

Secure Médical Mail®

Guide d'utilisation

Sommaire

Sommaire	2
Glossaire Technique	3
Messagerie Sécurisée.....	4
Quels sont les plus d'une messagerie homologuée GIP-CPS ?.....	5
Pré-requis techniques	5
Protocoles de messagerie supportés	5
Première exécution	6
Connexion	7
Interface principale	10
Iconographie des dossiers système d'un compte de messagerie	11
Iconographie du cycle de vie d'un message.....	11
Fonction d'envoi / réception	13
Accès à la fenêtre des correspondants	16
Accès au paramétrage de la messagerie – Gestion multi-comptes	17
Ajout/Modification d'un compte de messagerie.....	18
Gestion des certificats racine.....	25
Création d'un nouveau message.....	26
Sélection des destinataires	29
Cinématique d'envoi d'un message chiffré et signé	30
Éléments nécessaires pour le chiffrement d'un message	30
HPRIM Net	38

Glossaire Technique

Nous allons définir ici tous les termes techniques employés dans ce document.

Certificat : Le certificat numérique (ou électronique) se présente sous la forme d'un fichier. Il est composé d'un bloc de données contenant, dans un format spécifié, les parties suivantes :

- la partie **publique** d'une paire de clés asymétriques
- les informations sur le porteur de cette paire de clés, telles que son identifiant, son nom, son adresse e-mail, son titre, le nom de l'entité qui a délivré ce certificat, sa période de validité, etc...

Il existe plusieurs types de certificats : les certificats de signature, les certificats de chiffrement, les certificats racines (voir ci-dessous).

Certificat de signature : il permet d'authentifier l'auteur d'un document électronique et de garantir l'intégrité du message. Ce certificat est présent dans la carte CPS.

Certificat de chiffrement : il est composé de deux clés, le certificat privé et le certificat public (*nommé « Certificat de confidentialité » sur l'annuaire du GIP-CPS*).

Le certificat de chiffrement permet de crypter un document électronique que seul le destinataire pourra décrypter. Le chiffrement est réalisé avec la partie publique d'une paire de clés asymétriques, analogue à un cadenas (le document électronique est placé dans un coffre verrouillé par le cadenas) que seul le destinataire pourra déchiffrer grâce à la partie privée d'une paire de clés asymétriques, analogue à une clef (permettant d'ouvrir le coffre verrouillé).

Certificat d'authentification : certificat non utilisé. Il permet d'établir une connexion distante sécurisée.

Liste de révocation (CRL) : CRL pour (Certificates Revocation List). Quelle qu'en soit la raison (perte, vol, changement d'information identifiant le porteur, ...), un certificat peut être révoqué (détruit). Dans ce cas l'identifiant du certificat est ajouté à une liste de façon à informer les applications de ne plus faire confiance à ce certificat.

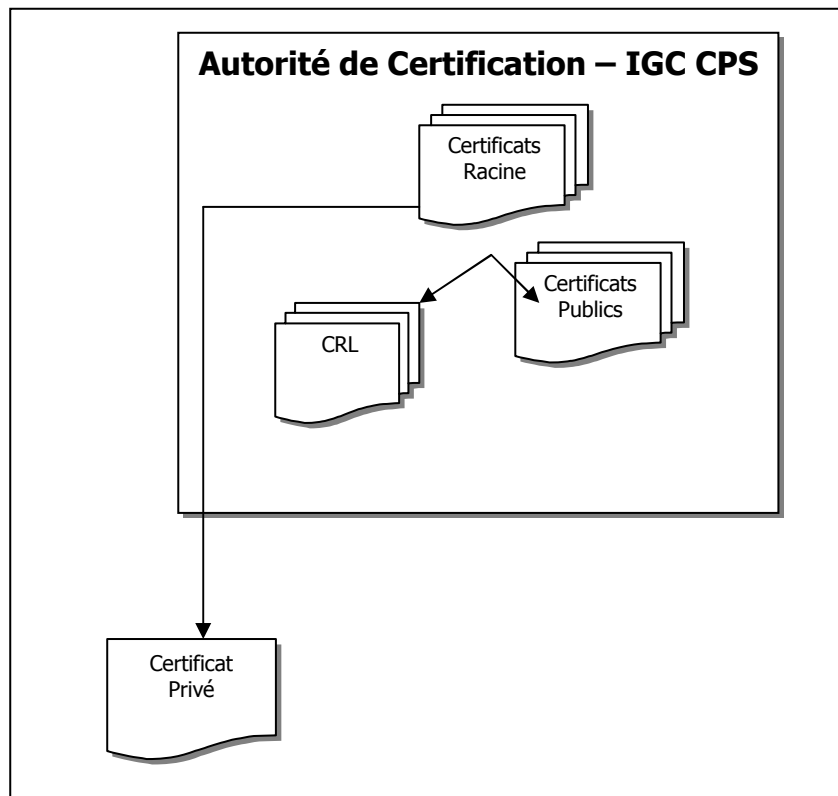
Cette liste a une durée de validité très courte (environ 3 jours) et doit être mise à jour régulièrement. Si cette liste est périmée, aucun certificat ne peut être validé et la mise à jour de la liste de révocation devient alors **obligatoire** avant tout accès à un certificat.

Autorité de Certification (AC) : elle a pour mission de signer les demandes de certificat et de signer les listes de révocation. Cette autorité est la plus critique.

Certificat racine : ce certificat est généré par l'Autorité de Certification. Il permet de valider la propriété et la conformité des différents certificats et de la liste de révocation.

Ce certificat représente l'identité de l'Autorité de confiance. Tous les certificats émis par l'Autorité de confiance reposent sur ce certificat racine pour pouvoir être valides.

IGC : C'est l'Infrastructure de Gestion des Clefs.



Messagerie Sécurisée

Une messagerie sécurisée permet l'échange de messages signés et/ou chiffrés.

Un message signé garantit l'intégrité du message et authentifie l'expéditeur :

- **la signature numérique** garantit à un niveau de sécurité très élevé que l'émetteur est bien la personne que vous connaissez (l'usurpation d'identité est alors très difficile) et que le message n'a pas été falsifié en cours de route
- **un message chiffré** garantit la confidentialité du message
- **le chiffrement** (ou cryptage) vous assure que le message n'a pas été lu en cours de route

Une messagerie sécurisée élimine 90% des risques relatifs à l'e-mail, principal vecteur d'infection actuellement.

Pour chiffrer un message, l'expéditeur doit posséder le certificat public (= certificat de confidentialité – définition de l'annuaire du GIP-CPS) du destinataire, sans quoi le chiffrement est impossible.

Si un message est envoyé à plusieurs destinataires et que l'expéditeur n'a pas la totalité de leurs certificats publics, on lui propose de supprimer les destinataires n'ayant pas de certificat public ou de ne plus chiffrer le message.

Pour déchiffrer un message, l'utilisateur qui reçoit le message doit posséder son certificat privé.

Quels sont les plus d'une messagerie homologuée GIP-CPS ?

La signature du message est effectuée par la carte CPS. Le certificat de signature est donc obligatoirement le certificat de signature stocké dans la carte CPS.

Le certificat de chiffrement est fourni soit par le GIP-CPS, soit par une autre organisation (dans ce cas, il faudra inclure les certificats racine de cette organisation).

Il existe un lien entre le N°ADELI (bientôt le n° RPPS) et le certificat privé.

Pour pouvoir déchiffrer un message, le certificat privé doit être installé ET la carte CPS doit être signée dans le lecteur.

Si le professionnel de santé n'a pas sa carte CPS ou que le lecteur est en panne, il existe un mode de secours, via un mot de passe, qui permet à l'utilisateur de déchiffrer ses messages.

Pour pouvoir chiffrer un message, le certificat privé doit être installé ET la carte CPS doit être signée dans le lecteur. Sans carte CPS ou en cas de panne de lecteur, il est impossible de chiffrer un message.

Tout ceci n'est évidemment pas valable dans une messagerie classique qui n'est ni homologuée GIP-CPS et n'a aucune connexion à un lecteur CPS.

Pré-requis techniques

- JRE 1.4.2 installé sur le poste
- composants CPS 5.03 installé sur le poste
- Internet Explorer 6.00 minimum


Protocoles de messagerie supportés

- SMTP
- ESMTP
- POP
- LDAP

Première exécution

Lors de la première exécution, il vous sera demandé de créer votre premier utilisateur qui sera administrateur de la messagerie.

L'utilisateur administrateur a le droit de créer et de supprimer d'autres utilisateurs.



Vous devez obligatoirement renseigner le login utilisateur, le mot de passe de secours (composé de 6 caractères au minimum) au cas où la carte CPS ne serait pas utilisable, et la confirmation du mot de passe de secours.

La catégorie est obligatoirement « **Administrateur** ».

Nous vous conseillons de prendre le même login que celui de la carte CPS, et de créer cet utilisateur en fonction des données de la carte CPS en utilisant le bouton « **Lecture de la carte CPS** » (la saisie du code PIN de votre carte n'est pas nécessaire à ce niveau).

Connexion

Lors de l'exécution de la messagerie, il y aura une lecture préalable de la carte CPS pour connaître son détenteur.



Le login utilisateur sera donc renseigné par rapport à celui indiqué sur la carte CPS.

Seule la saisie du code PIN de la carte CPS est nécessaire au login.

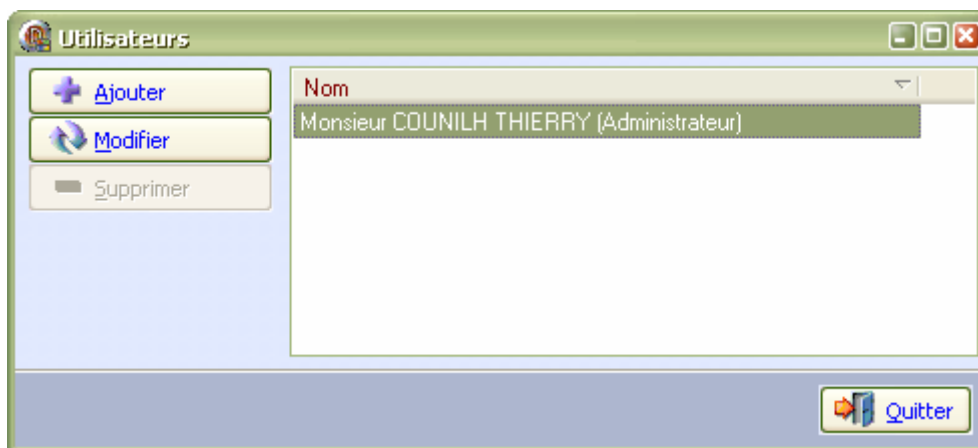
Si la carte CPS insérée dans le lecteur n'est pas la bonne, il est possible de la relire après l'avoir changée et cliqué sur le bouton « **Changer de carte CPS** ».

Pour pouvoir vous connecter avec le mot de passe de secours, il suffit de cliquer sur le bouton « **Login sans CPS** » et d'indiquer votre login utilisateur et le mot de passe de secours.

Après vous être connecté avec la carte CPS et si vous êtes administrateur de la messagerie, vous aurez accès au paramétrage des utilisateurs (bouton « **Paramétrage des utilisateurs** » en bas à gauche de la fenêtre).

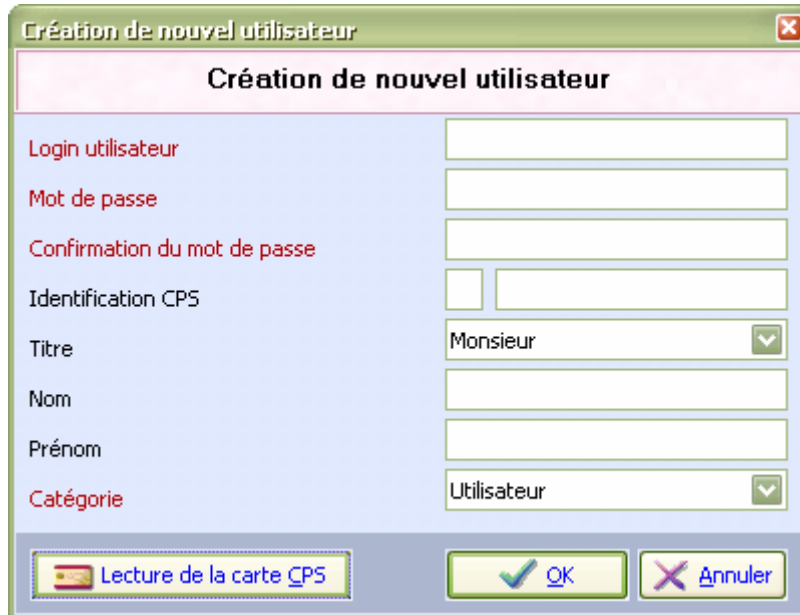


Liste des utilisateurs de la messagerie :



L'utilisateur connecté ne peut être supprimé et est obligatoirement de catégorie administrateur.

