Certificats électroniques

• préambule

Cette présentation va tenter de répondre aux interrogations suivantes :
- les différents types,
- aspects techniques et juridiques, logiciels qui les supportent,
- peut-on se contenter de certificats auto-signés ?
- comment ça se passe au CNRS ? comment ça se passe ailleurs ?
- ...

Pour plus de détails reportez-vous sur les sites suivants, où j'ai moi même puisé de nombreuses informations :

http://www.urec.cnrs.fr/igc/Certifs_CNRS.html
http://www.cru.fr/igc

http://www.math.jussieu.fr/informatique/certificats/certificat.html

N'hésitez pas non plus à utiliser votre moteur de recherche favori 

Les différents types

- **certificats de personne**

  propres à un individu (carte d'identité)
  - authentification
  - confidentialité
  - signature
  - non répudiation

- **certificats de service**

  propres à un serveur (web, courrier, horodatage, ...)
  - authentification
  - confidentialité

Les différents types

- **certificats autorité de certification**

  propres à chaque autorité de certification (CA)
  - signature
  - authentification

  des certificats émis par cette autorité

- **listes de révocations**

  propres à chaque autorité de certification (CA)
  - publication

  des certificats émis par cette autorité et qui ont été, par la suite, révoqués

Certificat (norme) X509

- **un fichier contenant**

  - sujet
  - clé publique
  - signature de la clé publique (auto-signée ou réalisée par un CA)
  - numéro de série
  - période de validité
  - usage (courrier, signature, serveur, application, CA)
  - peut aussi contenir le(s) certificat(s) de(s) CA

- **chaînage récursif des signatures**

  Chaque certificat est signé par l'autorité de certification qui l'a émis
  De même que chaque certificat d'une autorité de certification est signé soit par :
  - une autre autorité de certification
  - par elle-même (dans ce cas le certificat est le certificat "racine" de l'AC)

Les différents formats de fichiers

- **DER** extensions usuelles: .der, .cer, .crt, .cert

  Utilisé pour encoder des certificats X509 en notation ASN.1

  ASN.1 Abstract Syntax Notation number One

- **PEM** extensions usuelles: .pem, .cer, .crt, .cert

  Peut contenir des clés privées, des clés publiques et des certificats X509
  Le format PEM est du DER encodé en base64 auquel sont ajoutés des en-têtes ASCII

- **PKCS#12** extensions usuelles: .p12, .pfx (Microsoft)

  C'est le format communément utiliser pour stocker un certificat et sa clé privée associée dans un fichier protégé en confidentialité et intégrité par un mot de passe

  PKCS Public Key Cryptography Standards

  PKCS#1 à PKCS#15 standards définissant les formats des éléments de cryptographie

Les différents formats de fichiers

- **CRLs** extensions usuelles: .crl

  Listes de révocations au format PEM ou DER
  Ce fichier contient la liste des certificats révoqués.

- **PKCS#7** extensions usuelles: .p7s (données signées), .p7m (données chiffrées)

  Un message signé a en pièce jointe un fichier qui contient la signature (.p7s).
  Le contenu d'un message chiffré est placé dans une pièce jointe (.p7m).

- **PKCS#10** extensions usuelles: .csr, .req

  Au format PEM ou DER , contient une requête de signature de certificat (CSR).

  CSR Certificate Signing Request

- **PKCS#11** Cryptographic Token Interface Standard

  Définie l'interface de communication avec les clés cryptographiques.

3 algorithmes de crypto

- **à sens unique**

  irréversible, le texte chiffré ne peut pas être déchiffré

  UNIX crypt, MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm)

- **asymétriques**

  une paire de clés, l'une sert pour chiffrer, l'autre pour déchiffrer

  RSA (Rivest, Shamir & Adleman), DSA (Digital Signature Algorithm)

- **symétriques**

  la même clé sert pour chiffrer et déchiffrer

  DES (Data Encryption Standard), TripleDES,
  IDEA (International Data Encryption Algorithm), Diffie-Hellman, blowfish,
  AES (Advanced Encryption Standard) / Rijndael (Daemen & Rijmen)

RSA (Rivest, Shamir & Adleman)

- l'algorithme est dit asymétrique car il fonctionne avec une paire de clés, l'une des deux clés est utilisée pour chiffrer, l'autre pour déchiffrer

- chacune des deux clés (de la même paire) peut indifféremment servir, soit pour chiffrer, soit pour déchiffrer

- ce qui a été chiffré avec l'une des deux clés ne peut être déchiffré qu'avec l'autre clé de la même paire

- l'une des deux clés est appelée la «clé secrète ou privée», l'autre la «clé publique»

T = message en clair, C = message chiffré

on peut indifféremment :

- soit coder avec la clé publique : C = T(clé publique) et décoder avec la clé secrète : T = C(clé secrète)

- soit coder avec la clé secrète : C = T(clé secrète) et décoder avec la clé publique : T = C(clé publique)

mais on ne peut pas coder et décoder avec la même clé:

- C = T(clé publique) suivi de C(clé publique) ou C = T(clé secrète) suivi de C(clé secrète) ne redonnent pas T

envoyer un message signé (et crypté)

Alice

- écrit le message destiné à Bill
- génère l'empreinte (avec un algorithme à sens unique) du message
- code l'empreinte générée avec sa **clé secrète de Alice** réalisant ainsi une signature
- (éventuellement) code le message avec la **clé publique de Bill**
- envoie ensemble le message (chiffré) et la signature à Bill ~~%$?&§~~

Bill

- reçoit le message (chiffré) et la signature
- décode le message avec sa **clé secrète de Bill**
- génère l'empreinte du message en clair avec le même algorithme à sens unique que Alice
- décode la signature avec la **clé publique de Alice**
- compare les deux empreintes (décodée et générée) et si elles sont identiques alors le message:
  - émane bien de Alice
  - il n'a pas été falsifié au cours de son acheminement
  - Alice ne peut pas nier qu'elle l'a écrit et envoyé

Cette méthode est utilisée avec tous les systèmes à clés publiques, PGP (Pretty Good Privacy), OpenPGP, GnuPG, etc..., mais seul l'utilisation de certificats signés, par une autorité de certification "reconnue", permet de garantir que les clés publiques de Alice et de Bill sont bien les leur. Et dans cas Alice et Bill vérifieront aussi, en utilisant la chaîne de certification, l'authenticité de leurs clés publiques respectives.

création d'un certificat

Alice

- crée une paire de clés
- garde et mets en sécurité sa **clé secrète de Alice**
- envoie son identité et sa **clé publique** à l'Autorité de Certification

Autorité de Certification (AC)

- reçoit l'identité et la **clé publique de Alice**
- génère de façon aléatoire un challenge
- code le challenge avec la **clé publique de Alice**
- envoie le challenge chiffré à Alice

- reçoit le challenge chiffré
- décode le challenge avec sa **clé secrète de Alice**
- renvoie le challenge en clair à l'Autorité de Certification

- reçoit le challenge en clair et le compare avec celui généré
- vérifie l'identité de Alice par le biais de l'**Autorité d'Enregistrement (AE)**
- crée alors le certificat de Alice avec : l'identité et la **clé publique de Alice** et l'identité de l'Autorité
- génère une empreinte du certificat créé
- code l'empreinte avec sa **clé secrète d'Autorité**
- envoie le certificat (ainsi) signé à Alice

Les aspects juridiques

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

La LCEN :

LIBERALISATION DE LA CRYPTOLOGIE

La cryptologie fait l'objet d'une nouvelle libéralisation. La base du régime de la cryptologie dans le secteur des technologies de la communication prévoit :

- deux emplois pour la cryptologie selon qu'elle sert à garantir la confidentialité ou l'identification et l'intégrité (signature électronique),
- quatre finalités : l'importation, l'exportation, la fourniture et l'utilisation.

Article 31 de la LCEN :

(A propos du régime de fourniture de prestation de cryptologie, qui s'applique aux certificateurs dans leur activité d'émission de certificats électroniques)

- Obligation de déclaration de l'activité de fourniture de prestations de cryptologie auprès du Premier Ministre, dans des conditions définies par un décret en conseil d'état ;
- Obligation de secret professionnel pour les personnes exerçant cette activité

Article 30 de la LCEN :

- L'utilisation des moyens de cryptologie est libre.
- La fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres.
- La fourniture, l'importation et l'exportation d'un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont soumis à autorisation du Premier Ministre.

9/11/2004 Robert LONGEON – matinée de sensibilisation à la "Sécurité informatique" 1

Les aspects juridiques

Cette page et les 3 suivante sont extraites du document cité ci-dessous :
http://www.cru.fr/igc/signature_electronique.pdf
rédigé en 2003 par Florent Guilleux du Comité Réseau des Universités

Loi du 13 mars 2000	- validité de l'écrit sous forme électronique - reconnaissance juridique de la signature électronique - démonstration de fiabilité à la charge du signataire
Décret du 30 mars 2001	- définition de la signature électronique sécurisée présumée fiable : -> inversion de la charge de preuve mais nécessité de : - certification du dispositif de création de signature électronique - qualification du prestataire de services de certification électronique
Décret du 18 avril 2002	- description du processus de certification des produits et systèmes relatifs aux technologies de l'information - conditions d'agrément des organismes chargés de l'évaluation
Arrêté du 31 mai 2002	- description du processus qualification des prestataires de service de certification électronique - conditions d'agrément des organismes d'évaluation des prestataires de service de certification électronique

Les aspects juridiques

Type de signature	Conditions de validité[1]	Présomption de fiabilité
Signature électronique	Le procédé de signature assure l'identification du signataire et la garantie de l'intégrité de l'acte	non
Signature électronique sécurisée	Signature électronique : - propre au signataire ; - créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; - garantissant avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable.	non
Signature électronique sécurisée présumée fiable	Signature électronique sécurisé - établie à l'aide d'un dispositif de création sécurisée ; - dont la vérification repose sur l'utilisation d'un certificat électronique qualifié.	oui

[1] De plus l'écrit sous forme électronique sur lequel est apposée la signature doit respecter les deux conditions définies dans la loi du 30 mars 2000 lui permettant d'être admis au même titre que l'écrit sous forme papier :
1. la personne dont émane l'écrit peut être dûment identifié;
2. l'écrit est établi et conservé dans des conditions de nature à en garantir l'intégrité.

Les aspects juridiques

La signature électronique sécurisée est recevable comme preuve en justice mais la démonstration de fiabilité du procédé de signature est à la charge du signataire. Cependant la charge de preuve est inversée si la signature électronique est *présumée fiable*. Pour cela elle doit respecter les exigences suivantes :

1. elle est établie à l'aide d'un *dispositif de création sécurisée* ;
2. la vérification de cette signature repose sur l'utilisation d'un *certificat électronique qualifié*.

3.1 Dispositif de création de signature électronique sécurisé

Pour être qualifié de *sécurisé*, un dispositif de création de signature électronique doit :

1. respecter les exigences définies dans l'article 3 du décret, notamment que "les données de création de signature électronique peuvent être protégées de manière satisfaisante par le signataire contre toute utilisation par des tiers" ;
2. **être certifié conforme à ces exigences par un organisme agréé** (objet du décret du 18 avril 2002).

Les aspects juridiques

3.2 Certificat électronique qualifié

Pour être considéré comme *qualifié*, un certificat électronique doit comporter des éléments définis dans l'article 6 et **être délivré par un prestataire de services de certification électronique respectant certaines exigences**, définies dans le même article, notamment :

- assurer le fonctionnement d'un service permettant à la personne à qui le certificat électronique a été délivré de **révoquer sans délai et avec certitude** ce certificat ;
- utiliser des systèmes de conservation des certificats électroniques garantissant notamment que l'accès du public à un certificat électronique ne peut avoir lieu sans le consentement préalable du titulaire du certificat ;
- pour la délivrance du certicat, exiger la présentation d'un document officiel d'identité et conserver les caractéristiques et références des documents présentés ;
- avant la délivrance d'un certificat, informer la personne par écrit des modalités de contestation et de litige.

Les prestataires de services de certification électronique qui satisfont à toutes ces exigences peuvent demander à être reconnus comme *qualifiés*, **ce qui vaut présomption de conformité aux exigences** (objet du décret du 31 mai 2002).

Les aspects juridiques

- **au CNRS**
- **au CRU**

Je n'ai trouvé (ou pas assez cherché) les informations me permettant de savoir si les IGC ou AC de ces 2 organismes :
- ont été certifiées conforme aux exigences de la signature électronique sécurisée par un organisme agréé;
- satisfont aux exigences du certificat électronique qualifié et ont demandées à être reconnues comme qualifiées.

- **dans les offres commerciales**

les IGC ou PKI

• Gestion des clefs ©

L'utilisation de bi-clef entraîne la nécessité de publication, en toute confiance, de la clef publique. Cette publication doit offrir l'assurance que :
- la clef est bien celle appartenant à la personne avec qui les échanges sont envisagés;
- le possesseur de cette clef est « digne de confiance »;
- la clef est toujours valide.

