

Délégation aux systèmes d'information

SIGNATURE ÉLECTRONIQUE ET CERTIFICAT

Quelques points clefs

Avertissement

Ce document a été rédigé dans le seul but d'aider les utilisateurs novices de signatures électroniques et de certificats à s'initier à ces techniques en leur fournissant quelques explications simples.

Il n'a pas pour objectif de se substituer à une formation, à des ouvrages ou à la documentation qui accompagne ces outils.

Il a un parti pris dans l'illustration qui repose sur l'outil de gestion *options internet* de Microsoft®¹. Pour autant les informations fournies sont similaires dans tous les autres environnements et les explications sont les mêmes quels que soient les logiciels utilisés.

La terminologie utilisée dans ce secteur est souvent littéralement traduite de l'anglais (américain) ce qui peut lui donner parfois une emphase inappropriée.

Enfin ce fascicule peut comporter des erreurs qui pourraient être signalées à :

Contact*dsi.finances.gouv.fr (merci de remplacer * par @)

¹ Accès dans :

- q l'environnement MICROSOFT INTERNET EXPLORER® avec la fonction *Outils puis Options internet*. Choisir l'onglet *Contenu* puis presser le bouton *certificats*.
- q l'environnement MOZILLA® et NETSCAPE® avec la fonction *Edition puis préférences*. Choisir le panneau *Certificats* puis presser le bouton *Gestion des certificats*.

La signature électronique et le certificat



La signature électronique permet de mettre en œuvre un certain nombre de fonctions indispensables à la sécurité des échanges sur l'internet.

Si ses concepts et sa mise en œuvre sont simples, il n'en va pas de même de son usage pratique qui demande un minimum d'apprentissage.

En outre utiliser convenablement des outils, et ceux-ci en particulier, nécessite de bien comprendre leurs conséquences afin d'engager sa responsabilité de façon consciente et opportune.

Cet obstacle franchi il n'en demeure pas moins que l'ultime difficulté sera toujours de pouvoir s'assurer que celui avec qui je traite (eg : l'émetteur d'un message) est bien celui qu'il dit être (il a signé son message avec sa clef privée), puisque par construction sur l'Internet n'importe qui peut s'adresser à moi .

Bien entendu il est possible que je me fasse communiquer en face à face les éléments d'identification de chaque émetteur (le : la clef publique), mais si j'ai des centaines de correspondants la limite est vite atteinte.

Il faudra donc avoir recours à un intermédiaire dont la fonction sera de me garantir que celui qui s'adresse à moi est bien celui qu'il dit être.

Je vais donc devoir sous-traiter l'identification à un tiers de confiance qui me garantira que l'identité du porteur du certificat est vraie et que la clef privée pour signer est valide (celle qui est associée au certificat et donc au bon code secret).

En résumé, la signature ce sont les outils techniques qui peuvent être utilisés entre des internautes qui se connaissent a priori (ou dont les données ne sont pas importantes) alors que le certificat c'est la confiance qui permet des échanges entre des internautes qui ne se verront jamais ou dont les données ont de la valeur.

LA SIGNATURE



Les 4 services rendus par les outils

1) INTÉGRITÉ :

Le message émis arrive sans altération au destinataire. Dans le cas contraire le message est signalé comme ayant été modifié.

2) AUTHENTIFICATION

L'émetteur est authentifié, c'est à dire que ce qu'il déclare être est exact, que l'origine du message ou de la transaction sont incontestables.

3) NON RÉPUDIATION

Il est possible de prouver qu'un message a été envoyé par un émetteur précis et seulement par lui. Réciproquement celui qui a envoyé ce message ne peut en refuser la propriété.

4) CHIFFREMENT

Le message clair est transformé en cryptogramme.



Comment ces 4 services sont-ils rendus ?

1) L'intégrité :

Une partie du message est extraite (*empreinte*, ou hachage ou condensé, etc.) grâce à la fonction mathématique de hachage². Cette empreinte est transmise avec le message dont il faut vérifier qu'il n'a pas été altéré.

A la réception du message, et avec la même fonction, on prend une empreinte du message qui est comparée avec celle qui a été transmise.

Si les deux empreintes sont identiques alors le message est intègre.

Pour s'assurer que l'empreinte elle-même est transmise de façon intègre (on pourrait remplacer le message et l'empreinte !) celle-ci est chiffrée avec la clef privée de l'émetteur (A). Elle sera déchiffrée avec sa clef publique par le destinataire.

Bien sur il est possible de se demander pourquoi prendre une empreinte plutôt que de chiffrer le message, ce qui rendrait le même service.