Ajout d'un nouvel utilisateur :



Création de nouvel utilisateur

Création de nouvel utilisateur

Login utilisateur

Mot de passe

Confirmation du mot de passe


Identification CPS

Titre

Nom

Prénom

Catégorie

 Lecture de la carte CPS

Modification d'un utilisateur :



Modification de l'utilisateur administrateur

Modification de l'utilisateur administrateur

Login utilisateur

Mot de passe

Confirmation du mot de passe

Identification CPS

Titre

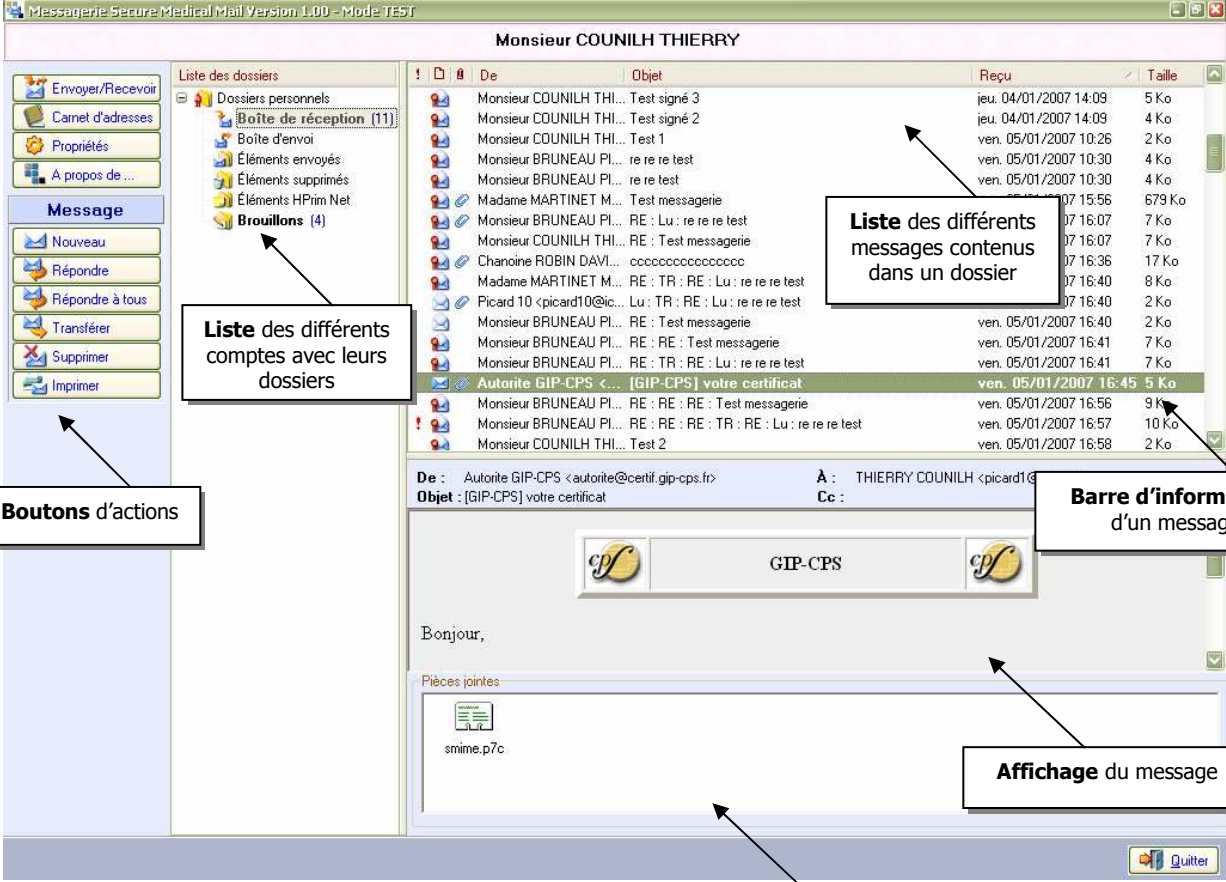
Nom

Prénom

Catégorie

 Lecture de la carte CPS







Interface principale











The screenshot shows the main interface of the 'Messagerie Secure Medical Mail Version 1.00 - Mode TEST' application. The window title is 'Monsieur COUNILH THIERRY'. The interface is divided into several sections:

- Left Panel (Boutons d'actions):** Contains navigation buttons such as 'Envoyer/Recevoir', 'Carnet d'adresses', 'Propriétés', 'A propos de...', and a 'Message' section with 'Nouveau', 'Répondre', 'Répondre à tous', 'Transférer', 'Supprimer', and 'Imprimer'.
- Folder List (Liste des dossiers):** Shows a tree view of folders including 'Dossiers personnels', 'Boîte de réception (11)', 'Boîte d'envoi', 'Éléments envoyés', 'Éléments supprimés', 'Éléments HPrim Net', and 'Brouillons (4)'.
- Message List (Liste des différents messages contenus dans un dossier):** A table listing messages with columns for 'De', 'Objet', 'Reçu', and 'Taille'. The selected message is from 'Autorite GIP-CPS <...> [GIP-CPS] votre certificat' received on 'ven. 05/01/2007 16:45' with a size of '5 Ko'.
- Message Header (Barre d'information d'un message):** Displays the sender 'Autorite GIP-CPS <autorite@certif.gip-cps.fr>', recipient 'THIERRY COUNILH <picard10@...>', and subject '[GIP-CPS] votre certificat'.
- Message Content (Affichage du message):** Shows the start of the message with 'Bonjour,' and a section for 'Pièces jointes' containing a file named 'snime.p7c'.
- Bottom Bar (Pièces jointes):** A status bar at the bottom of the message content area.

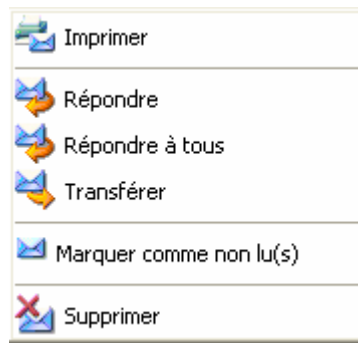
Iconographie des dossiers système d'un compte de messagerie

	Boîte de réception : les nouveaux messages reçus seront stockés dans ce dossier
	Boîte d'envoi : les nouveaux messages créés à envoyer seront stockés dans ce dossier
	Éléments envoyés : une copie des messages envoyés sera conservée dans ce dossier
	Éléments supprimés : les messages supprimés seront stockés dans ce dossier. Il faudra les re-supprimer ou vider ce dossier pour valider la suppression de ces messages
	Éléments HPrim Net : les messages HPRIM seront stockés dans ce dossier
	Brouillons : les messages en cours de création et non envoyés seront stockés dans ce dossier

Iconographie du cycle de vie d'un message

	Message non lu
	Message, chiffré et/ou signé, non lu
	Message lu
	Message, chiffré et/ou signé, lu
	Message lu et répondu
	Message, chiffré et/ou signé, lu et répondu
	Message lu et transféré
	Message, chiffré et/ou signé, lu et transféré

Un menu contextuel au niveau de chaque message permet de modifier son cycle de vie et d'accéder à certaines actions :

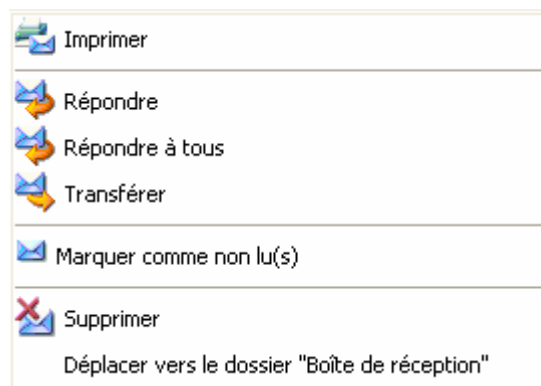


L'affichage des messages se fait au format HTML via le composant de Internet Explorer.

Lors de la suppression d'un message, celui-ci sera en fait déplacé dans le dossier « Éléments supprimés ».

Pour supprimer réellement ce message, il faudra le re-supprimer depuis le dossier « Éléments supprimés ».

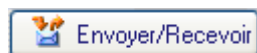
Pour récupérer un message supprimé contenu dans le dossier « Éléments supprimés », vous devez le sélectionner et choisir la fonction « **Déplacer vers le dossier "Boîte de réception"** » du menu contextuel.




Vous pouvez faire une multi-sélection pour la suppression des messages et pour la récupération des messages supprimés.

La possibilité de créer d'autres dossiers sera envisagée dans une future version.

Fonction d'envoi / réception



Le bouton  permet de garder la fenêtre ouverte après la fin des opérations d'envoi/réception.

Le bouton  permet de fermer automatiquement la fenêtre après la fin des opérations d'envoi/réception.

Cette fonctionnalité vous donne la possibilité d'envoyer et de recevoir des messages, ainsi que de mettre à jour au besoin vos CRLs (Certificat Révocation Lists). Ces CRLs sont nécessaires et doivent être à jour pour chiffrer un message. Vous devez donc effectuer cette action régulièrement.

Lorsque c'est nécessaire, les CRLs sont mises à jour pendant cette opération d'envoi/réception (environ tous les 3 jours). Les CRLs sont téléchargées depuis l'annuaire du GIP-CPS. Cette opération peut durer quelques minutes (environ 3 minutes). A tout moment, vous pouvez annuler cette opération (les opérations d'envoi – réception seront également annulées).

Le nombre de CRLs à télécharger est indiqué :



Ainsi que la progression du téléchargement :



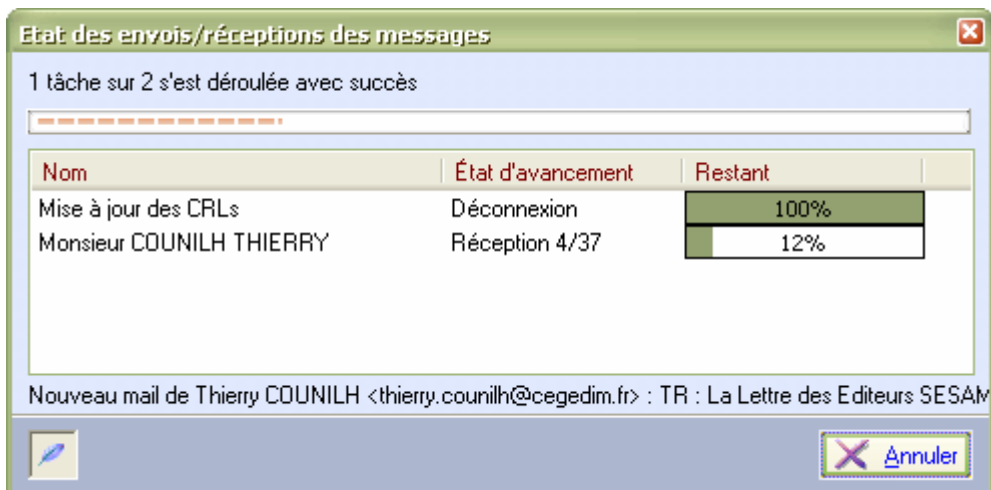
Etat des envois/réceptions des messages

0 tâche sur 2 s'est déroulée avec succès

Nom	État d'avancement	Restant
Mise à jour des CRLs	Téléchargement 2/14	14%
Monsieur COUNILH THIERRY	Connexion	0%

Annuler

L'opération d'envoi/réception est effectuée par la suite :



Etat des envois/réceptions des messages

1 tâche sur 2 s'est déroulée avec succès

Nom	État d'avancement	Restant
Mise à jour des CRLs	Déconnexion	100%
Monsieur COUNILH THIERRY	Réception 4/37	12%

Nouveau mail de Thierry COUNILH <thierry.counilh@cegedim.fr> : TR : La Lettre des Editeurs SESAM

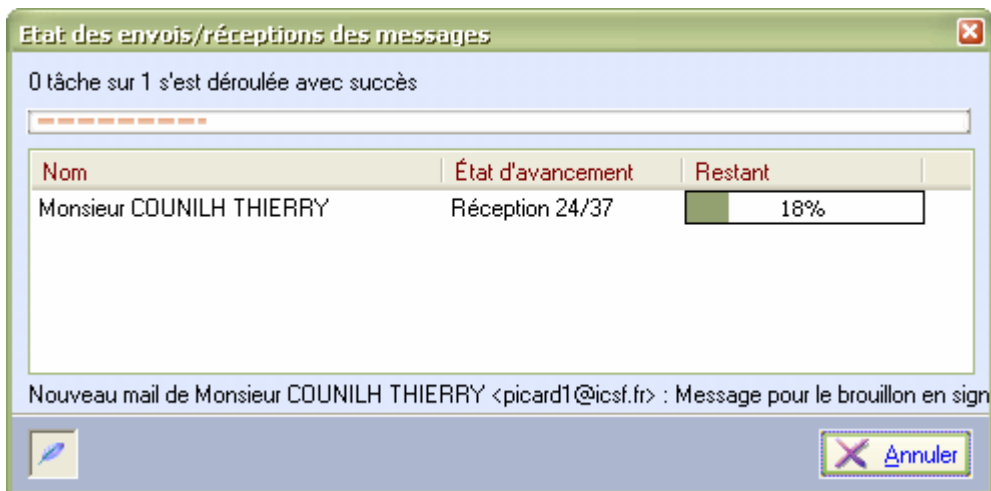
Annuler

L'existence de chaque message contenu dans la boîte aux lettres des comptes paramétrés est vérifiée dans la base de données du professionnel de santé. Si celui-ci est présent, on passe au message suivant. Autrement il est téléchargé puis stocké dans le dossier « Boîte de réception ».