La confiance est obtenue en associant au bi-clef un **certificat** délivré et géré par une entité elle-même de confiance : l'**Infrastructure de Gestion de Clefs**. Une IGC est donc une structure à la fois technique et administrative permettant une mise en place, lors de l'échange de clef, de *relations de confiance entre des entités morales et/ou physiques et/ou logiques*.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

la politique de certification

- **Critères pour construire une IGC ©**

De même que la sécurité se met en place en suivant une politique de sécurité définie préalablement, la mise en place d'une IGC oblige à une *définition de politique de certification* : « un ensemble de règles indiquant, ce pour quoi le certificat est applicable et par qui, et quelles sont les conditions de leur mise en oeuvre au sens juridique administratif et technique ».
La règle de base étant avant tout que les certificats et les moyens de mise en oeuvre soient définis en fonction de l'utilisation que l'on veut en faire.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

l'Autorité de Certification

- **Gestion des clefs** ©

Les informations spécifiques minimales entrant dans la composition du certificat : nom du propriétaire, durée de validité du certificat sont complétées par celles relatives à l'autorité qui les a validées.
Cette autorité, offrant toute confiance, et ayant elle-même un certificat (par auto-certification ou cautionnée par une autre autorité) se nomme *Autorité de Certification*.
La crédibilité (garantie) est assuré par le mécanisme de signature.
La signature du certificat est calculée par l'autorité de certification en prenant en compte la clef publique du demandeur, son identification et des informations complémentaires; celle-ci génère ce certificat en signant avec sa clef privée.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

l'Autorité de Certification

- **Gestion des clefs** ©

L'autorité de certification peut se situer à différents niveaux, elle peut être organisationnelle (exemple : CNRS, CRU) ou spécifique à un corps de métier (exemple : notaire) ou encore institutionnelle et dans ce cas cautionner au niveau national des autorités subalternes; elle alors nommée autorité racine.

L'autorité de certification s'appuie généralement sur deux autres entités qui travaillent par délégations : l'*Autorité d'Enregistrement* et l'*Opérateur de Certification*. Cependant elle garde la responsabilité des procédures et des principes de certification; c'est elle qui fait appliquer la politique de certification et elle est responsable pour ses utilisateurs du niveau de confiance fourni par l'IGC.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

l'Autorité d'Enregistrement

- **Gestion des clefs** ©

L'autorité d'enregistrement assure le contrôle des données identifiant le demandeur de certificat; c'est elle qui authentifie une demande de révocation qui sera ensuite exécutée par l'autorité de certification; elle assure lors de la délivrance d'un nouveau certificat (sur date de péremption atteinte) un recouvrement des certificats afin d'assurer la continuité pour la fonctionnalité signature et/ou chiffrement; elle travaille en étroite collaboration avec l'opérateur de certification; elle possède un bi-clef certifié pour s'authentifier auprès de l'autorité de certification et pour accomplir les tâches qui lui incombent.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

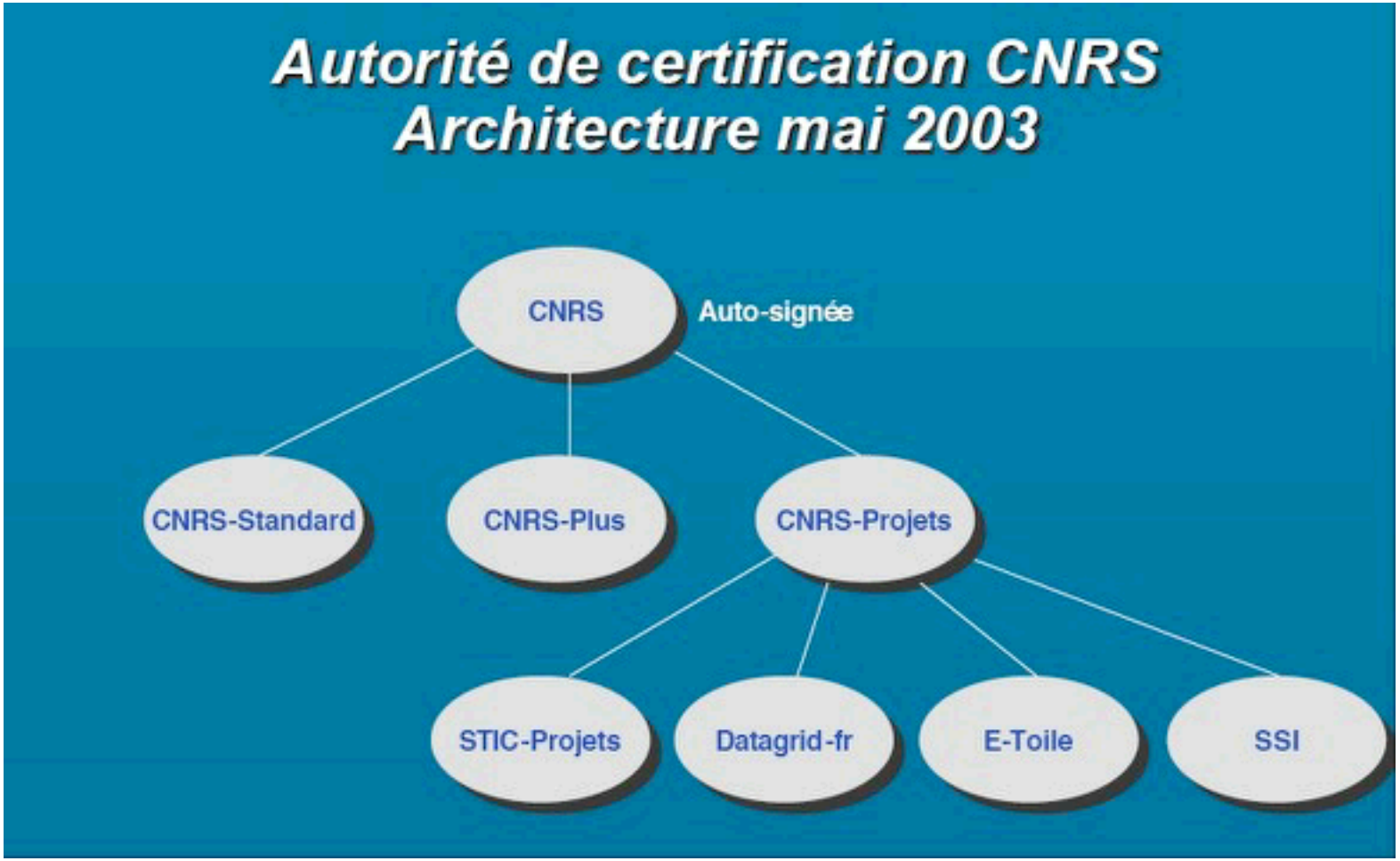
l'Opérateur de Certification

- **Gestion des clefs** ©

  L'opérateur de certification réalise la distribution sécurisée des certificats; il gère en collaboration avec l'autorité d'enregistrement les cycles de vie des certificats; en fonction de la politique de certification ce peut être lui qui génère les bi-clefs pour le compte des utilisateurs; il possède un bi-clef certifié pour s'authentifier auprès de l'autorité de certification et pour accomplir les tâches qui lui incombent.

© Nicole Dausque UREC mai 2000
http://igc.services.cnrs.fr/doc/IGC.pdf

l'AC du CNRS


Autorité de certification CNRS
Architecture mai 2003
CNRS
Auto-signée
CNRS-Standard
CNRS-Plus
CNRS-Projets
STIC-Projets
Datagrid-fr
E-Toile
SSI

les AE au CNRS

- **CNRS-Plus**

  - le délégué régional qui peut confier le rôle à une autre personne
  - c'est l'AE CNRS-Plus de la délégation
  - gère les AE des laboratoires de la délégation

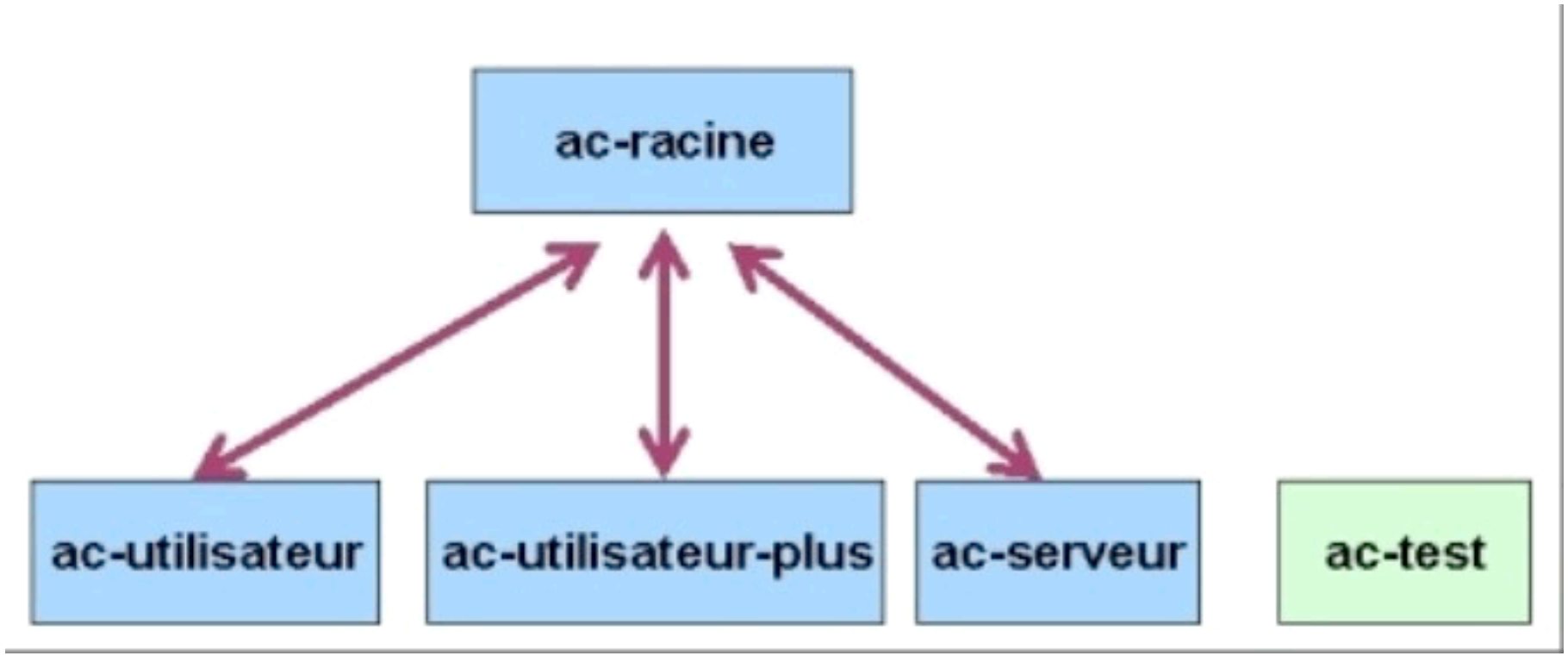
  http://www.urec.cnrs.fr/igc/Doc/Role.AE.CNRS-Plus.DR.pdf

- **CNRS-Standard**

  - par défaut le directeur de l'unité qui peut déléguer cette fonction à une ou plusieurs personnes du laboratoire
  - c'est l'AE CNRS-Standard de l'unité et possède un certificat CNRS-Plus
  - gère les certificats (CNRS-Standard) de personnes et de services pour l'unité

  http://www.urec.cnrs.fr/igc/Doc/Role.AE.CNRS-Standard.pdf
  http://www.urec.cnrs.fr/igc/Doc/modele.dir.lab.pdf

l'AC du CRU


ac-racine
ac-utilisateur
ac-utilisateur-plus
ac-serveur
ac-test

les AE au CRU

- **ac-utilisateur-plus**

  - le CRU lui-même

- **ac-utilisateur**

  - le RSSI et son suppléant ou une ou plusieurs personnes déléguées par l'établissement ayant signé une convention avec le CRU.
  - il possède un certificat ac-utilisateur-plus, mais :

  • l'emploi d'un support de protection des clés de type PKCS#11 est requis ;
  • l'enregistrement exige un critère supplémentaire de vérification de l'identité du demandeur par rapport facial avec le RSSI de l'établissement ou avec l'autorité d'enregistrement;
  • de plus l'opération doit être faite en présence du RSSI qui devra attester que la demande a été réalisée en utilisant une clé cryptographique.

- **ac-serveur**

  - le CRU lui-même ?
  - seul le RSSI est habilité pour demander un certificat serveur

les AC,AE,OC et IGC commerciales

- **elles sont nombreuses**

  - ???

Les aspects techniques

- **pour les AC commerciales**

  Les certificats de nombreuses AC commerciales sont déjà pré-installés dans la plus-part des navigateurs et outils de messagerie.

  Ce qui fait que nous nous rendons même pas compte, lors de l'établissement d'une connexion sécurisée (paiement par carte bleue, consultation de comptes bancaires), que le certificat (de l'organisme auquel nous nous connectons) et sa signature ont été vérifiés silencieusement car le ou les certificats de l'AC commerciale qui a émis le certificat pour cet organisme sont déjà installés dans notre navigateur.

Les aspects techniques

- **pour le CNRS**
- **pour le CRU**

Pour l'instant les certificats de ces deux AC ne sont pas pré-installés, ce qui nous vaut de nombreux messages d'erreur et/ou d'avertissement nous informant de la non reconnaissance et/ou de la non validité des certificats émis par ces deux organismes.

Cela devrait changer, le CNRS (et le CRU ?) a (ont) l'intention de demander à ce que leur certificats (AC) soient intégrés dans les navigateurs et outils de messagerie les plus courants.

En attendant il ne nous reste plus qu'a les installer et demander à nos correspondants et clients (accès à un serveur "web" sécurisé), en dehors de la sphère enseignement supérieur recherche, de les installer dans leur applications.

Cette situation est très gênante car elle introduit un doute et peut par la suite entraîner une perte de confiance en nos certificats.

certificats auto-signés ?

certificats auto-signés ?

- **Est-ce vraiment une bonne idée ?**

certificats auto-signés ?

- **Est-ce vraiment une bonne idée ?**

- **Et pourtant les certificats "racine" des AC**
  sont bel et bien auto-signés

certificats auto-signés ?

