

En pratique



Utilisation des certificats X.509v3

- × Commerce électronique, avec HTTPS (HTTP/SSL)
 - × Authentification SSL/TLS par certificat, obligatoire pour le serveur
 - × Authentification optionnelle pour le client (SSLv3/TLSv1)
- × Message électronique sécurisée
 - × Confidentialité et authenticité des messages
 - × Entre utilisateurs finaux, avec S/MIME
 - × Entre MTA, avec SMTP-TLS
- × Sécurisation des infrastructures réseau
 - × Tunnels IPSec
- × Gestion de l'entreprise
 - × Intégration aux ERP
- × Dématérialisation des procédures de l'administration
 - × Horodatage des documents, non répudiation des transactions
- × Contrôle d'accès et gestion de privilèges



Les certificats dans IE 5.0 : Panorama

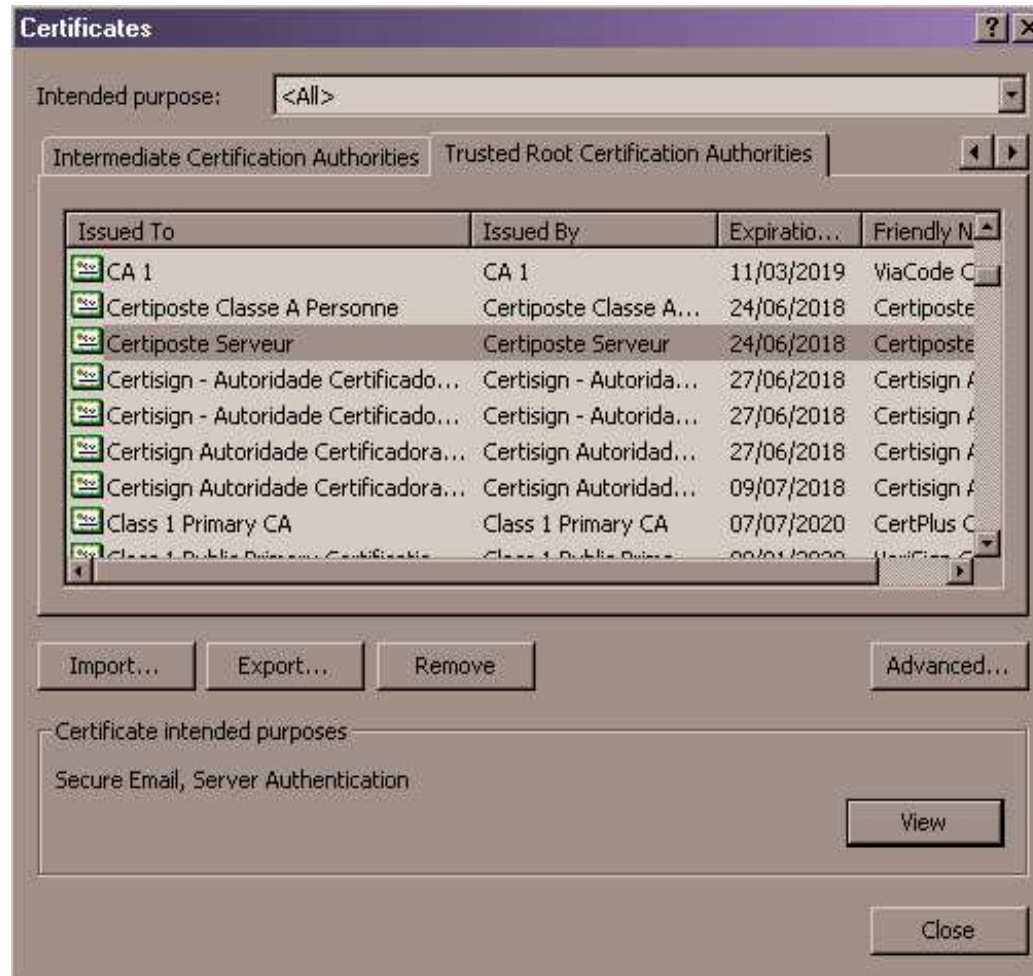
- × Trois grandes classes de certificats X.509
 - × Certificats Racines
 - × Certificats Intermédiaire s (autorités de certification non autosignées)
 - × Certificats Personnels (théoriquement non autorisées à délivrer de certificats)
 - × Manipulation des certificats X.509
 - × Via l'interface graphique
 - × Conviviale, mais peu pratique
 - × Via la suite d'outils "Authenticode for IE 5.0"
 - × Assez « puissante », mais non livrée en standard
 - × Exemple : Exportation des certificats racines
- ```
c:\ certmgr -add -all -c -s root -7 win2k_rootcerts.der
```
- × Résultat : Liste de 106 certificats, au format PKCS#7
    - × Certificats de confiance ?

```
DN : C=hk, O=C&W HKT SecureNet CA SGC Root...
DN : C=UY, O=ADMINISTRACION NACIONAL DE CORREOS...
DN : C=MX, CN=Autoridad Certificadora del Colegio Nacional de
Correduria Publica Mexicana, A.C., O=Colegio...
```