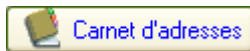
A la fin de cette opération, on vous indique le nombre de nouveaux messages reçus :



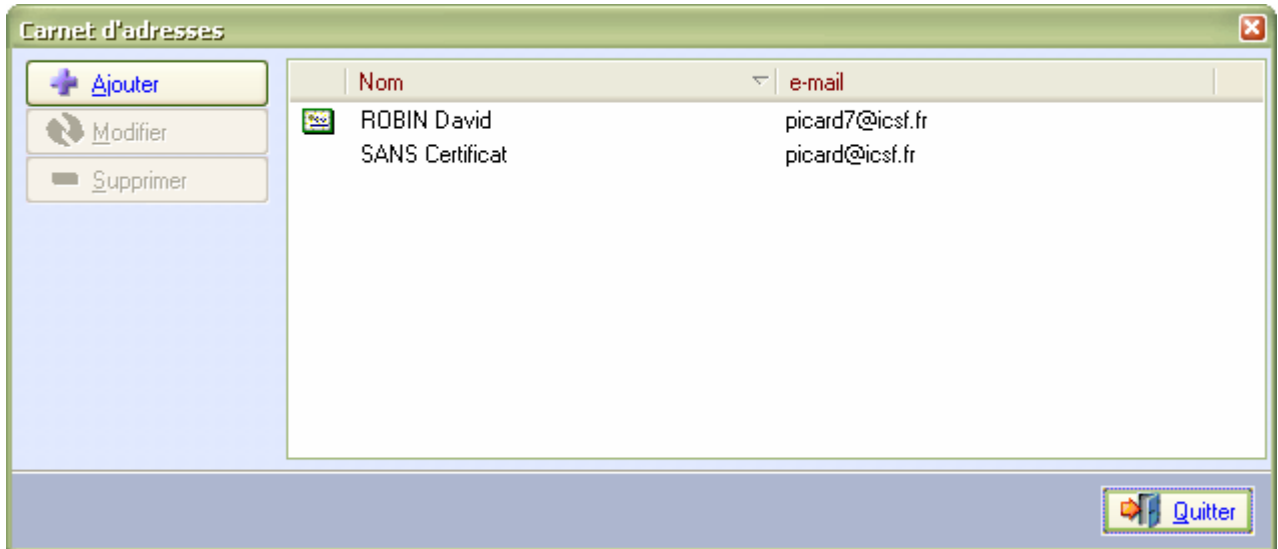
Dans le cas où le téléchargement des CRLs n'est pas nécessaire, seule l'opération d'envoi/réception est indiquée :



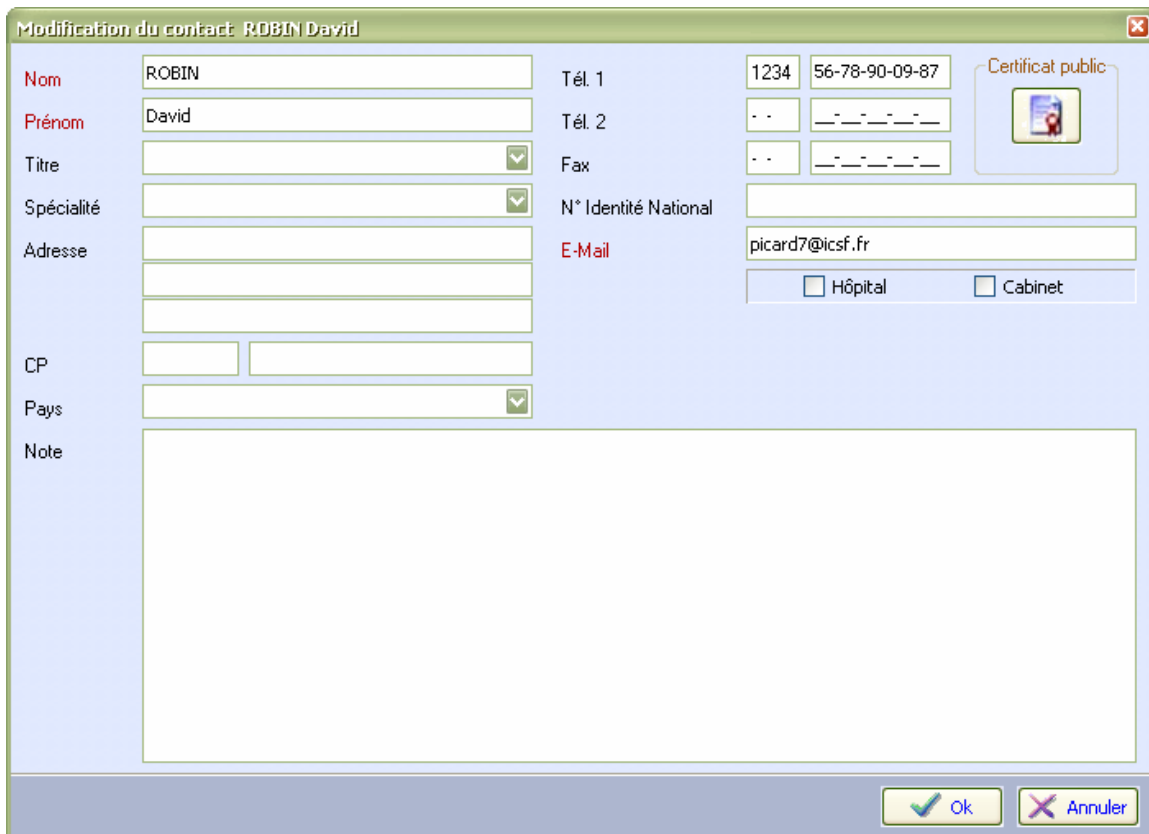
Accès à la fenêtre des correspondants




Liste des différents correspondants :



Fiche d'un correspondant en ajout/modification :



The screenshot shows a form titled "Modification du contact: ROBIN David" with a close button in the top right corner. The form is organized into several sections:

- Personal Information:**
 - Nom: ROBIN
 - Prénom: David
 - Titre: (dropdown menu)
 - Spécialité: (dropdown menu)
 - Adresse: (multiple text input fields)
 - CP: (two text input fields)
 - Pays: (dropdown menu)
 - Note: (large text area)
- Contact Information:**
 - Tél. 1: 1234 56-78-90-09-87
 - Tél. 2: (text input field)
 - Fax: (text input field)
 - N° Identité National: (text input field)
 - E-Mail: picard7@icsf.fr
- Professional Information:**
 - Certificat public: (checkbox) 
 - Hôpital: (checkbox)
 - Cabinet: (checkbox)

At the bottom right, there are two buttons: "Ok" (with a checkmark icon) and "Annuler" (with an X icon).

Seuls les champs en rouge sont obligatoires (nom, prénom et e-mail).

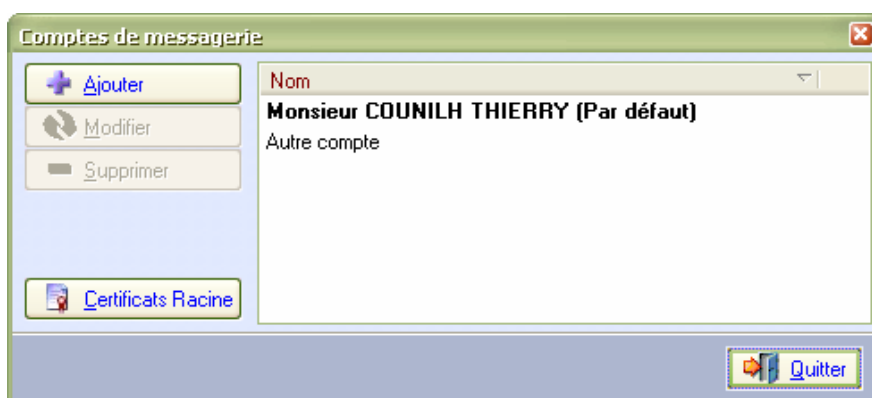
Accès au paramétrage de la messagerie – Gestion multi-comptes



Note importante sur le paramétrage des comptes de messagerie

Vous pouvez utiliser Secure Medical Mail® tout en conservant votre autre logiciel de messagerie non homologué GIP-CPS. Par contre, vous risquez de rencontrer les problèmes suivants dans cette configuration :

- Secure Medical Mail® bloque le compte de messagerie pendant ses communications avec le serveur de messagerie. Si votre logiciel de messagerie classique essaye de communiquer avec ce serveur en même temps, il ne pourra pas bloquer ce compte et générera donc une erreur de communication.
- Votre logiciel de messagerie classique ne peut pas déchiffrer ou valider une signature provenant des certificats du GIP-CPS sans une configuration préalable particulière. Vous obtiendrez donc une erreur lors de la lecture d'un e-mail sécurisé avec l'impossibilité de le lire, de répondre ou de le transférer. La seule action que vous pourrez faire avec ce message sera de le supprimer.
- un compte de messagerie est majoritairement configuré pour supprimer les messages après les avoir récupérés du serveur de messagerie. Secure Medical Mail® ne pourra donc pas recevoir les messages récupérés par votre messagerie classique et vice-versa (sauf configuration particulière).

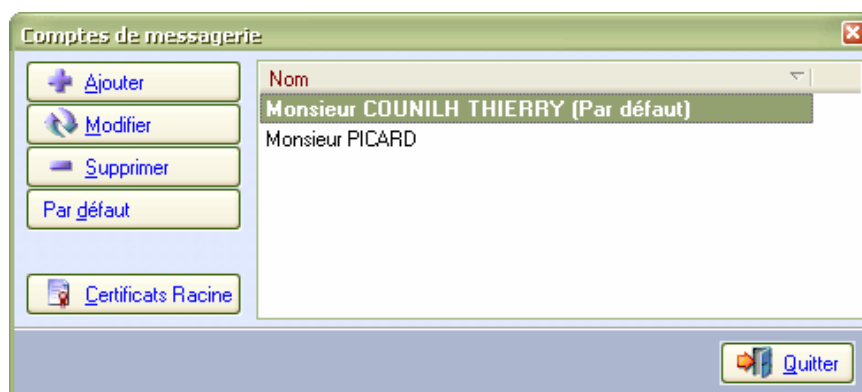


Cette boîte de dialogue permet de visualiser la liste des différents comptes de messagerie.

On offre la possibilité d'ajouter, de modifier ou de supprimer un compte de messagerie.

Le bouton « **Certificats racine** » sert à visualiser la liste des certificats racine du GIP-CPS, et à rajouter ou supprimer d'autres certificats racine d'autres organisations.

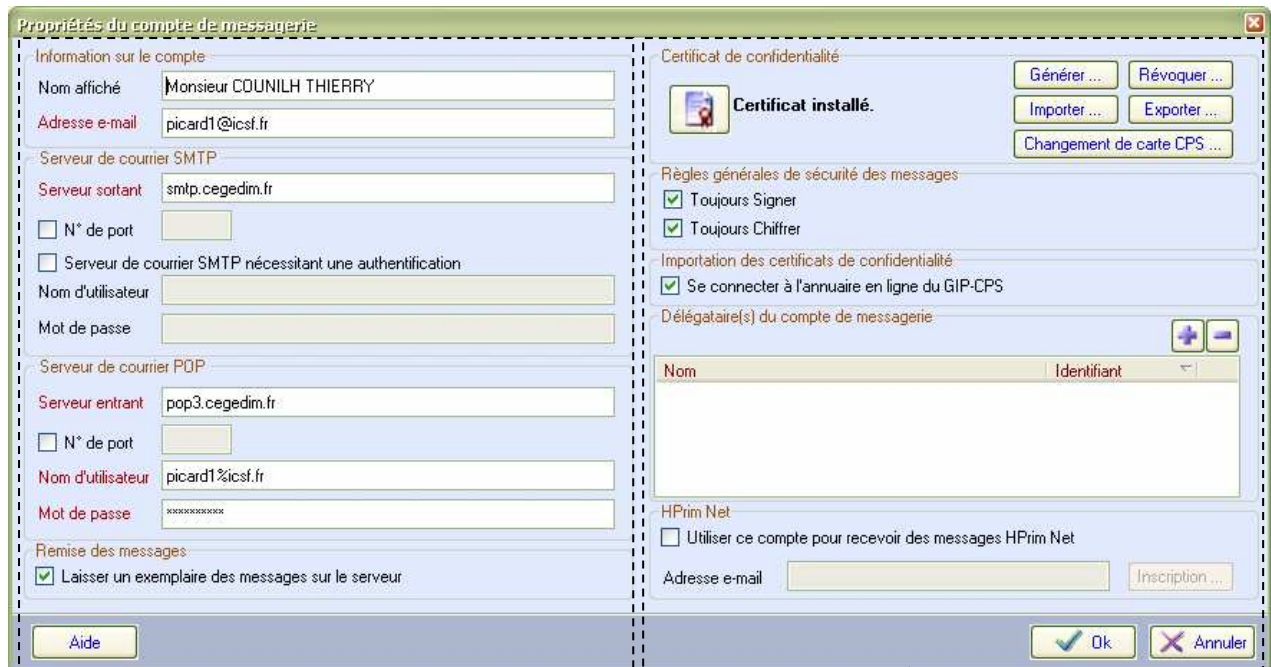
Le compte par défaut est le compte utilisé lors de la création d'un nouveau message. L'utilisateur peut changer le compte par défaut en le sélectionnant, puis en cliquant sur le bouton « Par défaut ».