- **Est-ce vraiment une bonne idée ?**

- **Et pourtant les certificats "racine" des AC**
  sont bel et bien auto-signés

  Mais, au vu de ce qui a été dit précédemment ...

certificats auto-signés ?

- **Est-ce vraiment une bonne idée ?**

  NON

  ou alors uniquement pour faire des essais avant de demander un certificat

- **Et pourtant les certificats "racine" des AC**

  sont bel et bien auto-signés

  Mais, au vu de ce qui a été dit précédemment ...

les logiciels

- **openssl**

La boîte à outils pour manipuler et créer tout les formats et types de fichiers de certificats, les IGC du CNRS et du CRU l'utilisent.
C'est aussi des librairies implémentant les protocoles :
- SSL (Secure Sockets Layer) v2/v3
- TLS (Transport Layer Security) v1

http://www.openssl.org

les logiciels

- **S/MIME*** Multi purpose Internet Mail Extensions

  Tous les outils de messageries implémentant le S/MIME peuvent être utilisés pour signer et chiffrer des messages

- **SSL*** tous les protocole en **s**

  https , imaps, pops, smtps, ftps

  Toutes les applications implémentant SSL (souvent compilées avec openssl) peuvent être utilisées pour :
  - authentifier le service avant d'établir la connexion sécurisé
  - authentifier les utilisateurs se connectant à ce service

* S/MIME n'implique pas SSL et réciproquement

les logiciels

• clients

Netscape Communicator entre les versions 4.75 et 4.79 (pas Netscape 6 et + donc)
Microsoft Internet Explorer 5.0.1 et versions supérieures (IE 5.5 sp2 fortement conseillé)
Outlook Express, ...

http://igc.services.cnrs.fr/doc/html/chap3.htm (mais date un peu)

Mozilla, Firefox, Thunderbird
Safari, Mail (OS X Panther 10.3.x)
mutt
...

• serveurs

apache, tomcat
imap
...

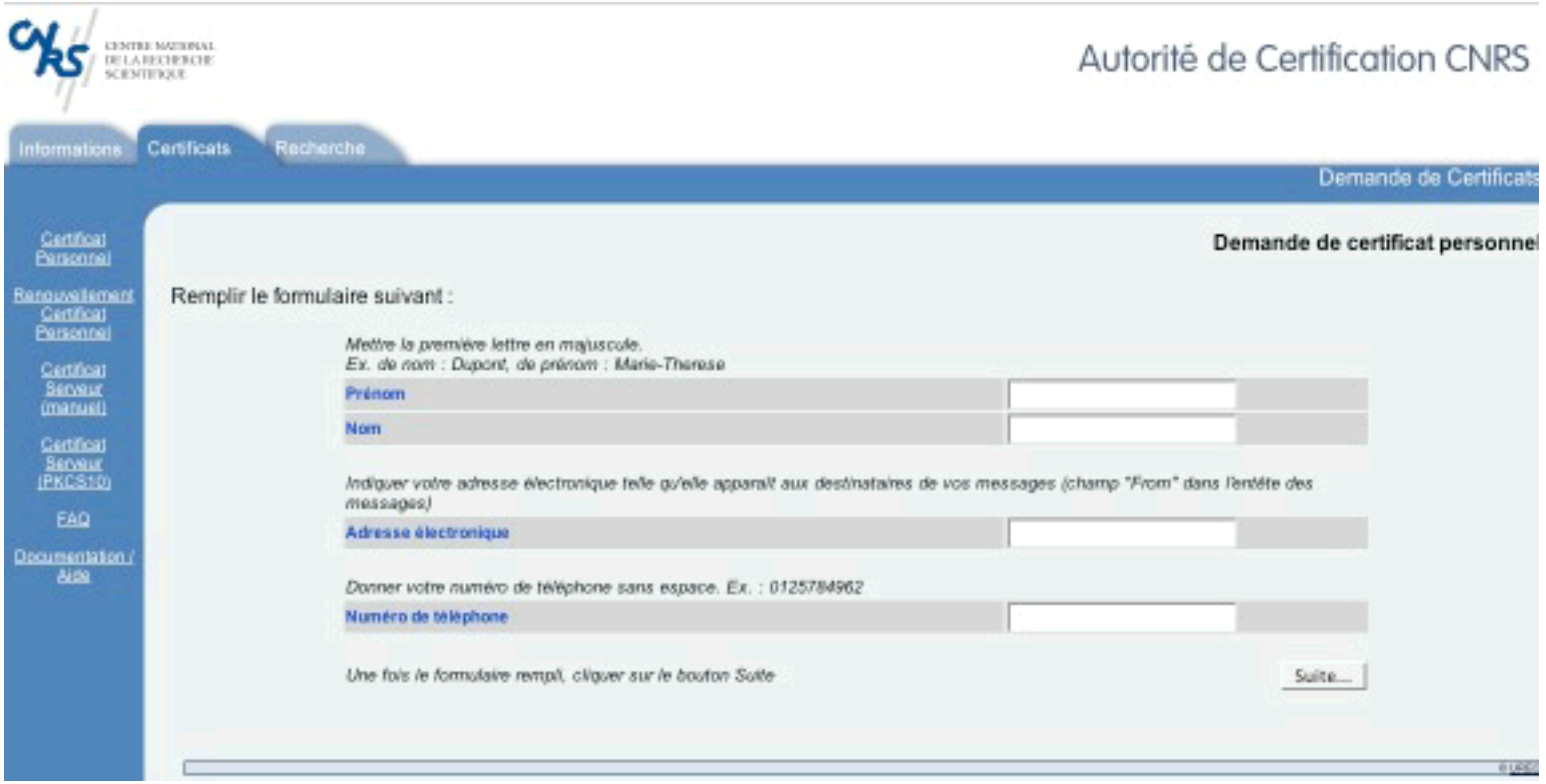
les logiciels

- **pour les AE**

Pour utiliser l'interface sur : https://ra.services.cnrs.fr
on ne peut utiliser que :
- Netscape Communicator 4.7
- Mozilla 1.7
- Firefox 1.0 car basé sur Mozilla 1.7

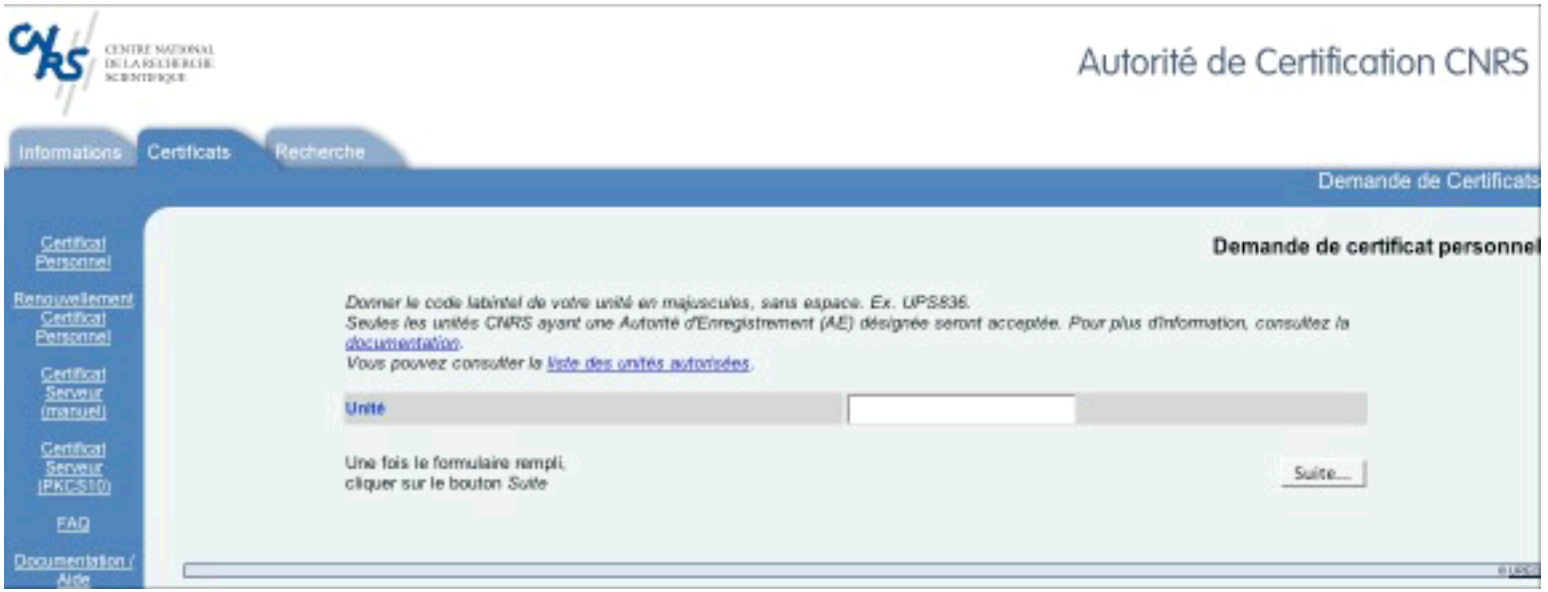
demander un certificat de personne

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html



demander un certificat de personne

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html



- ne pas se tromper dans le numéro de l'unité car c'est lui qui détermine vers quelle AE sera dirigée la requête

- si votre directeur n'a pas désigné d'AE vous ne pourrez pas obtenir de certificat

installer le certificat de personne

- suite à votre demande vous recevrez un premier courrier électronique vous demandant de confirmer votre demande de certificat

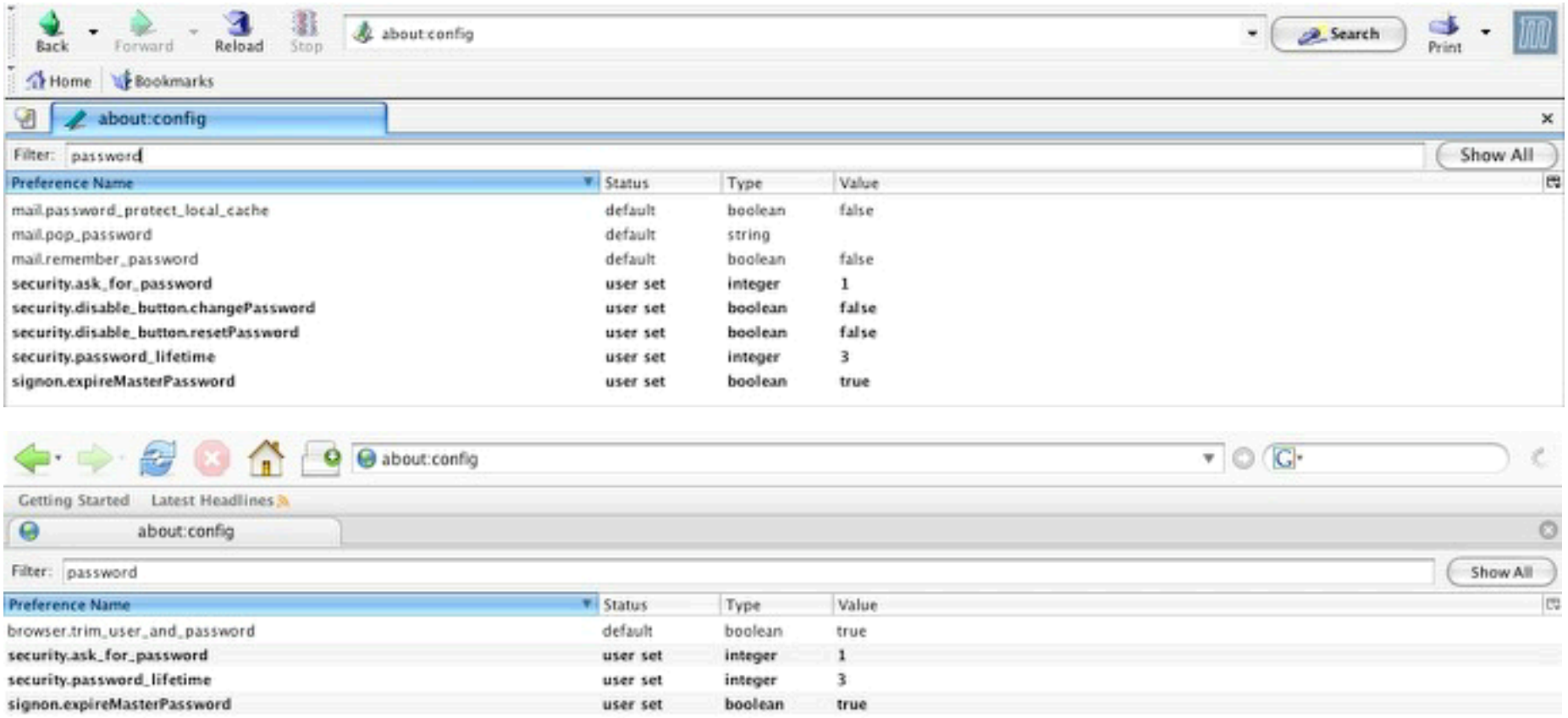
- si votre demande est validé par l'AE dont vous dépendez (qui au préalable vérifiera, en vous contactant que la demande émane bien de vous), vous recevrez un deuxième courrier vous informant comment récupérer votre certificat
ce courrier contient une URL, il est important de l'ouvrir avec le même navigateur, et ce sur la même machine, que celui qui a servi à faire la demande; en effet les 2 clés, la privée et la publique ont été générées par le navigateur mais seule le clé publique a été envoyé à l'AC pour création et signature du certificat