Ceci tient au fait que le chiffrement est lent et que la taille des fichiers à chiffrer peut-être considérable.

La fonction de hachage restitue une empreinte qui est indissociable du document dont elle est extraite et qui est de longueur fixe et brève. Ainsi la durée du chiffrement est-elle toujours identique qu'elle que soit la taille du fichier à signer.

(Remarque : c'est le chiffrement de cette empreinte qui interdit parfois aux messages signés de franchir certaines passerelles de messageries car les pare-feux ne pouvant en extraire le contenu aux fins d'analyse, refusent le transfert).

² Les deux algorithmes les plus utilisés sont SHA1 et MD5.

2) L'authentification :

A une clef A (privée) correspond une clef B (publique) et une seule, et réciproquement.

Signer un message c'est lui joindre une empreinte de ce message chiffrée avec la clef privée A et qui de ce fait ne pourra être déchiffrée qu'avec la clef publique B.

Comme la clef B ne peut déchiffrer que ce qui a été émis par la clef A alors le message est bien émis par le détenteur de la clef privée A.

3) La non répudiation :

Si je suis sûr qu'un message a été signé par une clef privée A (et je peux en être sûr puisque je détiens la clef publique B qui ne peut fonctionner qu'avec la clef privée A) alors le message n'a pu être émis que par celui qui utilise la clef A.

Bien sûr il reste la question de savoir si celui qui l'utilise et qui s'authentifie est bien celui qu'il prétend être (le fait d'avoir la carte de paiement ne fait pas de moi son titulaire, il me faut aussi disposer du code) et cela c'est le rôle du certificat.

4) Le chiffrement :

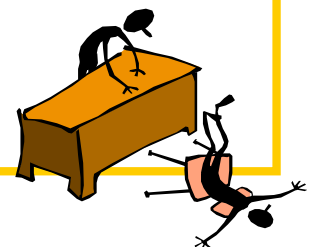
Le chiffrement avec des clefs asymétriques a ceci de remarquable que ce qui est chiffré avec l'une des deux clefs peut être déchiffré par l'autre (et bien sûr par elle seulement !).

C'est cette particularité qui est utilisée pour l'authentification : je chiffre l'empreinte avec ma clef privée – et je suis seul à pouvoir le faire – et le destinataire déchiffre avec ma clef publique – et tout le monde peut le faire.

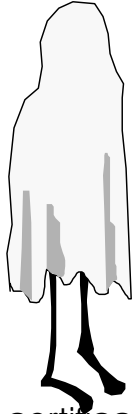
Pour envoyer un message chiffré dont on veut s'assurer que seul le destinataire pourra le lire c'est le contraire :

il faut utiliser sa clef publique pour chiffrer le message et lui seul avec sa clef privée pourra le rendre clair.

Ce qui rend le chiffrement périlleux c'est qu'en cas de perte de la clef privée il est alors impossible de déchiffrer les données qui sont alors perdues. C'est pourquoi les organisations ne fournissent cela qu'avec précautions. Certaines acceptent de « séquestrer » les clefs de chiffrement mais ceci pose des questions juridiques et techniques fort complexes et dont les réponses sont très coûteuses.



La signature est personnelle, tout prêt est interdit...



Le certificat associe la signature (couple clefs privée-publique) à une personne identifiée. Il le fait car sa délivrance est subordonnée à un minimum de contrôles d'identité dont le niveau fonde la confiance.

Ainsi les téléprocédures du MINEFI utilisent-elles uniquement des certificats délivrés en face à face et dont la qualité technique et le modèle économique ont fait l'objet d'audits.

Ce certificat pour être utilisé convenablement devrait toujours être associé à un code personnel, souvent appelé code PIN (Personal identification number). Ceci permet de procéder non seulement à l'identification, *je dis qui je suis*, mais aussi à l'authentification, *je suis qui je dis que je suis*, car je suis le seul à connaître le code.

On voit par là que la signature qui est placée sous le contrôle exclusif du titulaire ne peut être « prêtée » occasionnellement lors de congés ou d'absences à un secrétariat, un collaborateur ou un collègue.

La confiance serait profondément trahie et la réputation du titulaire détruite. En outre en cas de problèmes le titulaire serait pris dans une étreinte fatale :

- ∅ s'il reconnaît qu'il y a eu fausse signature il admet la rupture du contrat et il met la personne à laquelle il a confié le code dans une situation périlleuse puisque elle a fait un faux.
- ∅ - S'il ne veut pas admettre la fausse signature alors il assume les conséquences de l'opération puisque il est réputé avoir lui-même réalisé l'opération.



