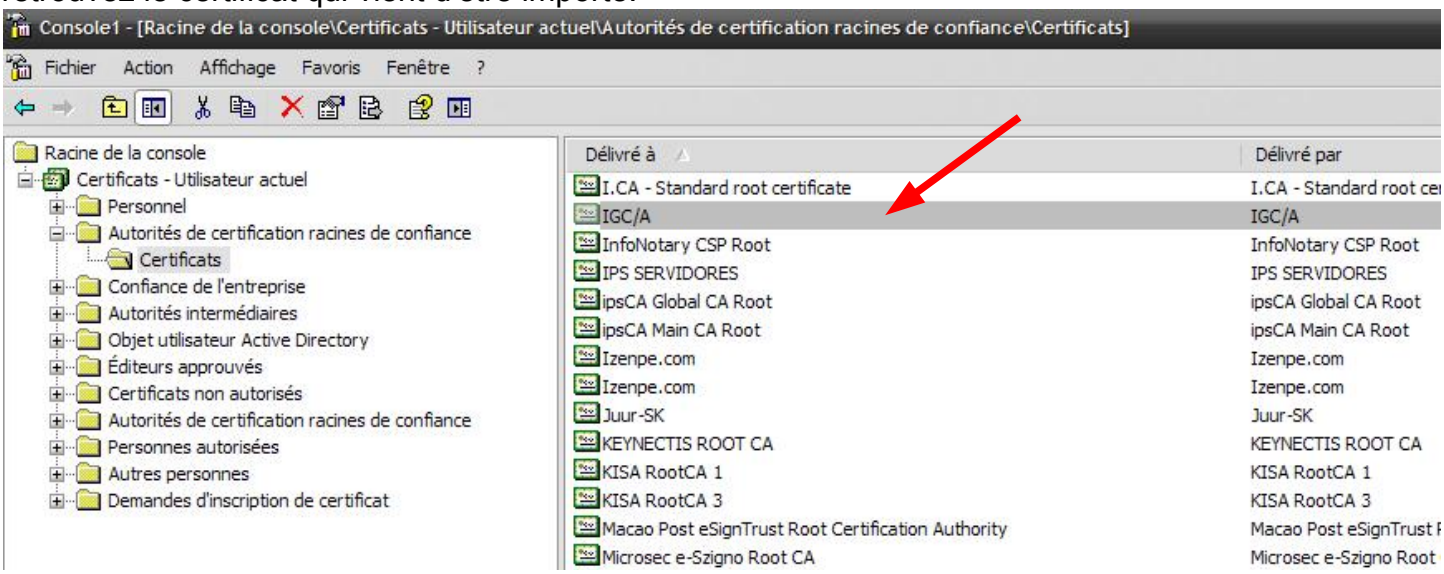
Cliquer sur « Terminer ».



Enfin, cliquer sur « OK »



Maintenant, quand vous consultez la liste des certificats racines des autorités de certification, vous retrouvez le certificat qui vient d'être importé.

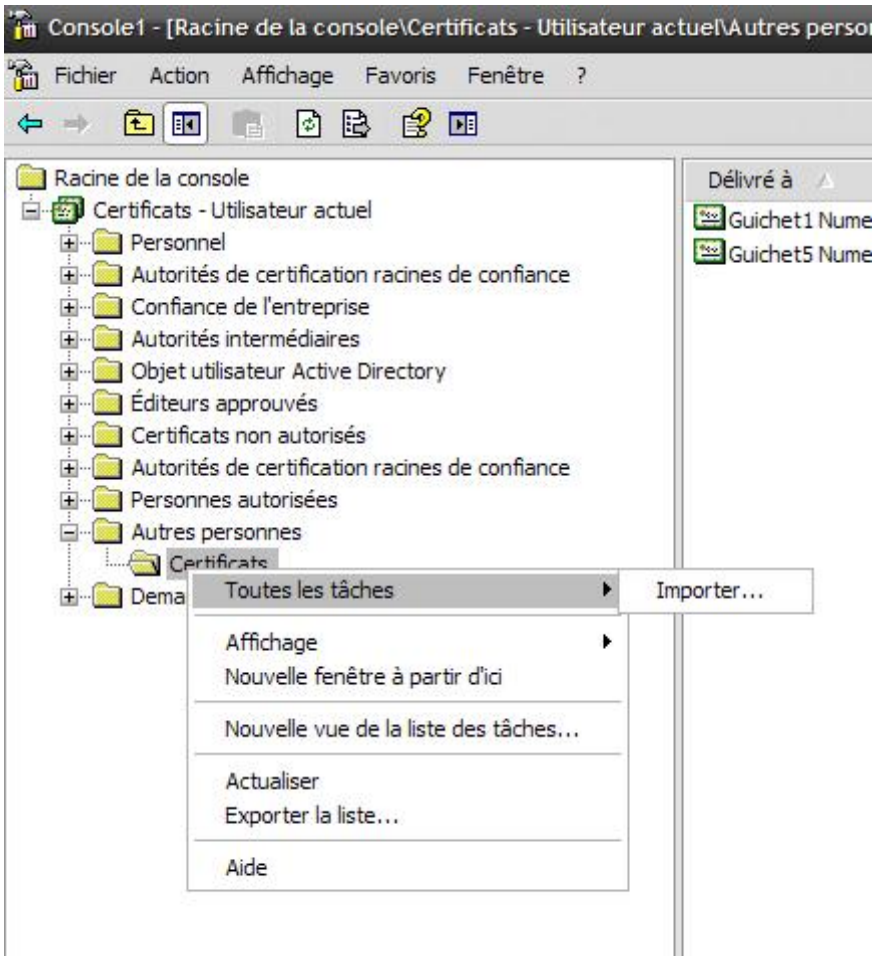


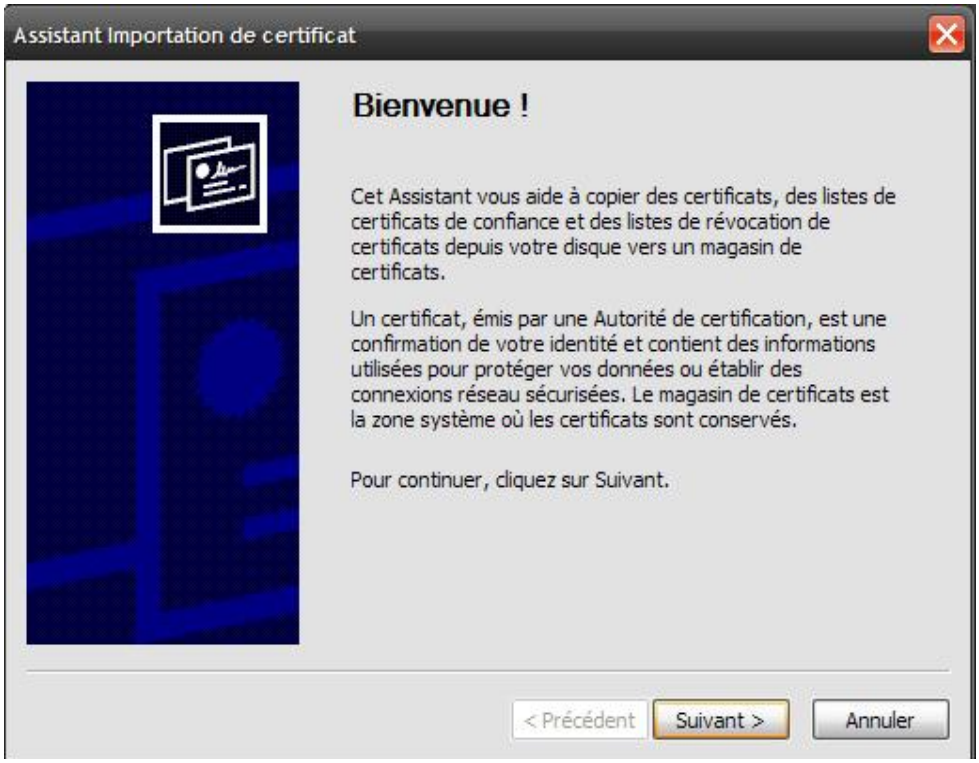
Recommencer l'opération pour les trois autres certificats racines de la chaîne de certification fournie par le ministère, selon l'ordre annoncé dans le fichier LisezMoi.txt. Ne pas fermer la console.