- le fait d'ouvrir cette URL installera votre certificat personnel ainsi que ceux des AC dans votre navigateur
à cette étape le navigateur vous demandera (si cela n'a pas déjà été fait) d'initialiser le mot de passe pour protéger vos certificats

master password

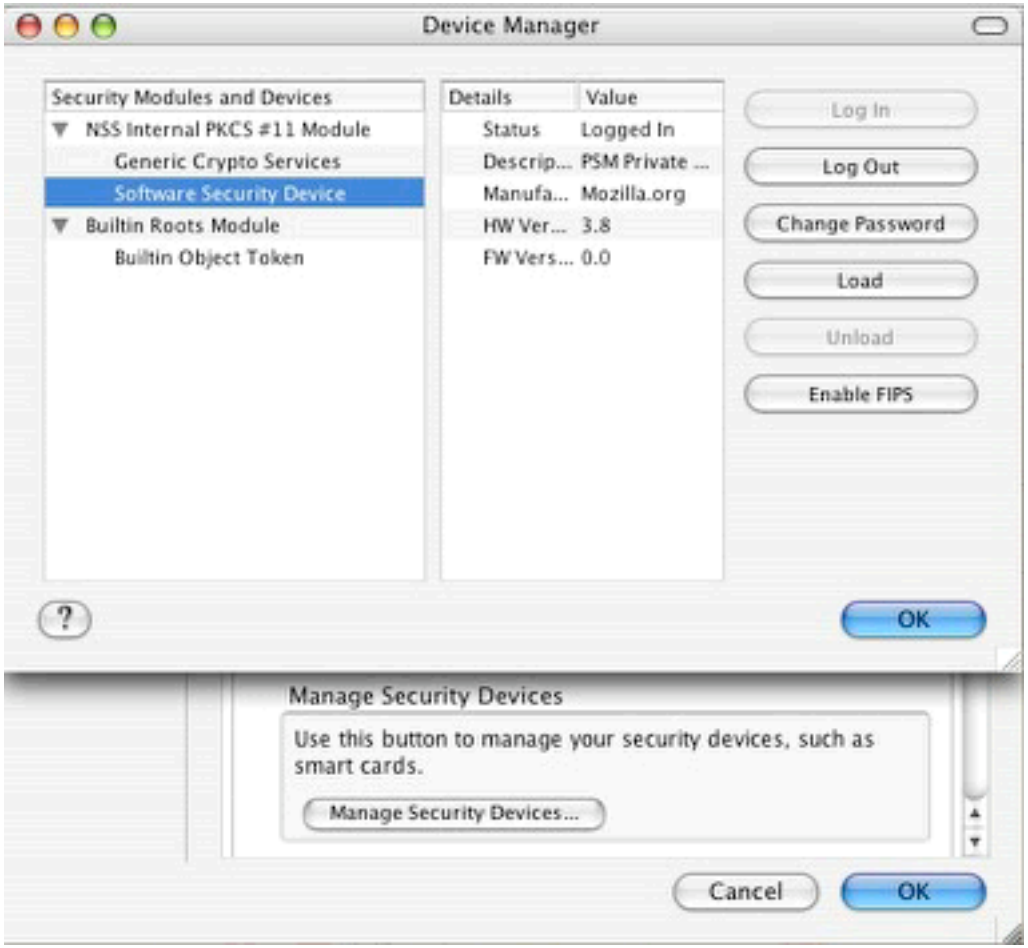
- vérifier aussi le réglage de quand vous est demandé le mot de passe, le préférable est à chaque fois que vous en avez besoin
- malheureusement cette fonctionnalité n'existe pas dans "Firefox"

master password



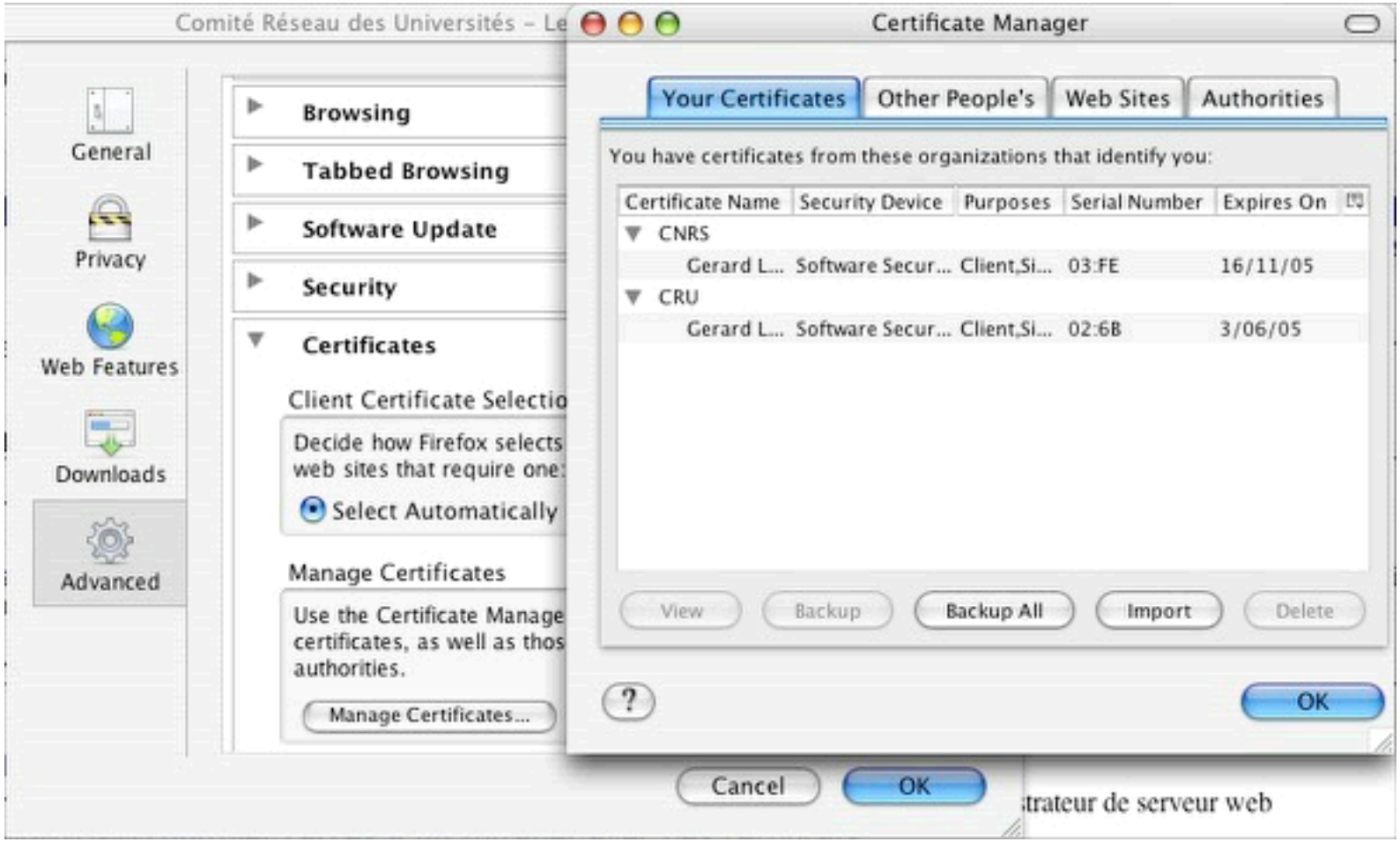
- il est possible, aussi, de faire ce réglage en utilisant l'URL interne "about:config"; ce qui devrait permettre de faire ce réglage dans "Firefox", mais cela ne semble pas vouloir fonctionner