Ajout/Modification d'un compte de messagerie

L'écran de propriétés d'un compte de messagerie est divisé en deux parties :

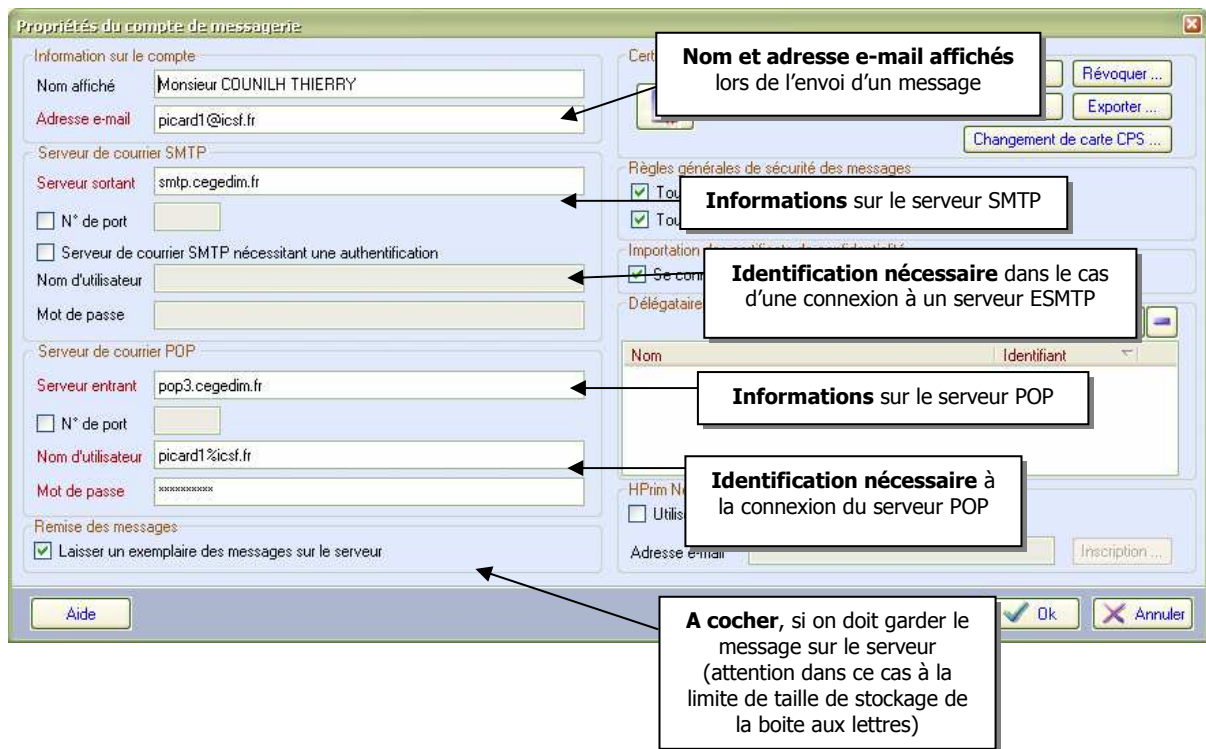
- une partie décrivant les différents paramètres nécessaires à la connexion au serveur de messagerie
- une partie décrivant les différents paramètres de sécurité



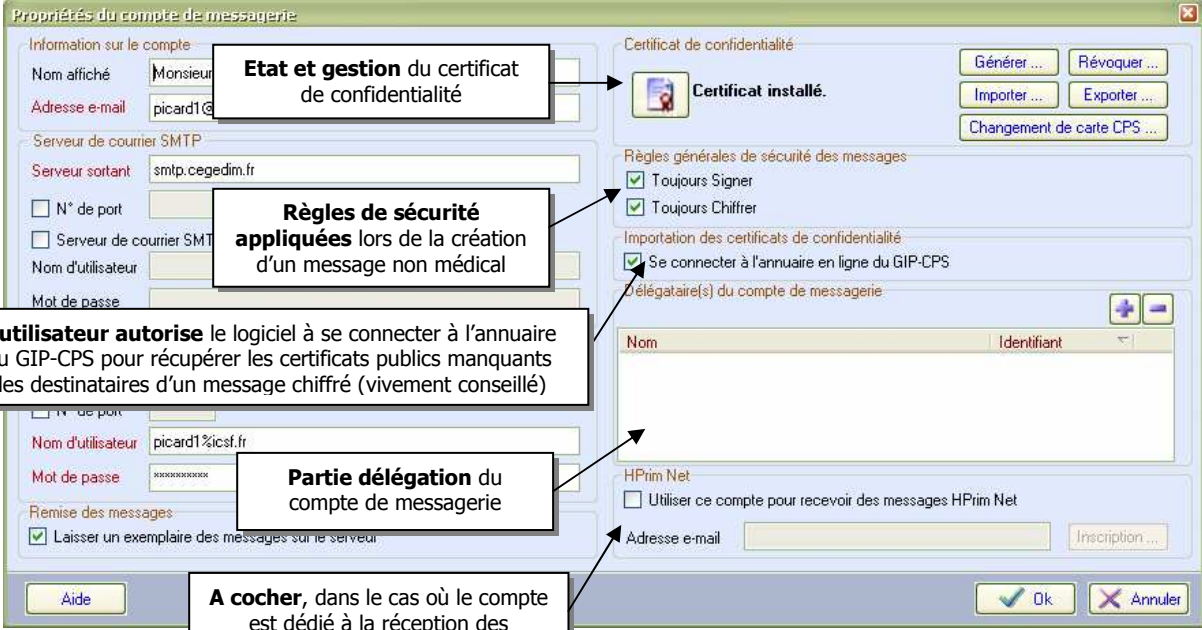
Partie paramétrage
serveur

Partie sécurité du
compte

Paramétrage de la partie serveur :



Paramétrage de la partie sécurité :



Etat et gestion du certificat de confidentialité

Règles de sécurité appliquées lors de la création d'un message non médical

L'utilisateur autorise le logiciel à se connecter à l'annuaire du GIP-CPS pour récupérer les certificats publics manquants des destinataires d'un message chiffré (vivement conseillé)

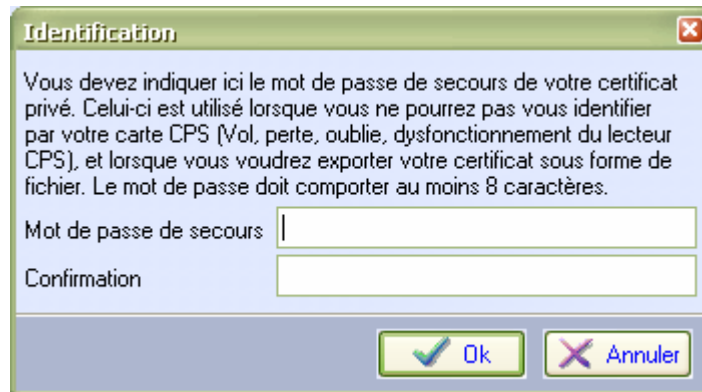
Partie délégation du compte de messagerie

A cocher, dans le cas où le compte est dédié à la réception des messages HPRIM Net

Générer ...

Ce bouton sert à demander l'enregistrement d'un certificat privé dans l'annuaire du GIP-CPS. C'est la première action à effectuer pour pouvoir chiffrer un message.

Une boîte de dialogue permettant de définir votre mot de passe de secours (dans le cas où le lecteur CPS ne fonctionnerait pas, ou si vous n'avez pas votre carte CPS) apparaîtra.



Identification

Vous devez indiquer ici le mot de passe de secours de votre certificat privé. Celui-ci est utilisé lorsque vous ne pourrez pas vous identifier par votre carte CPS (Vol, perte, oubli, dysfonctionnement du lecteur CPS), et lorsque vous voudrez exporter votre certificat sous forme de fichier. Le mot de passe doit comporter au moins 8 caractères.

Mot de passe de secours

Confirmation

Cette demande sera émise par le biais d'un message automatique envoyé immédiatement. Le certificat sera disponible quelques minutes plus tard dans votre boîte aux lettres, lors d'une opération d'envoi/réception. Il sera automatiquement configuré pour ce compte de messagerie.

Un message sera affiché pour vous en avertir.

PS : le message envoyé au GIP-CPS n'est pas stocké dans les éléments envoyés.

Révoquer ...

Ce bouton permet de faire une demande de révocation d'un certificat.

Vous pouvez effectuer cette demande dans le cas :

- de la diffusion accidentelle du certificat privé
- d'un changement d'adresse mail du compte de messagerie

Cette demande sera émise par le biais d'un message automatique envoyé immédiatement. Vous recevrez un message de confirmation quelques minutes plus tard dans votre boîte aux lettres, lors d'une opération d'envoi/réception.

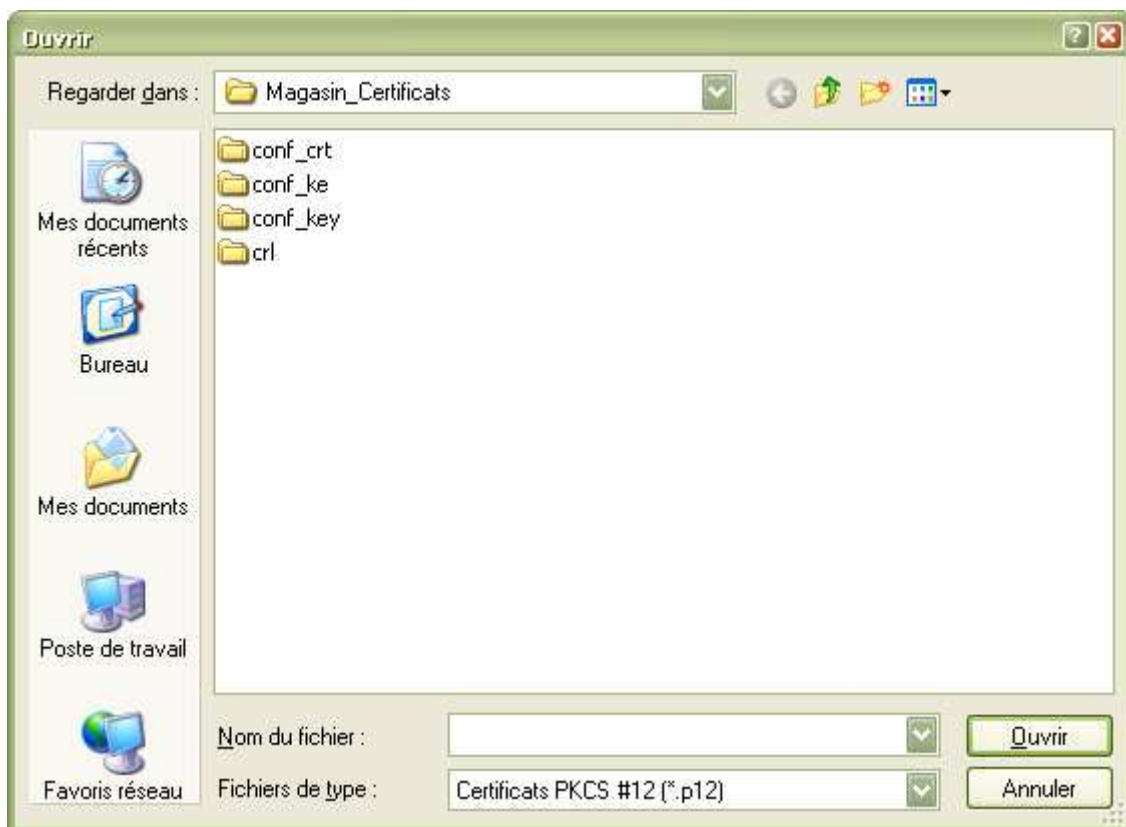
Un message sera affiché pour vous en avertir.

PS : le message envoyé au GIP-CPS n'est pas stocké dans les éléments envoyés.

Importer ...

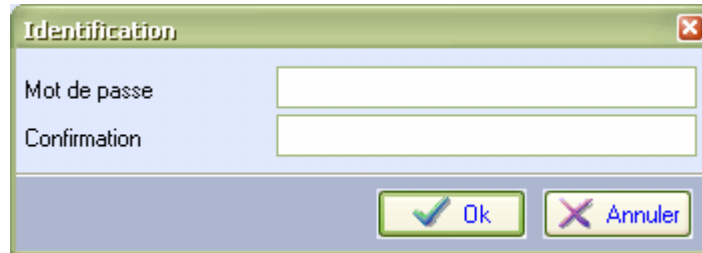
En cliquant sur « **Importer** », vous pouvez récupérer un certificat sous la forme d'un fichier. Cette fonctionnalité vous permet par exemple de récupérer un certificat depuis un backup.

