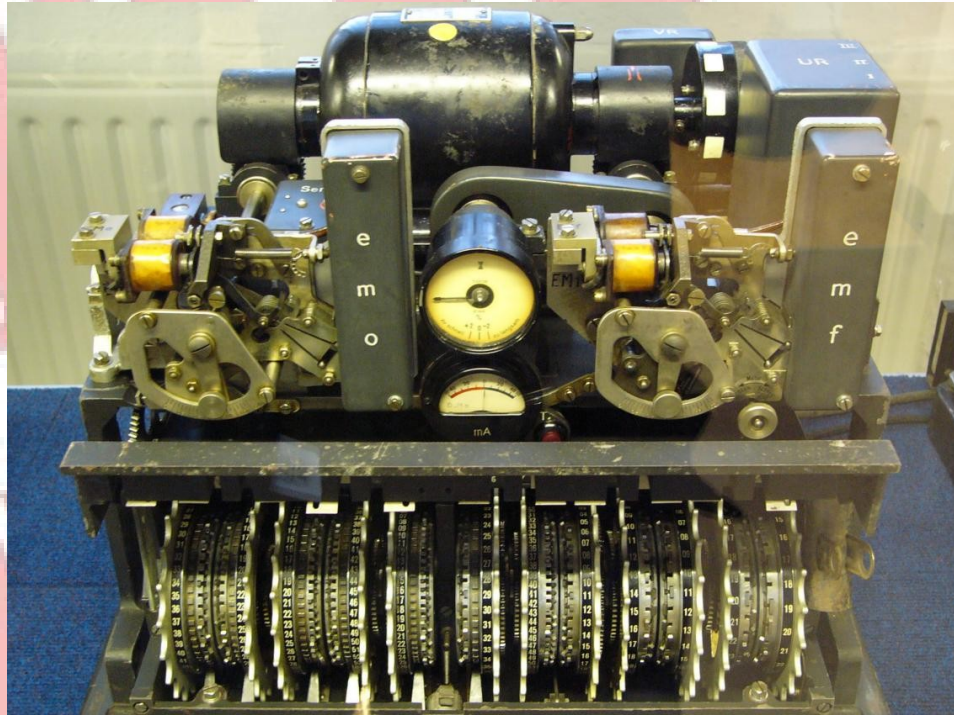


Cryptographie et sécurité informatique



La machine de Lorenz était utilisée pour chiffrer les communications militaires allemandes de haute importance pendant la Seconde Guerre Mondiale

Sommaire

La cryptographie

.....symétrique

.....asymétrique

La signature numérique

La fonction de hachage

OpenSSL

Le certificat électronique

L'Autorité de Certification (AC)

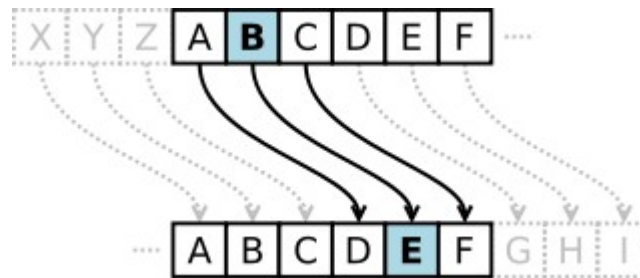
Serveurs sécurisés (HTTPS/SSL)

Les certificats dans le navigateur Mozilla

Le certificat personnel

La cryptographie **symétrique** (ou cryptographie à clé secrète)

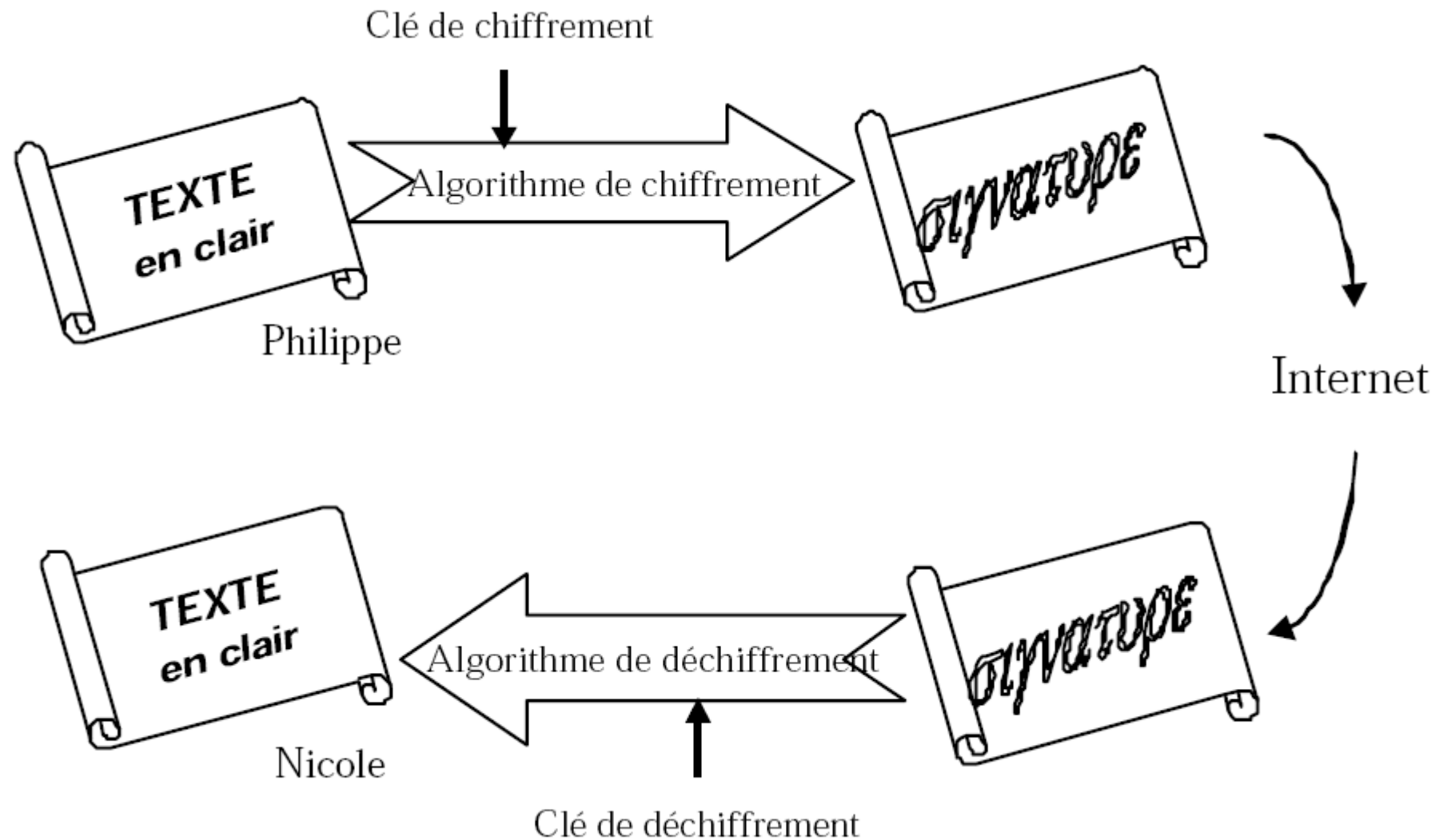
Exemple: le chiffrier de Jules César (substitution)



clé – une information devant permettre de chiffrer et de déchiffrer un message et sur laquelle peut reposer toute la sécurité de la communication

ALICE DOLFH

Communication chiffré avec algorithme **symétrique**



La cryptographie **asymétrique** (ou cryptographie à clé publique)

La fonction à sens unique - **peut être aisément calculée, mais difficile à inverser**

$$y = f(x)$$

$$x = f^{-1}(y)$$

Exemple: le problème de la factorisation

Soit deux nombres premiers p et q . Calculer $x = pq$ est facile, même si p et q sont très grand. Par contre, retrouver p et q à partir de x est irréalisable en pratique, si q et p sont suffisamment grands.

Fonctions (clé publique) à brèche secrète, qui leur permet de revenir facilement en arrière, par exemple en utilisant une clé privée.

en plus...

Le mécanisme d'authentification garantit la provenance des informations chiffrée.

$$x = f^{-1}(f(x))$$

L'algorithme asymétrique de cryptographie à clé publique **RSA** (Rivest, Shamir, Adleman)

Création des clés

- on choisit **p** et **q** deux nombres premiers distincts
- on note **n** leur produit, appelé module de chiffrement: **$n = pq$**
- on calcule l'indicatrice Euler de **n**: **$\Phi(n) = (p-1)(q-1)$**
- on choisit **e** un entier premier avec **$\Phi(n)$** , appelé exposant de chiffrement
- comme **e** est premier avec **$\Phi(n)$** , on obtient d'après la théorème de Bachet de Méziriac, qu'il est inversible module **$\Phi(n)$** , i.e. il existe un entier **d** tel que **$ed \equiv 1 \pmod{\Phi(n)}$** .
d est l'exposant de déchiffrement

Le couple **(n,e)** est appelé clé publique alors que le couple **(n,d)** est appelé clé privée.

Exemple: A veut envoyer un message chiffré à B

chiffage

déchiffrage

soit le message "entier" $m < n$

ciffré en:

$$c = m^e \pmod n$$

$$m = c^d \pmod n$$

A envoie le message chiffré à B



A



B

(n,e) clé publique de B

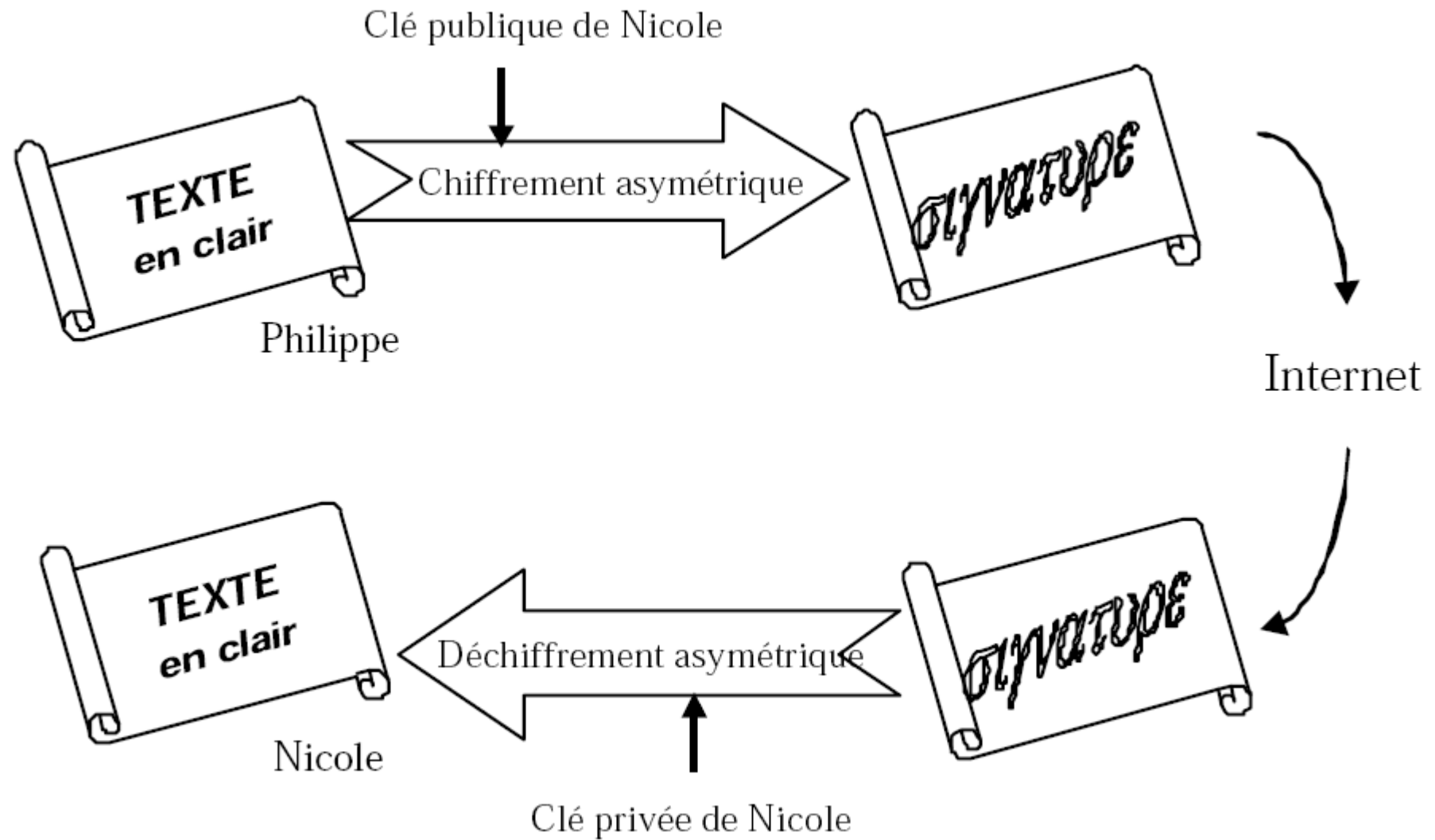
(n,e) clé publique

A obtien la clé publique de B

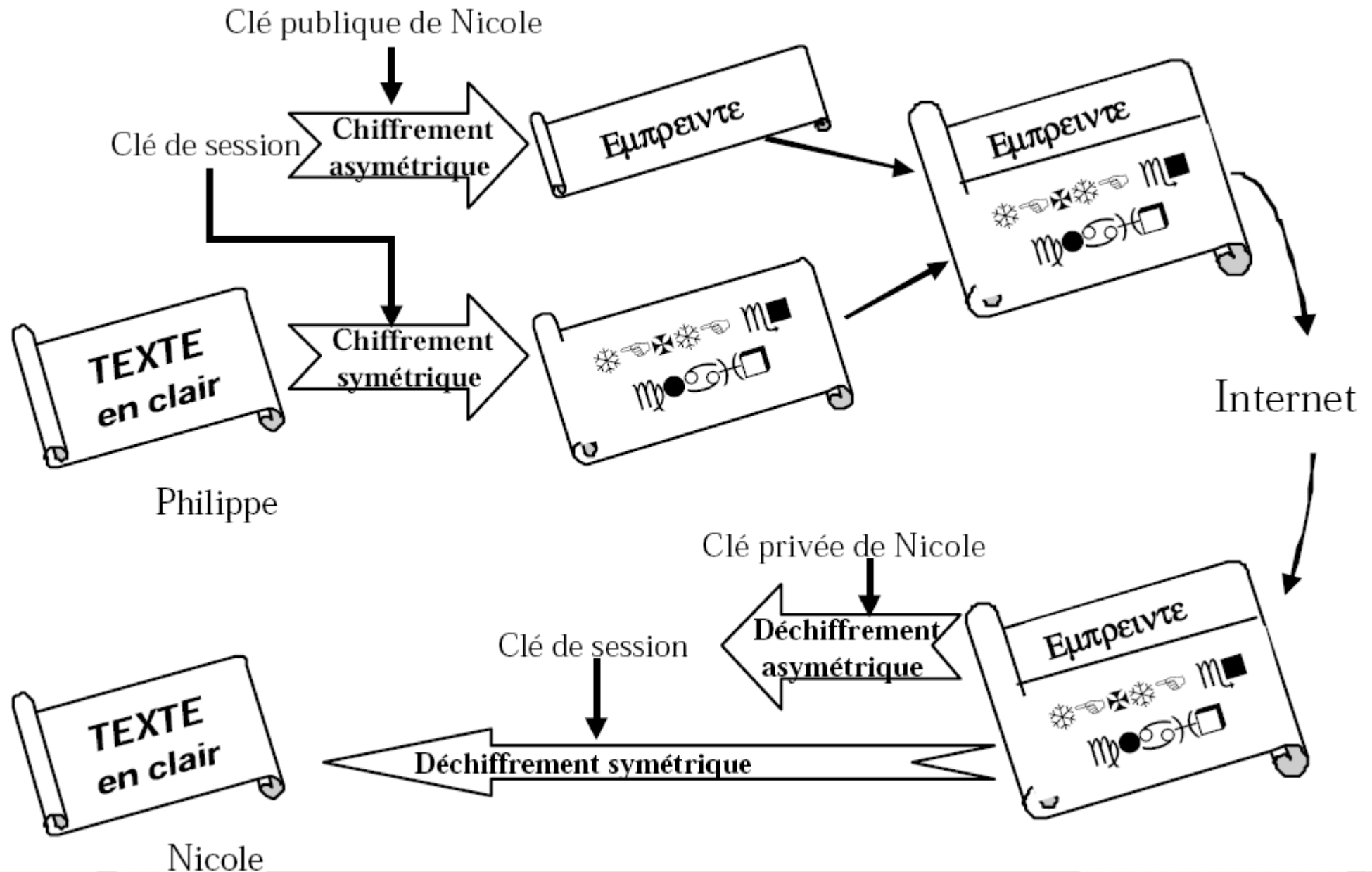
(n,d) clé privée

Communication chiffré avec algorithme **asymétrique**

8



Chiffrement avec **clé de session** (moins coûteux en temps de calcul)



ssh, slogin, scp, ... (avec clé de session)

la machine serveur clralicep06:

`/etc/ssh/ssh_host_key` (avec le permissions `-rw-----` et chiffré)
`/etc/ssh/ssh_host_rsa_key.pub` (avec le permissions `-rw-r--r--`)

```
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAorAzrTvkERNYJwo1VEwnA+5Ct14P8Qn5+k
LvCCNHWDyMC6K2zsttB4zakMYk0sDTccbymaTFh7Poy++xSRNE/3KjFSMSGNHCzZTVHJxF
sn6eB+9ZECOo0+fgjYrmUee95KXwkJ98pHl4h6usMHQUP0qXQcVN1YB/8uFdUQsUqW0=
root@clralicep06
```

la machine client clralice07:

`/home/user/.ssh/known_host`

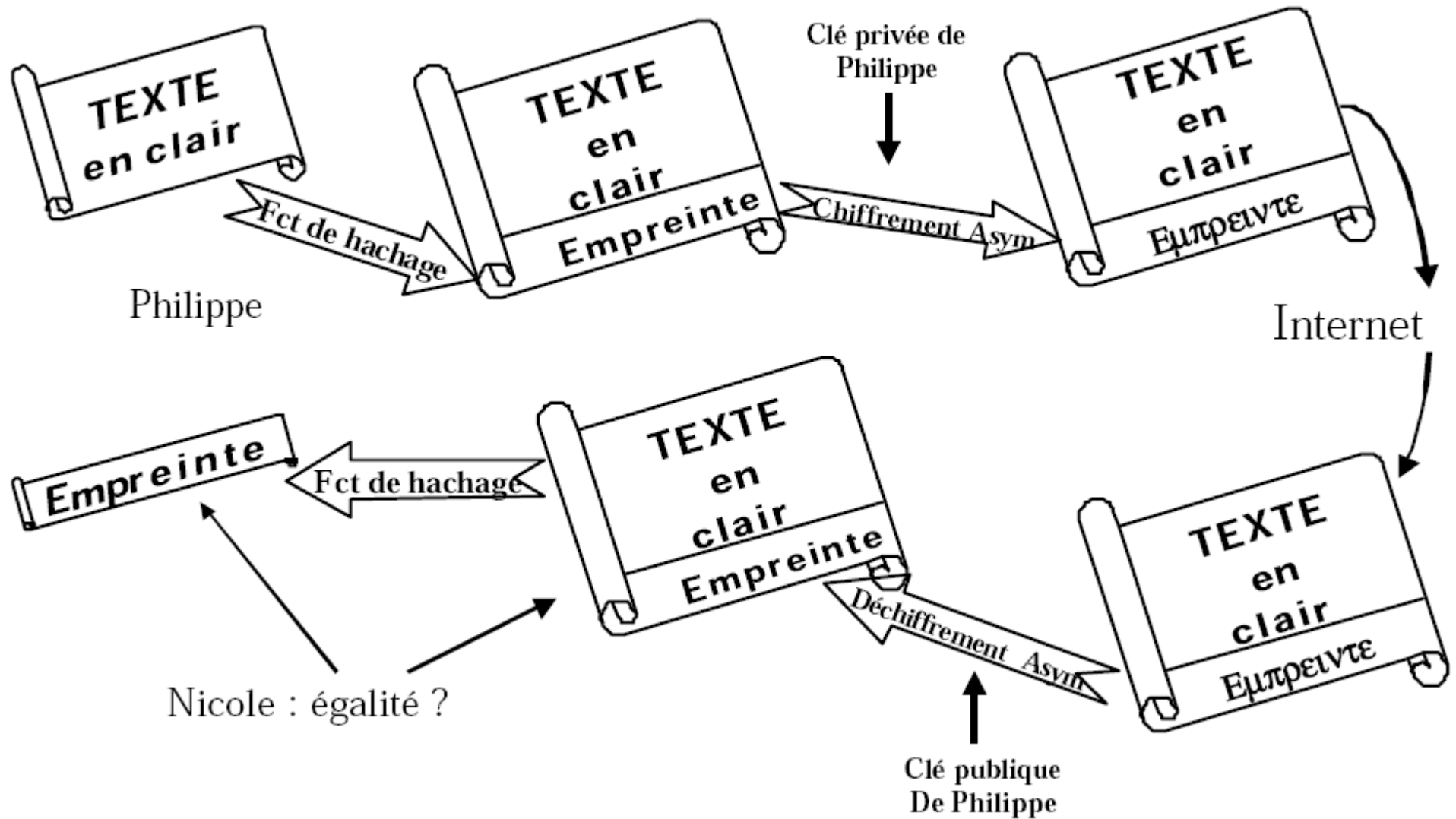
```
clralicep06,134.158.125.37 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAorAzrT
vkERNYJwo1VEwnA+5Ct14P8Qn5+kLvCCNHWDyMC6K2zsttB4zakMYk0sDTccbymaTFh7Po
y++xSRNE/3KjFSMSGNHCzZTVHJxFsn6eB+9ZECOo0+fgjYrmUee95KXwkJ98pHl4h6usMH
QUP0qXQcVN1YB/8uFdUQsUqW0=
```

La signature numérique

- **authentique** = l'identité du signataire doit pouvoir être retrouvée de manière certaine
- **infalsifiable** = quelqu'un d'autre ne peut pas se faire passer pour un autre
- **non réutilisable** = elle fait partie du document signé et ne peut être déplacée sur un autre document
- **inaltérable** = une fois un document signé, on ne peut plus le modifier
- **irévocable** = la personne qui a signé ne peut le nier

Valeur légale: depuis mars 2000, la signature numérique d'un document a en France la même valeur légale qu'une signature sur papier.

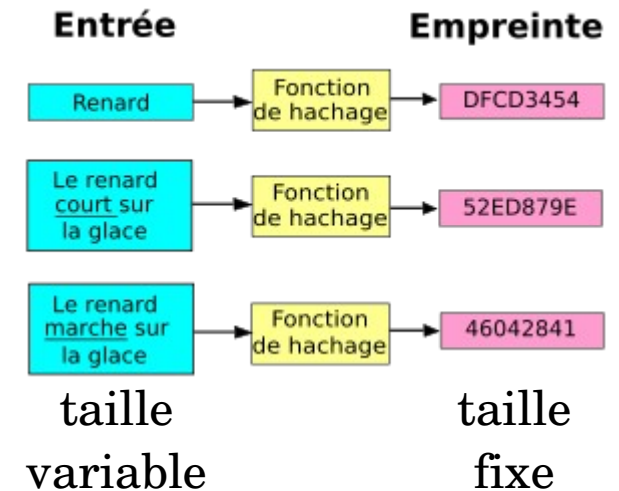
Documents signés



Fonction de hachage

Fonction qui fait subir une succession de traitements à un donnée quelconque fourni en entrée pour en produire une “empreinte” (ou somme de contrôle, ou condensat) servant à identifier la donnée initiale.

Exemple: la fonction de hachage MD5
(Message Digest 5)
avec la commande **md5sum** sous linux

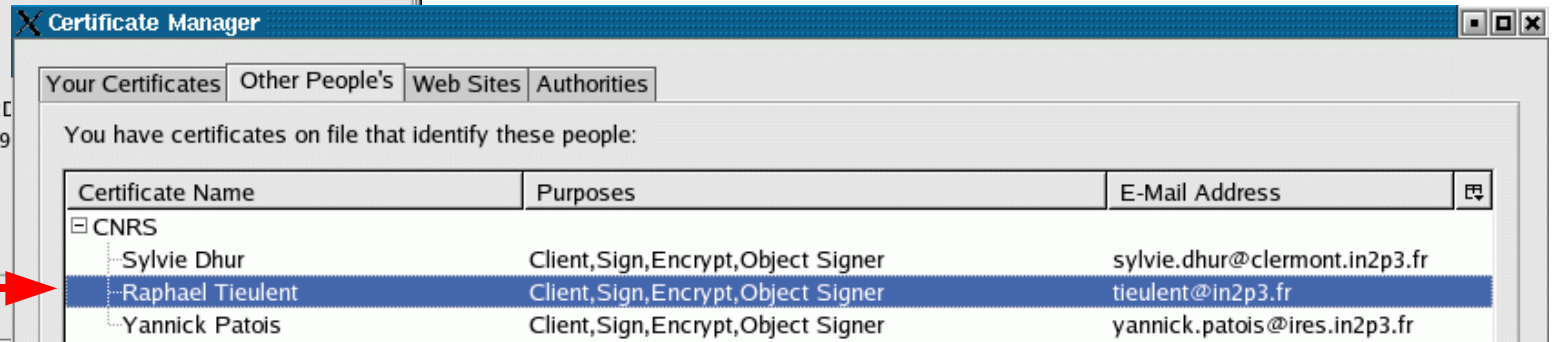
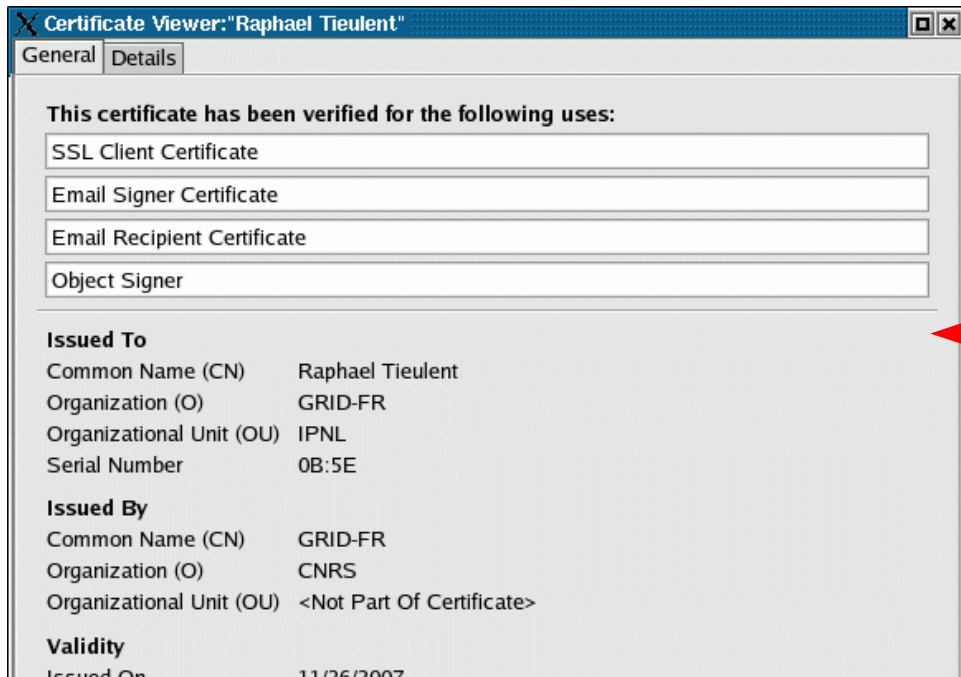


```
user@host:home> md5sum Umzug.txt
afc2cfdd713085ada557875ff2ba9aa6  Umzug.txt
```

```
user@host:home> md5sum Umzug.txt > Hash.txt
```

```
user@host:home> md5sum -c Hash.txt
Umzug.txt: OK
```

La messagerie signée



OpenSSL

la boîte à outils de chiffrement

Génération d'une clé privée:

```
openssl genrsa -des3 -out privkey.pem 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for privkey.pem:
Verifying - Enter pass phrase for privkey.pem:
```

privkey.pem

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,0452E016497A1941

5XpV4uqqUR5E4Pger6dlXxVYRE5nGRhTACp9mc4csMemXnBJMc7HR1eQeb0kv/my
vYFggswO2u5w37X1xG7Jr1zsgYlCmIuiRRaR3ZrevJeGD0u7007p3tUjMbm1+BmV
4AC1DeDelXz4EFYVzflxYmaIxMuFJAZJa0ShSBdLXVchiczLSo8eCQQPl8F33wH/
...
FwyOLHUbE96rmgpra+A9bOds7KM4Wf60ax4uWTcL05/pn8lcwB0i9F46nK9ahpsl
TBC1Zzn1b6AoQRh/RAjgsfOKd3Gx/TwSFsxwFTGnz2ujLN5OESvW7hugi/f50IDs
-----END RSA PRIVATE KEY-----
```

OpenSSL, continué

Génération d'une clé publique à partir d'une clé privée:

```
openssl rsa -in privkey.pem -pubout -out pubkey.pem
```

pubkey.pem

Simple chiffrage d'un fichier (liste des chiffres avec `openssl list-cipher-commands`):

```
openssl enc -des3 -in Umzug.txt -out Umzug.enc  
enter des-ede3-cbc encryption password:
```

et le déchiffrage:

```
openssl enc -d -des3 -in Umzug.enc -out Umzug.txt  
enter des-ede3-cbc decryption password:
```

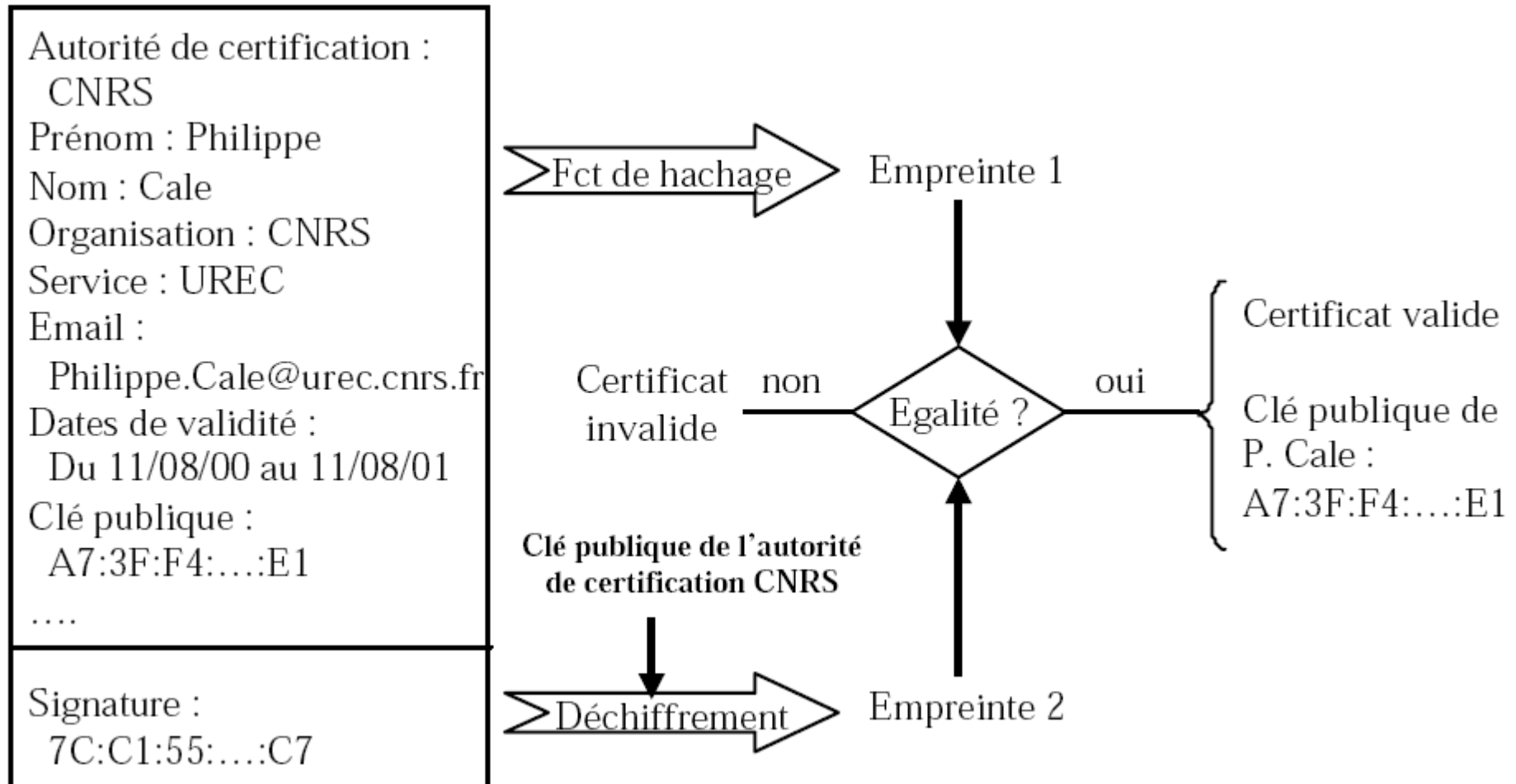
Créer une “empreinte” d'un fichier (fonction de hachage) et signer avec la clé privée:

```
openssl dgst -sha1 -sign privkey.pem -out Umzug.txt.sha1 Umzug.txt  
Enter pass phrase for privkey.pem:
```

Vérifier une empreinte signée avec la clé privée en utilisant la clé publique:

```
openssl dgst -sha1 -verify pubkey.pem -signature Umzug.txt.sha1 \  
Umzug.txt  
Verified OK
```


Le certificat électronique (une carte d'identité numérique)



L'autorité de certification fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique.

L'authentification; les autorités de certification

18

La procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur ...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications ...).

l'Autorité de Certification CNRS-Standard

<http://igc.services.cnrs.fr/CNRS-Standard>

CNRS-Projets

GRID-FR

<http://igc.services.cnrs.fr/GRID-FR>

(accès grilles de calcul et sites web sécurisés)

Dictionnaire:

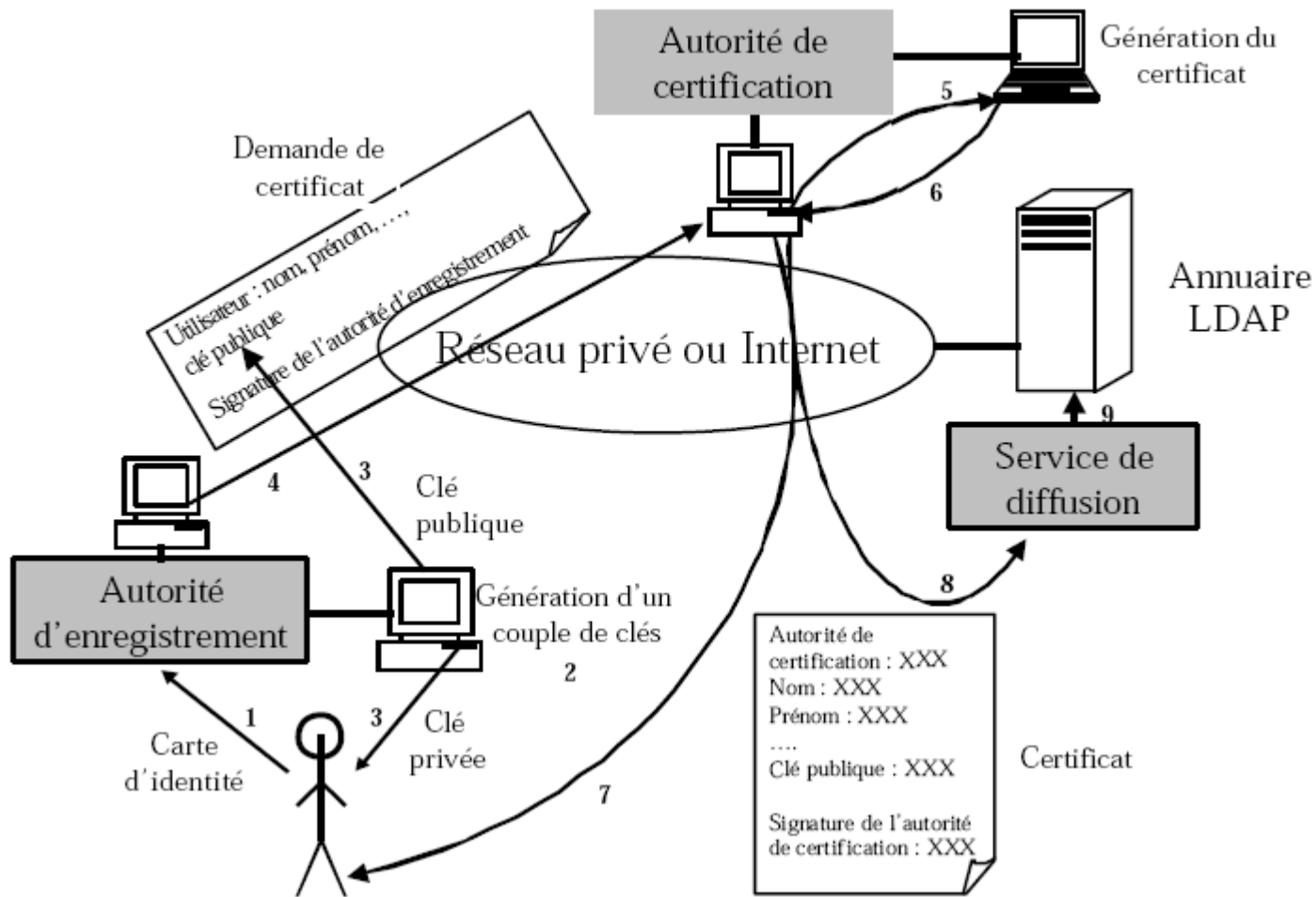
IGC – infrastructure de gestion de clés

ICP – infrastructure à clés publique

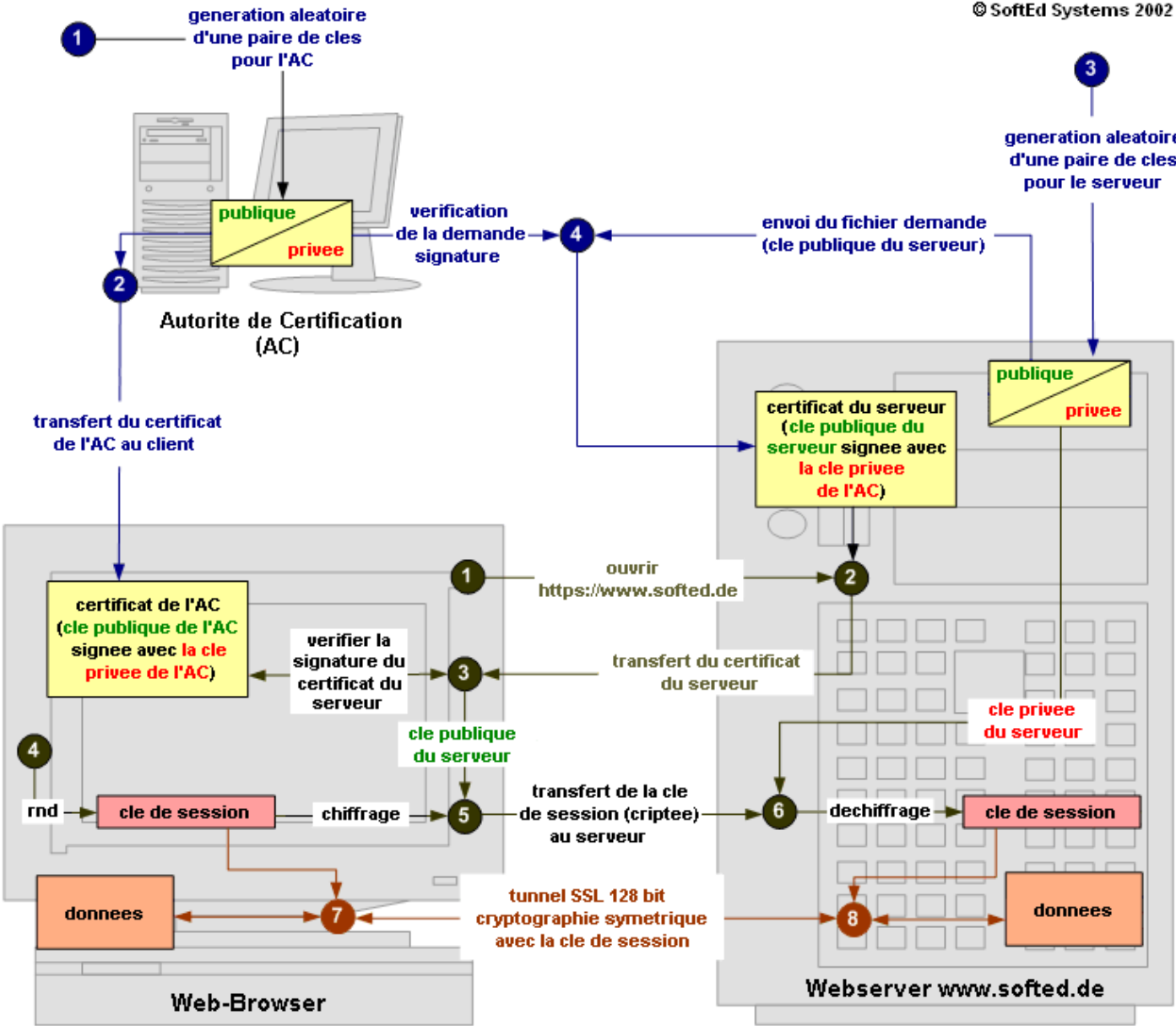
PKI – public key infrastructure



Les étapes pour la création d'un certificat



Deroulement d'une connexion SSL entre le client (Web-Browser) et un serveur HTTPS (Webserver)



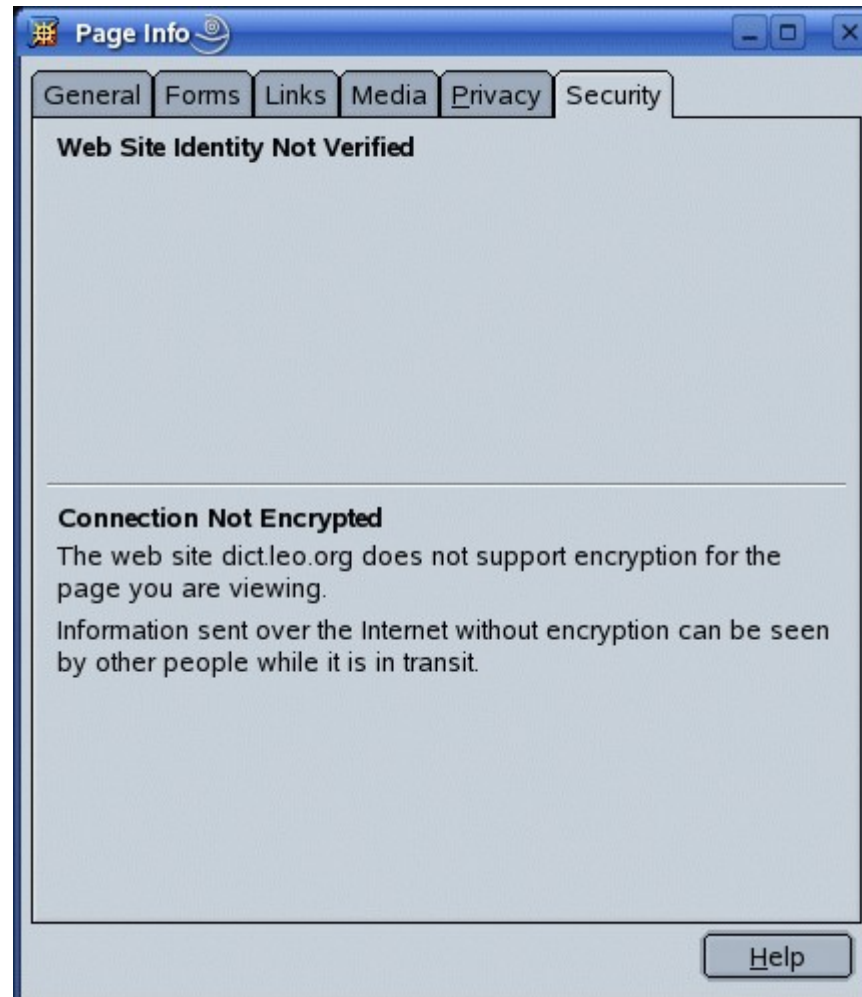
Exemple: serveur sécurisé du “Crédit Agricole Centre France”²¹



le serveur qui héberge cette page n'est pas sécurisé !

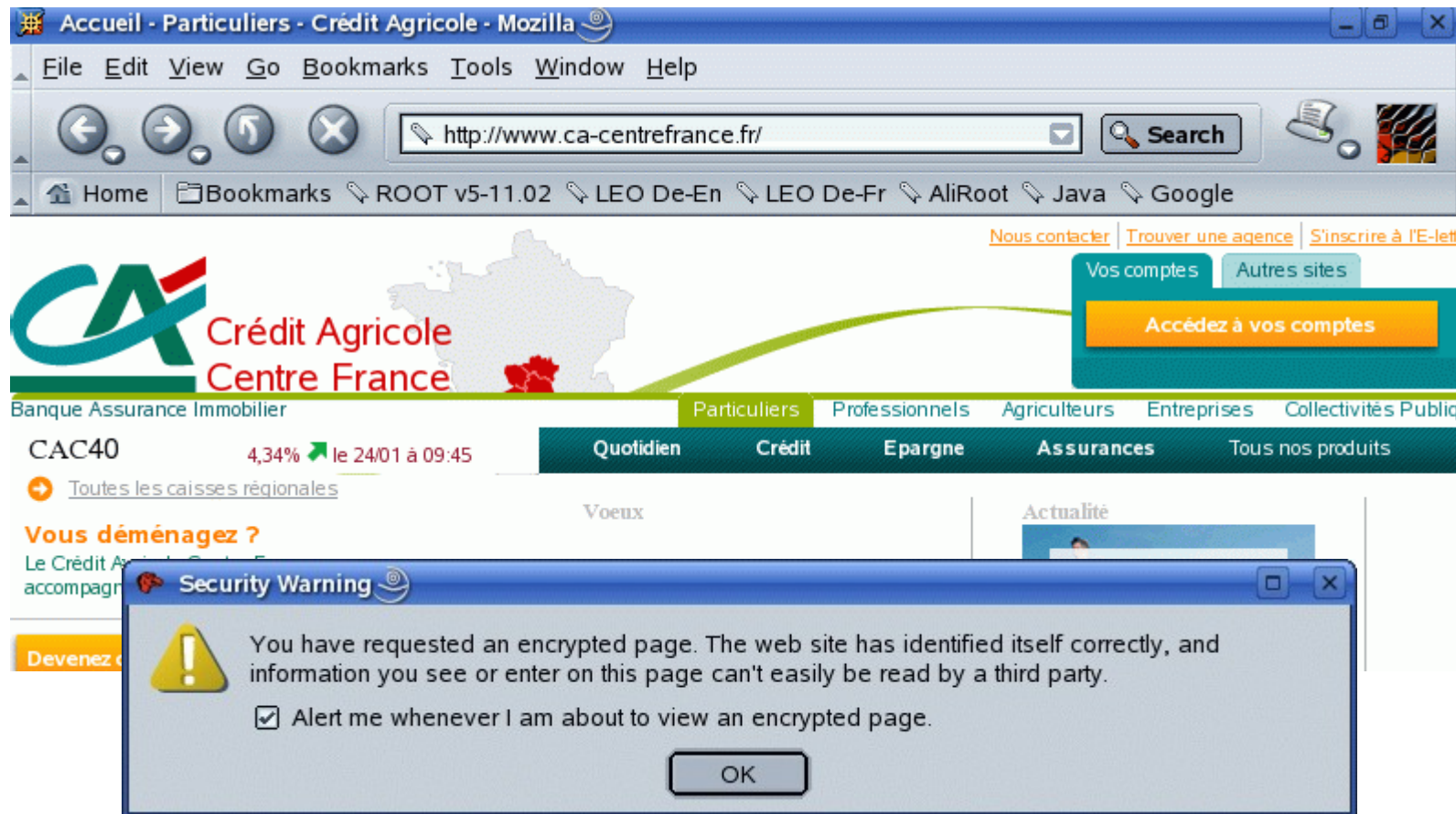
Informations sur le site web

22



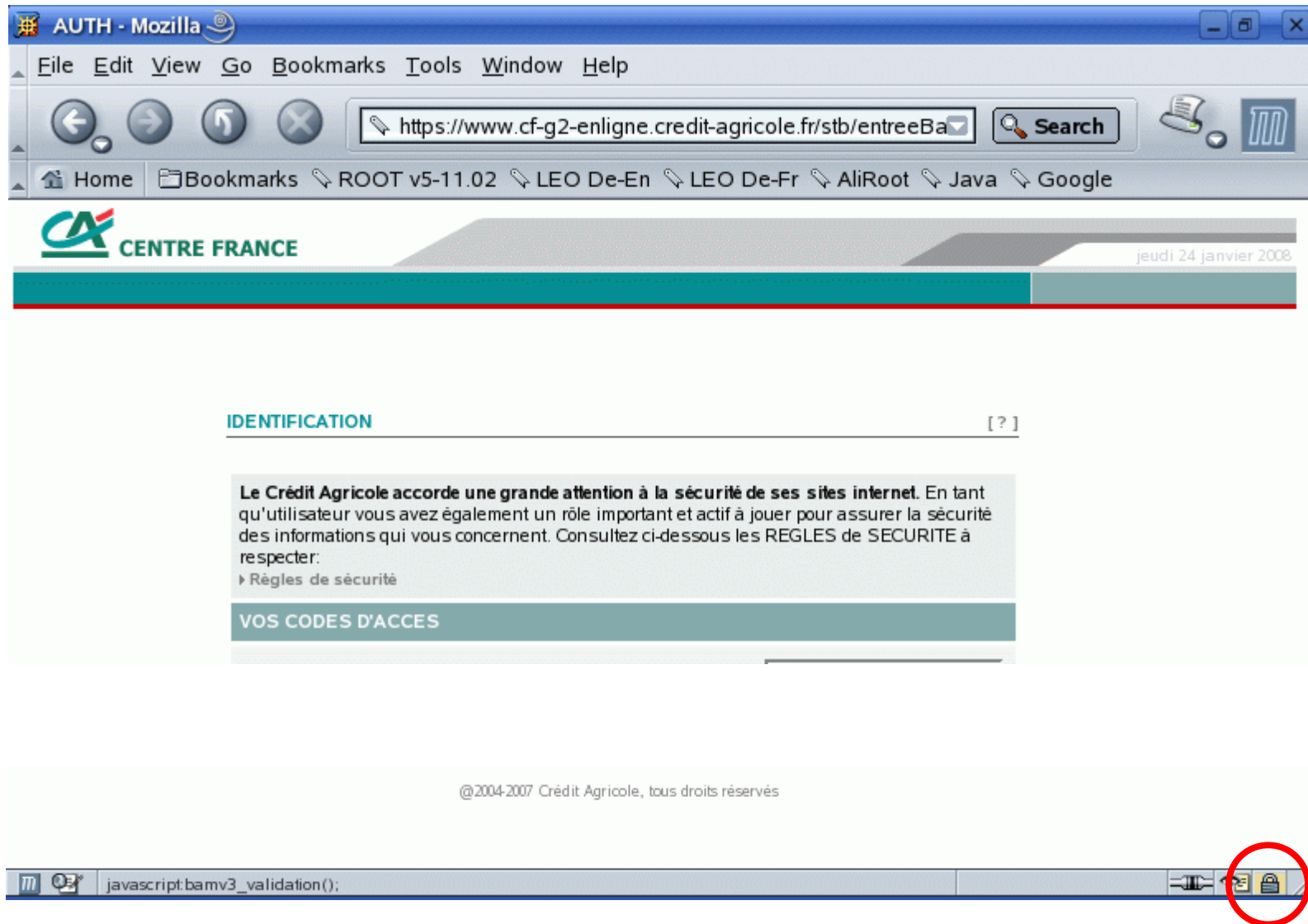
“Accédez à vos comptes”

23



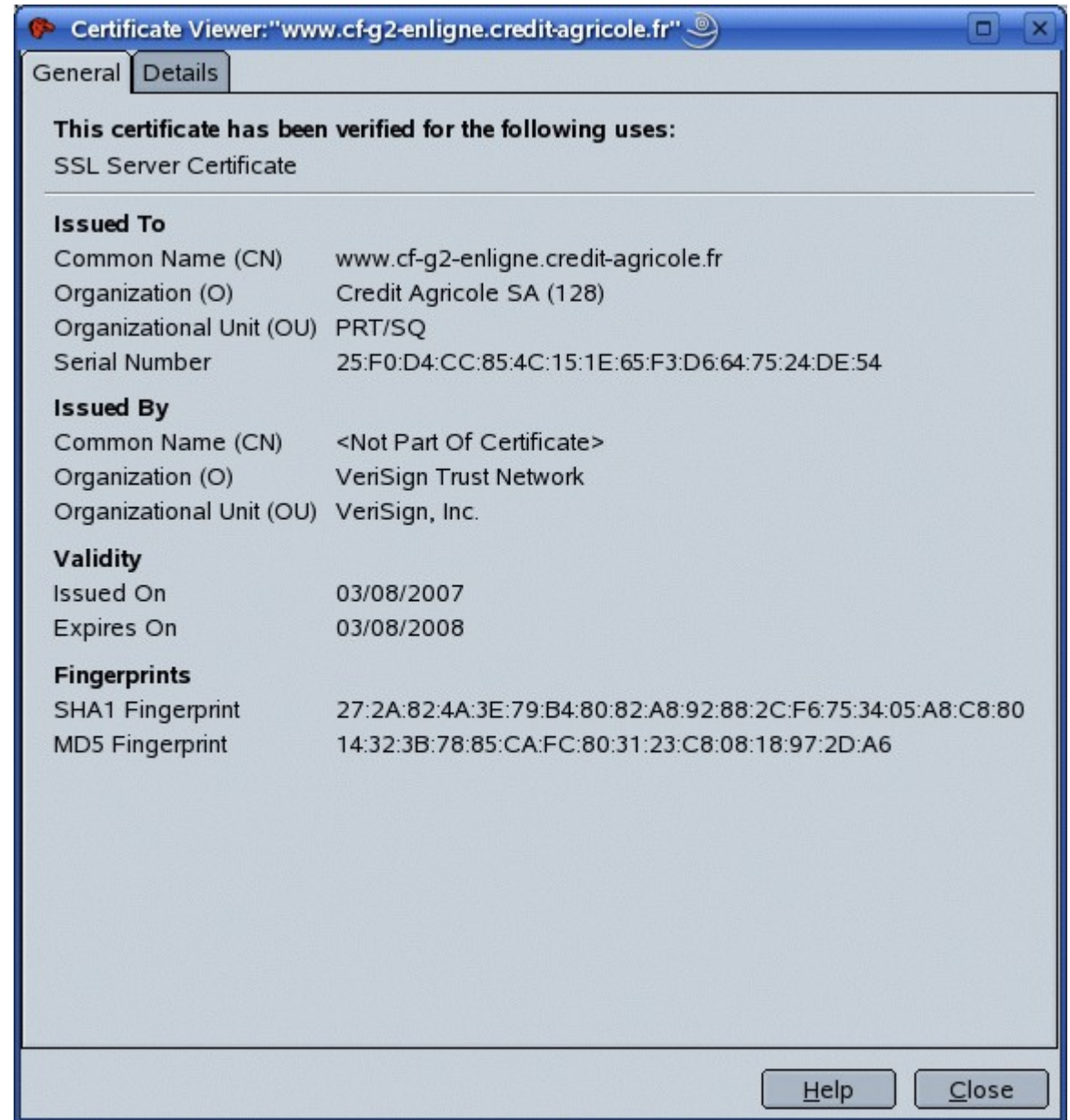
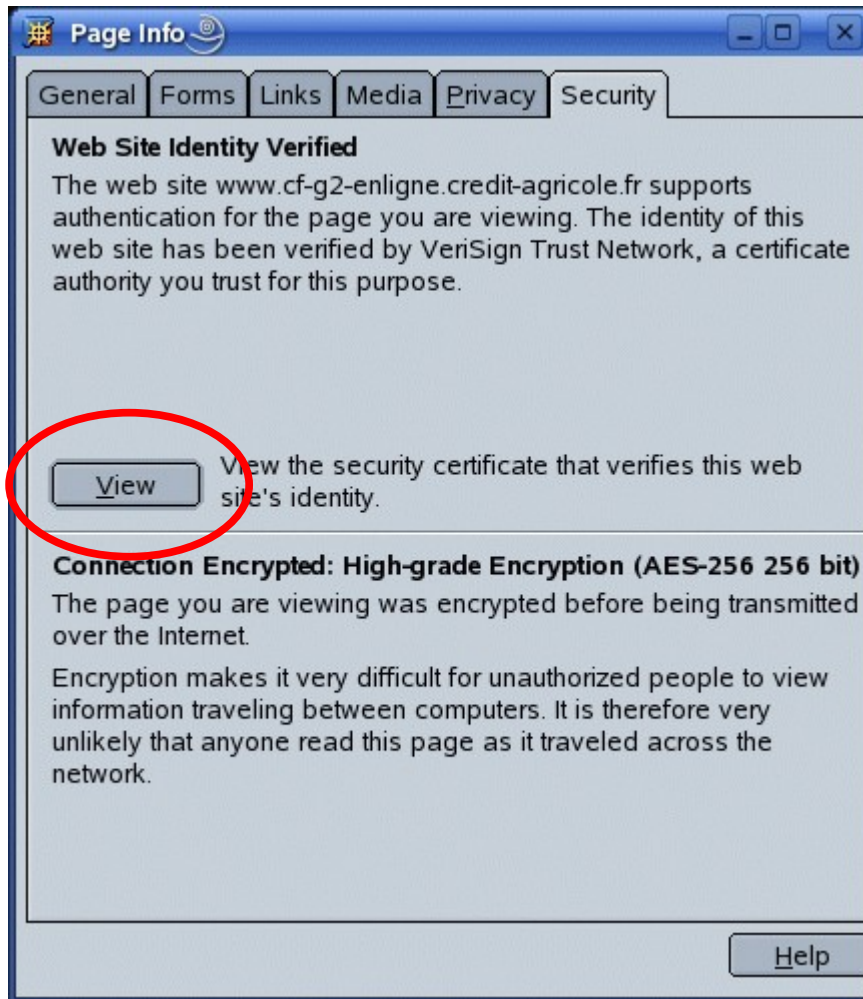
redirection vers une page hébergée par un serveur sécurisé !

La page sécurisée



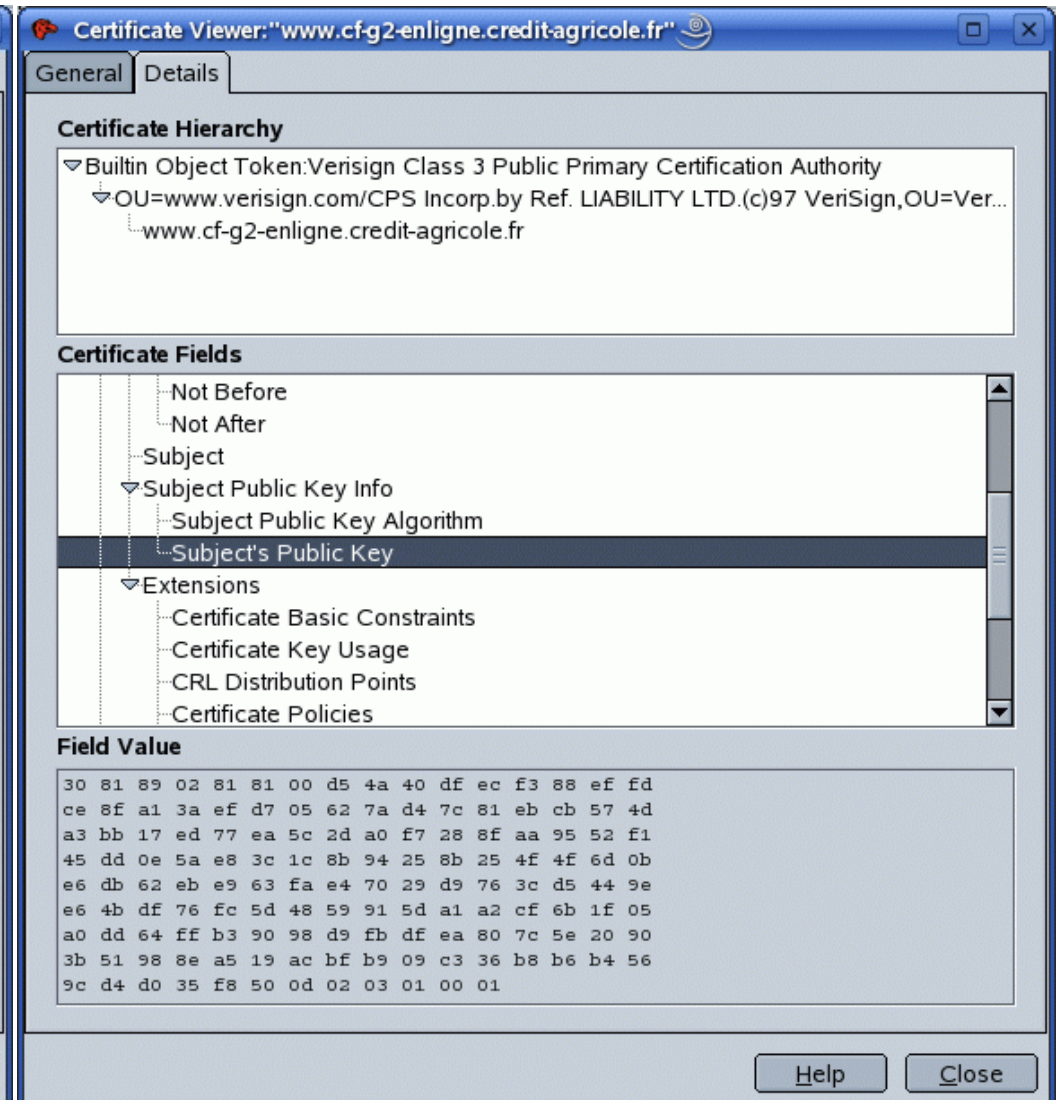
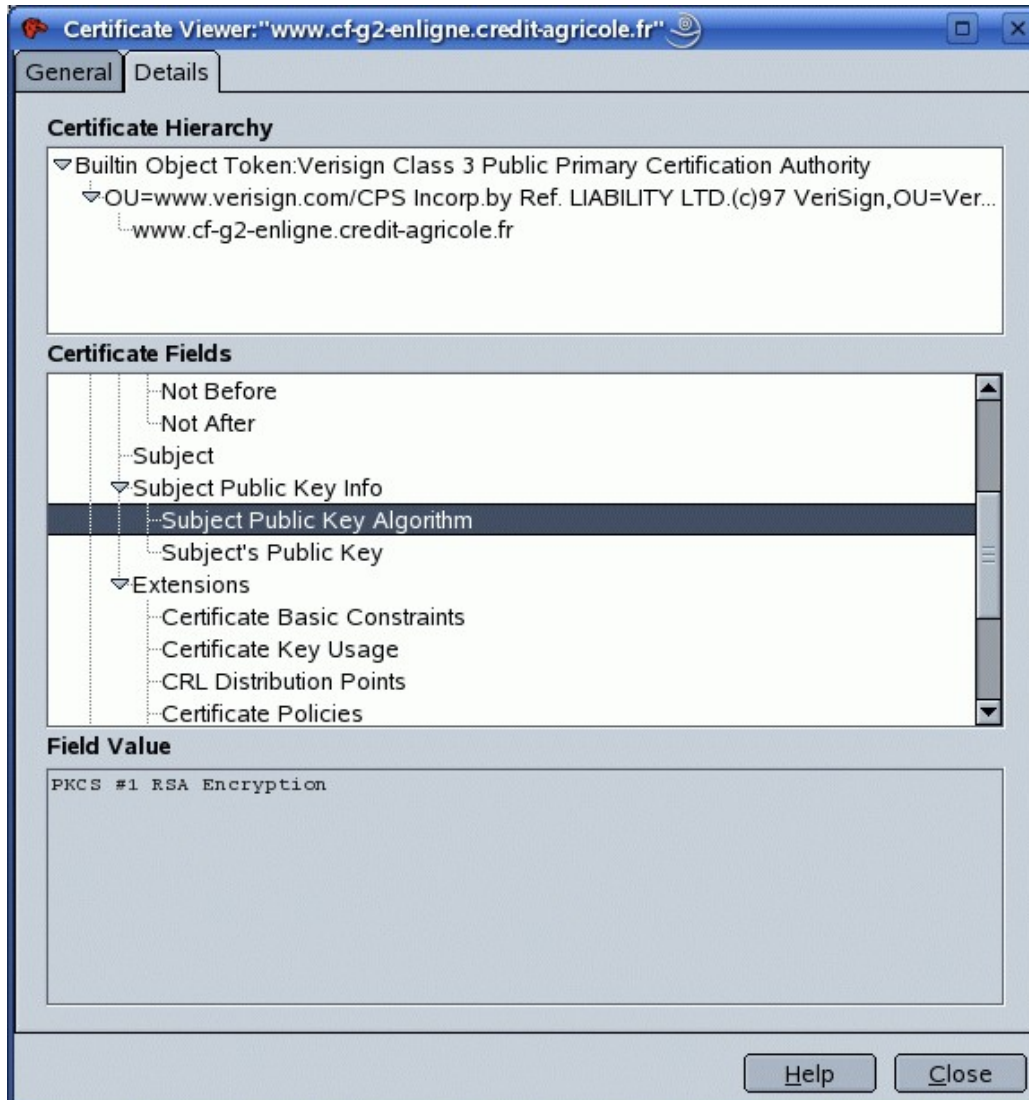
Informations sur le site web

25

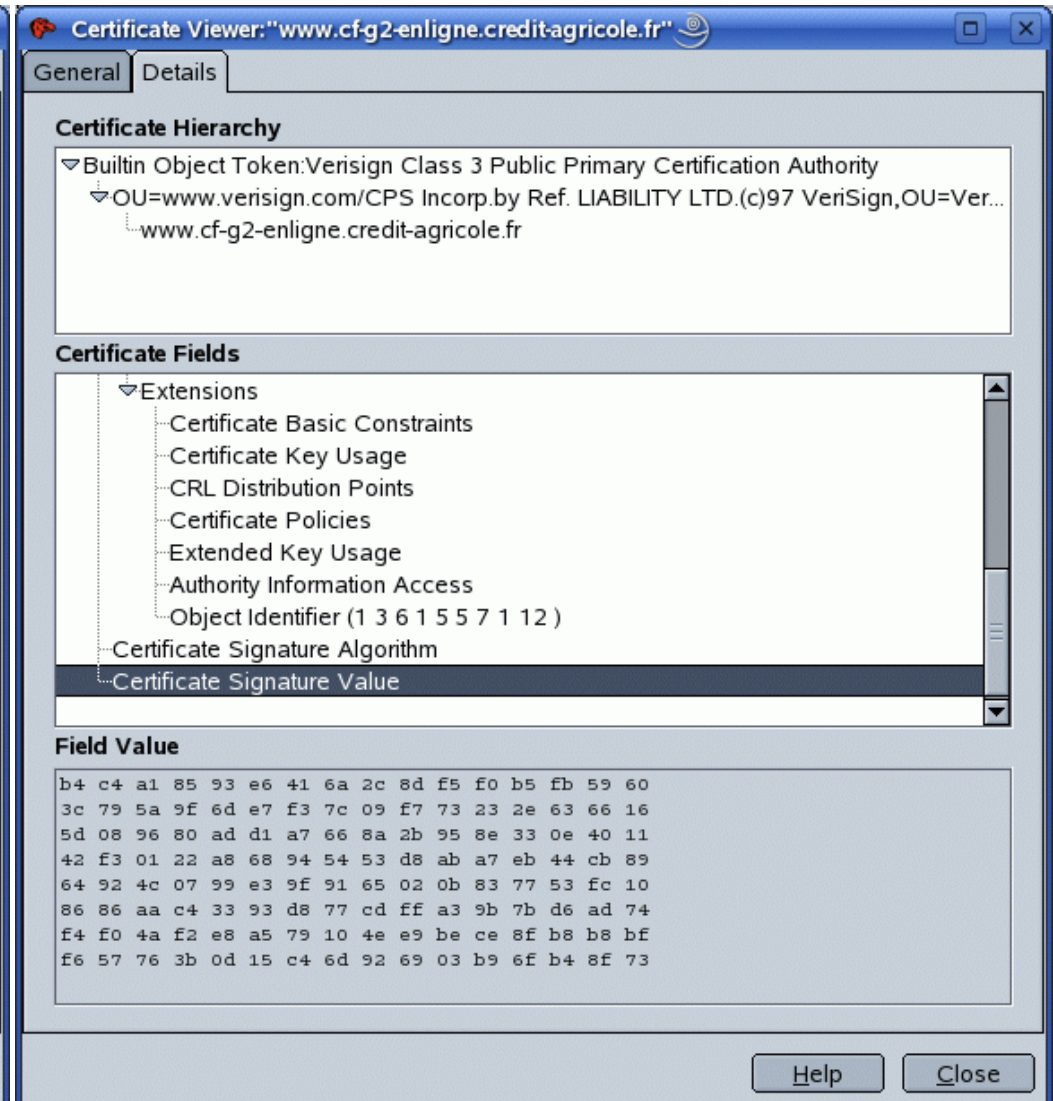