master password

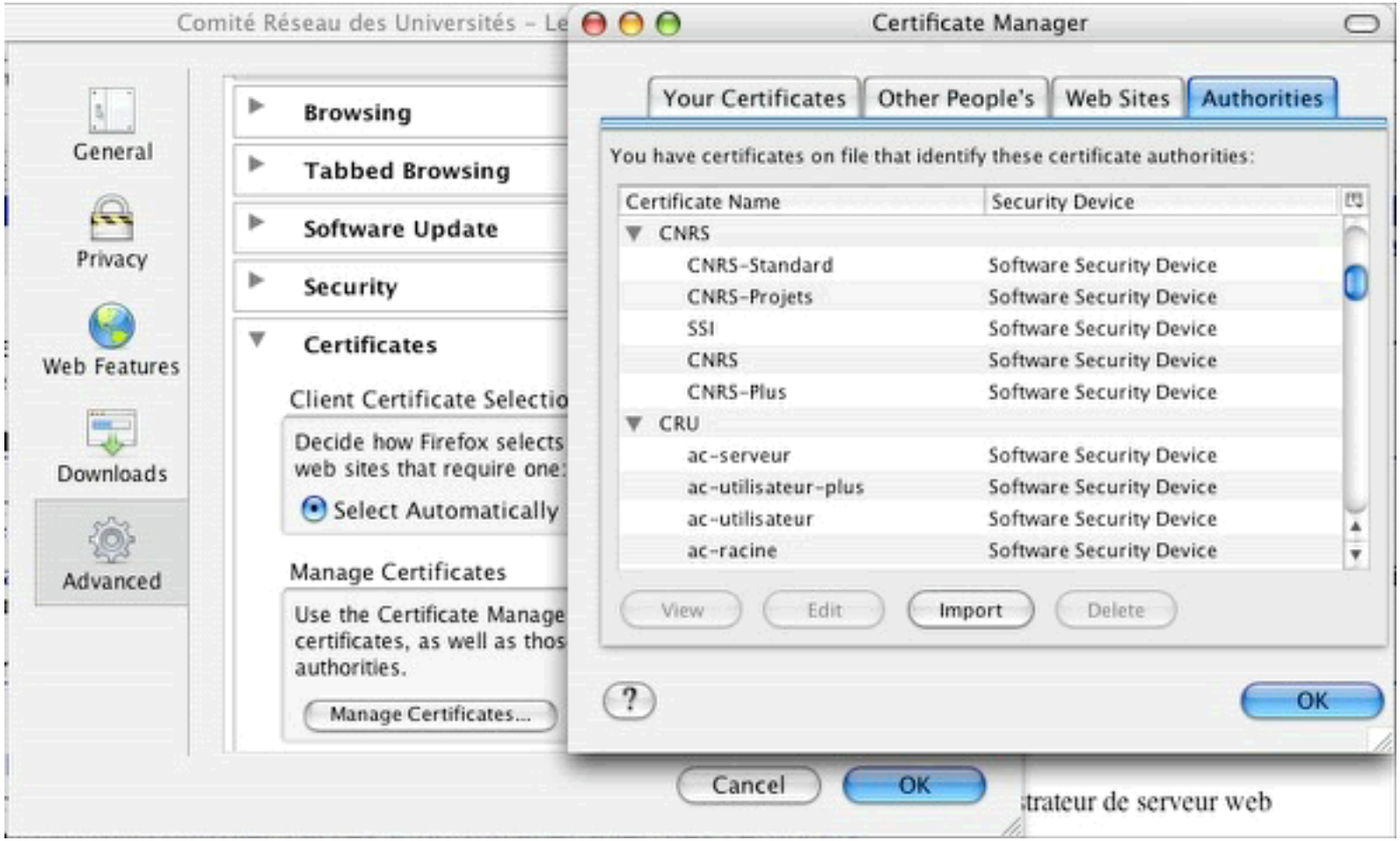


- une solution est d'utiliser

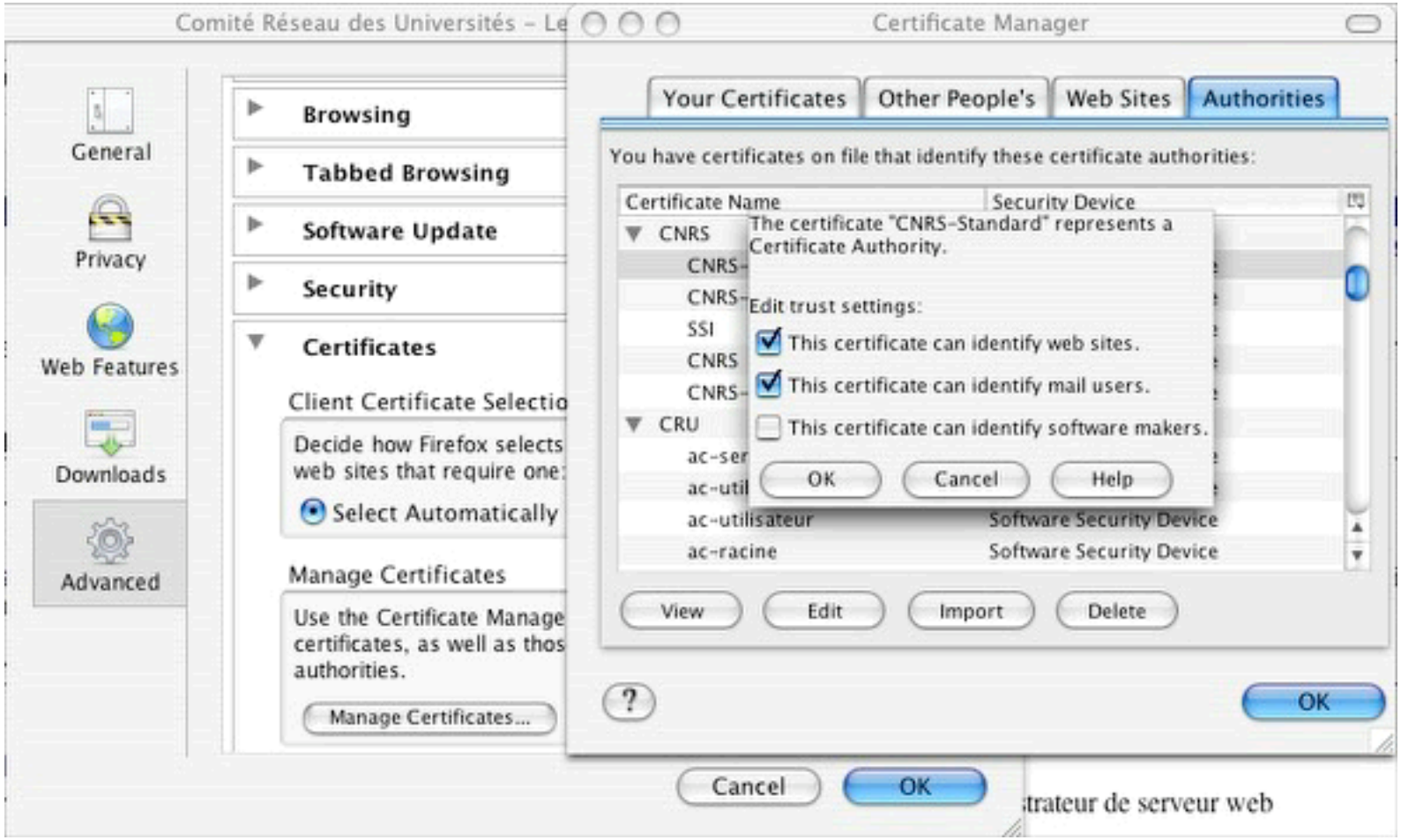
voir votre certificat personnel



voir les certificats des AC

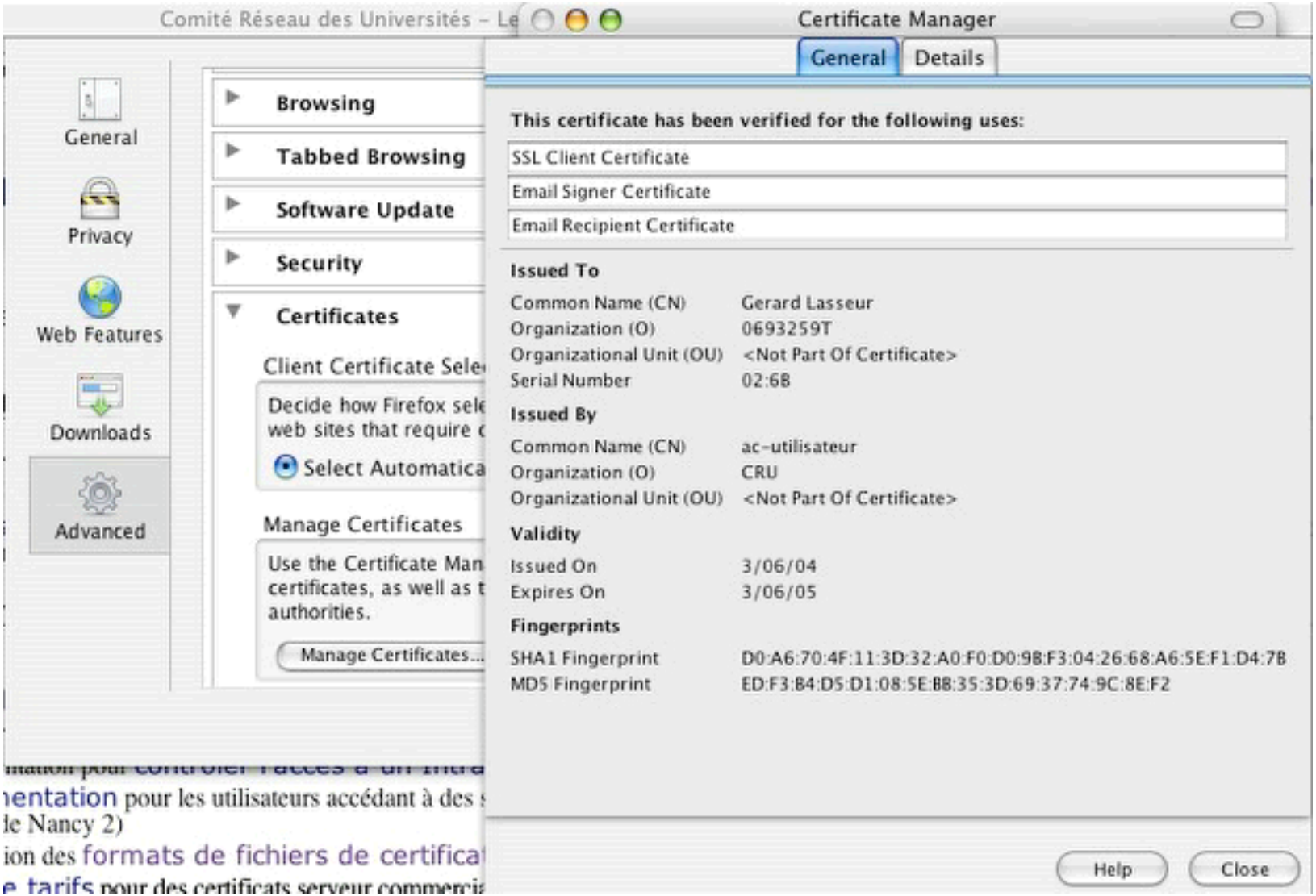


voir et modifier la confiance aux AC

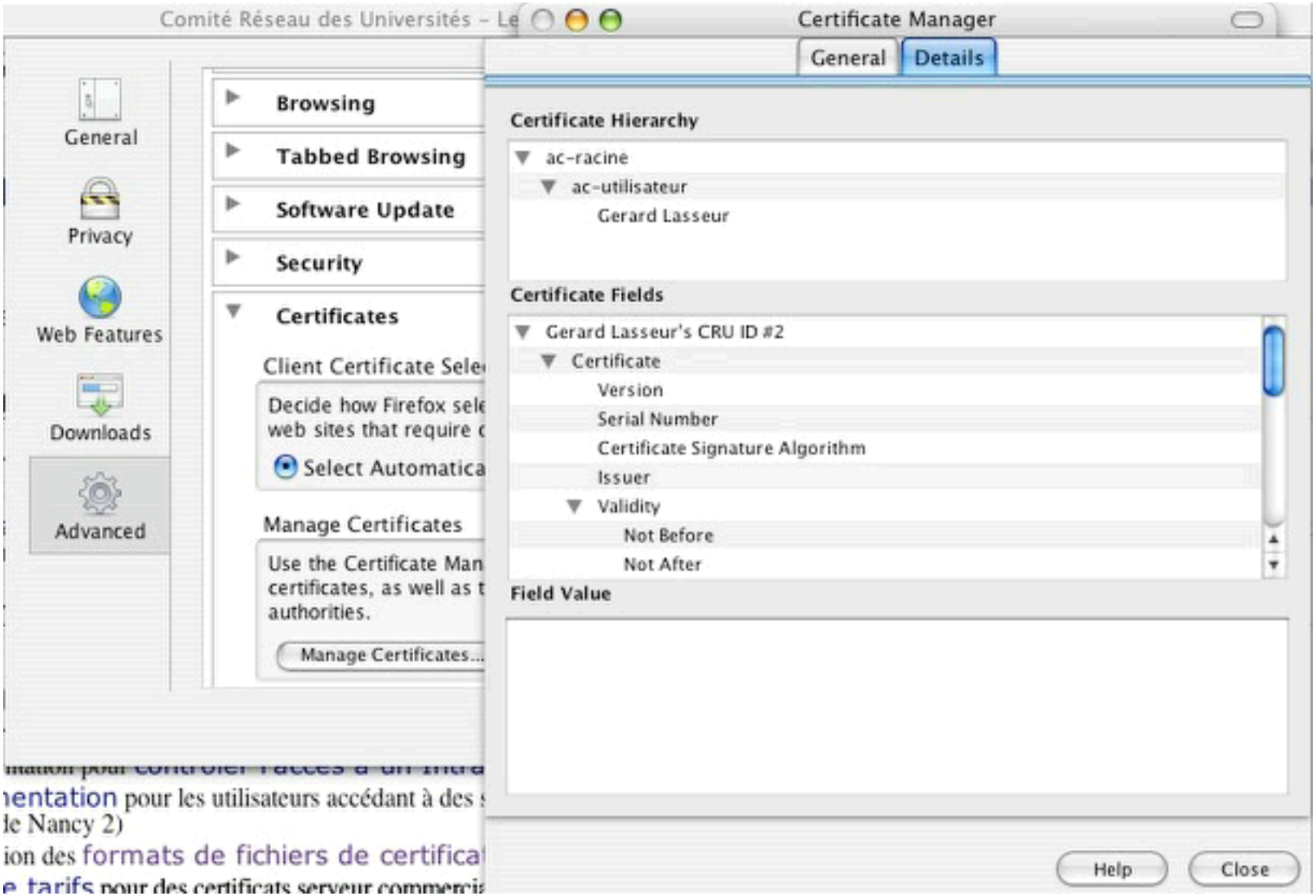


- après cette étape vous pourrez voir la confiance accordé à votre certificat, ses utilisations ainsi que sa chaîne de certification