Une boîte de dialogue permettant de sélectionner le certificat sous forme de fichier apparaîtra :

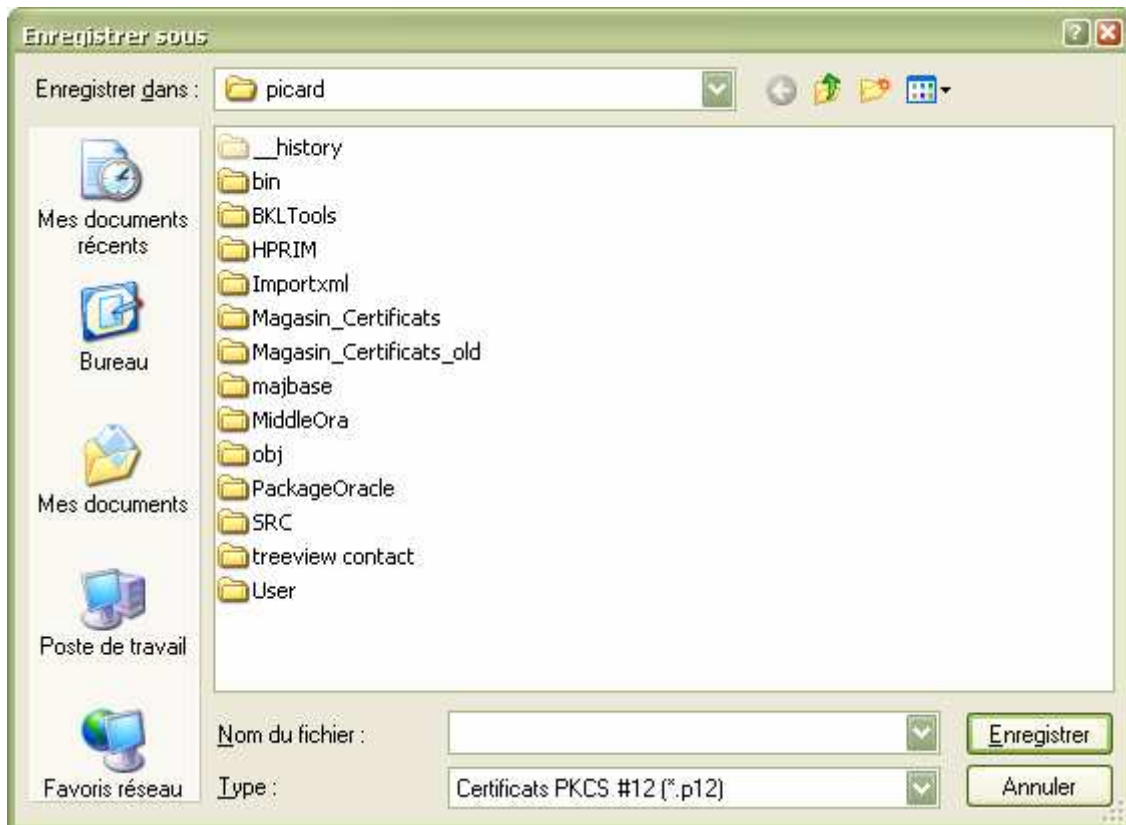


Exporter ...

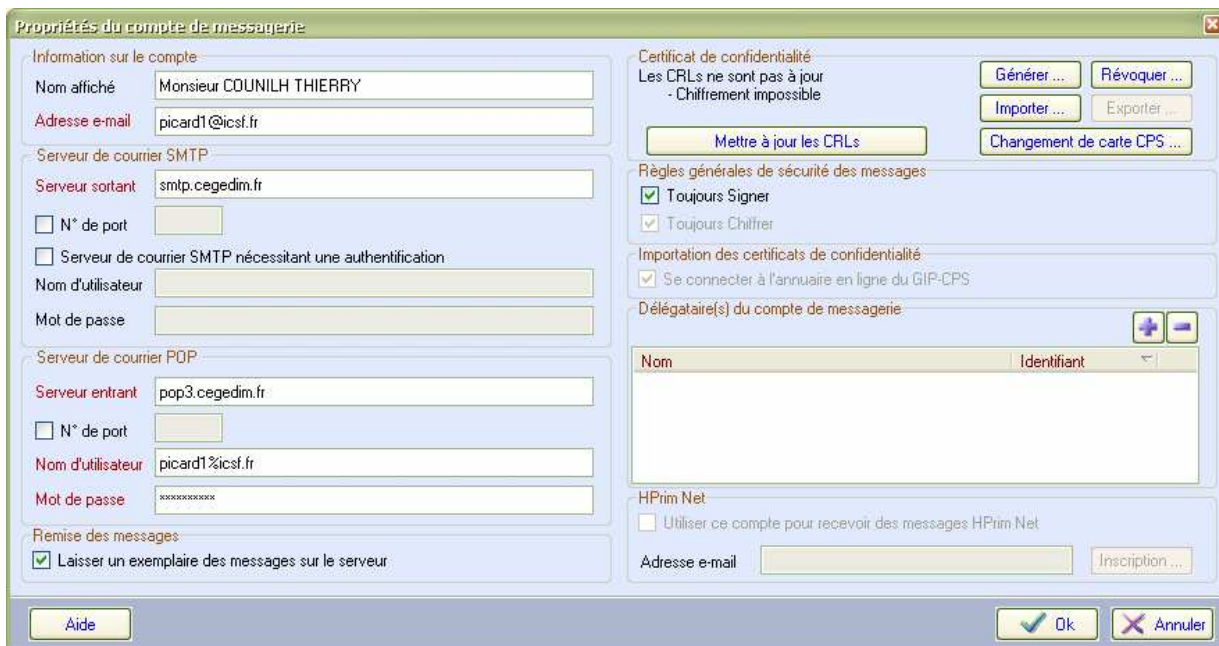
Permet de sauvegarder votre certificat vers un fichier (backup). Une boîte de dialogue pour saisir votre mot de passe de secours apparaîtra :



Puis, une autre boîte de dialogue pour sauvegarder le certificat apparaîtra :



Pour paramétrer la partie « **Certificat de confidentialité** », il est nécessaire d'avoir les CRLs à jour.
Si ces CRLs ne sont pas à jour (absentes ou révoquées), nous vous inviterons à les mettre à jour.



Propriétés du compte de messagerie

Information sur le compte
Nom affiché: Monsieur COUNILH THIERRY
Adresse e-mail: picard1@icsf.fr

Serveur de courrier SMTP
Serveur sortant: smtp.cegedim.fr
 N° de port
 Serveur de courrier SMTP nécessitant une authentification
Nom d'utilisateur
Mot de passe

Serveur de courrier POP
Serveur entrant: pop3.cegedim.fr
 N° de port
Nom d'utilisateur: picard1@icsf.fr
Mot de passe: *****

Remise des messages
 Laisser un exemplaire des messages sur le serveur

Certificat de confidentialité
Les CRLs ne sont pas à jour
- Chiffrement impossible
Générer ... Révoquer ...
Importer ... Exporter ...
Mettre à jour les CRLs
Changement de carte CPS ...

Règles générales de sécurité des messages
 Toujours Signer
 Toujours Chiffrer

Importation des certificats de confidentialité
 Se connecter à l'annuaire en ligne du GIP-CPS

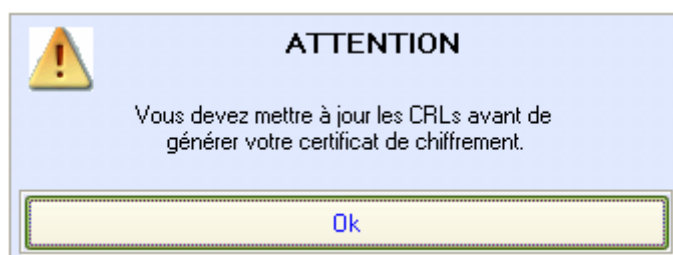
Déléataire(s) du compte de messagerie

Nom	Identifiant
-----	-------------

HPrim Net
 Utiliser ce compte pour recevoir des messages HPrim Net
Adresse e-mail
Inscription ...

Aide Ok Annuler


Si vous essayez de générer votre certificat alors que les CRLs ne sont pas à jour, le message d'avertissement suivant apparaîtra :




Délégation : Permet de déléguer la gestion de son compte de messagerie à un autre professionnel de santé.

De cette fenêtre, vous (le délégataire) pourrez visualiser les différents professionnels de santé (les délégués) à qui vous aurez délégué votre compte de messagerie.

Les délégués pourront visualiser et déchiffrer vos messages reçus. Mais ils ne pourront pas répondre en votre nom à ces messages.

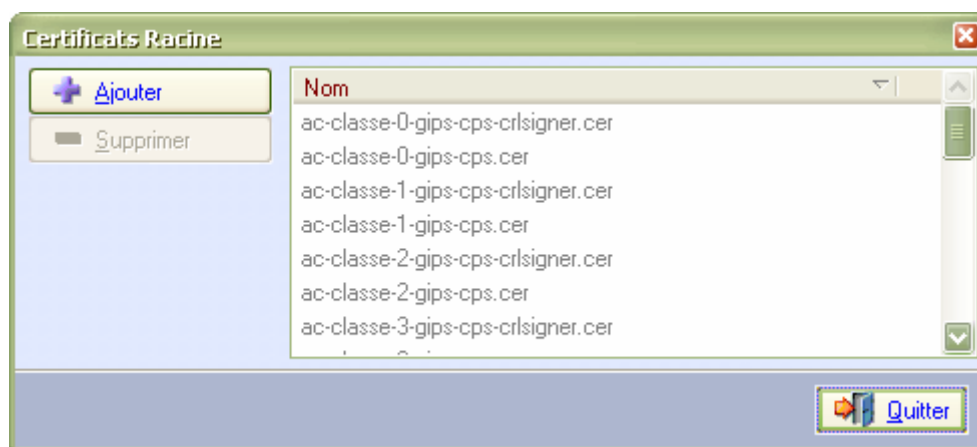
Pour pouvoir déléguer votre compte, vous devrez cliquer sur le bouton . Votre carte CPS sera lue et l'on vous demandera de saisir votre code PIN, puis une lecture de la carte CPS du délégué avec saisie de son code PIN sera demandée également.

Après cette série de validations, une délégation sera établie entre vous deux.

En cliquant sur le bouton , vous supprimerez une délégation avec le professionnel de santé sélectionné.

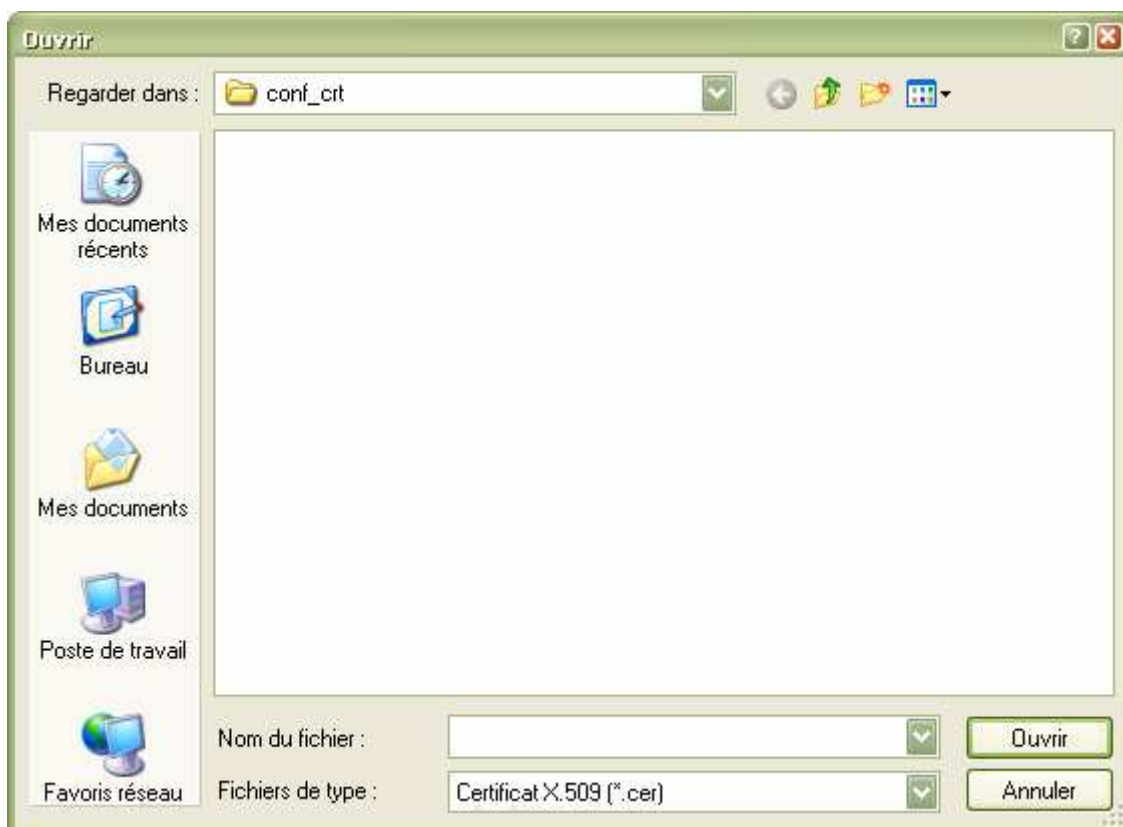
Gestion des certificats racine

Cette partie est expliquée en détail dans le chapitre « Cinématique d'envoi d'un message chiffré et signé ».