En réalité dans la majorité des cas la question posée est celle de la gestion du temps. On « prête » ou on « confie » sa signature lorsque il n'y a pas eu de délégation de faite et car on est pris de court.

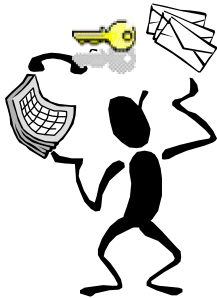
La délégation (momentanée ou permanente, limitée ou générale, etc.) n'est pas vraiment utilisée sauf dans des circonstances majeures, éloignement permanent, volumétrie excessive, car elle doit être anticipée et il est difficile et lent d'en informer ceux qui ont à en connaître (Eg : publication ou courrier préalable officiels, etc.). En outre les comportements actuels qui remontent à la nuit des temps administratifs permettent de s'en affranchir dans la majorité des cas.

Ce qui est donc essentiel c'est de définir à l'avance les règles d'usage et d'en assurer leur publication. Ceci facilite les pratiques et crée le climat de confiance nécessaire aux progrès de la dématérialisation.

La signature numérique rend-elle les mêmes services que celle qui est manuscrite ?

Non ! Elle en donne plus !

Les procédures administratives nécessitent souvent que plusieurs personnes puissent signer le même document, successivement ou simultanément. Dans certains environnements seuls les courriers signés par deux responsables ont un plein effet.



Les outils de signature électronique permettent d'intégrer plusieurs signatures dans un document et garantissent la mise en évidence des modifications introduites par un signataire

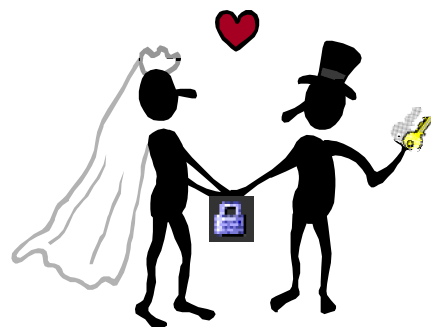
Ainsi il est possible d'avoir la certitude qu'un texte a bien été signé de façon identique par les signataires.

Ces outils travaillent soit avec des formats peu ou prou propriétaires (Eg : Adobe®), soit avec des formats ouverts (Eg : SXML).

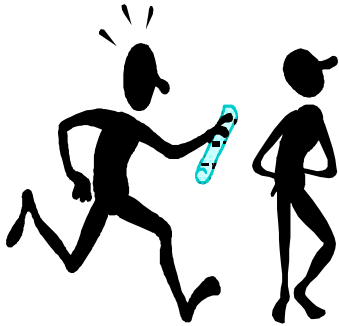
De plus la vérification de ces signatures pourra avoir lieu bien des années plus tard sans qu'il soit besoin de reprendre contact avec leurs titulaires.

Cette capacité à pouvoir être vérifiée en ligne, sans limite de temps et dans tous les environnements permet d'envisager une dématérialisation totale où les seuls freins seront les limites des outils et celles de l'imagination.

Ceci n'en fait pas pour autant la panacée et certaines circonstances ne semblent pas a priori propices à son usage...



LA CONFIANCE



Le certificat

Son usage essentiel est de permettre L' AUTHENTIFICATION

Qu'est-ce qu'un certificat ?

Selon le dictionnaire³: c'est un « écrit officiel ou dûment signé d'une personne compétente , qui atteste un fait ».

C'est un « écrit... :

il s'agit ici d'un fichier qui contient pour l'essentiel le nom du porteur et sa clef publique, ainsi que des informations de gestion (dates, algorithmes, etc.)

...officiel ou dûment signé d'une personne compétente... :

une organisation émettrice (personne compétente), ainsi la DPMA du MINEFI, la DGTPE, la DGI, les Autorités de certification qui vendent des certificats référencés, etc.

...qui atteste un fait :