Une fois l'ensemble de ces certificats importés, vous allez importer le certificat de chiffrement de Numéro unique, nécessaire pour chiffrer les mails envoyés à Numéro unique.

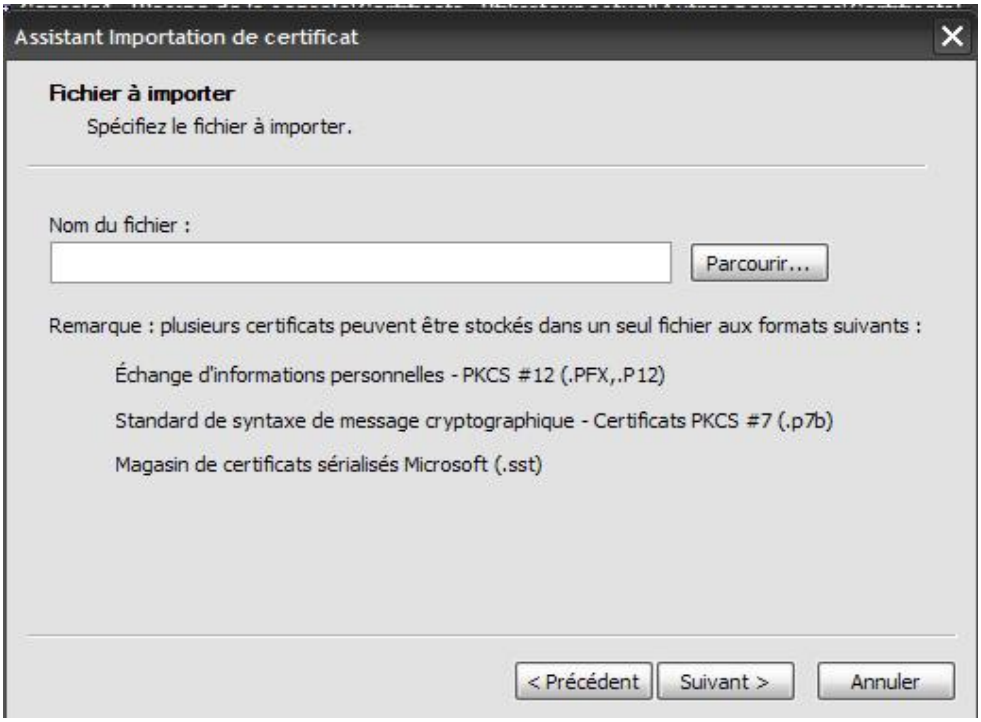
4.3 - Importer le certificat de chiffrement de Numéro unique

Dans l'arborescence de la console, déployer le dossier « Autres personnes » et faire clic droit sur le dossier « Certificats », puis, sélectionner « Toutes les tâches » et cliquer sur « Importer ».

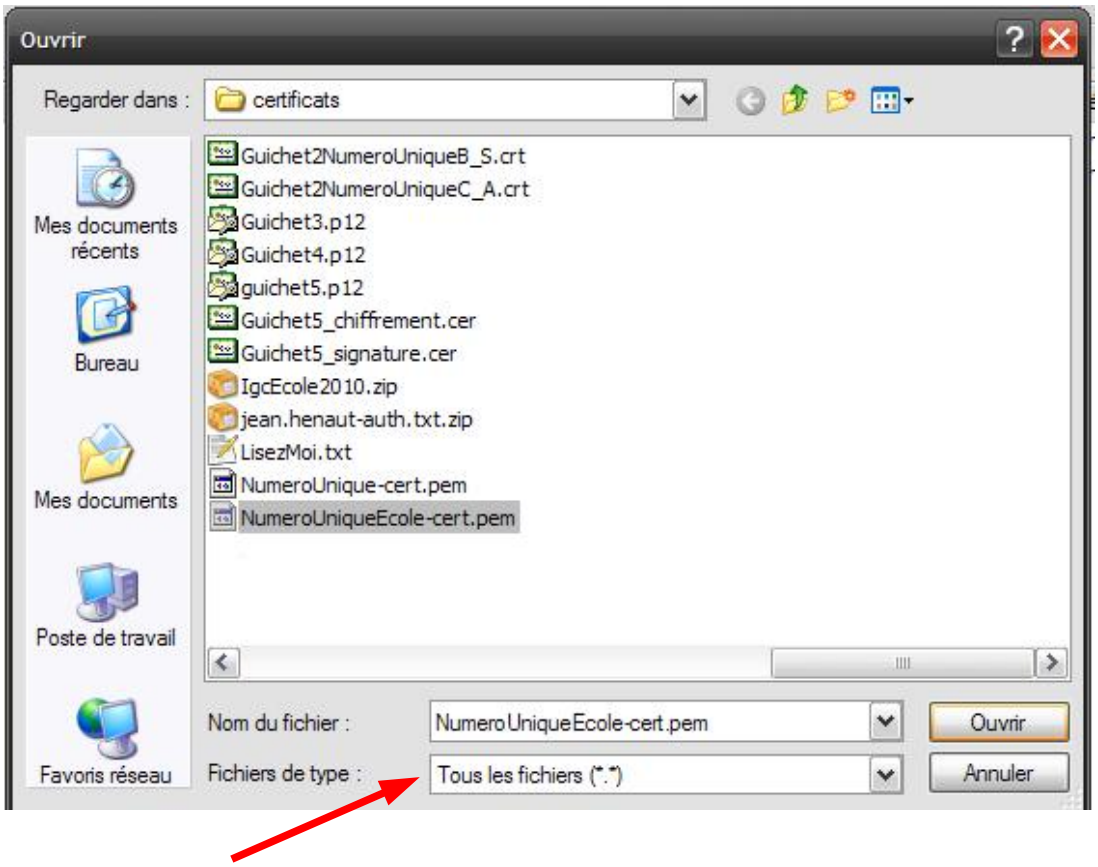




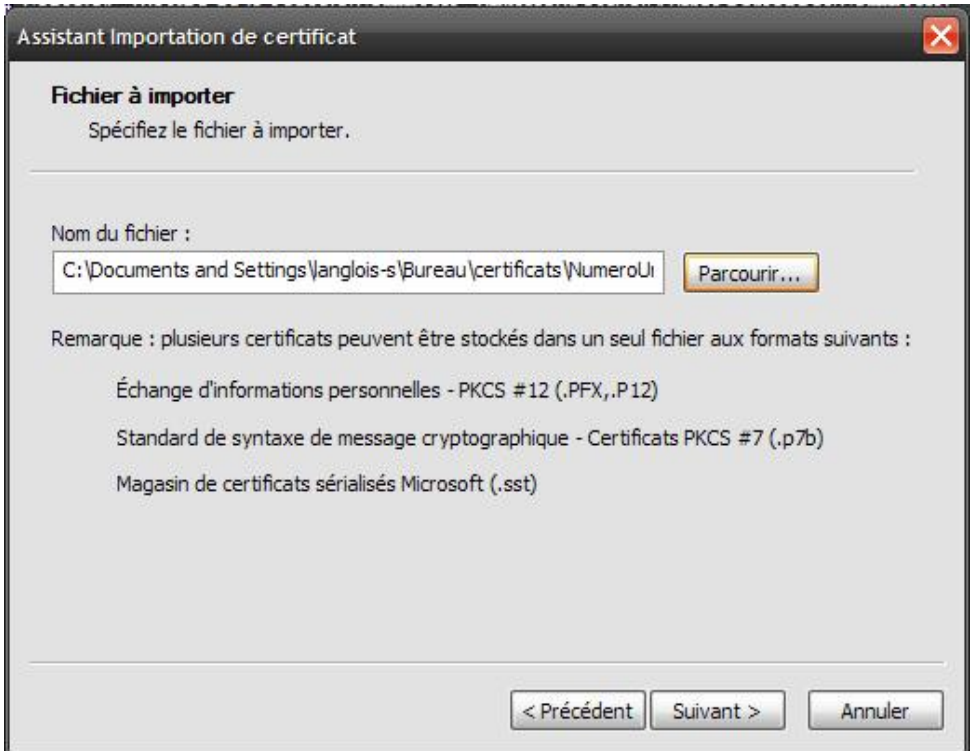
Cliquer sur « Suivant ».



Cliquer sur « Parcourir ». Puis, dans la liste « Fichiers de type », sélectionner « Tous les fichiers » afin de voir apparaître les certificats dont l'extension est .pem. Sélectionner « NumeroUnique-cert.pem ».