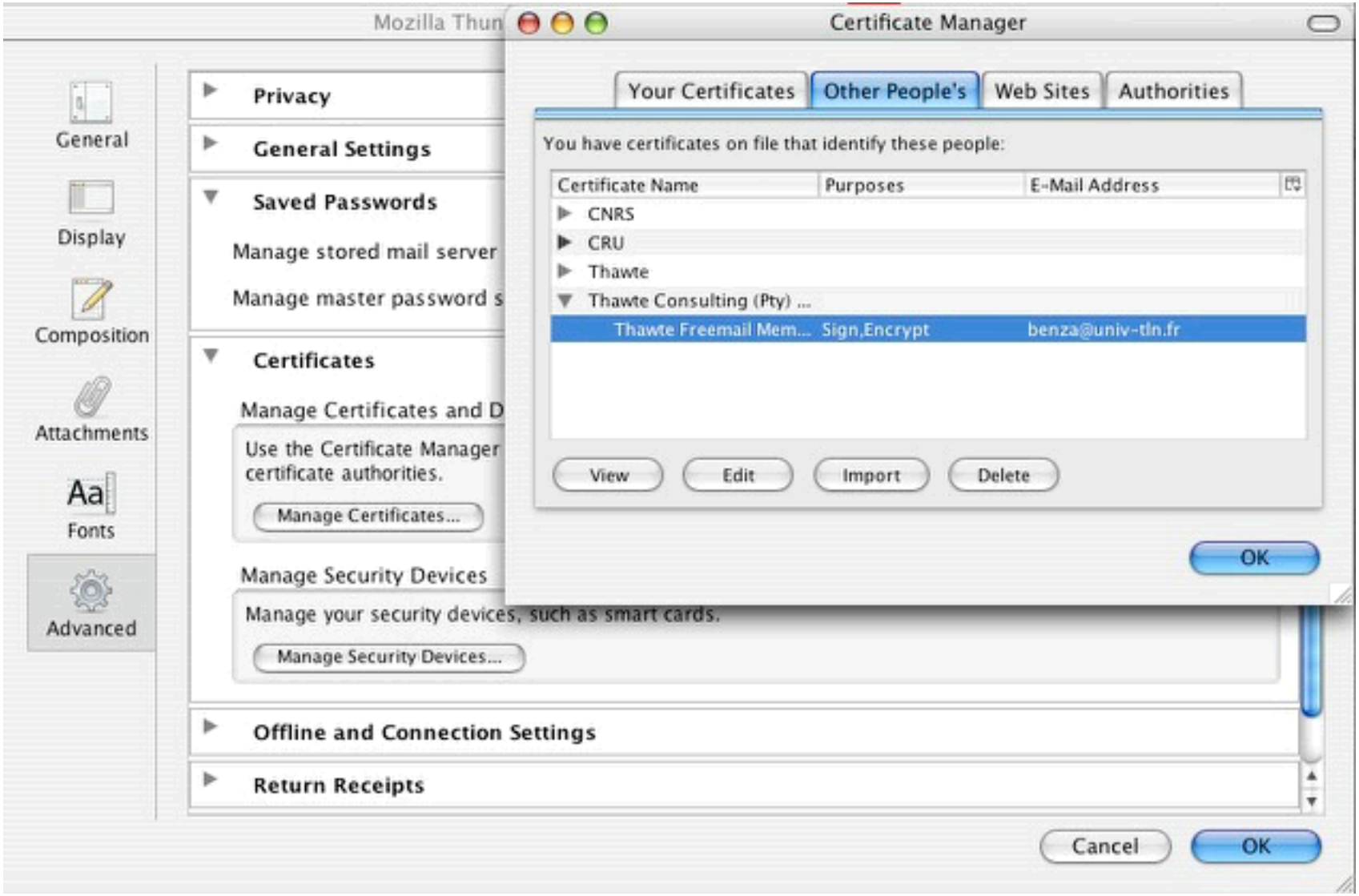
confiance et utilisations



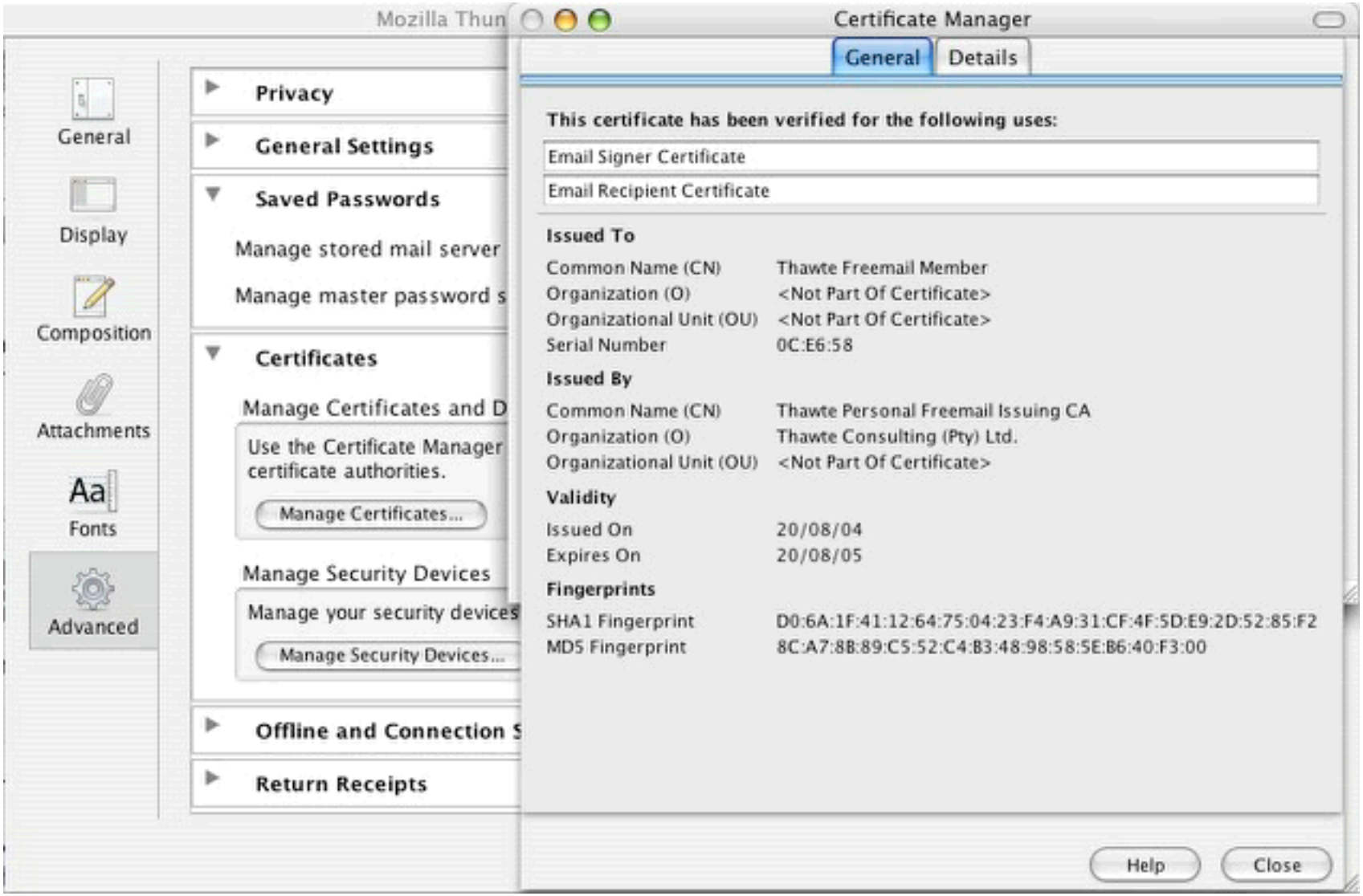
chaîne de certification



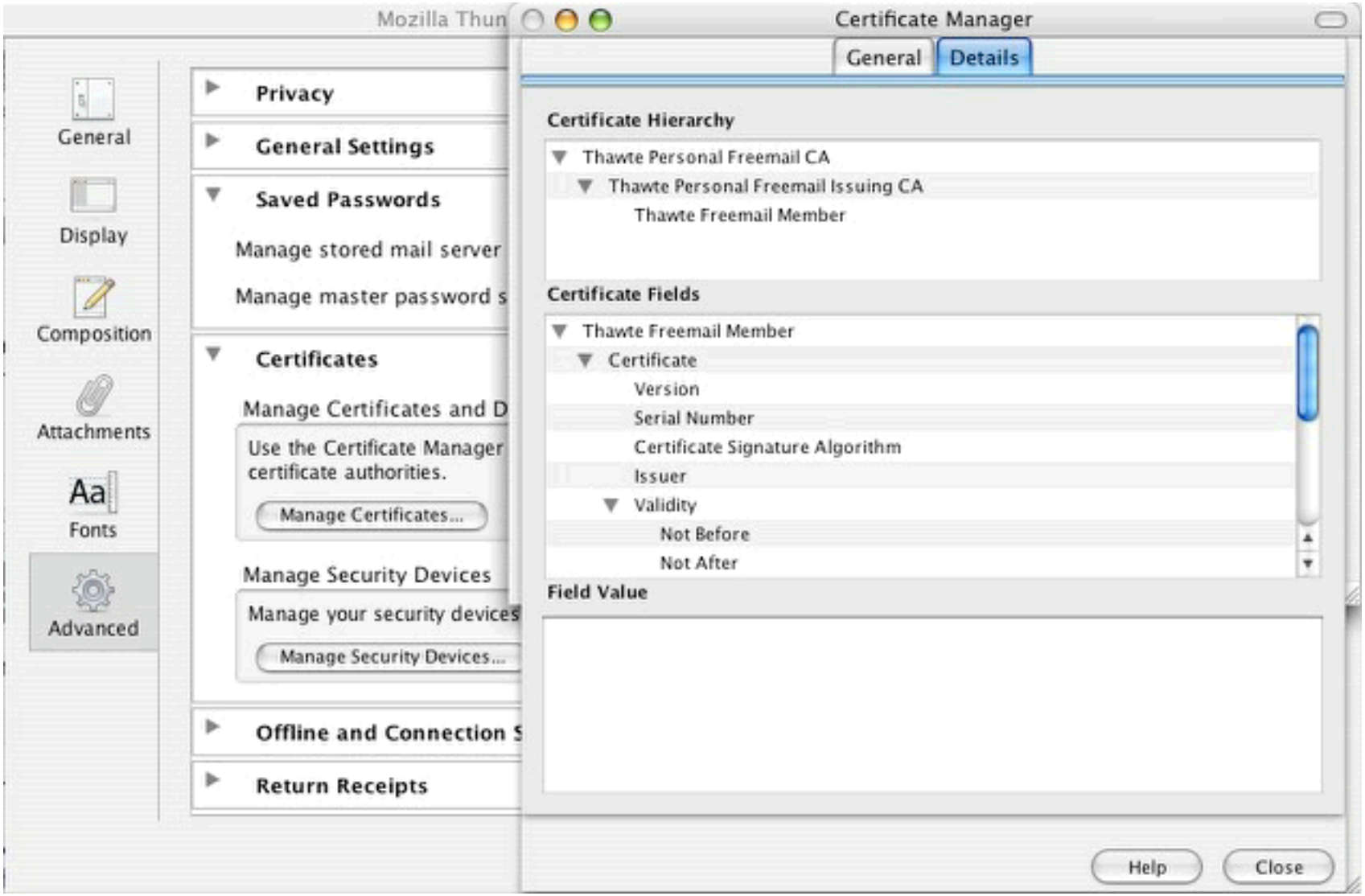
les certificats de vos correspondants



les certificats de vos correspondants



les certificats de vos correspondants



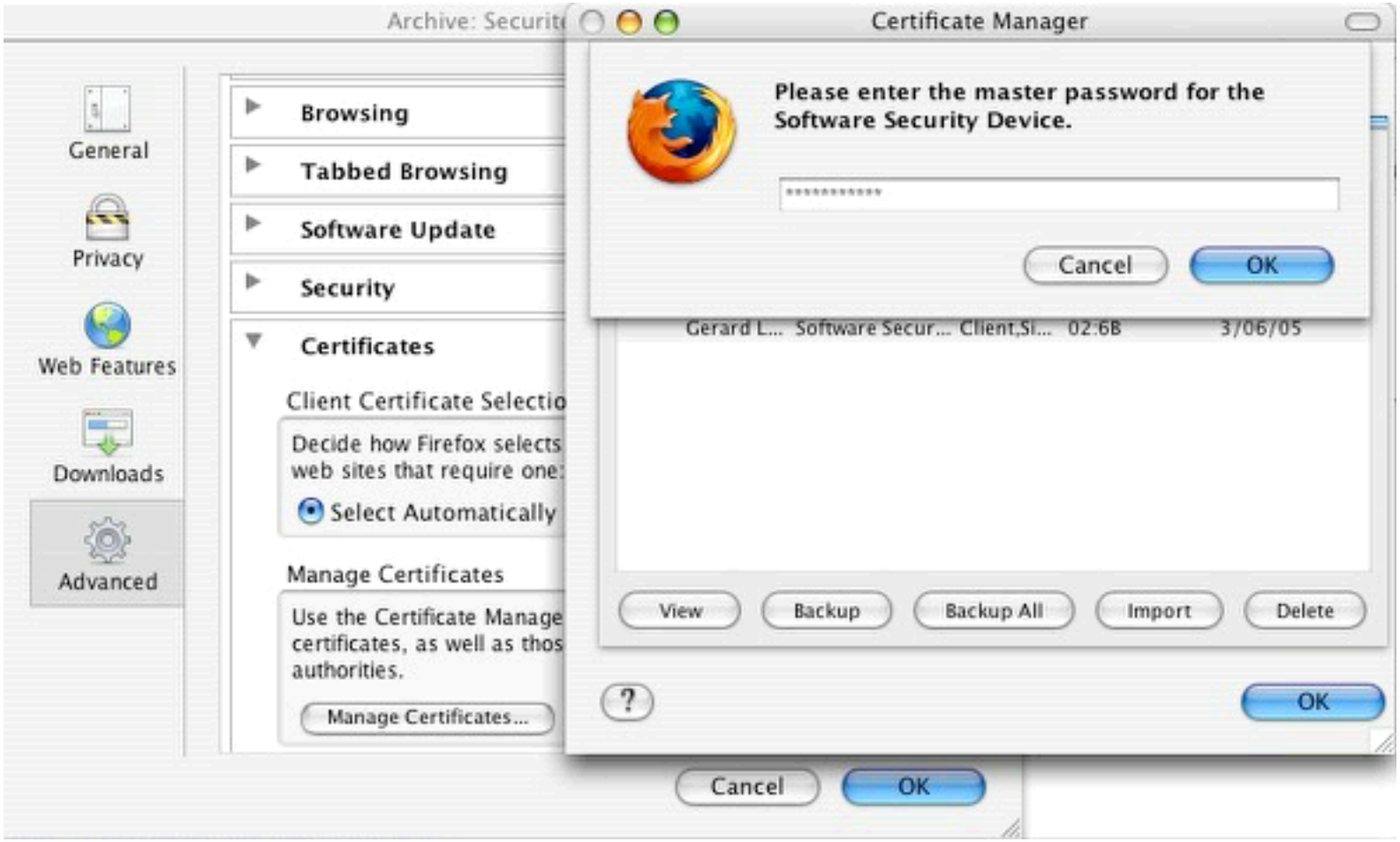
ensuite ... que faire ?

- **le certificat est dans le navigateur**

Il faut donc l'exporter pour pouvoir l'installer dans d'autres applications :
- autre navigateur
- outils de messagerie

ou sur d'autres ordinateurs, mais faire attention de ne pas l'oublier ...

exporter votre certificat personnel



- le mot de passe qui est demandé ici est celui du navigateur (initialisé à l'étape précédente) qui protège l'ensemble de vos certificats personnels

exporter votre certificat personnel

- le mot de passe demandé ici est celui qui protégera le fichier (.p12 PKCS#12) dans lequel sera stocké votre ou vos certificats personnels (contient la ou les clés privées)

utilisation de mon certificat PKCS12

- **l'application connaît le format PKCS#12**

  Le certificat peut donc être importer ou installer directement dans ces applications