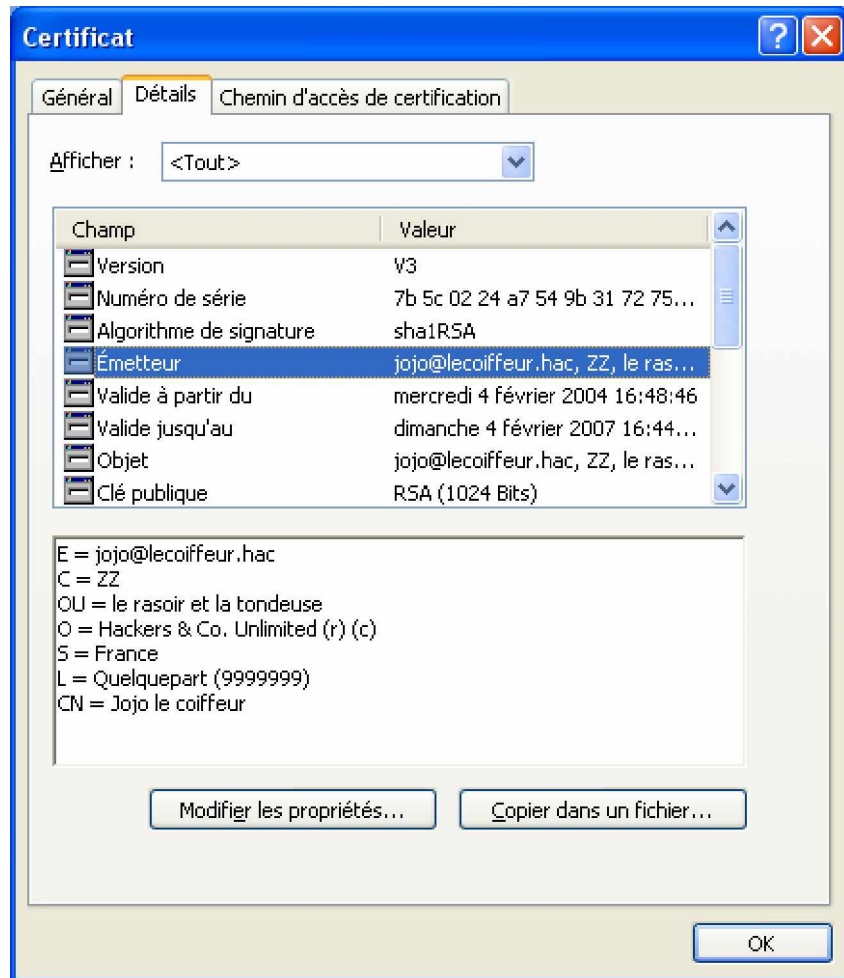
le contenu du fichier (clef publique du porteur, nom, etc.) est bien celui qu'il doit être et que ce contenu appartient à la personne qui le revendique.

Qu'y trouve t'on ?

- Le nom du porteur ,
- La clef publique du porteur de ce certificat,
- Les dates de validité,
- L'organisation (si nécessaire) à laquelle appartient le porteur ,
- L'adresse où trouver les listes de certificats révoqués (LCR),
- ET le nom de l'entreprise de confiance, c'est à dire de l'autorité de certification, qui a émis ce certificat,
- La signature de cette AC sur ce certificat,
- On pourrait aussi y trouver la photographie du porteur ou du logo de l'entreprise.
- Etc.

³ Les définitions sont extraites du Petit Larousse illustré.

Est-il possible de voir et de lire le contenu d'un certificat ?



Le contenu de celui-ci n'inspire pas la plus grande confiance ?
 Et pourtant l'essentiel n'est-il pas de s'assurer que ceux avec qui
 l'on va traiter (ou non !) sont bien identifiables et que le cas
 échéant il serait possible de les retrouver ?
 Alors comment faire pour répondre à ces questions ?

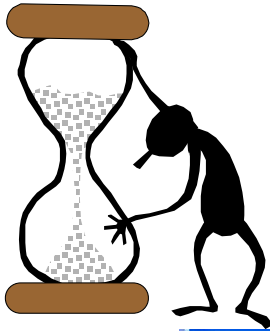


§ Il faut s'assurer que le certificat est utilisable et
 § il faut connaître l'autorité de certification qui a délivré le certificat et
 mesurer la confiance qu'il est possible de lui accorder, car c'est elle qui
 possède la preuve du lien entre la clef et son propriétaire de même qu'elle
 connaît son identité réelle, son domicile, etc.