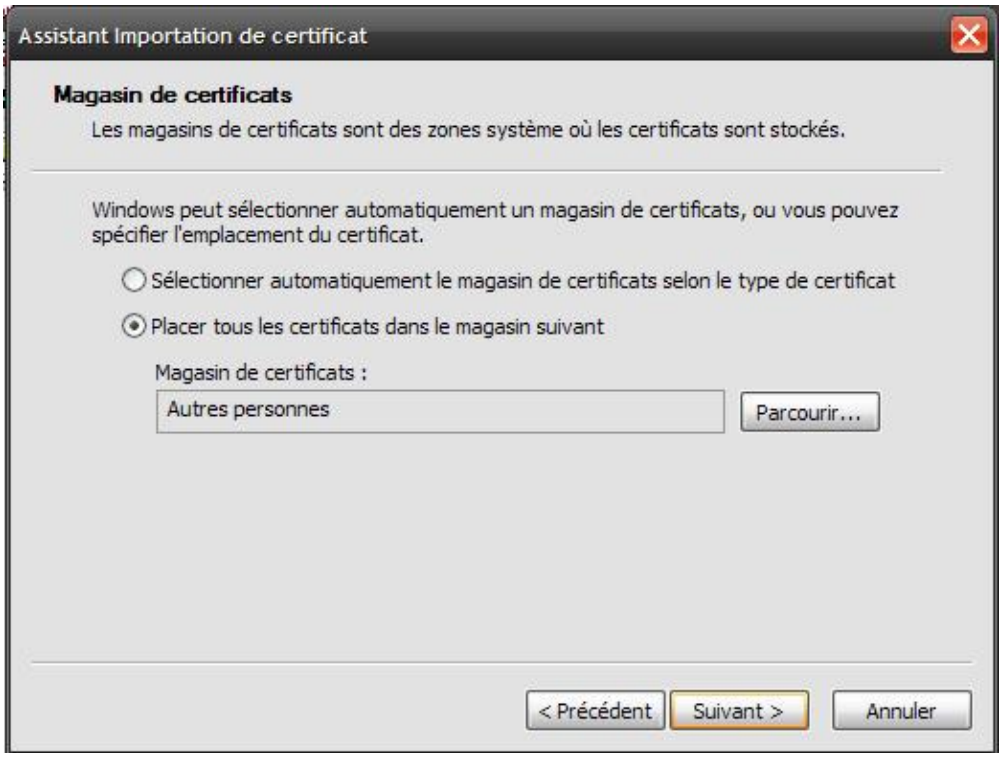


Cliquer sur « Ouvrir ».



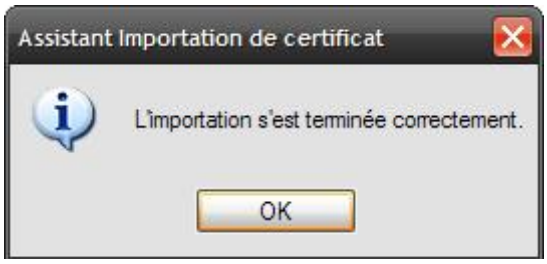
Cliquer sur « Suivant ».

Vérifier que « Placer tous les certificats dans le magasin suivant : Autres personnes » est coché. Puis, cliquer sur « Suivant ».

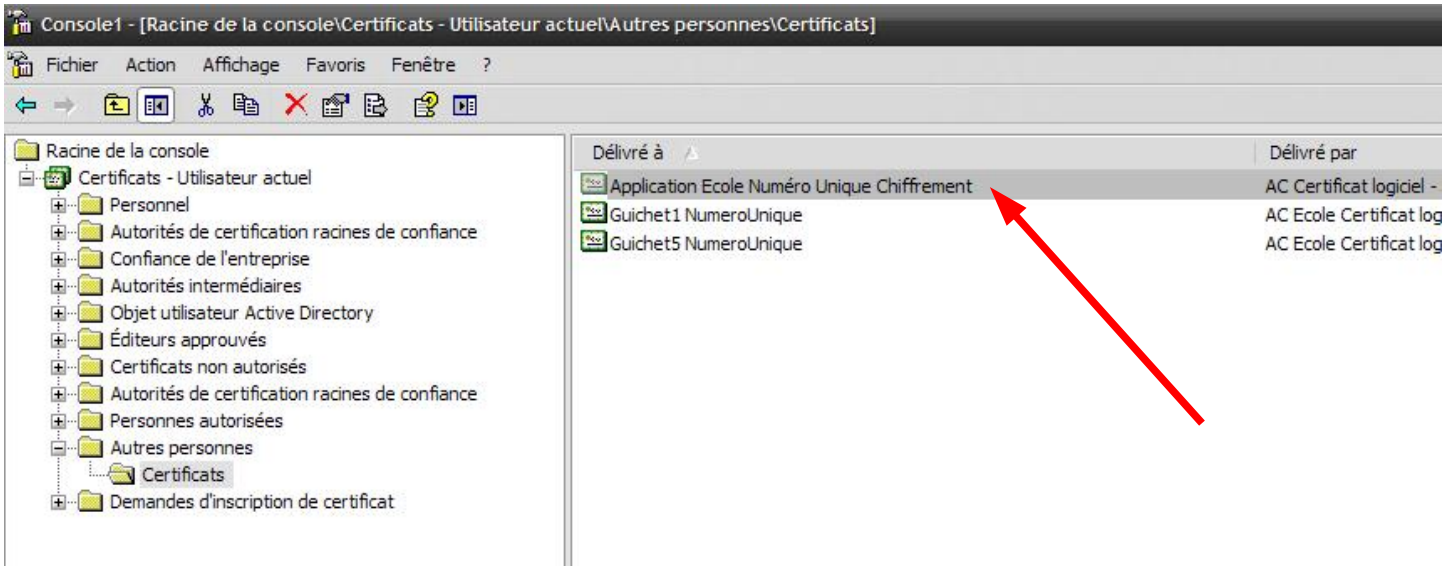


Cliquer sur « Terminer ».

Cliquer sur « OK ».



Maintenant, quand vous consultez la liste des certificats des autres personnes, vous retrouvez le certificat qui vient d'être importé.



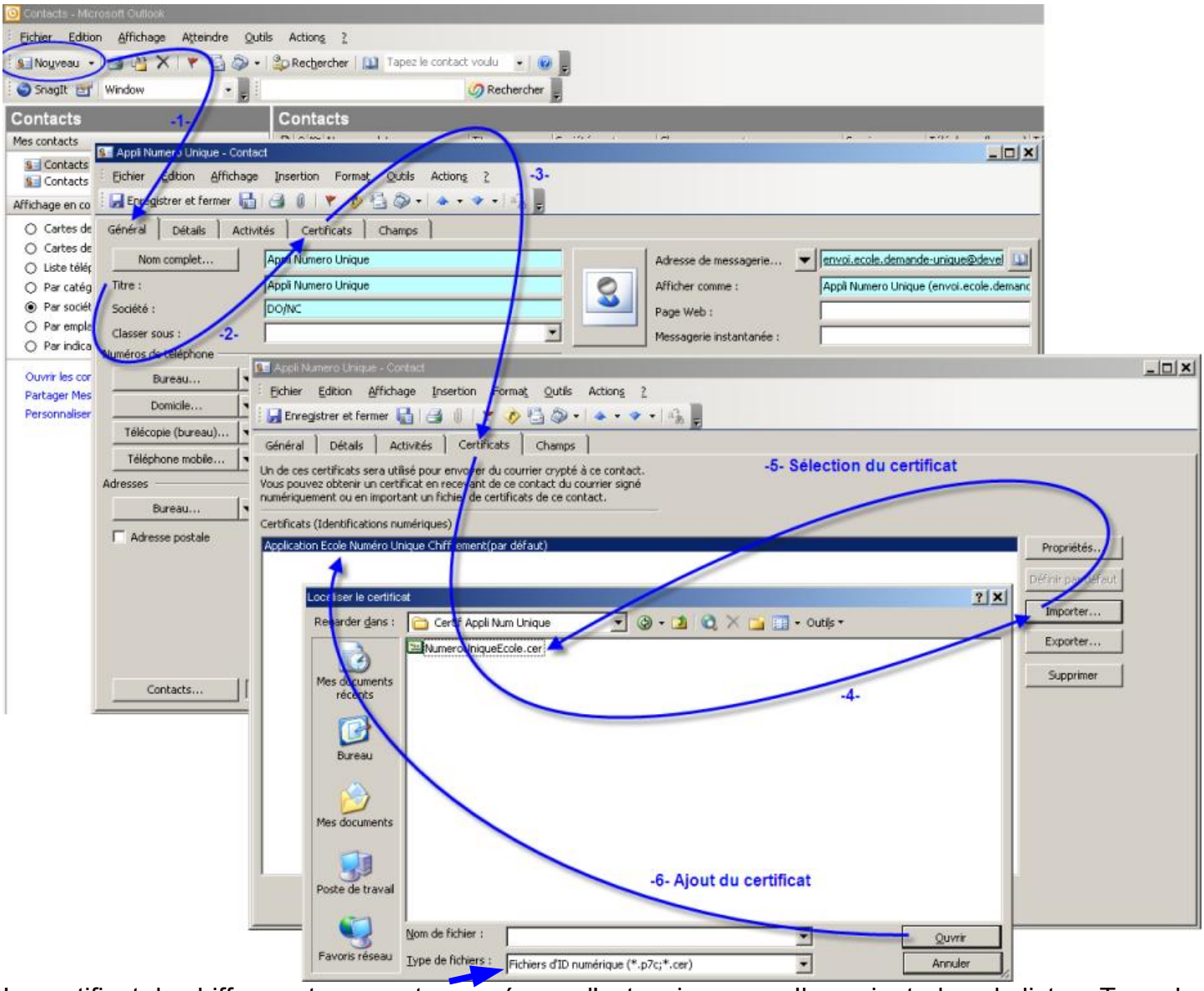
5 - Configuration des logiciels de messagerie et utilisation des certificats