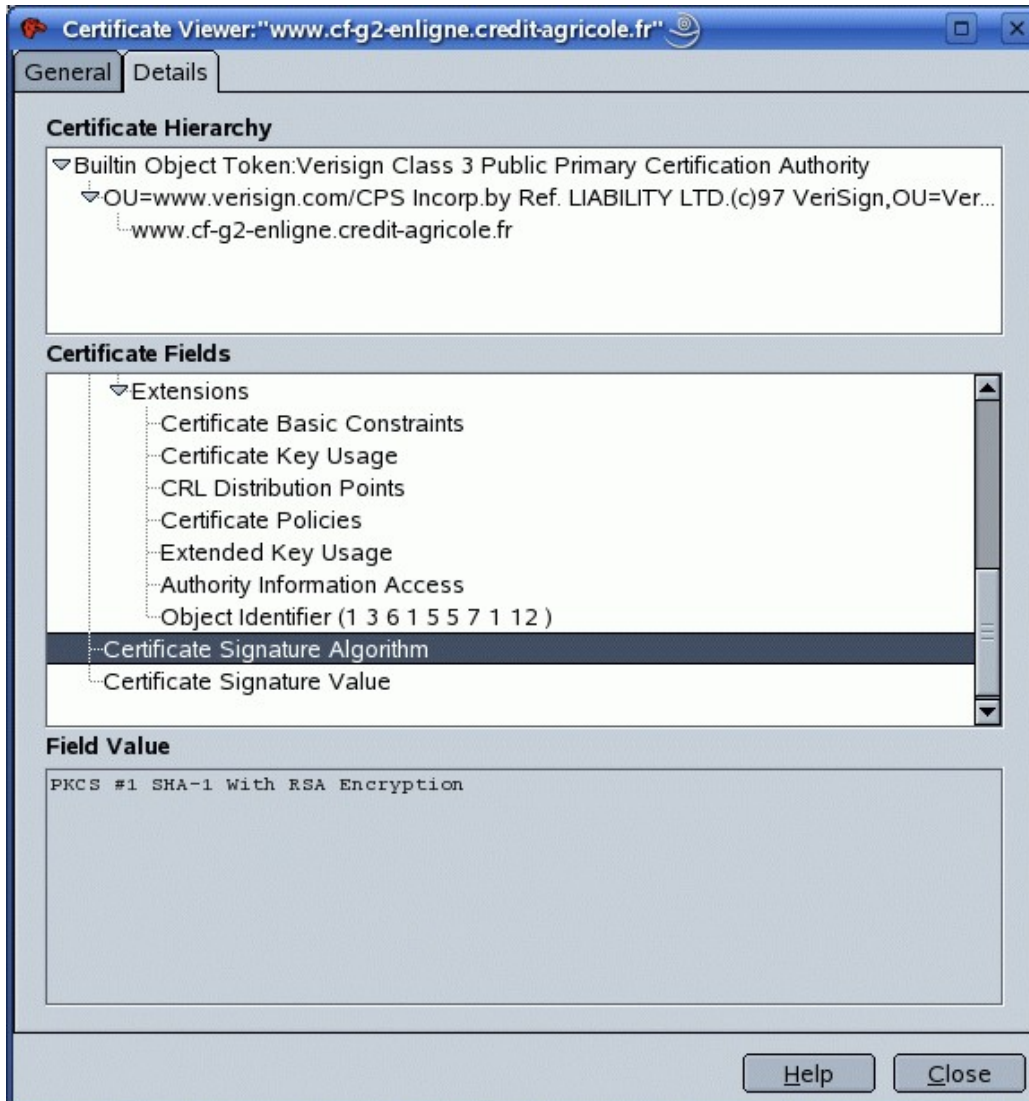


l'autorité de certification est
VeriSign

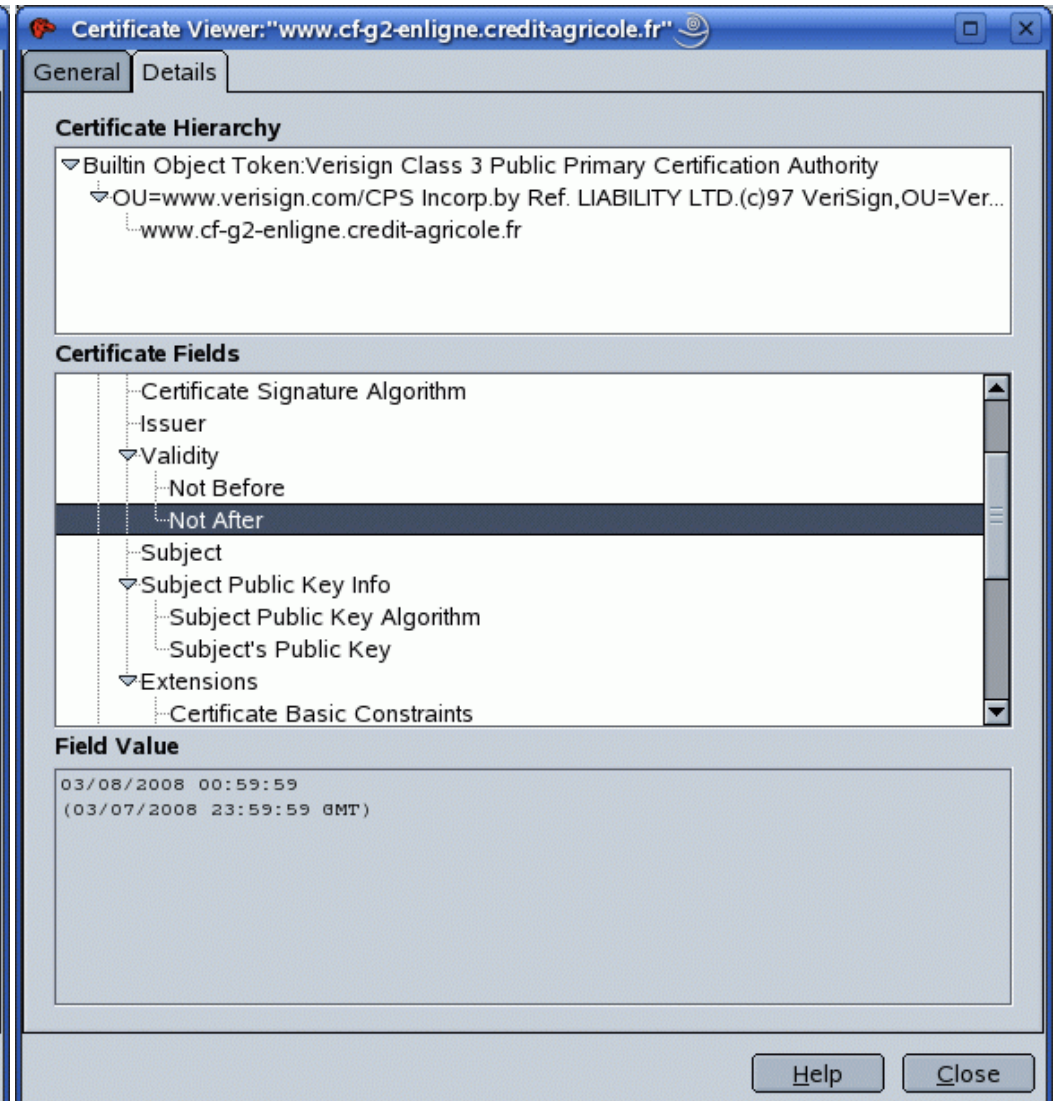
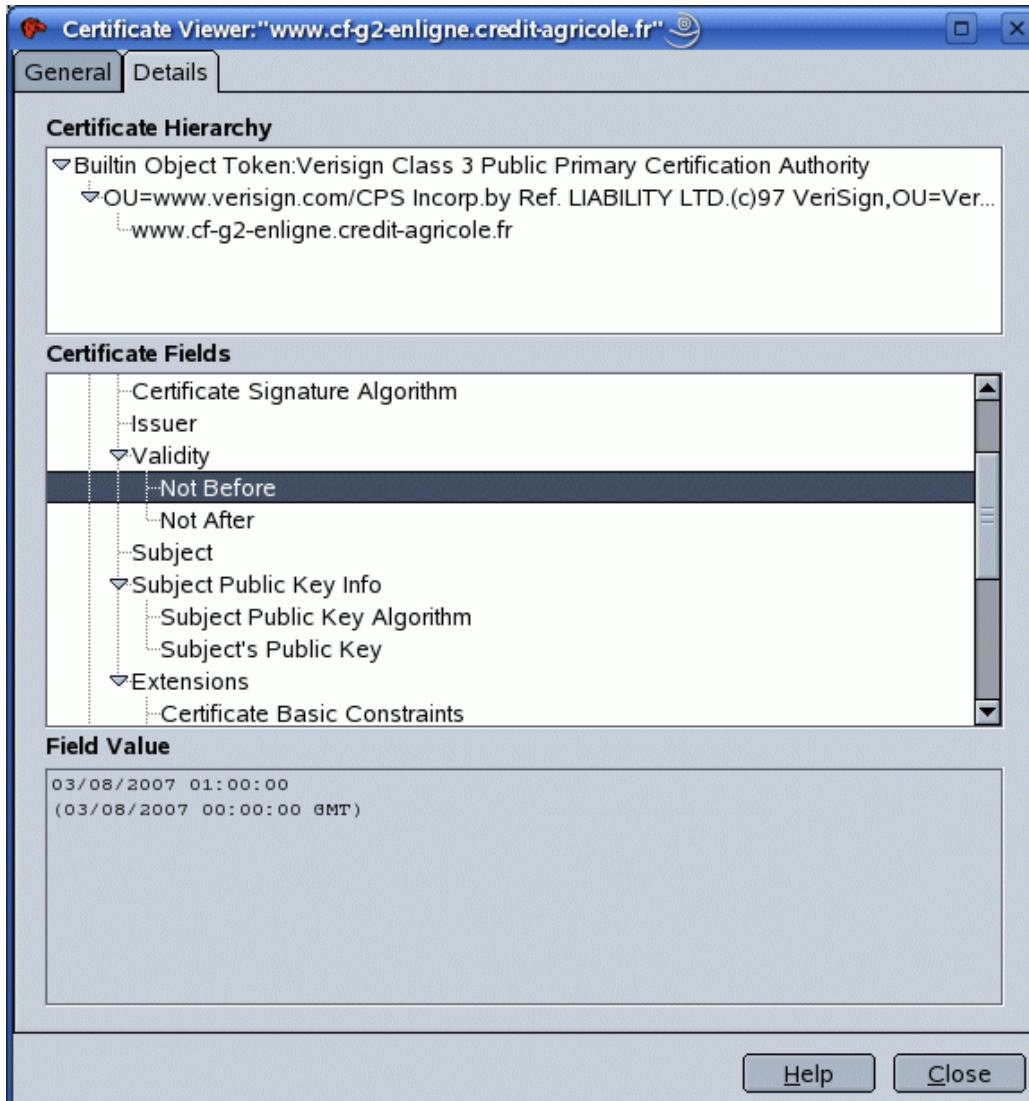
La clé publique du serveur et l'algorithme cryptographique ²⁶



La signature du certificat, faite par l'AC

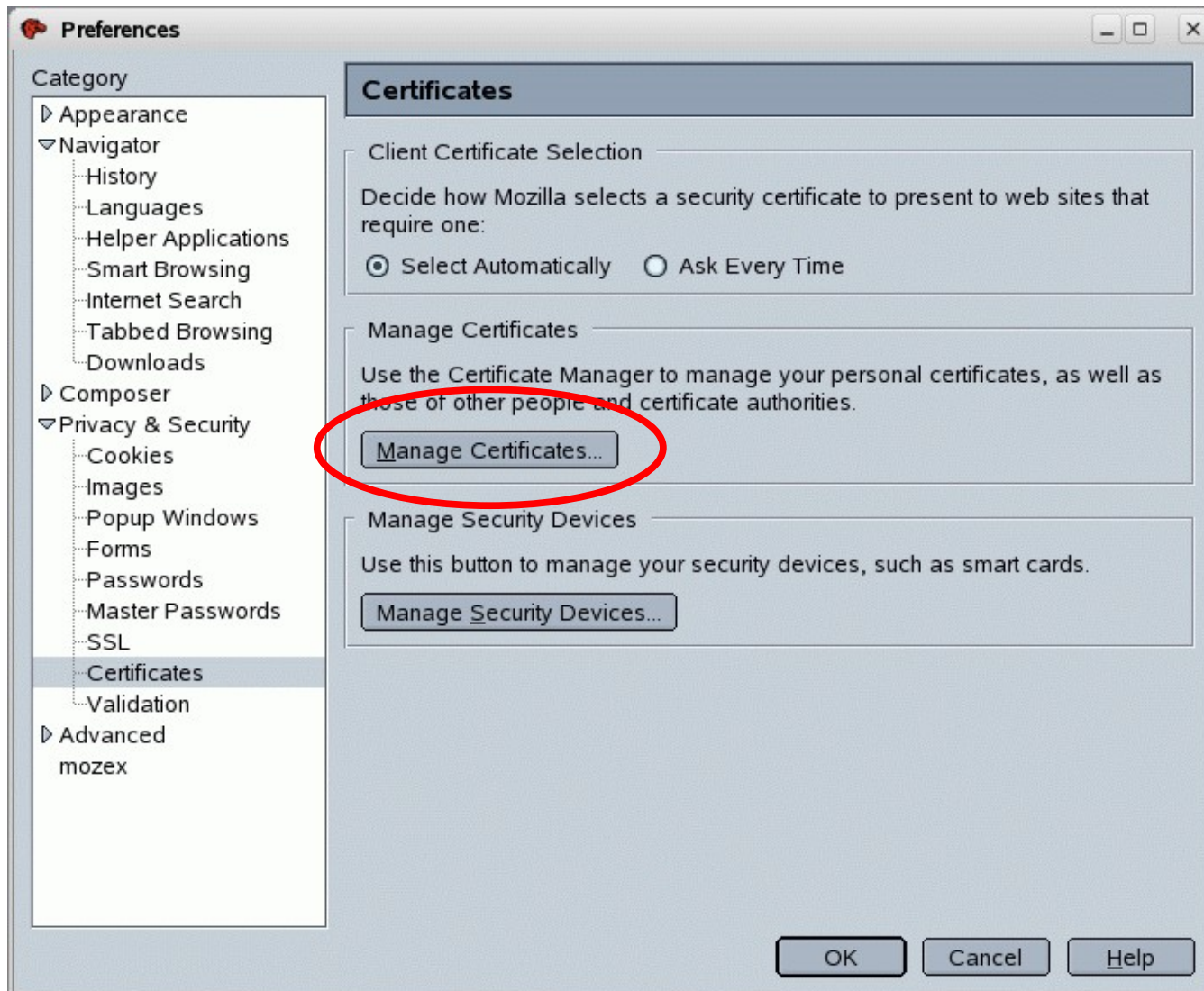


La limite de validité du certificat



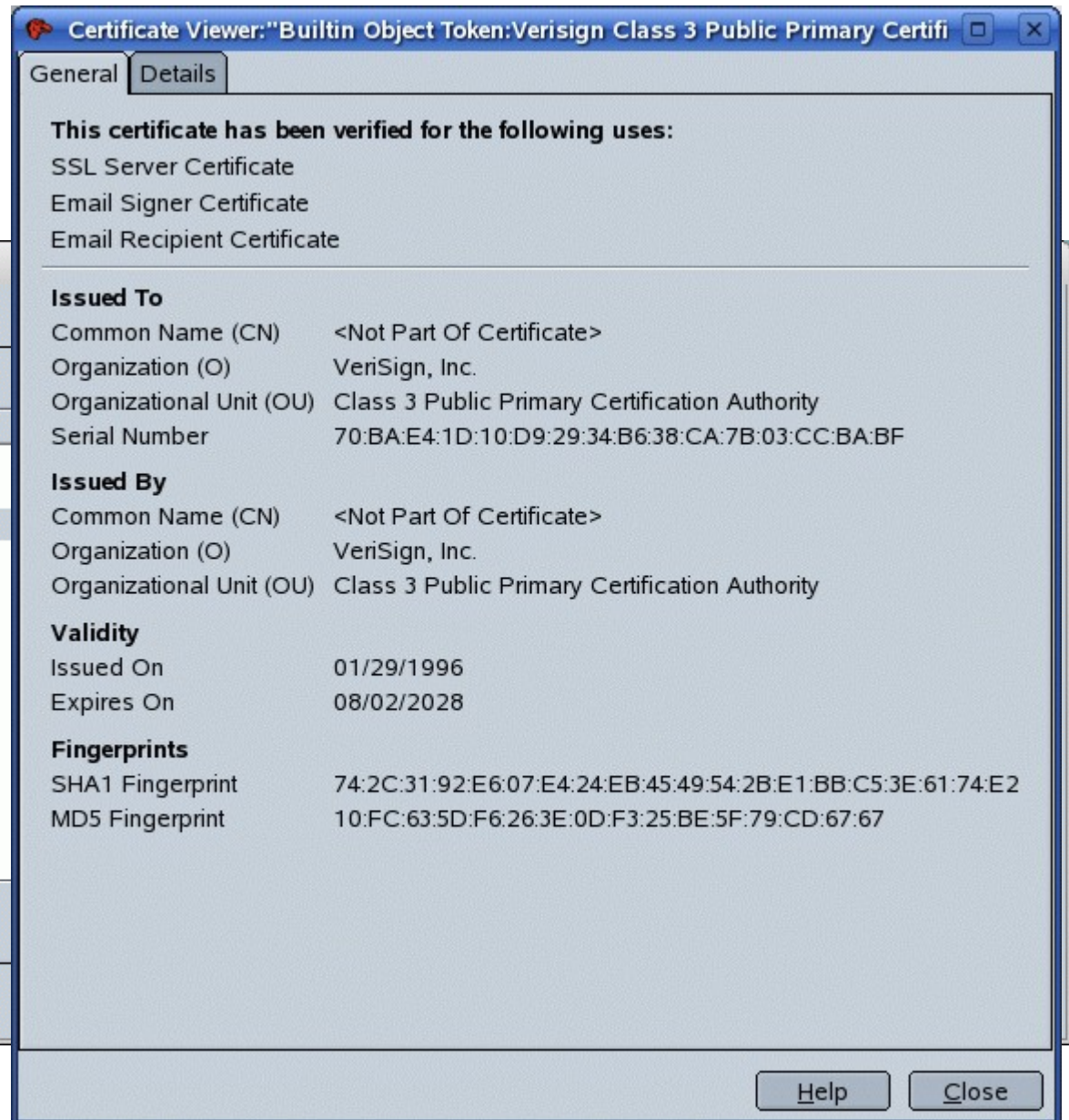
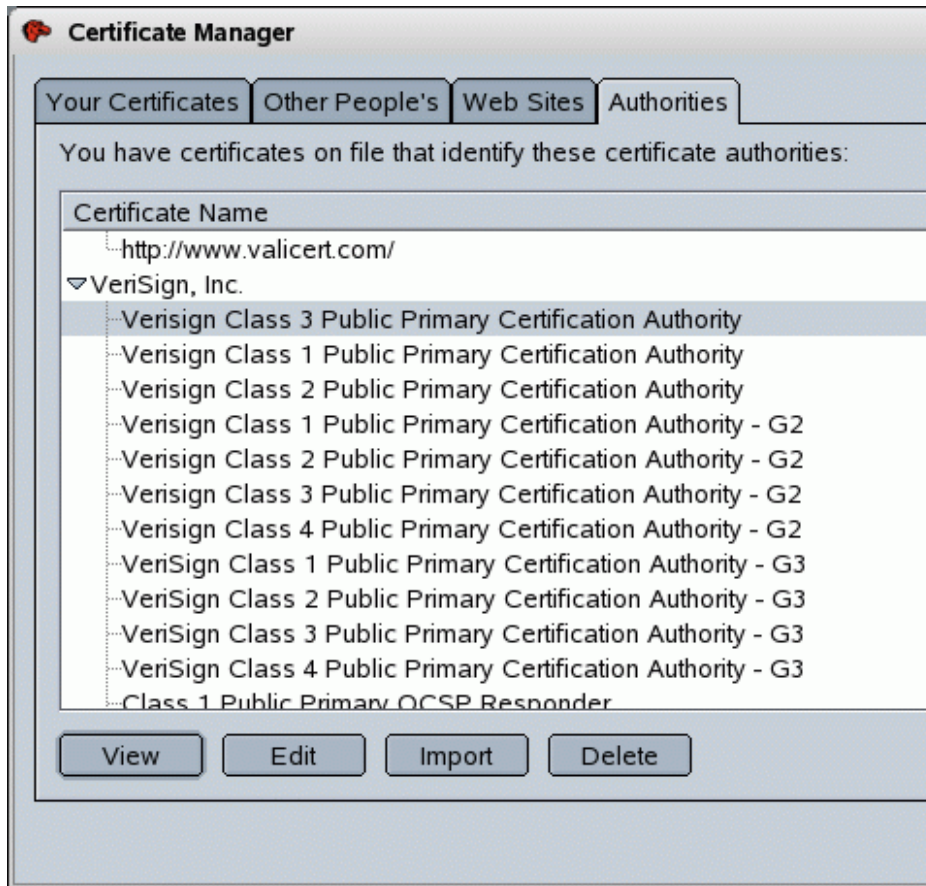
Les certificats dans le navigateur web (certificats des AC pre-installés)

Mozilla -> Edit -> Preferences... -> Privacy & Security -> Certificates

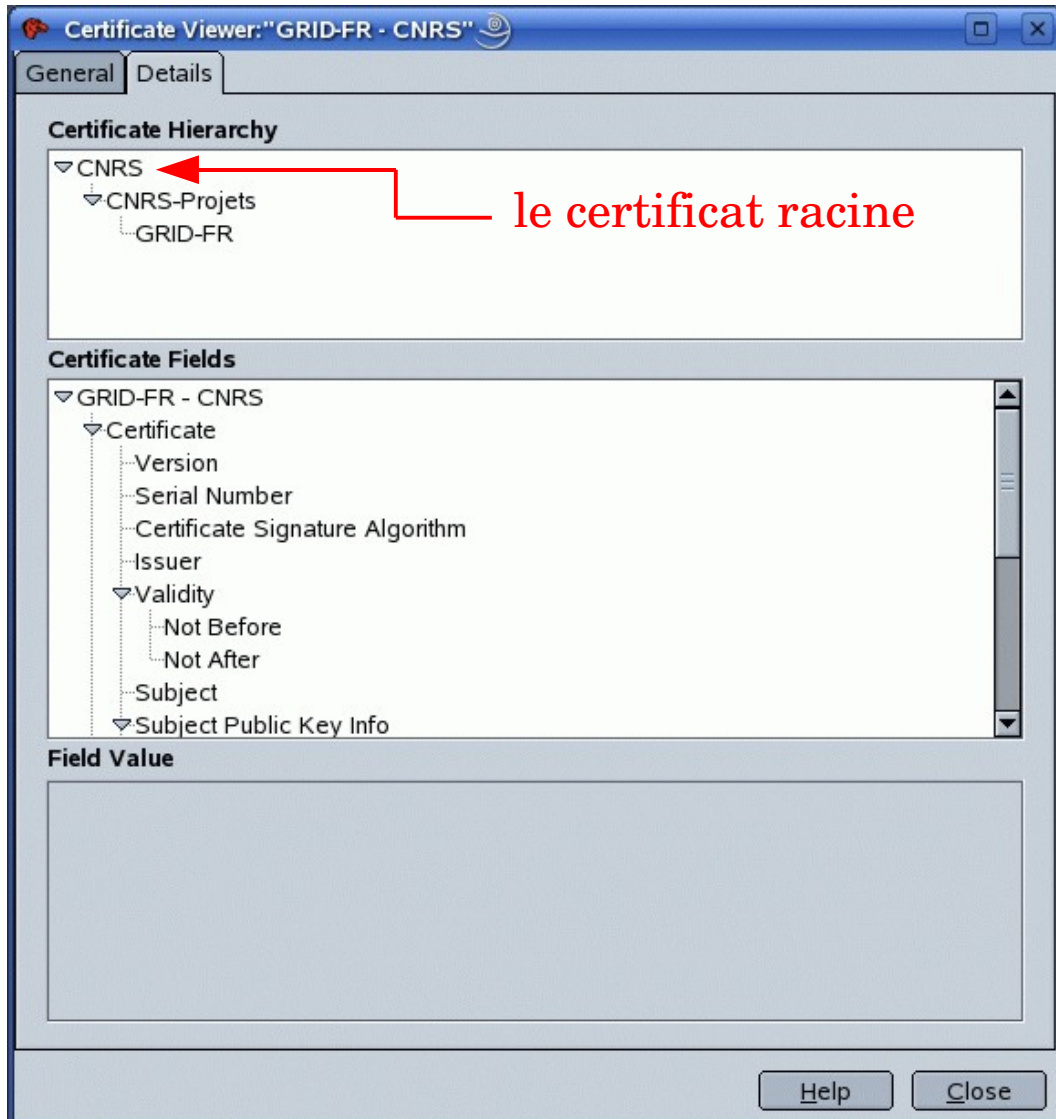


Le certificat de l'Autorité de Certification

l'onglet "Authorities"



L'hierarchie des certificats



certificat racine = certificat auto-signé (il n'existe aucune autorité supérieure)

l'autorité de certification du CERN

<https://ca.cern.ch/ca>



afin de se confier en certificats émis par CERN CA il faut faire confiance à CERN Root CA et CERN TCA également

IS Certificates Site - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://ca.cern.ch/ca/ Search

Home Bookmarks ROOT v5-11.02 LEO De-En LEO De-Fr AliRoot Java Google

CERN Home | IT Department | IT/IS Group Mail Services | Web Services | Win Services




CERN Certification Authority

CERN IT/IS Certificates Services


Home

Certificates administration

User Certificates


-  [Request or renew user certificate using Internet Explorer](#)
-  [Request or renew user certificate using Mozilla browser](#)
-  [Request or renew user certificate manually](#)




List and revoke certificates