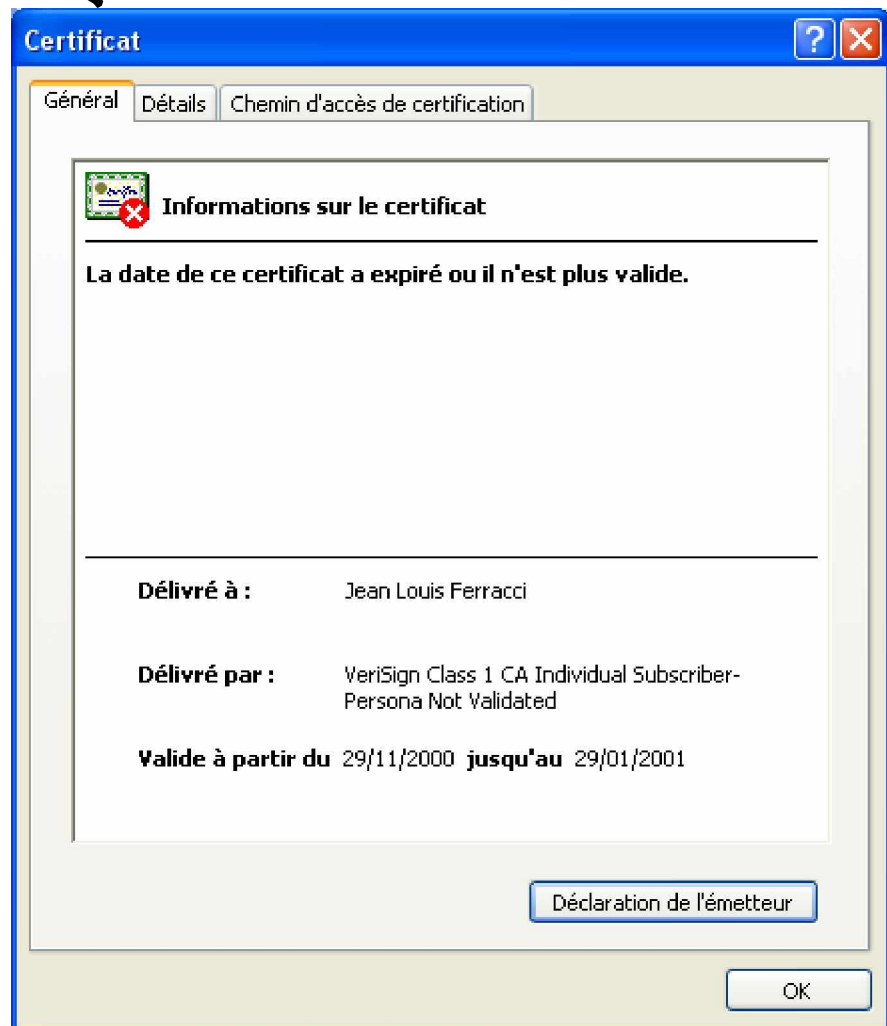
Comment vérifier un certificat ?

Trois éléments, au moins, du certificat doivent systématiquement être
 vérifiés :

- § la validité
- § la révocation
- § l'usage

La validité

L'outil de signature vérifie automatiquement la validité temporelle du certificat et donne un avertissement dans le cas où le certificat a expiré.





La révocation

Le deuxième élément à vérifier est que le certificat est toujours utilisable. Il faut s'assurer qu'il n'a pas été révoqué.

Cette révocation peut intervenir à la demande :

- § du porteur du certificat (Eg : en cas de perte du code secret –PIN-),
- § de l'autorité de certification (Eg : en cas de non paiement du certificat par le porteur),
- § de l'organisation qui a acheté un certificat pour l'un de ses membres lors du départ de celui-ci.

La révocation peut intervenir à tout moment et il faut donc vérifier le certificat à chaque utilisation.

L'utilisateur peut télécharger la liste des certificats révoqués publiée par l'AC émettrice du certificat :

Certificat

Général Détails Chemin d'accès de certification

Afficher : <Tout>

Champ	Valeur
Contraintes ...	Type d'objet: Entité finale, Contrainte de longueur
Points de dist...	[1]Point de distribution de la liste de révocation d...
Stratégies de...	[1]Stratégie du certificat : Identificateur de strate
Type de certi...	Authentification de client SSL (80)
2.16.840.1.1...	01 01 ff
Algorithme d'...	sha1
Empreinte nu...	ea 0c e3 ad c6 22 93 e3 64 f0 f6 12 f4 fd 83 42 1

[1]Point de distribution de la liste de révocation de certificats

Nom du point de distribution :

Nom complet :

URL=http://onsitecrl.certplus.com/BANQUEPOPULAIRENATEXISBANQ
UESPOPULAIRESNXBPCESAMRelationsFiscalesAC/LatestCRL
URL=ldap://ldap.certplus.com/cn=NATEXIS%20BANQUES%
20POPULAIRES%20-%20NXBP%20CESAM%20Relations%
20Fiscales%20-%20AC,ou=NXBP%20ENTREPRISES,o=BANQUE%

Modifier les propriétés... Copier dans un fichier...