Afin d'utiliser vos certificats de signature et chiffrement ainsi que le certificat de chiffrement de Numéro Unique, il convient de configurer votre logiciel de messagerie.
Sont présentées ci-après les configurations des logiciels les plus couramment utilisés soit : MS Outlook et Mozilla Thunderbird.

5.1 - Utiliser les certificats avec MS Outlook

5.1.1 - Etape 1 : Utiliser le certificat de chiffrement de Numéro unique

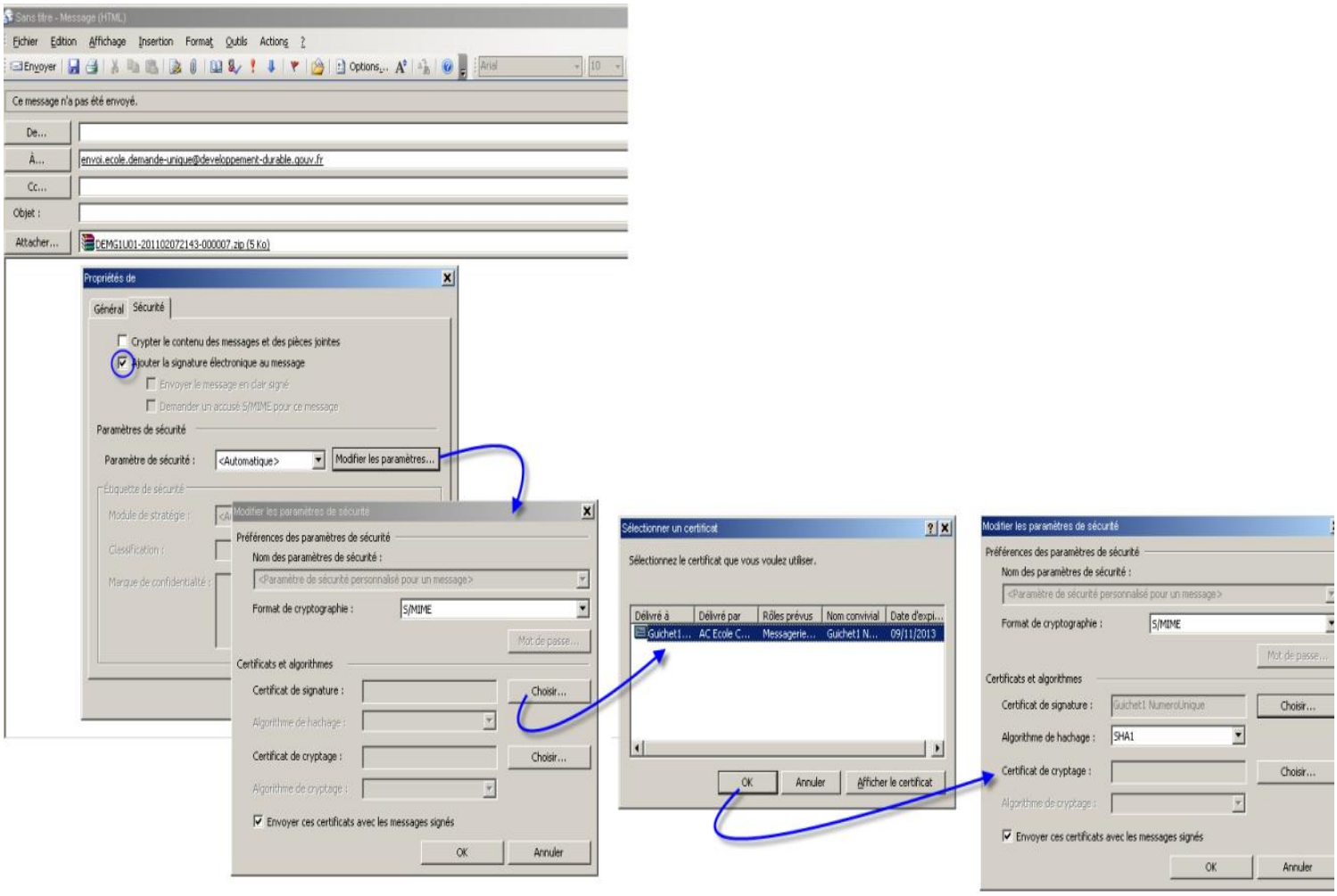
Créer un contact ayant pour adresse : envoi.demande-unique@developpement-durable.gouv.fr
Ajouter le certificat de chiffrement pour les mails à destination de ce contact :



Le certificat de chiffrement vous est envoyé avec l'extension .pem. Il convient, dans la liste « Type de fichiers », de sélectionner : « Tous les fichiers » afin de pouvoir le sélectionner.

5.1.2 - Etape 2 : Utiliser les certificats de signature et de chiffrement

Composition du mail, puis signature unitaire du mail (sinon paramétrage général pour signature sur l'ensemble des mails : via Outils -> option -> Sécurité)
On retrouve ici les certificats qui ont été importés dans le magasin des certificats Microsoft (voir chapitre 1).

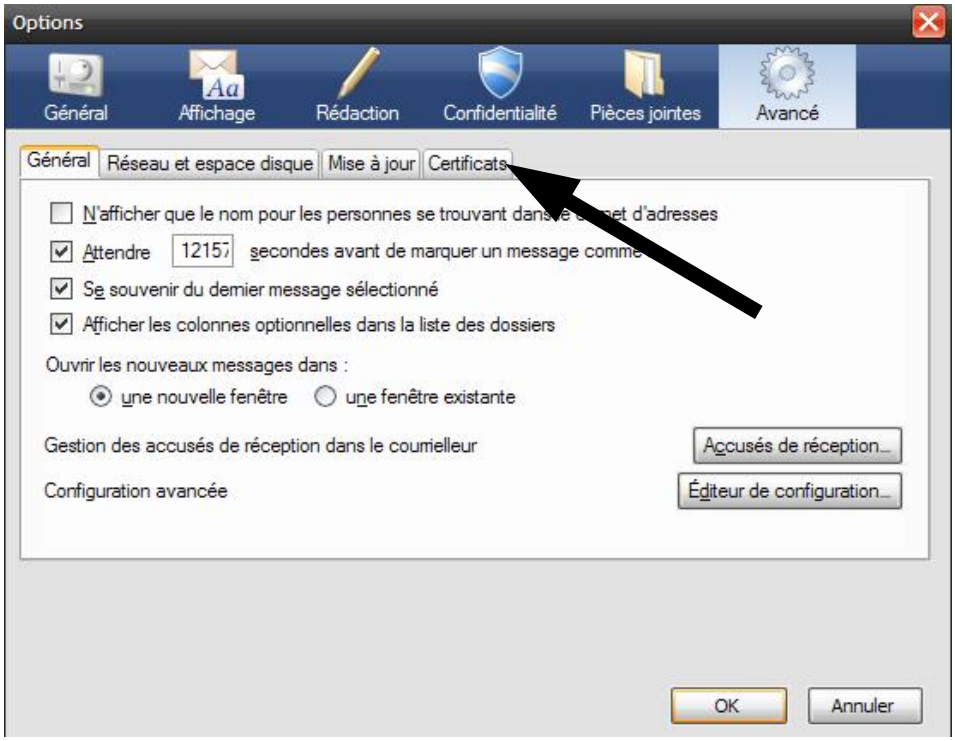


MS Outlook (et Lotus également) n'accepte pas de signer un mail pour lequel l'émetteur (adresse mail) n'est pas référencé dans le certificat. Dès lors, il est important que l'adresse transmise à l'autorité de certification lors de l'acquisition de votre certificat soit la même que celle transmise dans le questionnaire de collecte pour les modalités d'échanges de fichiers (paragraphe 5 du questionnaire).