-  [List and revoke certificates](#)





Trust CERN Certification authority

On a CERN Domain managed Windows machine, the CERN Root Certificate is trusted, so any CERN Certificate will be verified correctly, no specific action is required.

 On any other platform, the CERN Root Certificate needs to be trusted manually to allow CERN Certificate verification. To do this, install the Root Certificate using one of the following methods.

-  [Install Root certificate using Internet Explorer](#)
-  [Install Root certificate using Mozilla browser](#)
-  [Install Root certificate using Safari browser](#)




Download CA certificates and CRLs [\[Help\]](#)

-  [CERN Root CA certificate](#)
-  [CERN Root CA CRL](#)
-  [CERN Trusted Certification Authority certificate](#)
-  [CERN Trusted Certification Authority CRL](#)








Documentation

Contents



What are Certificates

-  [What are certificates](#)
-  [Why use CERN certificates](#)
-  [CNL Article about CERN CA \(pdf\)](#)



Faq

-  [Who can request a certificate](#)
-  [Who can request a Host certificate](#)
-  [Certificate Chain](#)
-  [Export your public key](#)
-  [Prepare renewal CSR with OpenSSL](#)
-  [Request Host certificate with OpenSSL](#)
-  [Use my Certificate in various Applications](#)

Grid usage

-  [How to use your certificate with grid-proxy-init](#)
-  [Grid users re-registering with a new certificate](#)

Internet Explorer usage

-  [Trust CERN Root Certificate](#)
-  [Export and import certificate with IE](#)

Les certificats personnels

33

Distinguished Name (DN)

/O=GRID-FR/C=FR/O=CNRS/OU=LPC/CN=Bogdan Vulpescu