OK

Liste de révocation des certificats

Général Liste de révocation

LCR téléchargée

Certificats révoqués :

Numéro de série	Date de révocation
39 36 35 31 33 39 37 37 39 35 36 32	mercredi 2 août 21
39 36 35 31 33 39 37 39 34 35 33 32	mercredi 2 août 21
39 36 35 37 32 31 33 33 35 38 37 35	mercredi 9 août 21
39 36 35 37 32 31 33 35 30 37 30 34	mercredi 9 août 21

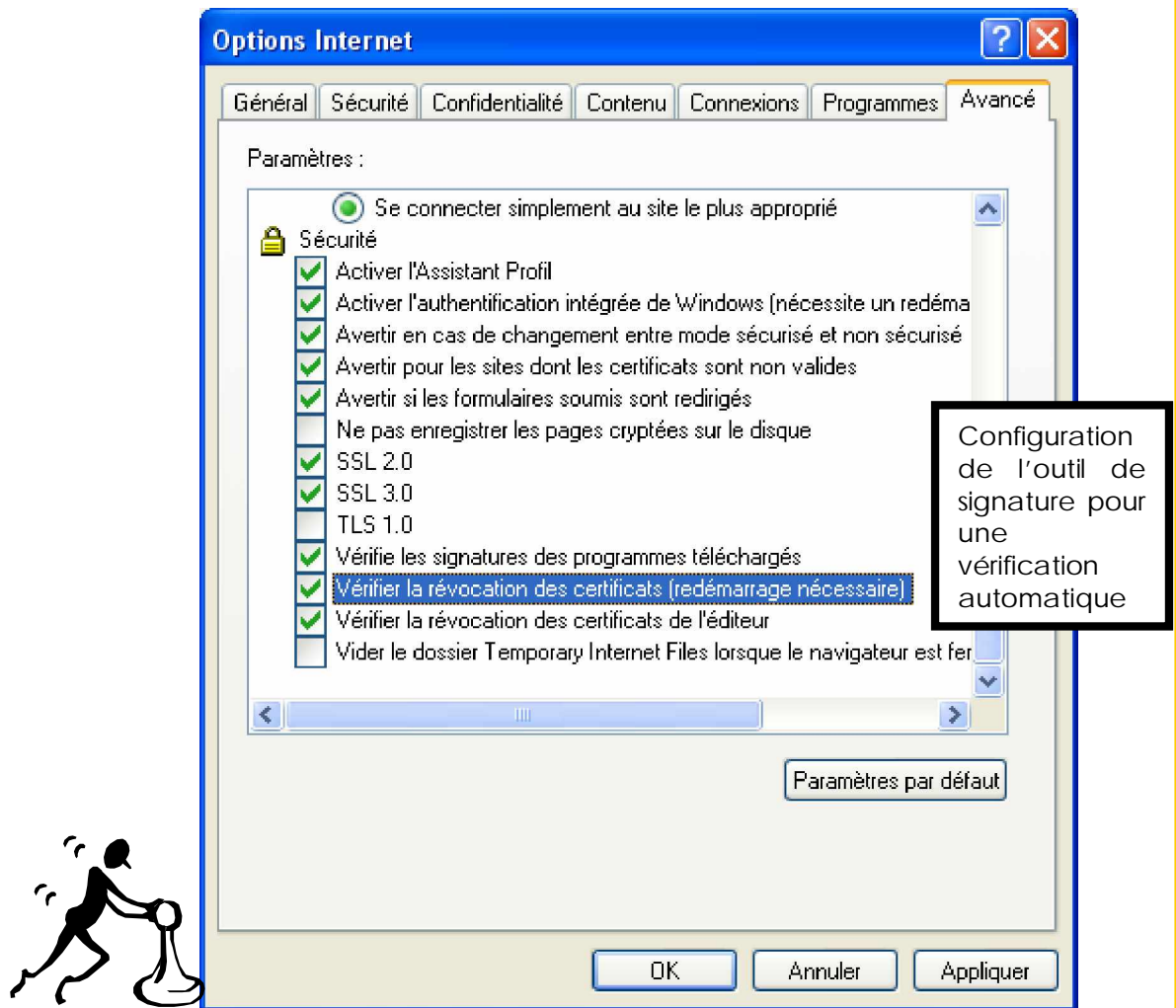
Entrée de révocation

Champ	Valeur

Valeur :

OK

...ou demander à l'outil de signature de le vérifier automatiquement :



Bien sur pour cela il faudra être connecté...



L'usage

Les autorités de certification sont très vigilantes sur le point de savoir si les conditions d'usage des certificats sont bien respectées.

Celles-ci font toujours l'objet d'une publication sur le site de ces organisations. Ces conditions sont appelées *Politiques de certification* et elles sont identifiées.