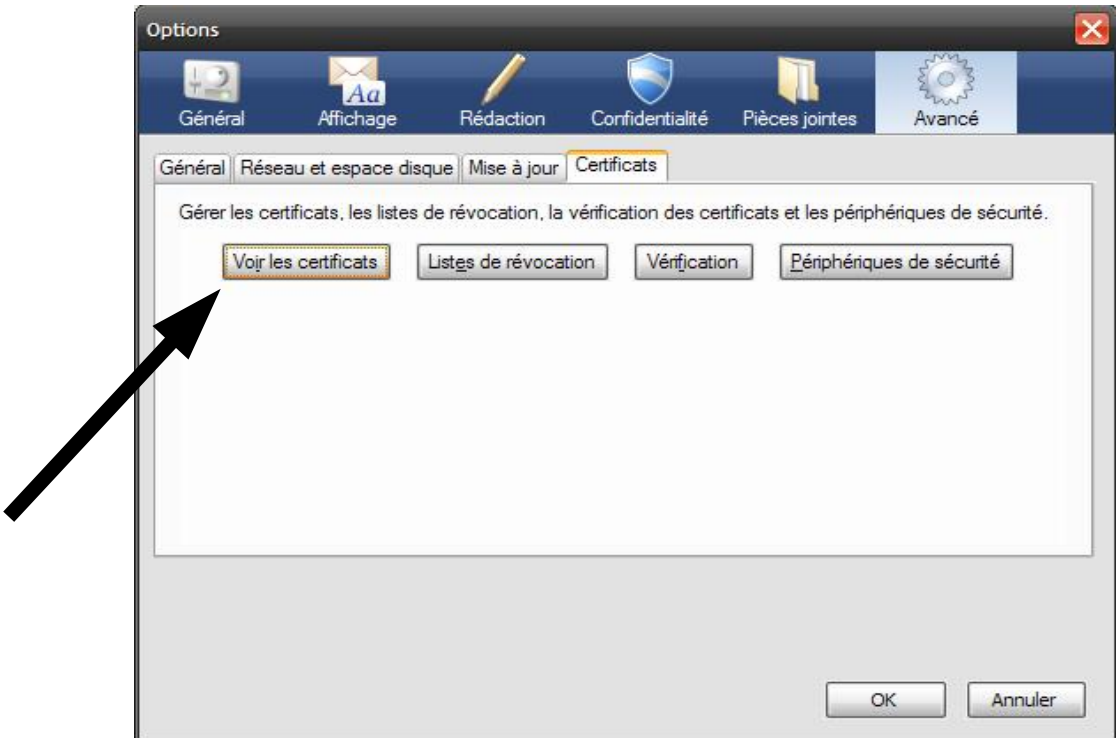
En cas de difficulté sur ce sujet, nous vous recommandons d'utiliser Mozilla Thunderbird, logiciel libre de messagerie, pour communiquer avec Numéro unique : en effet, avec cette messagerie, ce contrôle de concordance des adresses mail n'est pas fait.

5.2 - Utiliser les certificats avec Mozilla Thunderbird

Dans la barre d'outils, cliquer sur « Outils », puis « Options ». Dans la boîte de dialogue qui s'affiche, cliquer sur « Avancé ». Et se rendre sur l'onglet « Certificats ».

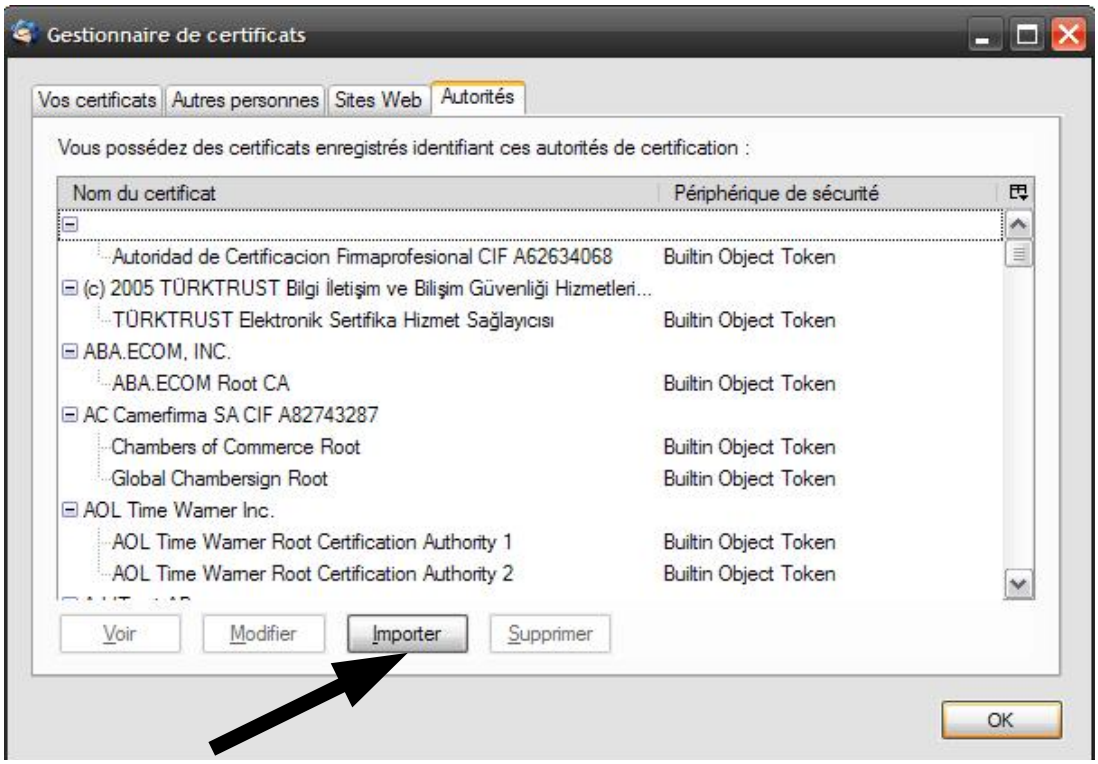


Cliquer sur « Voir les certificats ».