O - organizationName

C - countryName

OU - organizationalUnitName

CN - commonName

LDAP (Lightweight Directory Access Protocol) = une norme pour les systèmes d'annuaires (ldap://... , le DN est une entrée dans un annuaire LDAP).

Organisation Virtuelle (VO) = groupe abstrait d'individus ou institutions qui partagent les ressources de calcul d'une "grille" avec un but commun (ALICE, ATLAS, etc.)

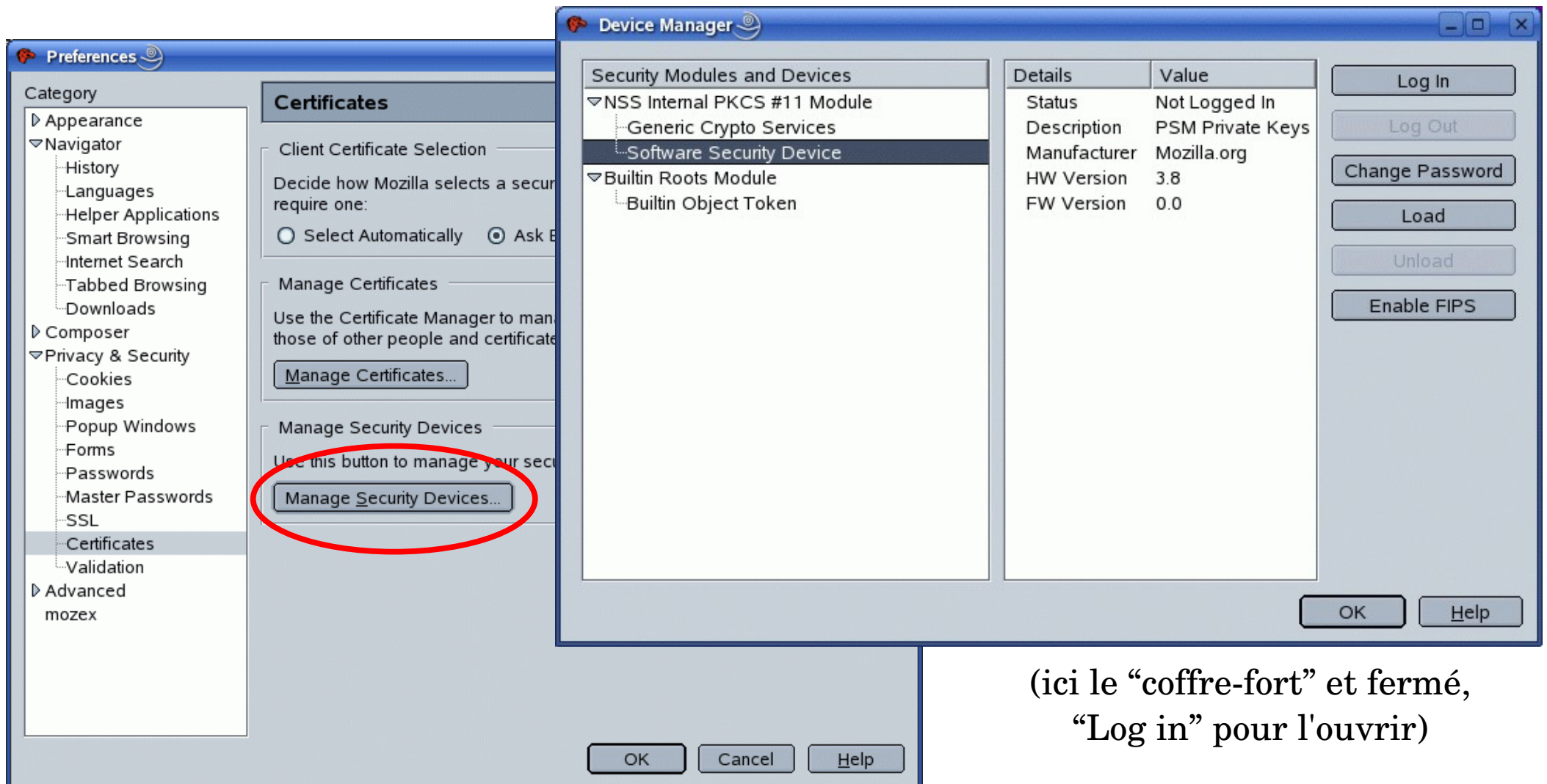
Le rôle dans le certificat – extension VOMS

VOMS (Virtual Organisation Membership Service) fournit le mécanisme d'autorisation basée sur les différents rôles au sein de l'organisation virtuelle

- admin, user, production, etc.

Software Security Device

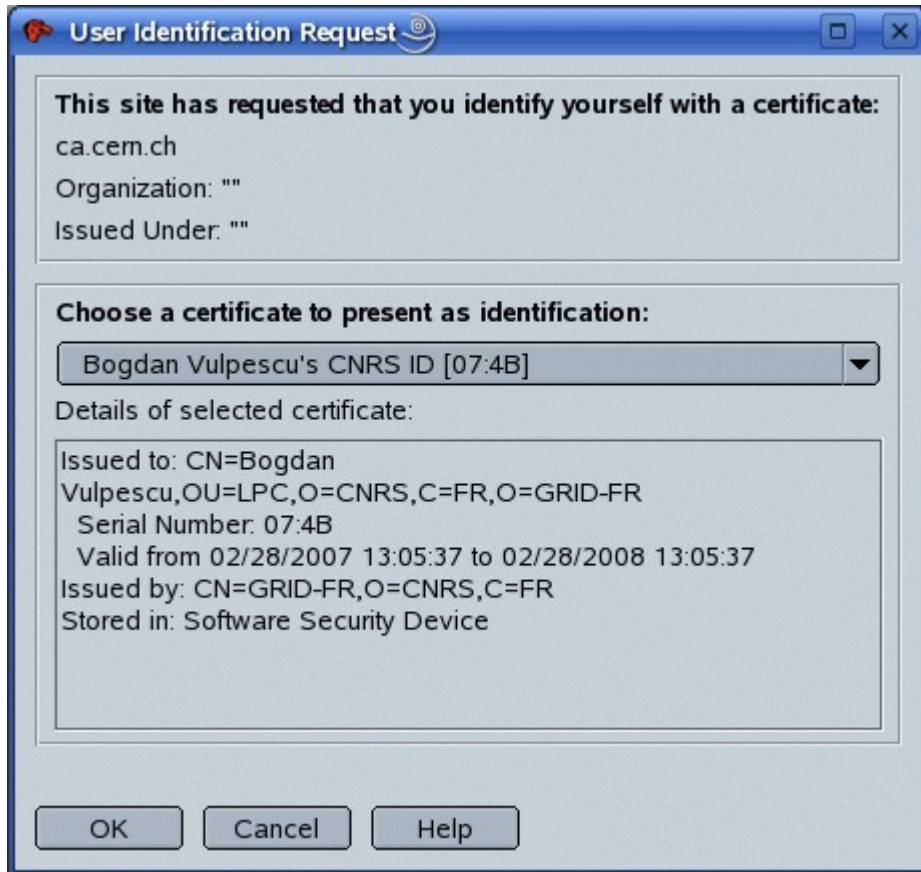
le “coffre-fort” du navigateur pour le stockage des données confidentielles
comme les certificats personnelles
la clé du coffre-fort s'appelle “**Master Password**”



(ici le “coffre-fort” et fermé,
“Log in” pour l'ouvrir)

Authentication avec un certificat personnel (e.g. <https://ca.cern.ch/ca>)

35

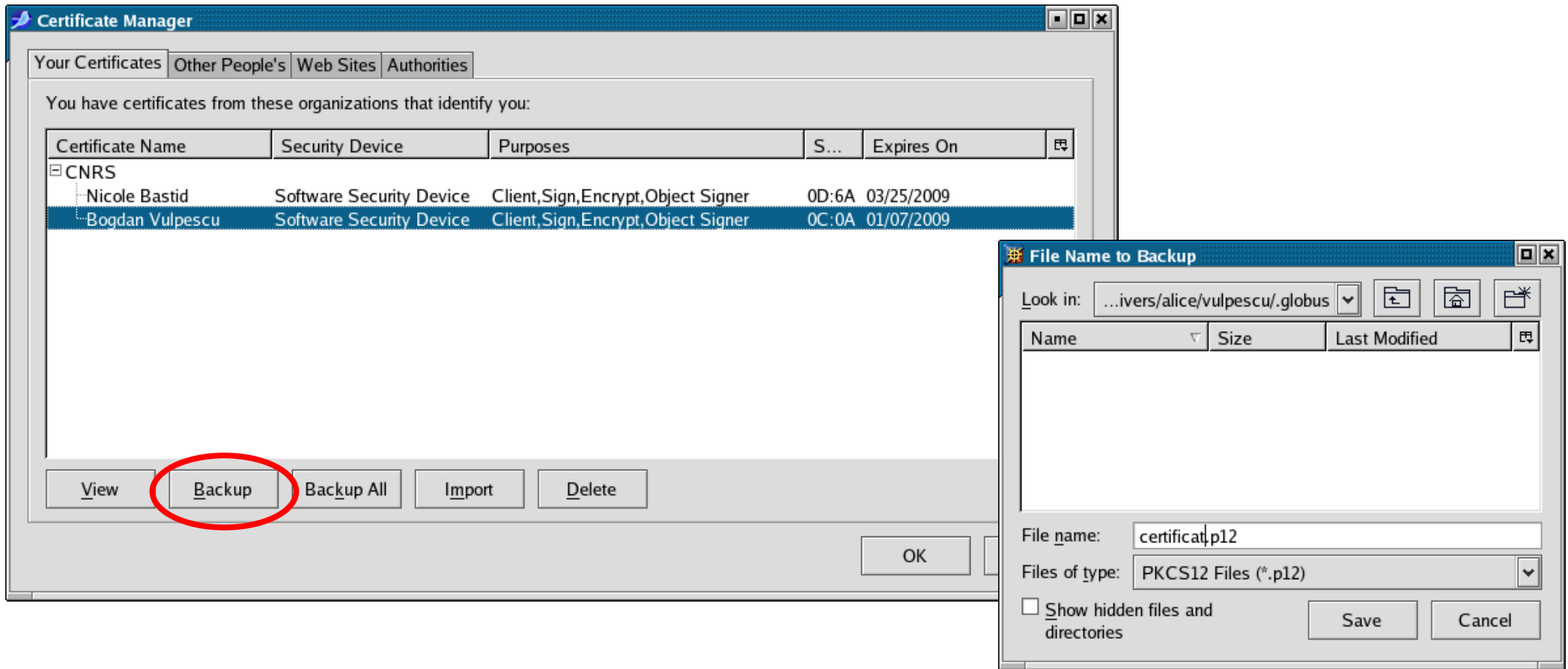


choisir un certificat et
OK + mot de passe “coffre-fort”
(à partir de ce moment il reste
ouvert jusqu'à la fin de la session)

Cancel

le serveur peut accepter une connexion
sans l'authentification du client mais,
éventuellement, sur un niveau de
confidentialité diminué

La création d'une paire de clés (publique/privés) à partir du certificat navigateur



Exemple: dans `$HOME/.globus/certificat.p12`

(PKCS#12 - Public Key Cryptography Standards #12)

Le certificat sera chiffré par
un mot de passe !

... encore une fois openssl ...