Ce numéro unique et l'adresse de publication peuvent être rappelés dans le certificat lui-même.

The screenshot shows the 'Certificat' dialog box with the 'Détails' tab selected. A table lists certificate fields:

Champ	Valeur
Contraintes de base	Type d'objet=Entité finale, Contrainte de l...
Stratégies de certificat	[1]Stratégie du certificat : Identificateur d...
Type de certificat N...	Authentification de client SSL (80)
Points de distributio...	[1]Point de distribution de la liste de révoc...
Algorithme d'emprei...	sha1
Empreinte numérique	5c 5d 6b a5 f0 24 f2 8f 05 4c 3d c0 61 ad t...

Below the table, the following details are shown:

- [1]Stratégie du certificat :
- Identificateur de stratégie=2,16,840.1.113733.1.7.1.8
- [1,1]Informations sur le qualificatif de stratégie :
- ID du qualificatif de stratégie = CPS
- Qualificatif :
- <https://www.verisign.com/rpa>

Avant d'utiliser de façon habituelle un certificat il est vivement recommandé de lire ce document afin d'en avoir un usage *ad hoc* et de bénéficier de la garantie de l'AC.

OID du document (numéro unique attribué par un organisme normalisateur. Sur l'internet l'ISO ou IANA.)

L'adresse (URL) où est publié le document

The screenshot shows the VeriSign website with the following content:

- VeriSign Inc. - www.verisign.com - Microsoft Internet Explorer
- Address bar: <https://www.verisign.com/repository/rpa.html>
- Navigation: Solutions | Products & Services | Support | About VeriSign | Contact | Search
- Section: **PRODUCTS & SERVICES**
- Sub-section: **VeriSign Relying Party Agreement**
- Text: YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING A VERISIGN TRUST NETWORKSM DIGITAL CERTIFICATE ("CERTIFICATE"), USING VERISIGN'S ONLINE CERTIFICATE STATUS PROTOCOL ("OCSP") SERVICES, OR OTHERWISE ACCESSING OR USING A VERISIGN OR VERISIGN AFFILIATE DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION LIST ISSUED BY VERISIGN, INC. ("VERISIGN CRL"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS OR USE ANY VERISIGN CRL BECAUSE YOU ARE NOT AUTHORIZED TO USE VERISIGN'S REPOSITORY OR ANY VERISIGN CRL. IN CONSIDERATION OF YOU AGREEING TO THE TERMS OF THIS RELYING PARTY AGREEMENT, YOU SHALL BE PERMITTED TO RELY ON CERTIFICATES ACCESSED BY YOU IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT.
- Section: **1. Background.** This Agreement becomes effective when you submit a query to search for a Certificate, or to verify a digital signature created with a private key corresponding to a public key contained in a Certificate, by downloading a VeriSign CRL, or when you otherwise use or rely upon any information or services

Comment faire confiance au certificat ?

En réalité c'est à l'autorité de certification (AC) qui a émis le certificat que l'on fait confiance

Il est possible que l'une de ces deux AC inspire plus de confiance que l'autre ?

Une autorité de certification est une entreprise qui garantit :