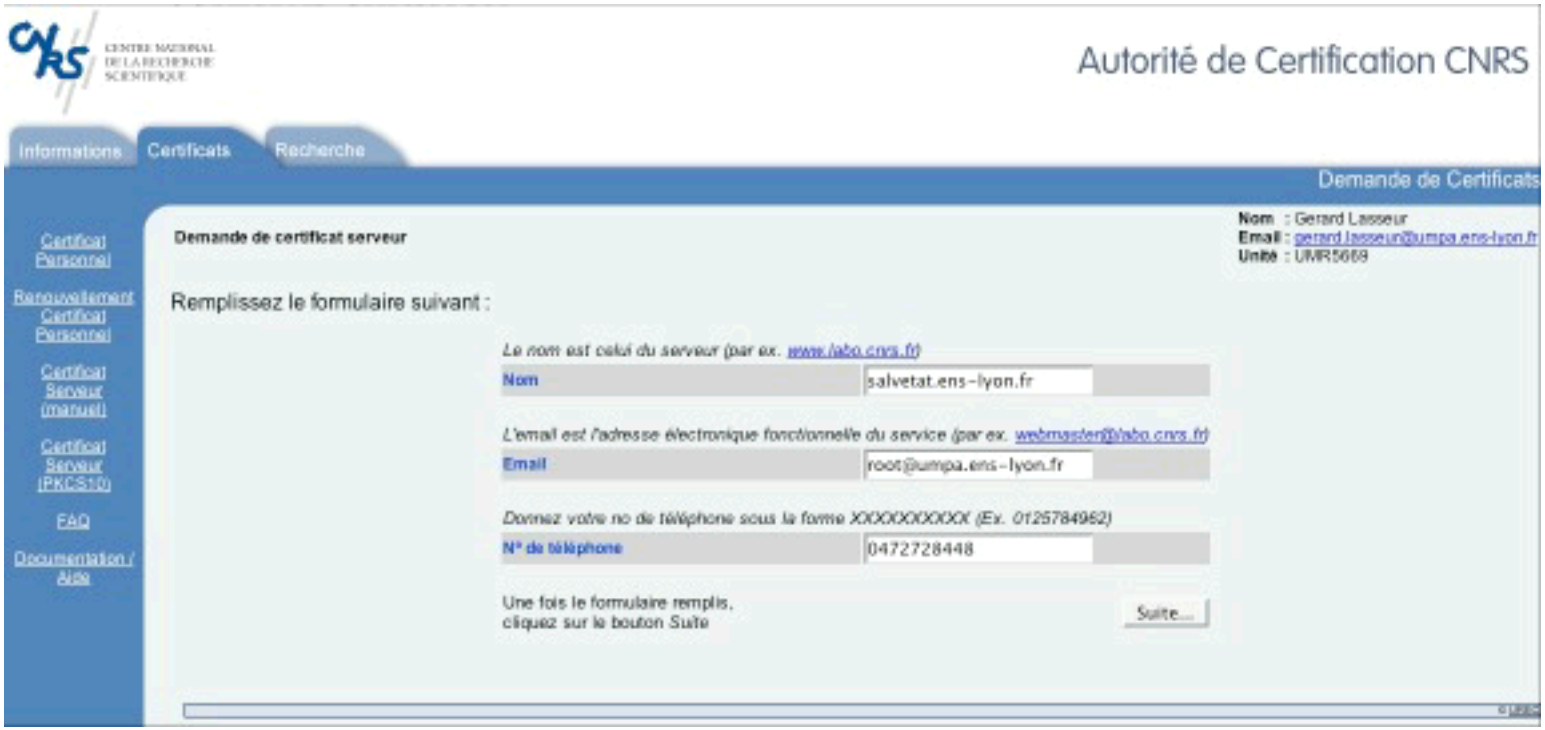
- **ne connaît pas le format PKCS#12**

```
openssl pkcs12 -in uncert.p12 \
        -clcerts -nokeys        -out uncert.crt     # le certificat
ou
        -nocerts [ -nodes ]*    -out uncert.key     # la clé privée protégée ou non par mot de passe
ou
        -clcerts  [ -nodes ]*   -out uncert.pem     # le certificat et la clé privée protégée ou non par mot de passe
ou
        -cacerts -nokeys        -out CA.crt         # la chaîne de certificats ou le certificat de(s) CA

Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

*ATTENTION : option totalement interdite avec un certificat de personne

demander un certificat de service

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html



- ici pas de numéro d'unité à fournir car au moment de la connexion à cette page votre certificat personnel a été utilisé pour vous identifié

- si vous n'en possédez pas vous ne pourrez pas demander un certificat de service

demander un certificat de service

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html

- confirmation par courrier comme pour un certificat de personne puis, récupération de 2 fichiers par courrier signé et crypté:
  - machine.crt le certificat et la clé publique
  - machine.key la clé privée en clair

machine = nom du serveur rentré dans le champ Nom du formulaire

créer une requête PKCS10

openssl req -new -out umpa.csr -keyout umpa.key [-nodes]

Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'umpa.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
---

créer une requête PKCS10

Country Name (2 letter code) [AU]:**FR**
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) []:.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**CNRS**
Organizational Unit Name (eg, section) []:**UMR5669**
Common Name (eg, YOUR name) []:**www.umpa.ens-lyon.fr**
Email Address []:**root@umpa.ens-lyon.fr**

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

créer une requête PKCS10

cat umpa.csr

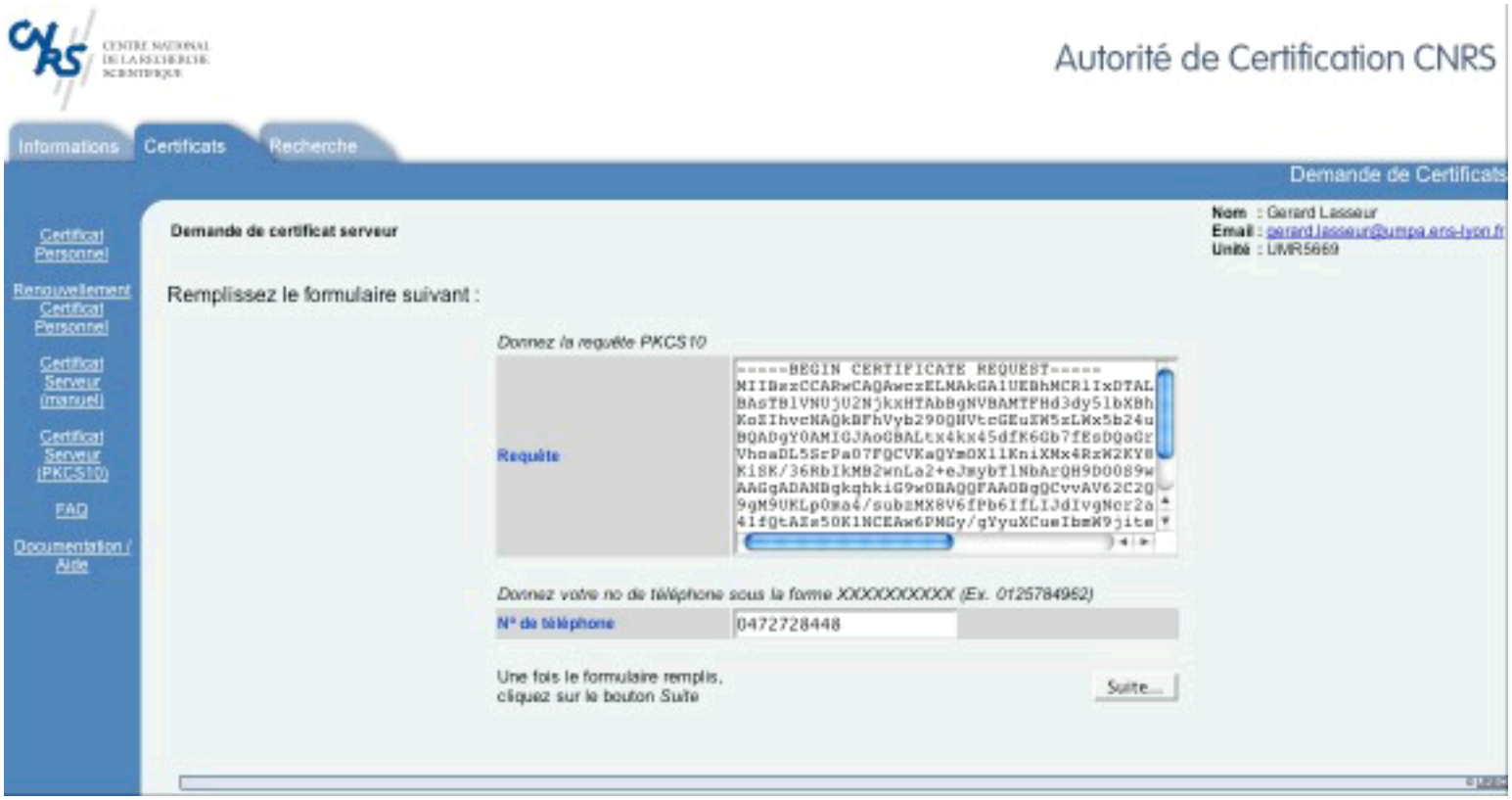
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBszCCARwCAQAwczELMAkGA1UEBhMCRlIxDTALBgNVBAoTBENOUlMxEDAOBgNV
BAsTB1VNUjU2NjkxHTAbBgNVBAMTFHd3dy51bXBhLmVucy1seW9uLmZyMSQwIgYJ
KoZIhvcNAQkBFhVyb290QHVtcGEuZW5zLWx5b24uZnIwgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBALtx4kx45dfK6Gb7fEsDQaGrI50sWMz1ODVsZJivL+L1JooC
VhoaDL5SrPa07FQCVKaQYmOXllKniXMx4RzW2KY86tkntUI96Pv2bWrDYsNviRux
KiSK/36RbIkMB2wnLa2+eJmybT1NbArQH9DO0S9wcMIG7uUtPsr+jKqGo/fFAgMB
AAGgADANBgkqhkiG9w0BAQQFAAOBgQCvvAV62C2QRfW2Xv1l9TZAQA7534OE0I5e
9gM9UKLp0ma4/subzMX8V6fPb6IfLIJdIvgNcr2aDEALYmJKkYA5zd8bMVVnO5dN
41fQtAZs50K1NCEAw6PMGy/gYyuXCueIbmW9jiteSxLRCKl+0u15za336Nie7+bO
oaB9O7bXRg==
-----END CERTIFICATE REQUEST-----
```

copier toutes les lignes entre et incluant :

```
-----BEGIN CERTIFICATE REQUEST----
-----END CERTIFICATE REQUEST-----
```

demander un certificat de service

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html



et les coller dans ce formulaire

demander un certificat de service

http://igc.services.cnrs.fr/CNRS-Standard/certificats.html

- confirmation par courrier comme pour un certificat de personne puis, récupération de 1 fichier par courrier signé et crypté:

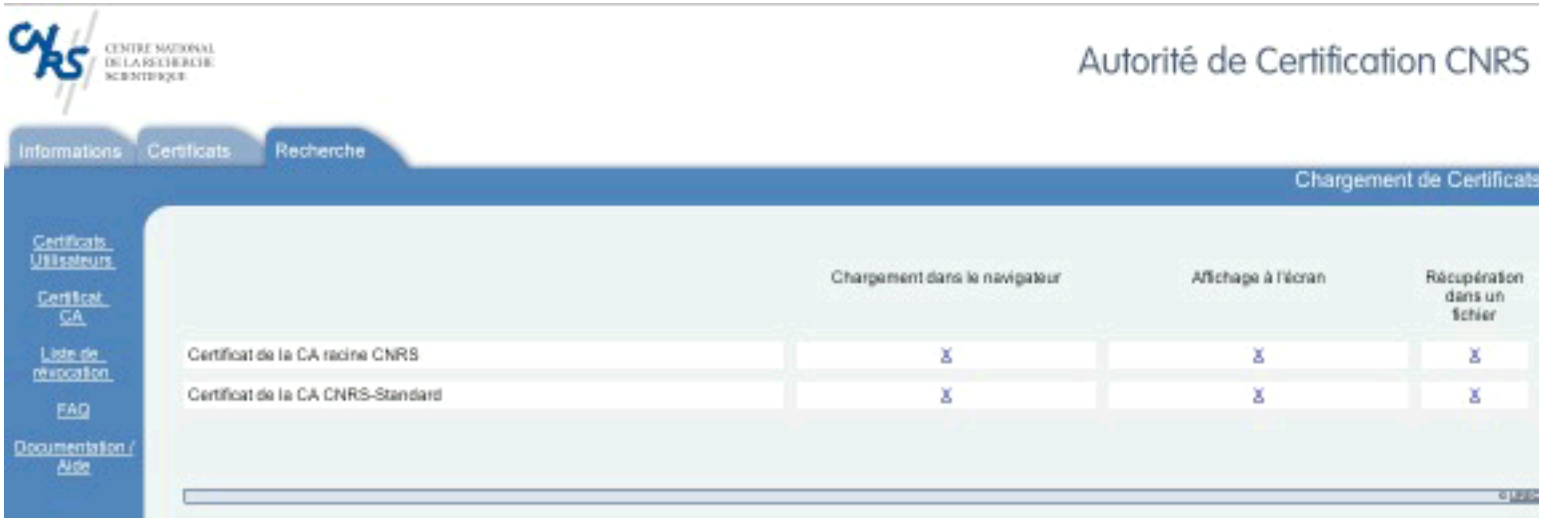
• machine.crt le certificat et la clé publique

machine = nom du serveur rentré dans Common Name (eg, YOUR name)

- la clé privée se trouve dans le fichier : machine.key que vous avez créé avec openssl

les certificats des CA

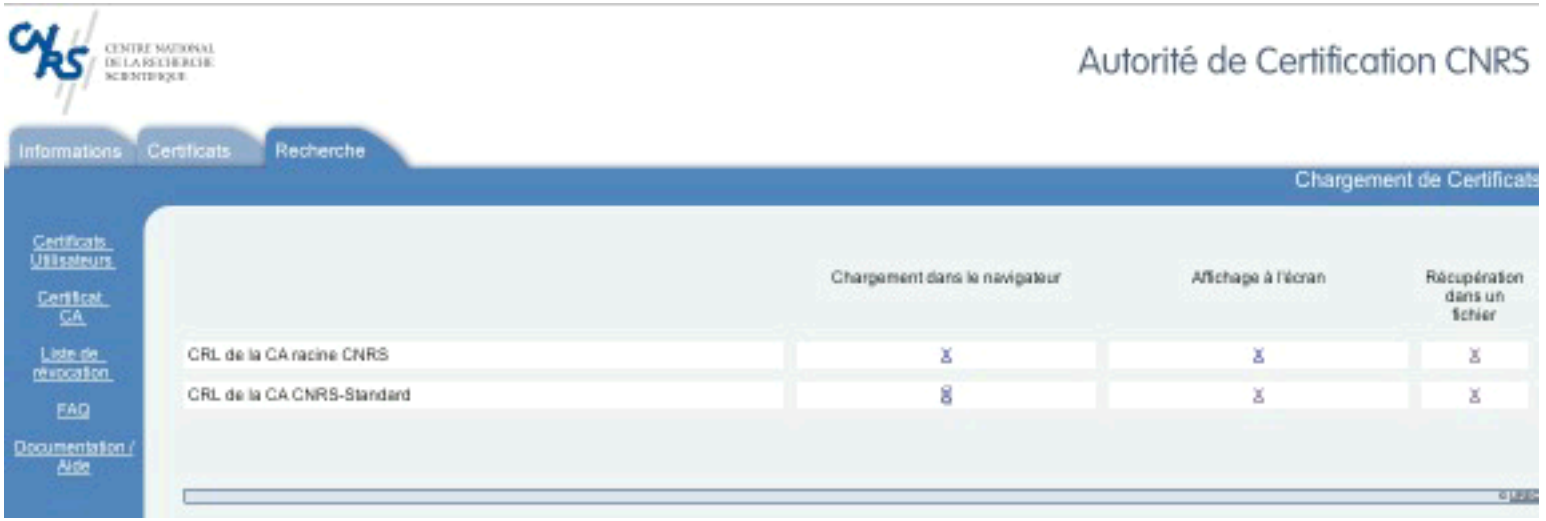
http://igc.services.cnrs.fr/igc/CNRS-Standard/recherche.html