```
cd $HOME/.globus
```

```
openssl pkcs12 -clcerts -nokeys -in certificat.p12 -out usercert.pem
```

```
Enter Import Password: ...
```

```
MAC verified OK
```

```
chmod 644 usercert.pem
```

publique, visible!

```
openssl pkcs12 -nocerts -in certificat.p12 -out userkey.pem
```

```
Enter Import Password: ...
```

```
MAC verified OK
```

```
Enter PEM pass phrase: ...
```

```
Verifying Enter PEM pass phrase: ...
```

```
chmod 600 userkey.pem
```

privée, secrète!

```
/.globus/
```

```
-rw----- 1 vulpescu alice 5912 Mar  5 11:15 certificat.p12
```

```
-rw-r--r-- 1 vulpescu alice 1932 Mar  5 11:18 usercert.pem
```

```
-rw----- 1 vulpescu alice 1919 Mar  5 11:17 userkey.pem
```

PEM (Base64 – chiffage) pass phrase: le mot de passe pour l'autorisation sur la grille.

... et comment vérifier le certificat sans le navigateur

L'autorité de certification qui a émis le certificat:

```
openssl x509 -noout -in usercert.pem -issuer  
issuer= /C=FR/O=CNRS/CN=GRID-FR
```

Le propriétaire du certificat:

```
openssl x509 -noout -in usercert.pem -subject  
subject= /O=GRID-FR/C=FR/O=CNRS/OU=LPC/CN=Bogdan Vulpescu
```

La validité du certificat:

```
openssl x509 -noout -in usercert.pem -dates  
notBefore=Jan  7 09:48:40 2008 GMT  
notAfter=Jan  7 09:48:40 2009 GMT
```

Tout:

```
openssl x509 -text -in usercert.pem  
... vraiment tout ...
```

Enregistrement d'un certificat personnel dans une VO du LCG³⁹

<http://lcg.web.cern.ch/lcg/users/registration/registration.html>



The screenshot shows a Mozilla Firefox browser window titled "LCG Users Registration - Overview". The address bar contains the URL "http://lcg.web.cern.ch/lcg/users/registrator". The page content includes a navigation menu on the left with items like "Project Structure", "Project Planning", "Press&Media", "Documents", "Dissemination", "Jobs", "Activities", "LCG Users", "LCG Sites", and "LCG Operations". The main content area features a blue header "LCG Users Registration" and a navigation bar with links: "Overview", "Digital Certificates", "Loading Certificates", "Certificate Troubleshooting", "Personal Information", "Virtual Organization", and "Contact User Support". The "Overview" section contains the following text:

Overview
Registration of some personal data is required before using LCG. Due to the continued evolution of the grid environment and associated access policies and procedures **users will be required to re-register each year** and will be pre-notified by email when this is necessary.

To register for LCG you must complete the steps described below.

1. Read the [Grid Acceptable Use Policy](#). You will be required to agree to adhere to these rules.
2. Obtain a valid personal digital certificate (sometimes called a PKI or X509 certificate). ([more information here](#))
3. Load your personal certificate onto your browser ([more information here](#))
4. Decide which Virtual Organization you are affiliated. ([more information here](#))
5. Candidates of the following VOs should click on the VO name now.
[ALICE](#), [ATLAS](#), [CMS](#), [LHCb](#), [DTEAM](#), [ESR](#), [HONE](#), [ILC](#), [ZEUS](#), [Biomed](#), [Pheno](#)
6. Users interested in other VOs, please search for your VO [on the CIC portal](#)..
If you can't find it please open a [GGUS ticket](#).

Enregistrement dans la VO ATLAS

(le certificat est déjà chargé dans le navigateur)

40

VOMRS - ATLAS - Mozilla

File Edit View Go Bookmarks Tools Window Help

https://lcg-voms.cern.ch:8443/vo/atlas/vomrs?path=/Roc Search

Home Bookmarks ROOT v5-11.02 LEO De-En LEO De-Fr AliRoot Java Google

ATLAS VO Registration

- [-] ATLAS Registration Home
 - . Registration (Phase I)
 - . Groups and Group Roles
 - . Required Personal Info
 - . Certificate Authorities

Registration (Phase I)

Welcome to the ATLAS VO user registration phase I page.

All fields on this page are required. After submitting this form, a confirmation email will be sent within 24 hours with further instructions. If you fail to follow the instructions within 15 days, your registration will be discarded and you will have to re-register.

If you don't receive the confirmation email, please check your email address in VOMRS and change it if necessary. If it was correct, contact [the VO administrator](#).

Email address :

Select representative :

Grid job submission rights :

Personal Information

First name:

Last name:

You are logged in as /O=GRID-FR/C=FR/O=CNRS/OU=LPC/CN=Bogdan Vulpescu
/C=FR/O=CNRS/CN=GRID-FR

Trouver l'AC pour les expériences au LHC

LCG Users Registration - Digital Certificates - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://lcg.web.cern.ch/LCG/users/registration/certificate.html

LCG home | Calendar | Meetings | Contact Us

LCG User Registration

- Project Structure
- Project Planning
- Press&Media
- Documents
- Dissemination
- Jobs
- Activities
- LCG Users
 - User Registration
 - Users Support
 - Exp.Int.Supp
- LCG Sites
- LCG Operations

Digital Certificates

To use LCG you must possess a personal digital certificate from a CA recognised by LCG. The certificate will be needed both during the registration process and when you submit jobs to the grid. LCG accepts certificates issued by CAs from the [International Grid Trust Federation \(IGTF\)](#) and the [Fermilab KCA](#). Choose one appropriate to your location.

Certification Authorities (CA) recognised by LCG

(Most people should find their CA here)

[IGTF CAs](#)

<http://lcg.web.cern.ch/LCG/users/registration/certificate.html>

<http://www.eugridpma.org/members/worldmap/>

EUGridPMA CA Locator Map - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.eugridpma.org/members/worldmap/

EUGridPMA Clickable Map of Authorities

The EUGridPMA itself does not issue certificates. It coordinates national and regional authorities that issue certificates to end entities. Please select your country from the map below to be redirected to the issuing certification authority. If your country is not located on the European continent, go to your regional PMA (see below) or have a look at the [full plain-text Authorities list](#).

EUGridPMA Structures

- Membership
 - IGTF
 - APGridPMA
 - TAGPMA
 - TERENA
 - TACAR
- Documents
 - Charter
 - Guidelines
 - CAOPS-WG Wiki (closed)
- Technical Info
 - CA Distribution download
 - Subject Locator
 - Find your local CA
 - Newsletter issues
 - Subscribe
 - Service notices
 - Nagios monitoring

Récapitulation

- 1) Demandez un certificat auprès d'une AC
- 2) Récupérez le certificat sur votre navigateur web
- 3) Créez votre paire de clés publique/privée avec openssl
- 4) Enregistrez votre certificat dans un VOMS (Virtual Organisation Membership Service) correspondant à votre organisation virtuelle (ATLAS, ALICE, BIOMED, etc.)
- 5) Chargez votre certificat sur un navigateur différent sur le même poste de travail ou sur un autre poste de travail (optionnel...)
- 6) Contactez une page qui demande autorisation par certificat personnel

Quelques ressources:

<http://igc.services.cnr.fr/Doc>

<http://ca.cern.ch/ca>

<http://www.auvergrid.fr/infos/Certificate.php>

Exercices avec le middleware gLite – interface utilisateur (UI)

- certificat personnel
 - ordinateur portable
 - connexion réseau cable dans la salle
 - noeud utilisateur clrpc174.in2p3.fr avec gLite UI 3.1.8-0
 - utilisateur/mot_de_passe pour les participants
-
- autorisation sur la grille
 - écrire des fichiers en format “jdl” (Job Description Language)
 - envoyer des jobs (très simple) sur la grille
 - récupérer les resultats
 - manipuler les fichiers sur la grille (éléments de stockage)
 - suivre le parcours d'un job sur la grille