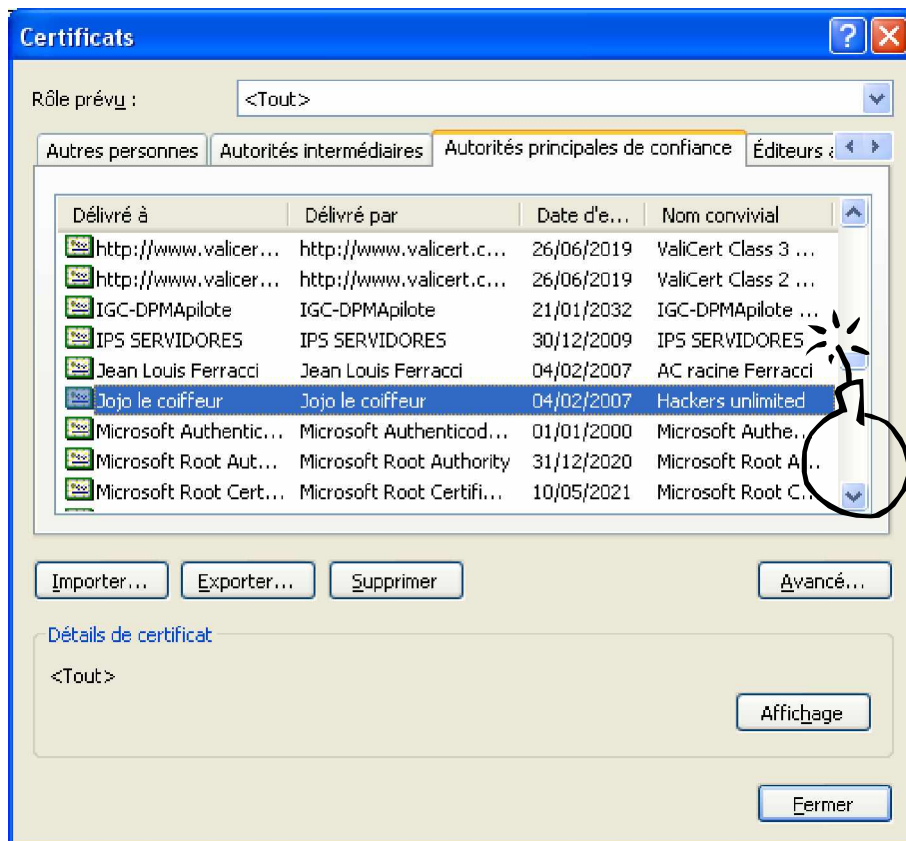
- ∅ l'identité de la personne qui utilise des clés de signature. Cette garantie peut être plus ou moins grande selon le protocole utilisé (et donc le coût). Les certificats utilisés par les téléprocédures du MINEFI sont tous délivrés en face à face avec une production de papiers d'identité, ainsi qu'il est prévu dans la PRIS V1.
- ∅ L'usage des clés par une personne qui en est la seule et unique propriétaire.

Le certificat concrétise cette garantie.

Comment faire confiance à une autorité de certification ?

Chacun le sait, la confiance ne doit être accordée que parcimonieusement et après investigations.

Il ne suffit pas en effet d'apparaître dans la liste des autorités principales de confiance de son outil de signature pour être une AC sérieuse apte à délivrer des certificats convenablement : Jojo le coiffeur s'est aussi immiscé dans la liste des autorités principales de confiance !



Mais alors à qui faire confiance si même ce qui apparaît dans le navigateur est sujet à caution?

L'usager a trois moyens à sa disposition :

er

Les institutions publiques publient des listes de certificats acceptables, ce que fait le MINEFI, et l'ADAE prendra le relais bientôt :

http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm

émis par des entreprises dont la réputation, le modèle économique et les processus techniques ont fait l'objet d'un audit, ce qui leur permet d'être référencé selon des critères de qualité élevés. Ceux-ci sont décrits dans la *politique de certification type* du MINEFI (même URL que ci-dessus) et dorénavant dans la *politique de référencement intersectoriel de sécurité* (PRIS) qui est disponible sur le site de l'ADAE.

Ces certificats sont acceptés pour toutes les téléprocédures de la sphère publique conformément aux prescriptions de l'ADAE. Il est possible de vérifier que Jojo le coiffeur n'y figure pas et donc d'être assuré que les envois signés et accompagnés par un certificat référencé offre toutes les garanties requises pour des échanges hautement sécurisés.

II^{ème}

Les éditeurs d'outils de signature (Lucent technology, Microsoft, Sun, etc.) intègrent dans les magasins de certificats, et dès la production, les certificats racines des AC qu'ils ont agréés selon un processus qui leur est propre. Il est bon de s'assurer que ceux qui y figurent sont bien ceux que l'éditeur a choisi d'y mettre en comparant la liste fournie par le navigateur et celle publiée sur leurs sites.

Il n'est pas inutile non plus de se souvenir que les prescriptions en matière de sécurité demandent une acceptation consciente des certificats. La bonne pratique consistant donc à ôter tous les certificats pour n'intégrer qu'au fur et à mesure ceux dont le besoin et la qualité justifient l'usage.

III^{ème}

Enfin il est possible de faire confiance à une AC dont on connaît les promoteurs.

En effet bien que ne figurant ni dans la liste publiée par le MINEFI ou l'ADAE, ni dans celles des éditeurs (en général car elles n'appartiennent pas au secteur marchand) elle sont tout à fait respectables.

Le MINEFI par exemple, mais le CNRS, le ministère de la Justice, de l'Education nationale, et bien d'autres organisations sont dans ce cas.

En résumé il y a donc les autorités de certification « conseillées », dont certains certificats sont référencés par l'Etat, voire par les éditeurs, et celles auxquelles il est fait confiance par un choix personnel et éclairé.

Ces certificats sont fiables, les règles d'usage sont connues et leurs titulaires identifiés pourront être retrouvés si nécessaire :

la confiance est établie.