- récupération des certificats des CA :
  - CNRS.crt
  - CNRS-Standard.crt

les listes de révocations des CA

http://igc.services.cnrs.fr/igc/CNRS-Standard/recherche.html



- récupération des listes de révocations des CA :
  - CNRS.crl
  - CNRS-Standard.crl

installer un certificat de service

```
cp machine.crt conf/ssl.crt/                                  # apache
cp machine.key conf/ssl.key/
chmod u=r conf/ssl.key/machine.key*
cp CA.crt conf/ssl.crt
cp CA.crl conf/ssl.crl

cat machine.crt machine.key > ssl/certs/service.pem           # imaps, pops
chmod u=r ssl/certs/machine.pem*
```

*ces fichiers contiennent la clé privée en "clair" (ce qui est normal, sinon il faudrait donner le mot de passe de la clé à chaque démarrage du service), il faut donc les protégés en limitant l'accès en lecture

installer un certificat de service

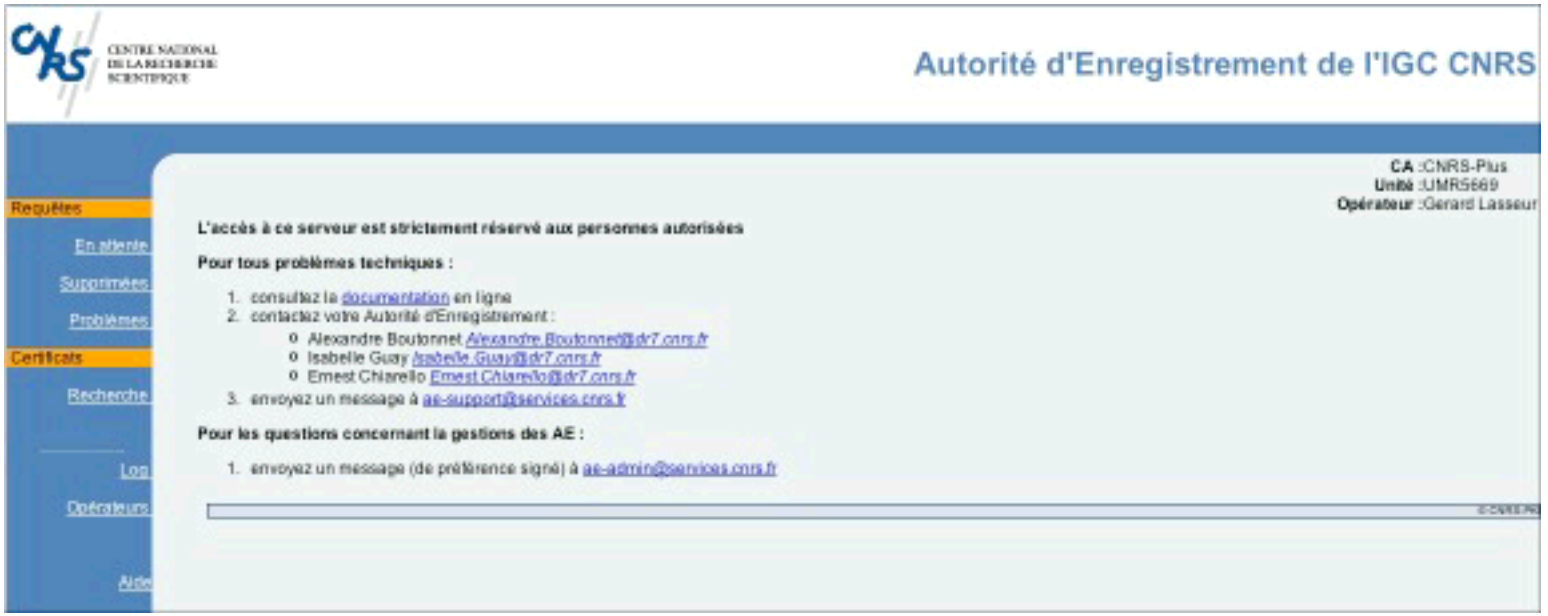
```
openssl pkcs12 -export \                                    # tomcat
      -in service.pem [ -name service ] \
ou
      -in machine.crt -inkey machine.key [ -name service ] \

et (éventuellement)
                  -CAfile CA.crt -chain [ -caname root ] \
            ou
                  -CApath répertoire -chain [ -caname root ... ]* \
-out service.p12
```

Enter Export Password:
Verifying - Enter Export Password:

*autant de fois qu'il y a de certificats de CA et dans l'ordre montant de la hiérarchie: du bas vers la racine (exemple : -caname CNRS-Standard -caname CNRS)

du coté AE au CNRS

https://ra.services.cnrs.fr/



du coté AE au CNRS

https://ra.services.cnrs.fr/

- dans la rubrique *Opérateurs* on peut voir ici que les AE (du CNRS) semblent être aussi considérées comme des OC (Opérateur de Certification)

du coté AE au CNRS

https://ra.services.cnrs.fr/

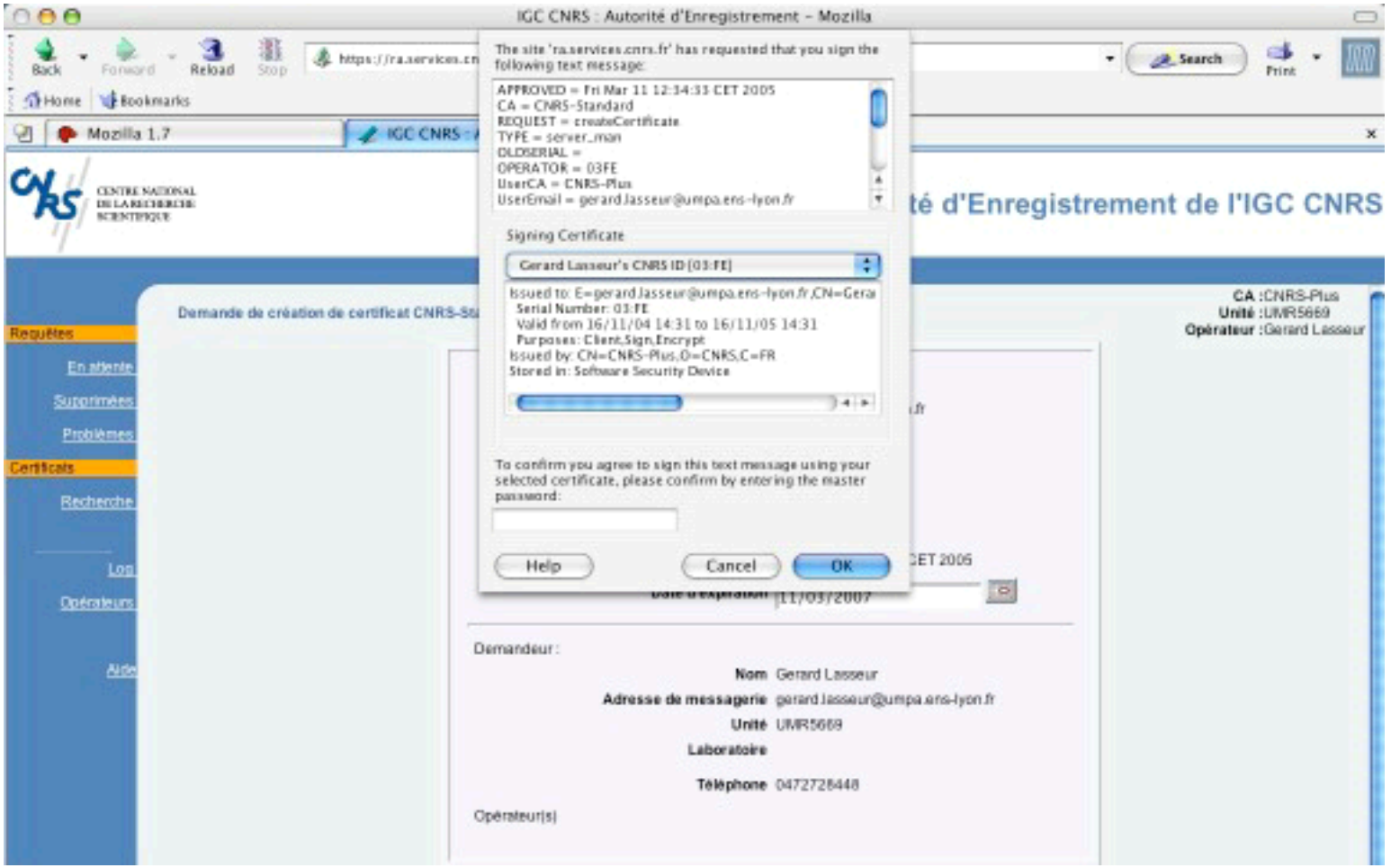
- dans la rubrique *En attente* vous pouvez consulter la liste des requêtes

du coté AE au CNRS

https://ra.services.cnrs.fr/

du coté AE au CNRS

https://ra.services.cnrs.fr/



du coté AE au CNRS

https://ra.services.cnrs.fr/

- la rubrique *Log* vous permets de consulter la liste des certificats que vous avez autorisés

aux dernières nouvelles

Principe Déploiement IGC-CNRS

- Depuis Mars 2004
  - Équipe logicielle (UREC),
  - Administrateurs IGC et Exploitation (DSI),
  - Support (DSI)
- Déploiement des certificats et support décentralisés :
  - Réaliser le support au plus près des utilisateurs
  - Répartir la charge du travail et l'appropriation du sujet.
- AE-CNRS-PLUS des Délégations Régionales :
  - Autorité Administrative (DSI depuis 09/2004)
- AE-CNRS-PLUS des laboratoires (Équipes RSI en délégations)
  - Autorité pour la délivrance des certificats CNRS-PLUS, support aux AE labos.
- AE-CNRS-STANDARD
  - Autorité pour la délivrance des certificats CNRS-Standard des personnels de leur unité, support auprès des utilisateurs

Réunion CSEC- 14 Mars 2005

aux dernières nouvelles

État du Déploiement (Fév2005)

- 2750 certificats CNRS-STANDARD valides
  - 10 Labos détiennent 25% des certificats CNRS-Standard valides.
- 400 certificats CNRS-PLUS (335 unités ont une AE)
  - Environ 1/4 des Unités CNRS ont une AE (1/5 en juin 2004)
- Toutes les Délégations ont une autorité d'enregistrement CNRS-PLUS pour les unités de leur Délégation.
- Réflexion sur l'organisation à mettre en place pour délivrer des certificats CNRS à des populations particulières (ex : personnels en détachement, à l'étranger).

Réunion CSEC- 14 Mars 2005

aux dernières nouvelles

Utilisation des Certificats CNRS

- Applications Régionales et locales
- Applications Nationales
  - Futur Proche :
    - Fin mars : nouvelle Application « Espace Chercheurs ». (accès possible certificat CNRS et user/mot de passe).
    - En cours : Étude pour la mise en place d'un accès par certificats pour d'autres applications (ex : le nouveau Labintel)
  - Futur SI (début 2007) : Accès SIG de Gestion et de Ressources humaines par Certificats
    - Accès privilégié par certificat (accès mot de passe uniquement en secours)

Réunion CSEC- 14 Mars 2005

un mot sur la sécurité

Un certificat est la carte d'identité (le passeport) qui authentifie, de façon unique, un utilisateur, une machine :

- il est donc incessible et appartient impérativement à :
  - l'utilisateur, pour un certificat de personne,
  - la machine, pour un certificat de service,

pour qui il a été demandé et puis attribué;

- il faut donc, aussi, veiller à ce que seul son propriétaire (pour un certificat de personne) soit en mesure de l'utiliser :
  - ne pas en laisser le libre accès en le protégeant avec un mot de passe "solide",
  - ne pas l'essaimer, l'installer uniquement dans les applications que vous utilisez régulièrement sur une machine "sure",
  - si vous devez l'utiliser, temporairement, dans une autre application et/ou sur une autre machine, effacez le immédiatement (de manière irréversible) dès que vous n'en avez plus besoin;
- pour un certificat de service vérifier que la clé privée n'est accessible en lecture que par le(s) serveur(s) qui l'utilise(nt).

un mot sur la sécurité

- **séquestre des clés**

Le CNRS n'assure aucun service de séquestre de clé privée, en cas de perte :
- du mot de passe qui la protège ou de celui qui protège le magasin de certificats
- du fichier la contenant

le certificat est irrémédiablement perdu et doit être immédiatement révoqué

- **compromission**

Si vous pensez que l'un de vos certificats a pu être compromis :
- oubli de votre certificat personnel sur une machine " étrangère "
- soupçon que quelqu'un a pu utiliser votre certificat
- accès frauduleux ou piratage d'une de vos machines sur laquelle est installée la clé privée, sans mot de passe, d'un certificat de service

il faut alors impérativement, et ce dans les plus brefs délais, faire révoquer ce(s) certificat(s)

La demande de révocation se fait auprès de votre AE

Enfin la ~~faim~~ fin

- **Démonstration(s)**

  Demande et installation d'un certificat :
  - de personne
  - de service

- **Question(s)**

  Ou vice-versa