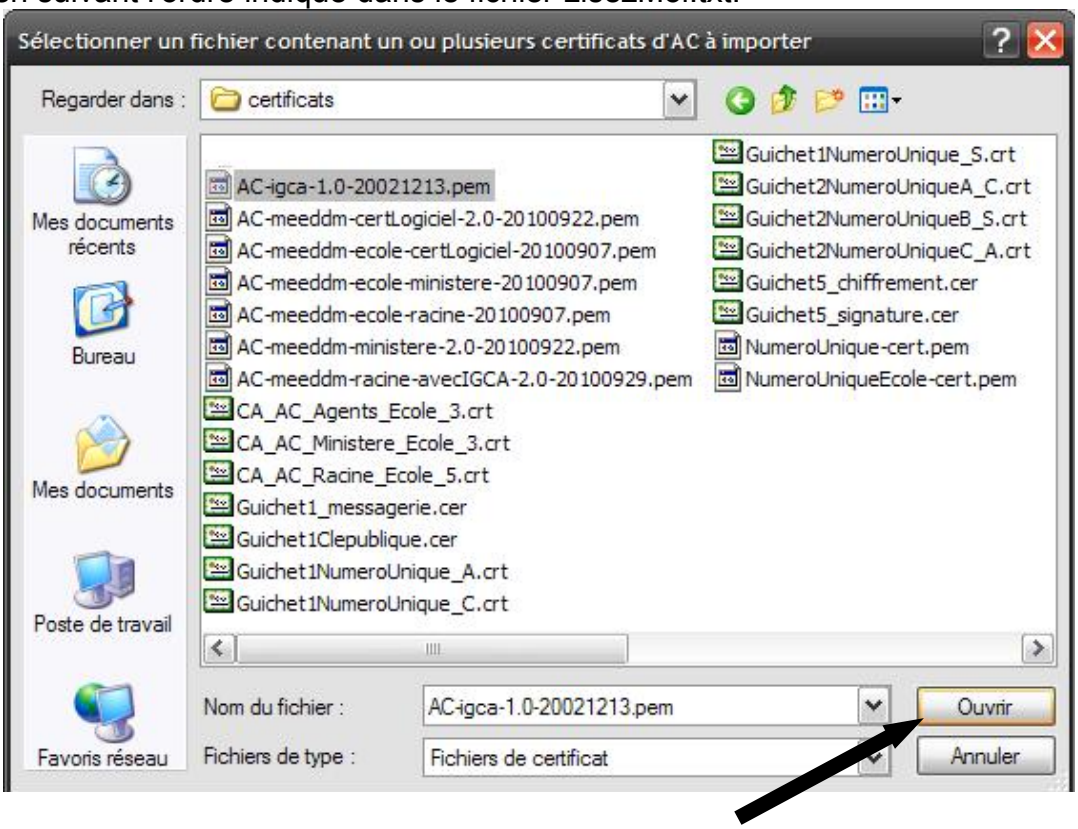
5.2.1 - Etape 1 : Importer les certificats racine (appelés également chaîne de certification ou chaîne de confiance)

Cliquer sur l'onglet « Autorités ». Puis, cliquer sur « Importer ».

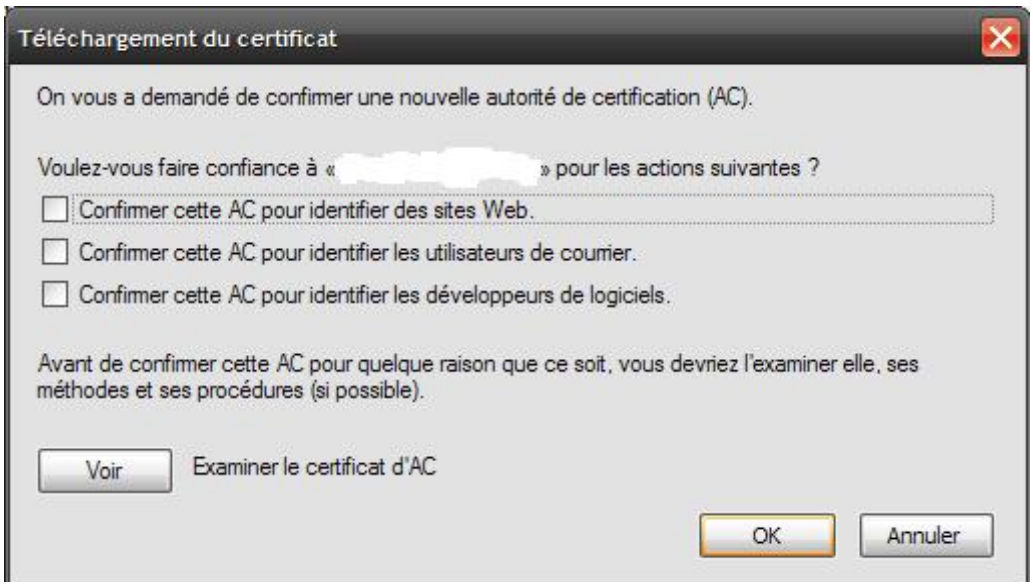


Rechercher et importer les éléments suivants :

- chacun des certificats racines fournis par l'autorité de certification qui a délivré le ou les certificat(s) à usage de chiffrement et de signature,
- chacun des certificats racines fournis par le ministère en accompagnement du certificat de chiffrement, en suivant l'ordre indiqué dans le fichier LisezMoi.txt.



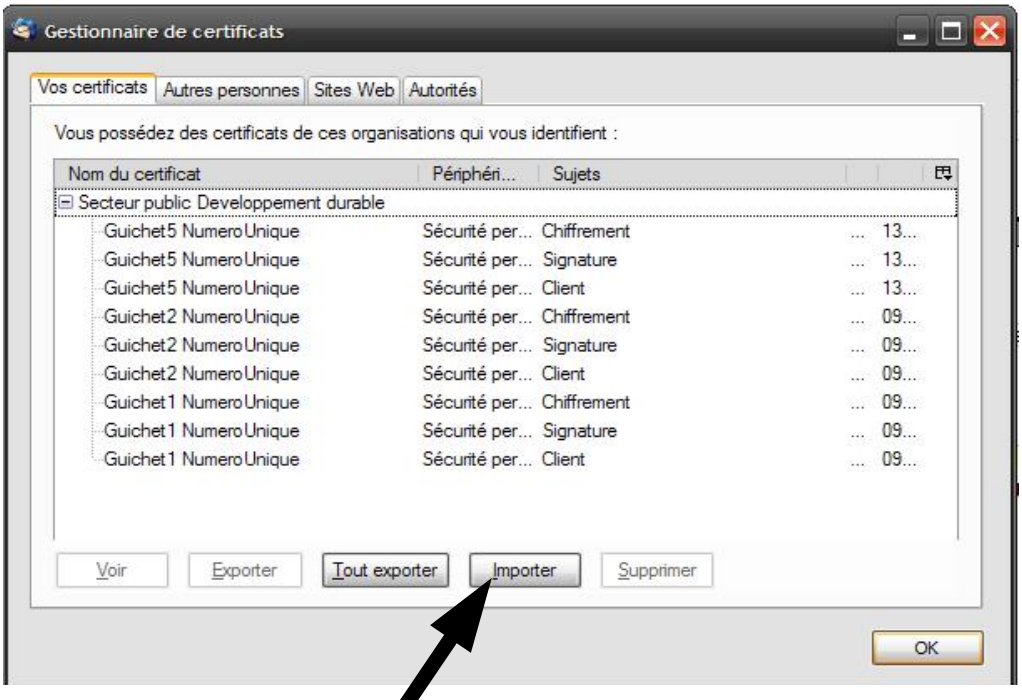
Pour la chaîne de certification du ministère : lorsque s'affiche la boite de dialogue suivante, cocher chacune des cases puis, cliquer sur OK.



Dès lors que l'ensemble des certificats racines des chaînes de certification sont installés, il est désormais possible d'importer vos certificats de chiffrement et de signature ainsi que le certificat de chiffrement de Numéro unique dans Mozilla Thunderbird.

5.2.2 - Etape 2 : Importer vos certificats de signature et chiffrement

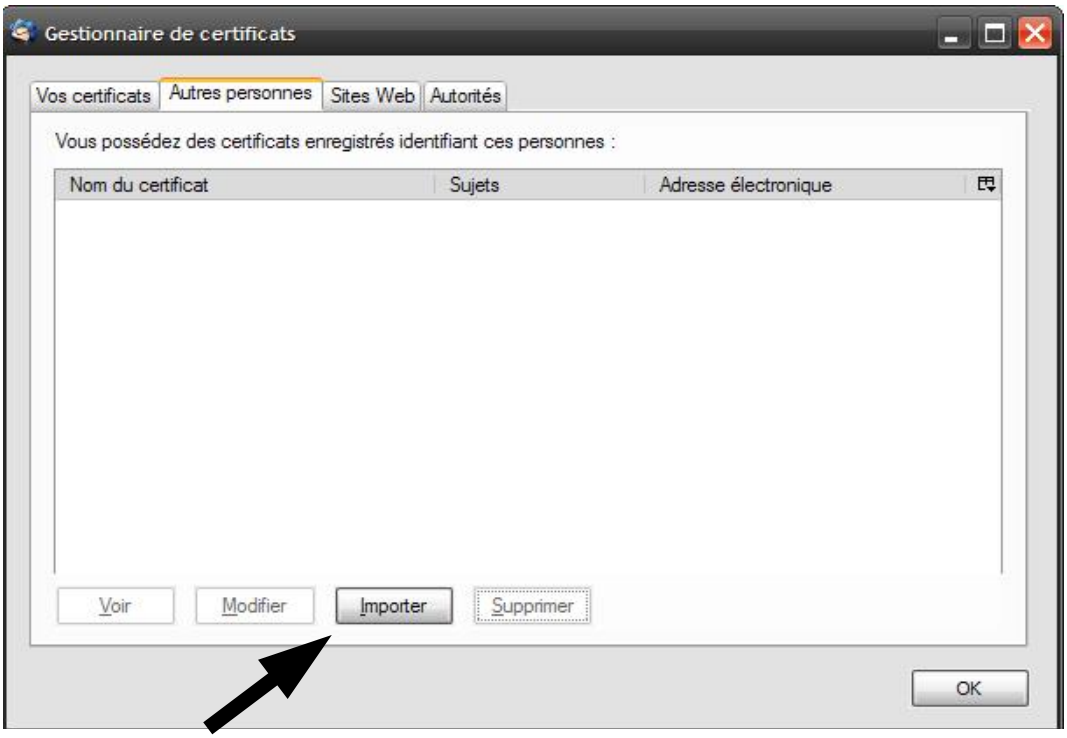
Se rendre sur l'onglet « Vos certificats », toujours dans la même boîte de dialogue. Puis, cliquer sur « Importer ».