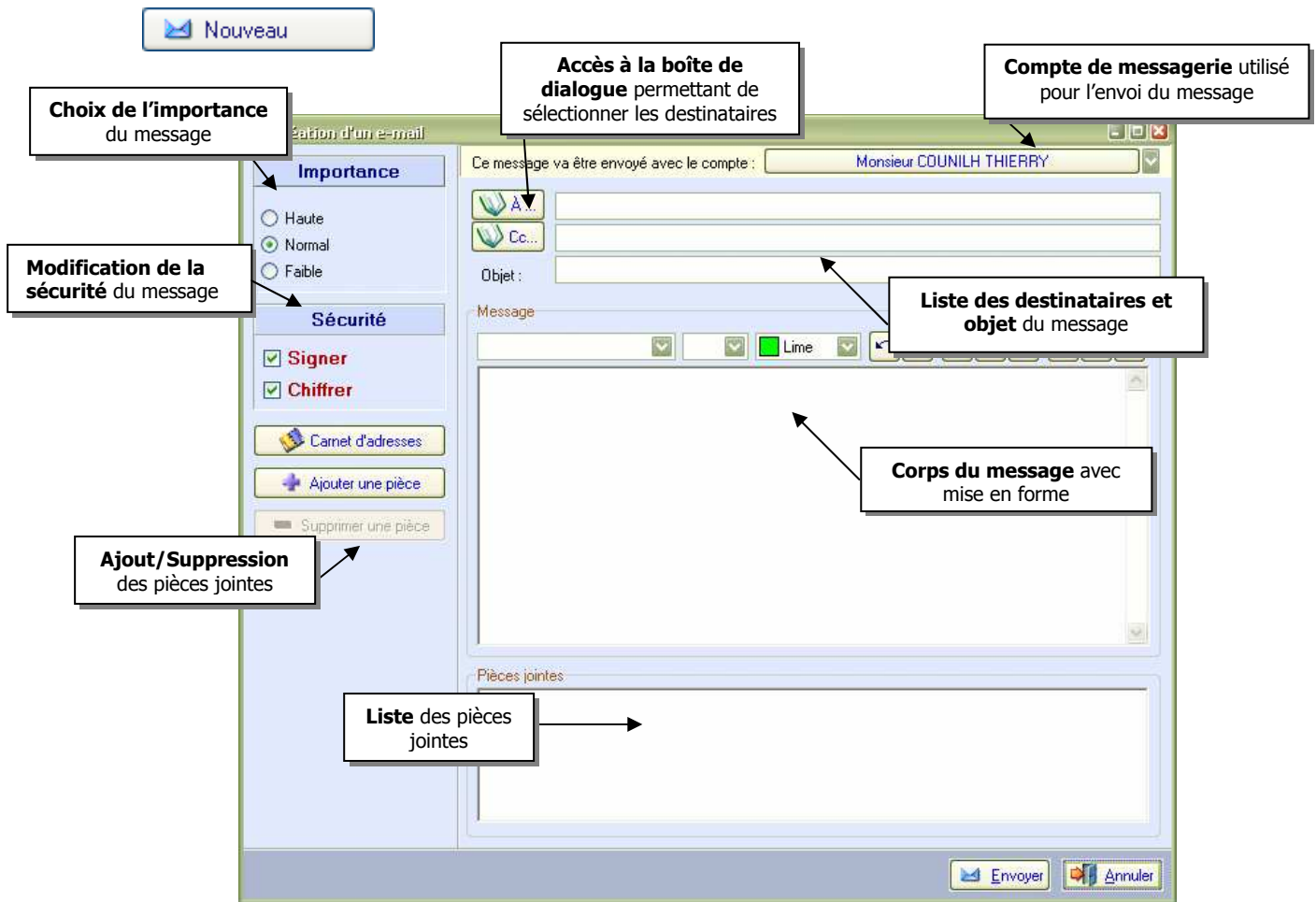
Les certificats racine grisés ne sont pas supprimables (cas des certificats racine du GIP-CPS).

Lors de l'ajout d'un certificat racine, la boîte de dialogue permettant de sélectionner le fichier contenant le certificat racine apparaît :



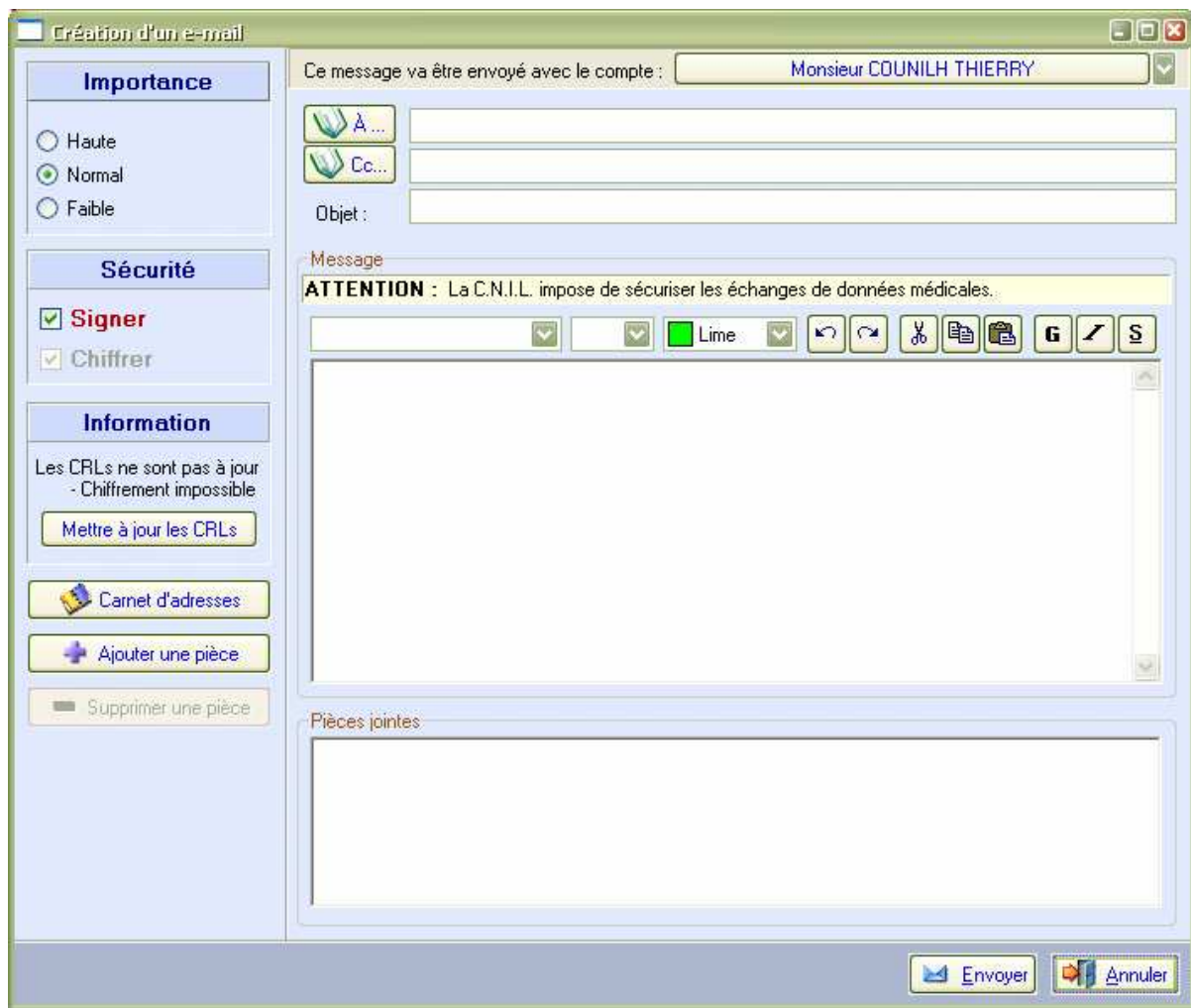
NB : la suppression d'un certificat racine ne sera effective que lors du redémarrage de l'application.

Création d'un nouveau message



La création d'un nouveau message se fait en HTML via le composant d'édition HTML de Internet Explorer.

Dans le cas où les CRLs ne seraient pas à jour, le chiffrement ne sera pas possible. Par contre vous aurez la possibilité de les mettre à jour directement :



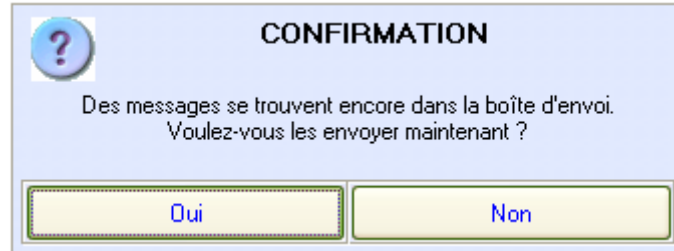
Si vous commencez un nouveau message et que vous cliquez sur « **Quitter** » ou sur la croix de fermeture de la fenêtre, on vous proposera de stocker votre message dans le dossier « **Brouillons** » pour pouvoir le continuer plus tard.



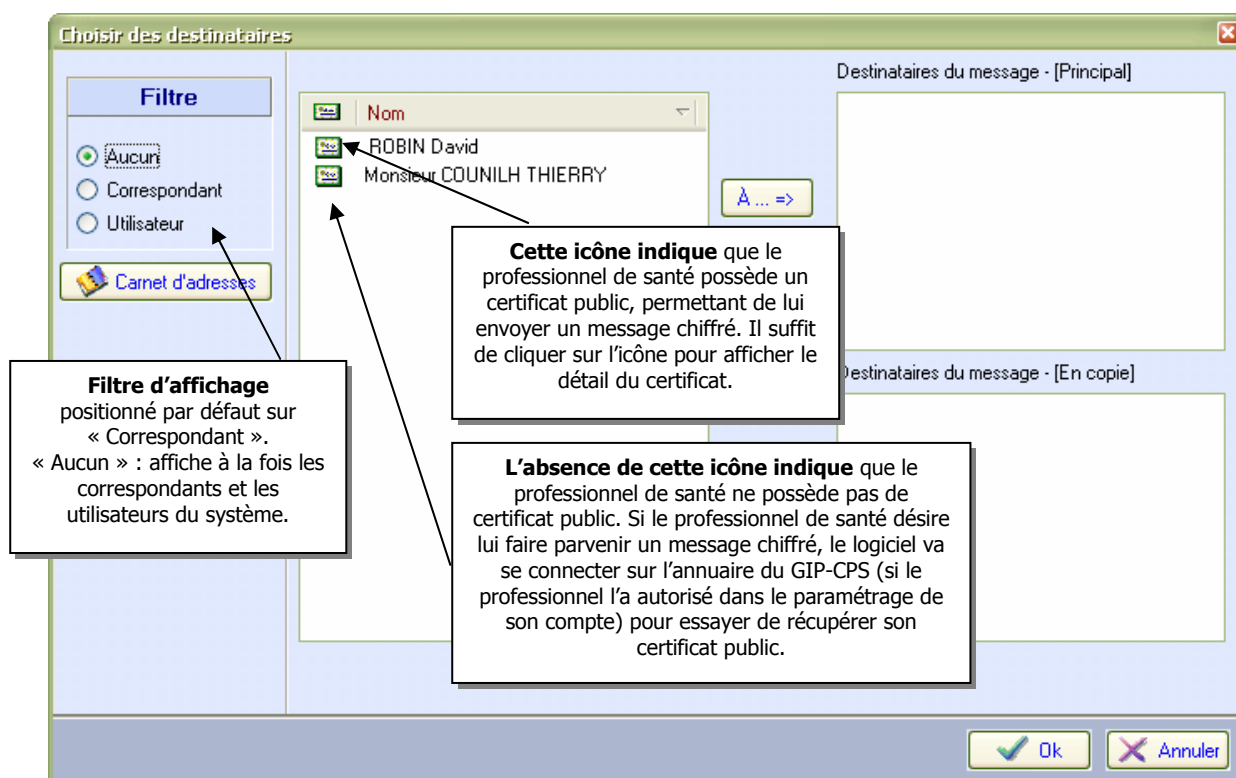
Si vous cliquez sur le bouton « **Envoyer** », vous avez le choix entre :

- **envoi immédiat**, le message sera stocké dans le dossier « Boîte d'envoi » et une opération d'envoi sera réalisée sur le compte sélectionné
- **envoi différé**, le message sera stocké dans le dossier « Boîte d'envoi » et sera envoyé lors d'une opération d'envoi/réception

Dans le cas où vous fermez votre messagerie alors qu'il y a des messages non envoyés dans votre boîte d'envoi, vous verrez le message suivant :



Sélection des destinataires



Il sera affiché dans cet écran la liste des correspondants et des utilisateurs du système.

Par défaut, le filtre sera positionné sur « Correspondant ».

Cinématique d'envoi d'un message chiffré et signé

Éléments nécessaires pour le chiffrement d'un message

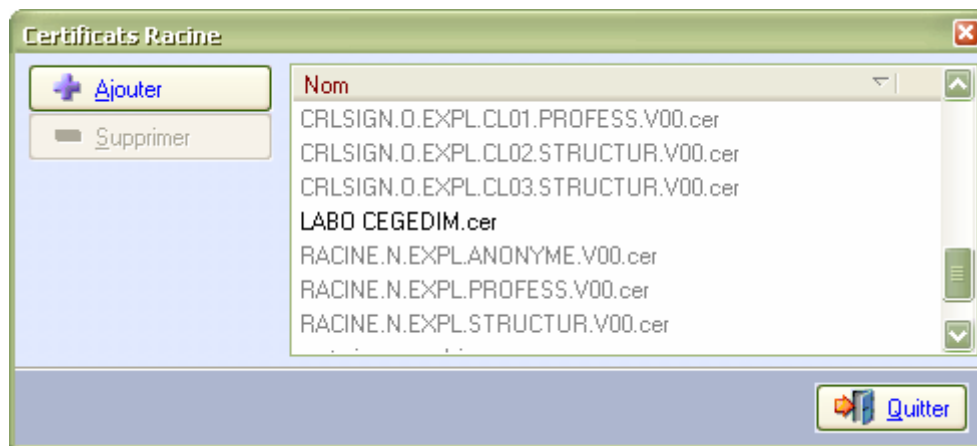
Vous devez paramétrer une chaîne de certification complète :

- les AC (Autorités de certification) Racines (Pré-Installées)
- un certificat numérique personnel
- les CRLs à jour

Pour le cas du GIP-CPS, les AC Racines existent en version de production ou en version de test. Le logiciel de gestion de cabinet sera livré paramétré avec toutes les AC Racines du GIP-CPS en version de production.

Vous aurez la possibilité de rajouter d'autres AC Racines d'une autre organisation.

Pour cela vous devrez, depuis le client de messagerie, accéder à la fonction « **Propriétés** » et cliquer sur le bouton « **Certificats Racine** » :



Vous ne pourrez pas supprimer les AC Racines pré-installées du GIP-CPS. Vous pourrez cependant ajouter ou supprimer d'autres AC Racines d'autres organisations.

Lors de l'ajout d'un certificat, une boîte de dialogue permettant de sélectionner un fichier s'ouvrira.

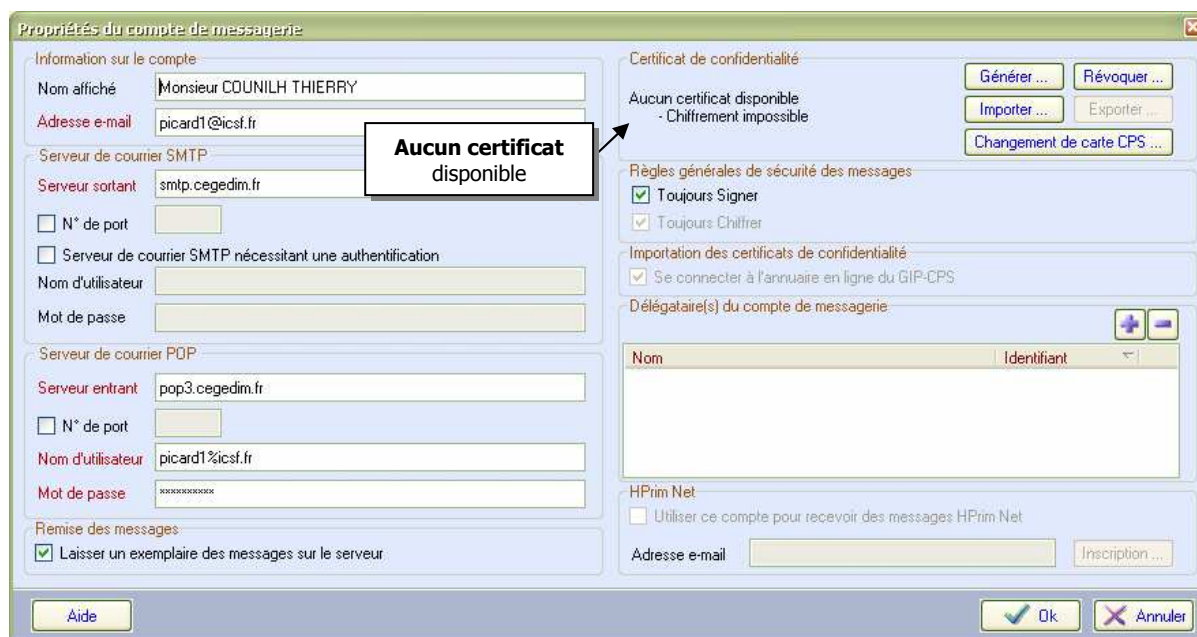
Lors de la suppression d'un certificat racine, un message de confirmation vous sera proposé.

La suppression ne sera effective que lors du prochain lancement du logiciel (déchargement en mémoire du certificat racine).

NB : dans le cas où vous supprimez un certificat racine par erreur, le fait de l'ajouter aussitôt, sans avoir relancé le logiciel générera une erreur indiquant que le certificat racine existe déjà.

Vous devez avoir un certificat personnel paramétré sur le compte de messagerie que vous souhaitez utiliser pour signer et chiffrer vos messages. Vous ne pouvez avoir qu'un seul certificat par activité présente sur votre carte CPS.

Pour cela, allez sur le paramétrage de votre compte de messagerie :

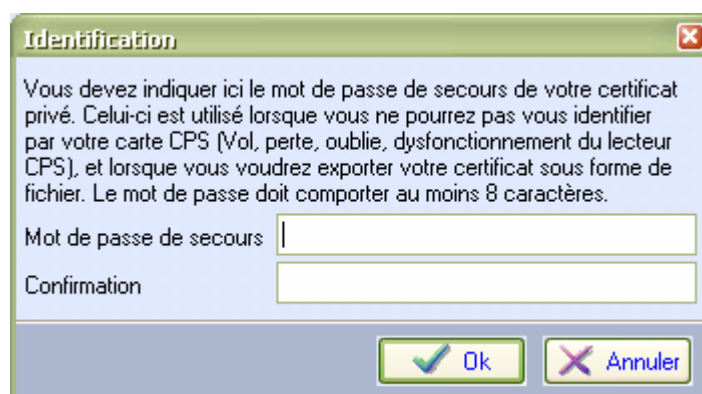


Vous pouvez demander au GIP-CPS un certificat de confidentialité en utilisant le bouton « Générer... ».

Une demande de confirmation sera proposée :

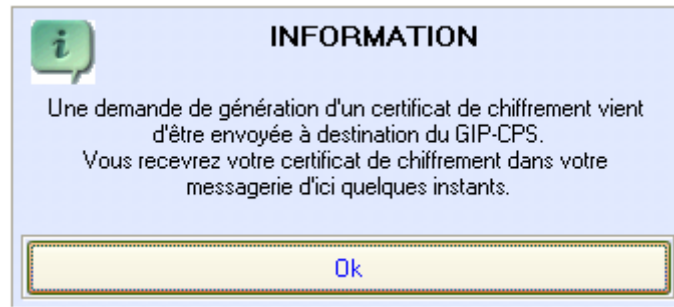


Si vous n'avez pas votre carte CPS pour déchiffrer un message (vol, perte, oubli), votre mot de passe de secours sera demandé.



Dans le cas où votre carte CPS possède plusieurs situations d'exercice, vous devrez choisir la situation d'exercice pour laquelle vous demandez un certificat de confidentialité.

Le message de confirmation suivant sera affiché :



Quelques minutes plus tard, un e-mail du GIP-CPS sera disponible dans votre « **boîte de réception** », après une opération « **Envoyer / Recevoir** ».

Soit l'opération se passe bien, et vous obtiendrez le nouveau certificat qui sera automatiquement installé.

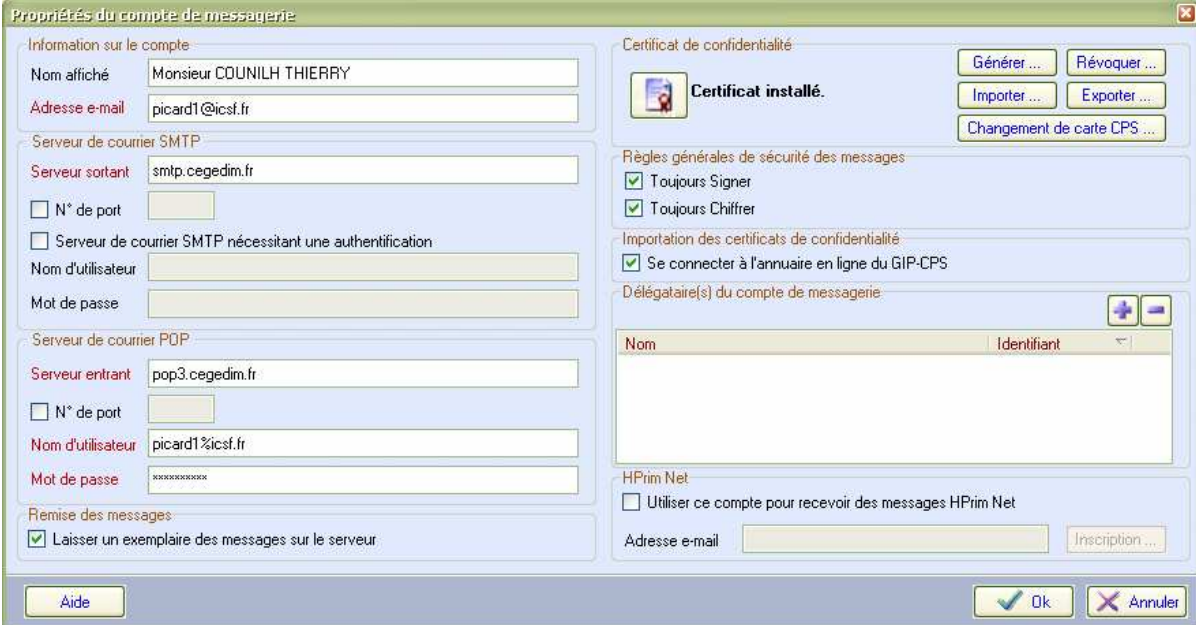
Dans le cas contraire, vous serez averti d'une erreur et vous devrez donc renouveler l'opération ultérieurement.

Le certificat public - ou certificat de confidentialité - associé au certificat privé sera disponible sous 24 à 48 heures sur l'annuaire du GIP-CPS. Il faudra donc attendre 24 à 48 heures avant de pouvoir recevoir un message sécurisé.

Si l'opération s'est bien passée, le certificat sera automatiquement installé sur votre compte de messagerie.

Les options suivantes seront alors automatiquement activées :

- toujours signer
- toujours chiffrer
- se connecter à l'annuaire en ligne du GIP-CPS



Propriétés du compte de messagerie

Information sur le compte
Nom affiché: Monsieur COUNILH THIERRY
Adresse e-mail: picard1@icst.fr

Serveur de courrier SMTP
Serveur sortant: smtp.cegedim.fr
 N° de port
 Serveur de courrier SMTP nécessitant une authentification
Nom d'utilisateur
Mot de passe

Serveur de courrier POP
Serveur entrant: pop3.cegedim.fr
 N° de port
Nom d'utilisateur: picard1@icst.fr
Mot de passe: *****

Remise des messages
 Laisser un exemplaire des messages sur le serveur

Certificat de confidentialité
Certificat installé.
Générer ... Révoquer ...
Importer ... Exporter ...
Changement de carte CPS ...

Règles générales de sécurité des messages
 Toujours Signer
 Toujours Chiffrer

Importation des certificats de confidentialité
 Se connecter à l'annuaire en ligne du GIP-CPS