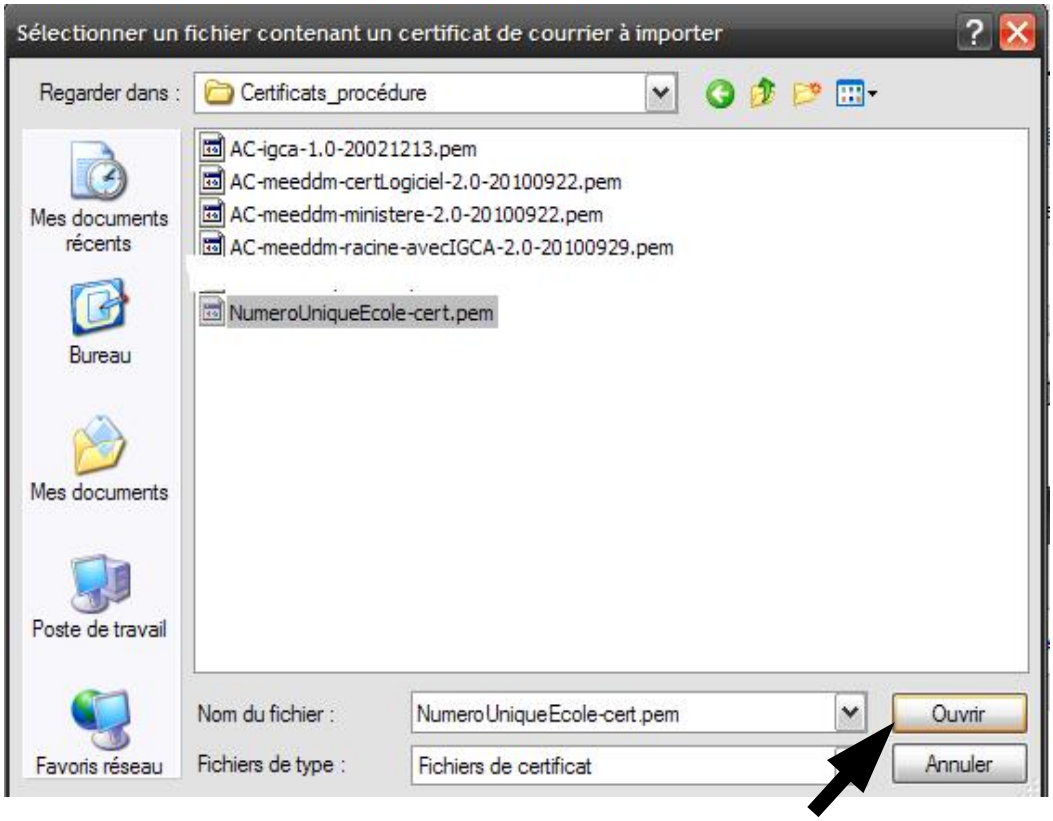
Rechercher et importer vos certificats (mot de passe demandé).

5.2.3 - Etape 3 : Importer le certificat de chiffrement Numéro unique

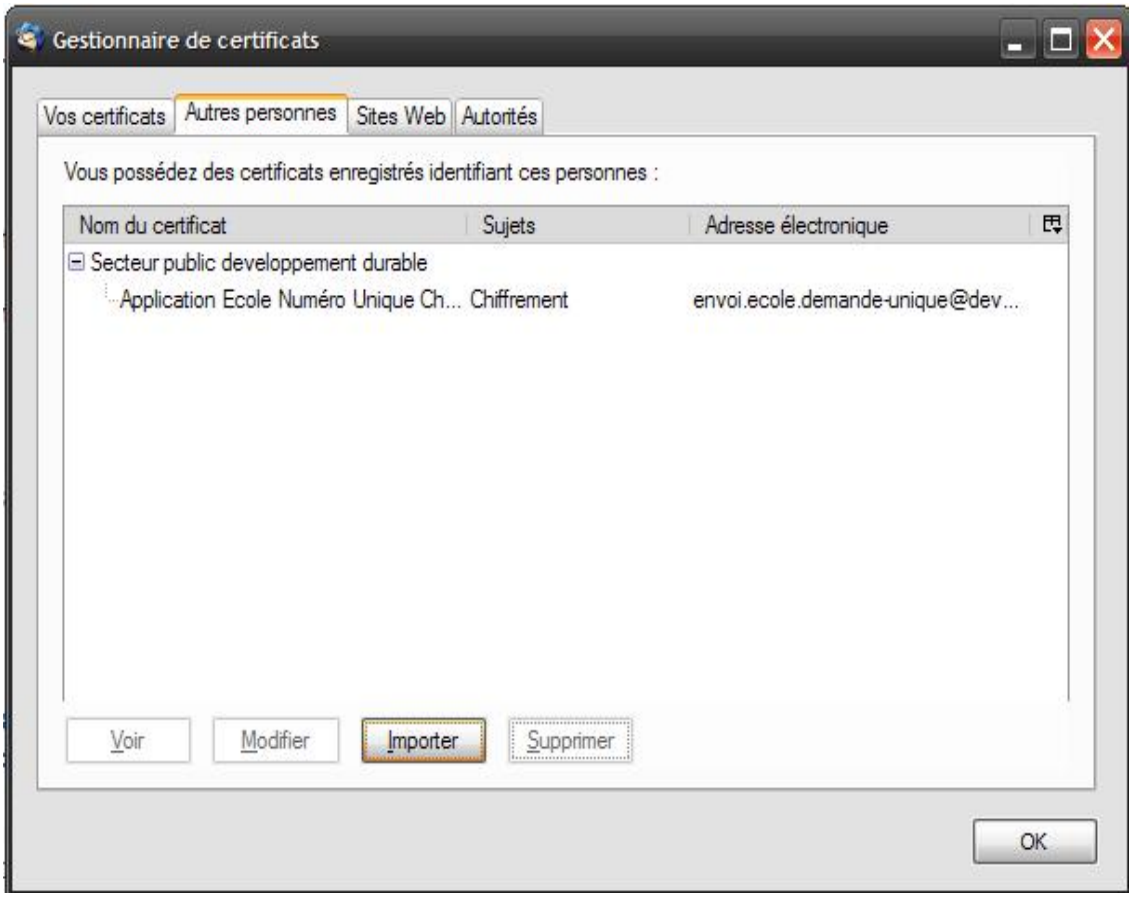
Se rendre sur l'onglet « Autres personnes » et cliquer sur « Importer ».



Puis, rechercher la clé publique de chiffrement de Numéro unique et cliquer sur « Ouvrir ».