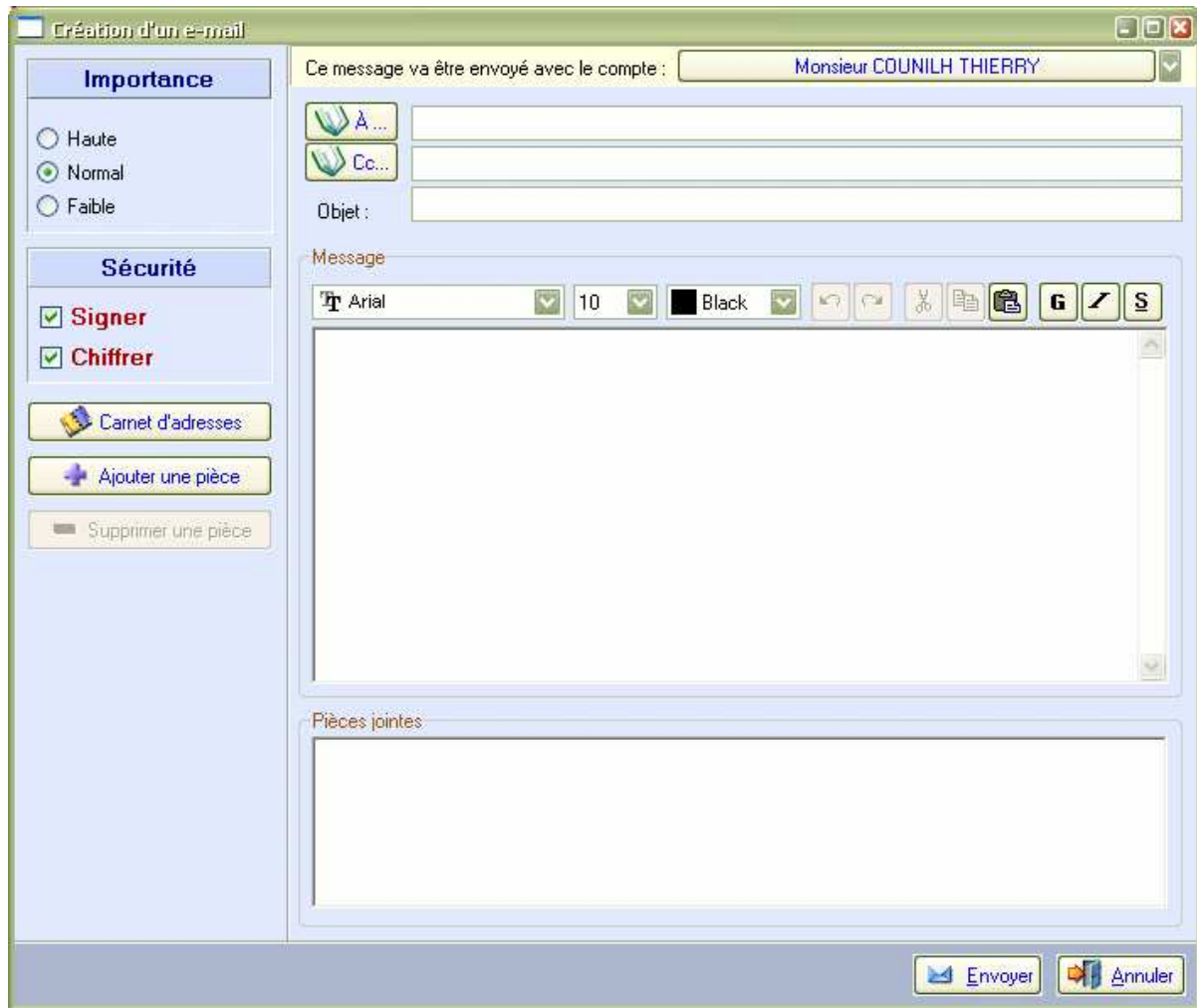
Délégué(s) du compte de messagerie



Nom	Identifiant
-----	-------------

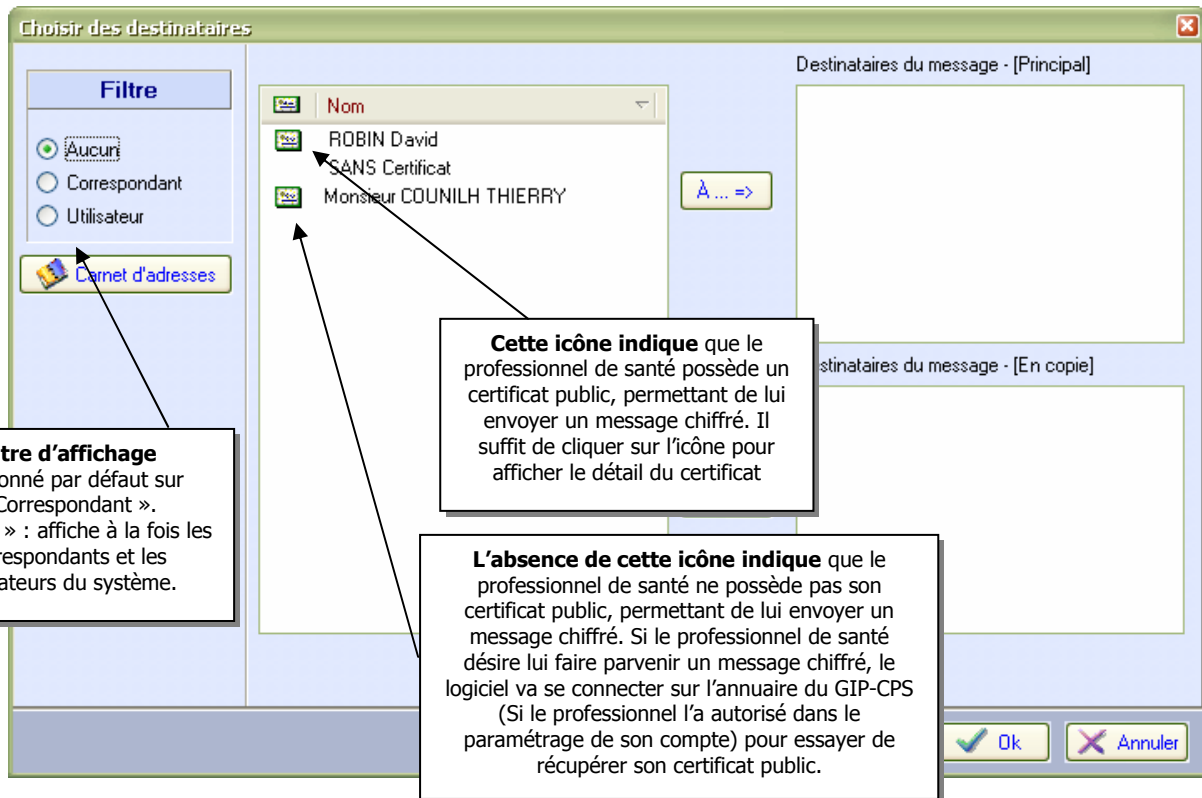
HPrim Net
 Utiliser ce compte pour recevoir des messages HPrim Net
Adresse e-mail Inscription ...

Aide Ok Annuler

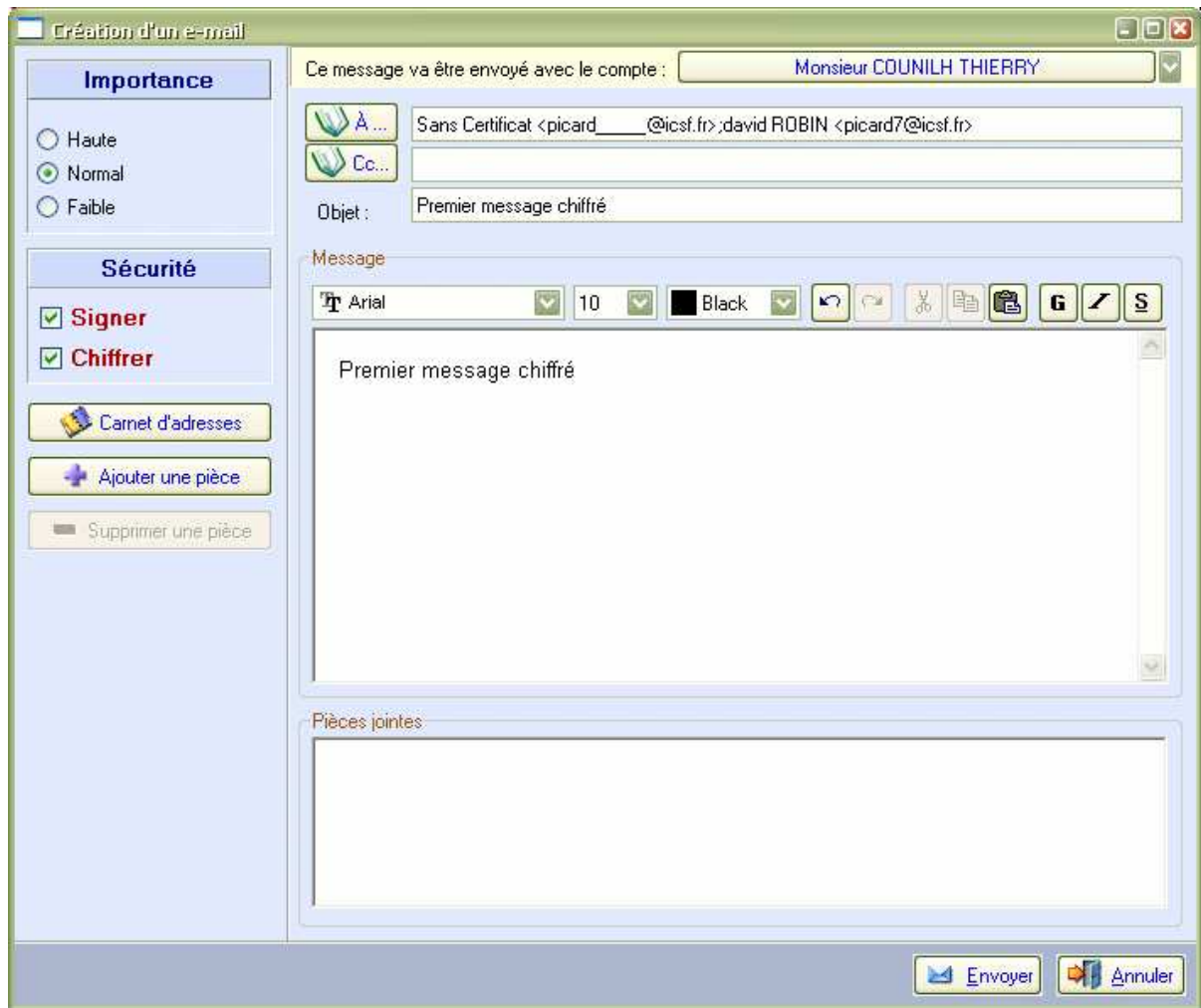
Vous pouvez maintenant envoyer votre premier message sécurisé :



Pour le choix des destinataires, cliquez sur les boutons  ou  :

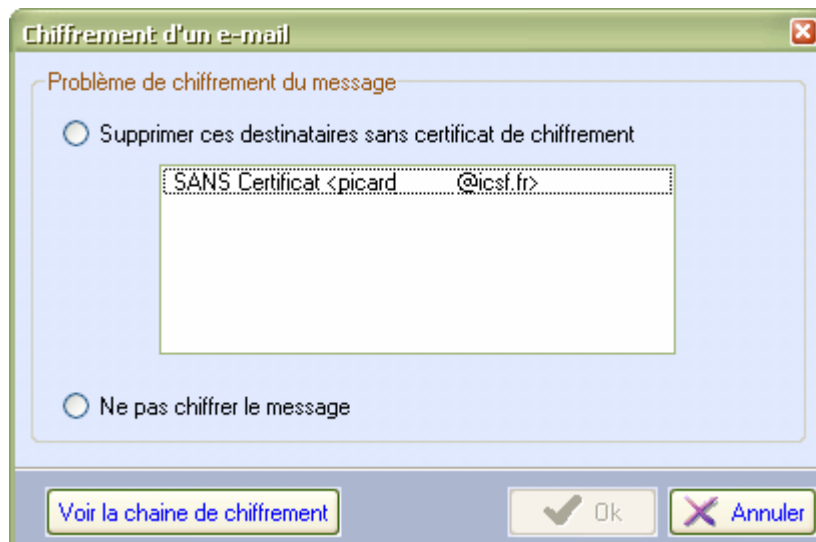


Pour cet exemple, nous allons volontairement envoyer un message à un correspondant qui n'existe pas.



Lors de l'envoi du message, étant donné qu'il manque le certificat public de « Sans certificat », et que le professionnel de santé a autorisé le logiciel à se connecter sur l'annuaire public du GIP-CPS, celui-ci va essayer de récupérer le certificat public de l'utilisateur picard@icsf.fr. S'il n'existe pas, il essaiera ensuite de récupérer le certificat public de « Sans Certificat ».

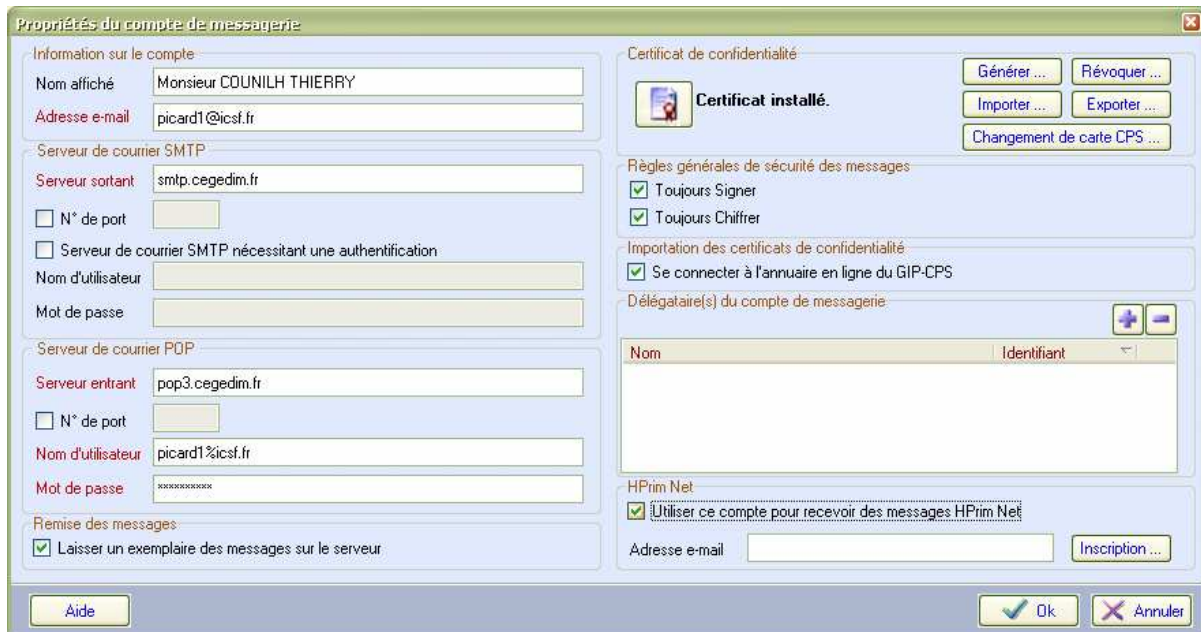
Après cette étape, s'il manque toujours les certificats publics de certains destinataires, la fenêtre suivante s'affichera :



Une fois le destinataire « Sans Certificat » supprimé des destinataires, le message sécurisé est envoyé.

HPRIM Net

Pour activer la réception des messages HPrim Net, vous devez configurer un compte de messagerie dédié à cette action.



Inscrivez-vous ensuite à chacun des serveurs des laboratoires desquels vous souhaitez recevoir des résultats, en indiquant leurs adresses mail puis en cliquant sur le bouton « **Inscription...** ».

Si vous activez « **Utiliser ce compte pour recevoir des messages HPrim Net** », vous aurez accès à un nouveau dossier de stockage dans votre client de messagerie nommé « **Éléments HPrim Net** ».



Tous les messages HPrim'Net seront stockés dans le dossier éléments HPrim Net lors d'une opération d'envoi/réception.

Les différentes pièces jointes des messages Hprim seront stockées dans le répertoire configuré dans le fichier standalone.ini via la clé CHEMIN_HPRIM.

Les équipes CLM vous souhaitent une bonne utilisation de votre messagerie médicale sécurisée SMM.





Chaque jour à vos côtés ■

Cegedim Logiciels Médicaux (Groupe Cegedim)
122, rue d'Aguesseau – 92641 Boulogne-Billancourt Cedex
CLMinfos@cegedim.fr