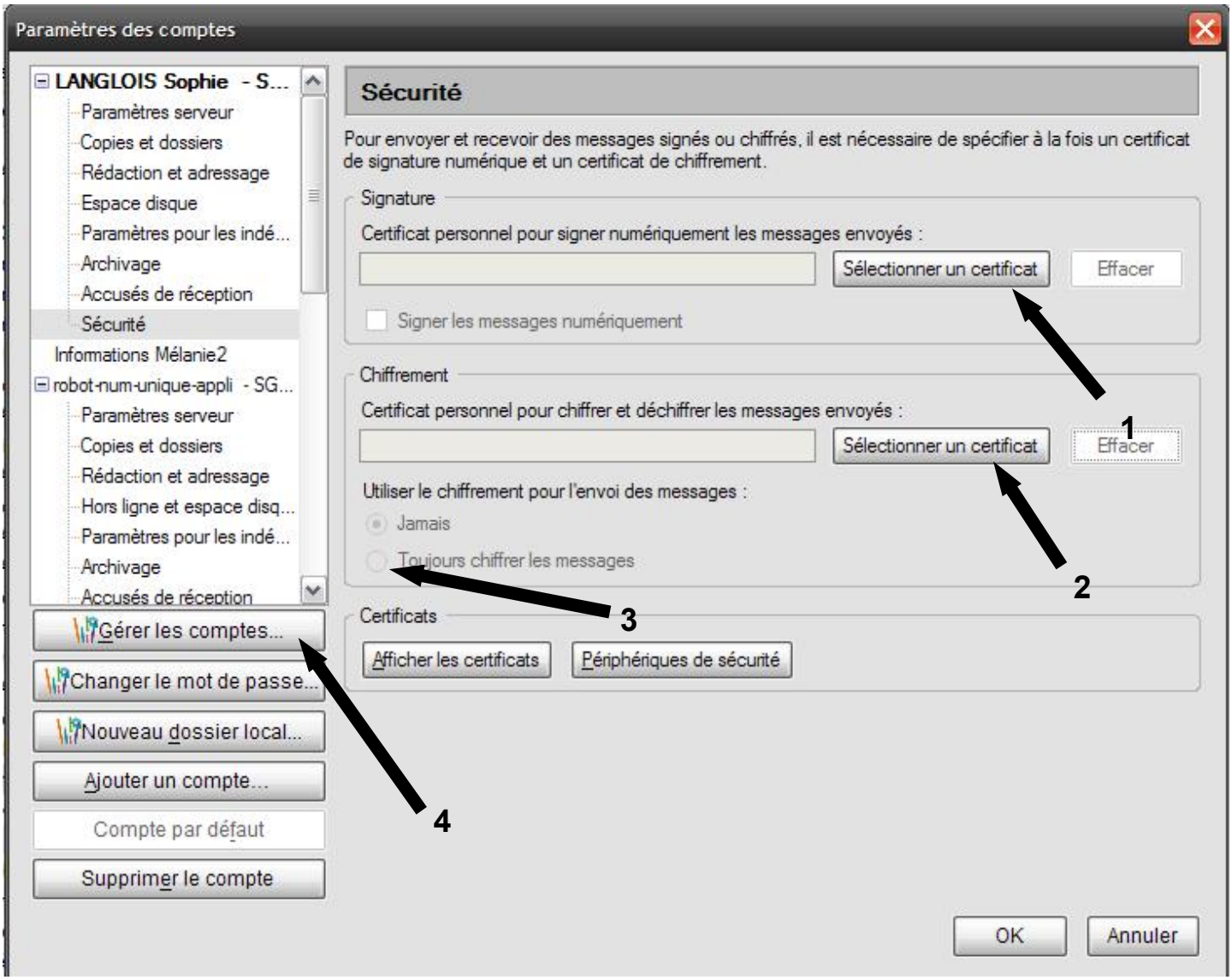


La boîte de dialogue apparaît ensuite de la manière suivante, le certificat a correctement été importé. Cliquer sur « OK ».



5.2.4 - Etape 4 : Paramétrer votre compte de messagerie

Il suffit désormais d'aller paramétrer le compte de messagerie émetteur / récepteur des mails. Dans la barre d'outils de Thunderbird, cliquer sur Outils / Paramétrage des comptes.

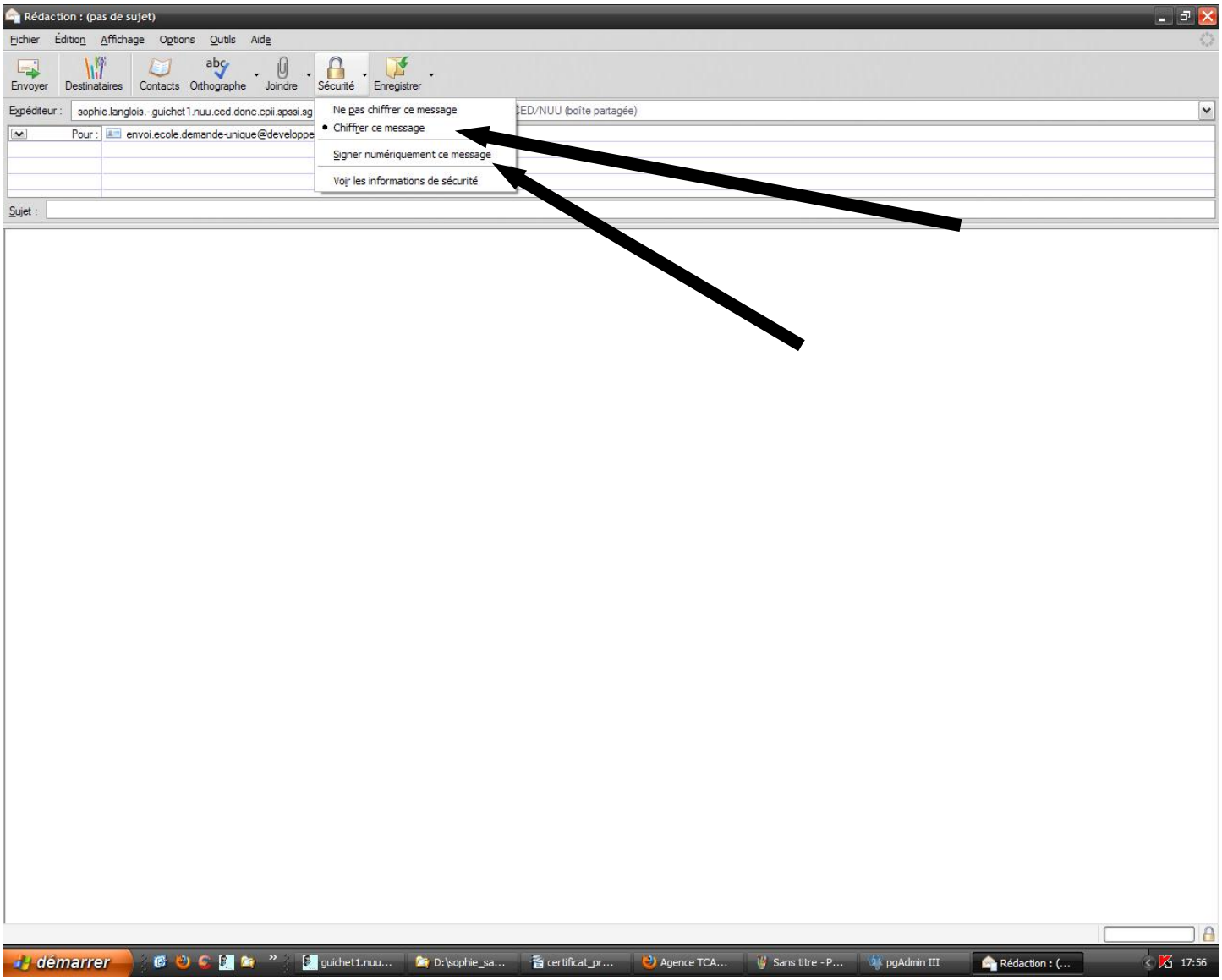


1- Dans le cadre « Signature », y référencer votre certificat de signature,
2- Dans le cadre « Chiffrement », y référencer votre certificat de chiffrement,
3- Cocher « Toujours chiffrer les messages »,
4- Cliquer sur « Gérer les comptes » pour mettre à jour votre compte de messagerie (suivre les indications indiquées dans les boîtes de dialogues successives)

Redémarrer le logiciel de messagerie.

5.2.5 - Etape 5 : Composer un message à destination de Numéro unique

Enfin, lorsque vous composez votre message à destination de envoi.demande-unique@developpement-durable.gouv.fr, vérifier les éléments suivants :



Il convient de cocher « Chiffrer ce message » si ce n'est déjà fait et de cocher « Signer numériquement ce message ». Vous joignez le zip contenant la ou les demandes et vous pouvez envoyer le message.


Ressources, territoires, habitats et logement
Énergies et climat
Développement durable
Prévention des risques
Infrastructures, transports et mer
Présent
pour
l'avenir