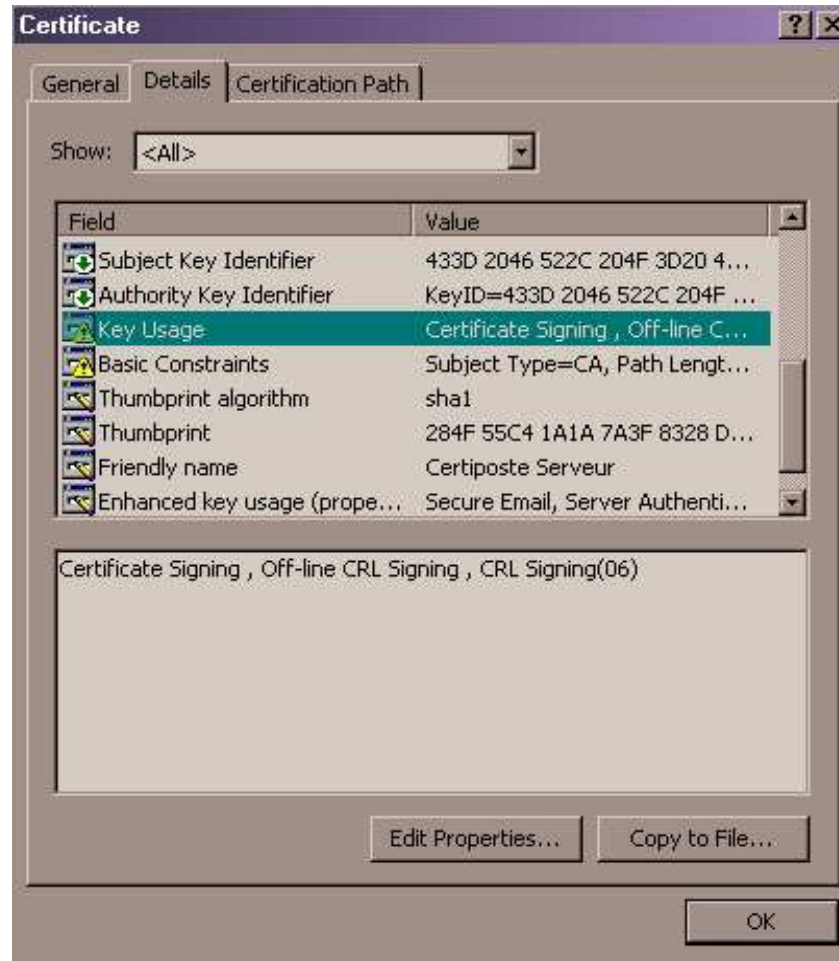


# IE 5.0 : Autorités de certification (1/3)



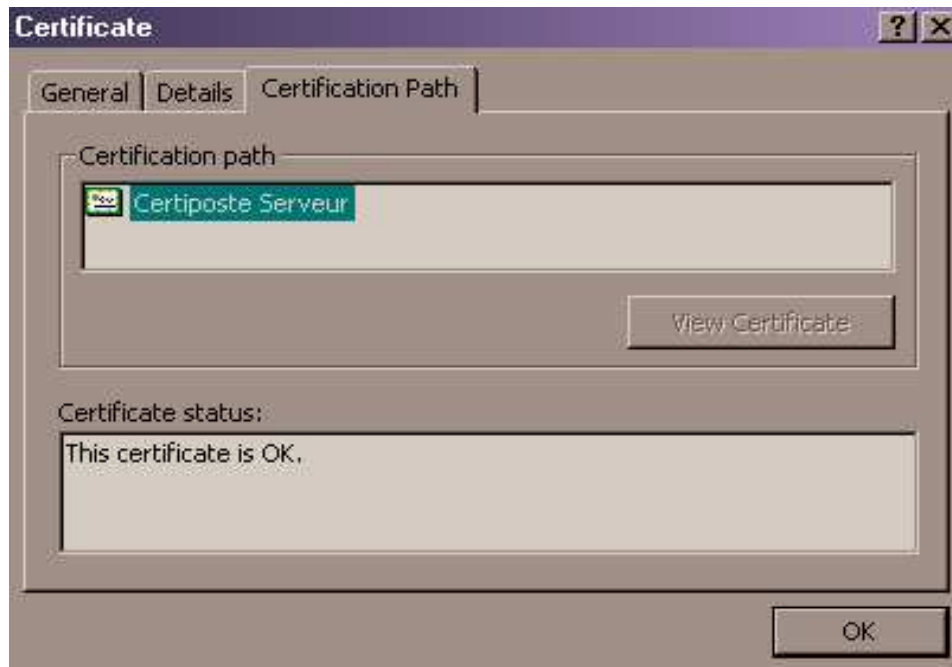


# IE 5.0 : Autorités de certification (2/3)



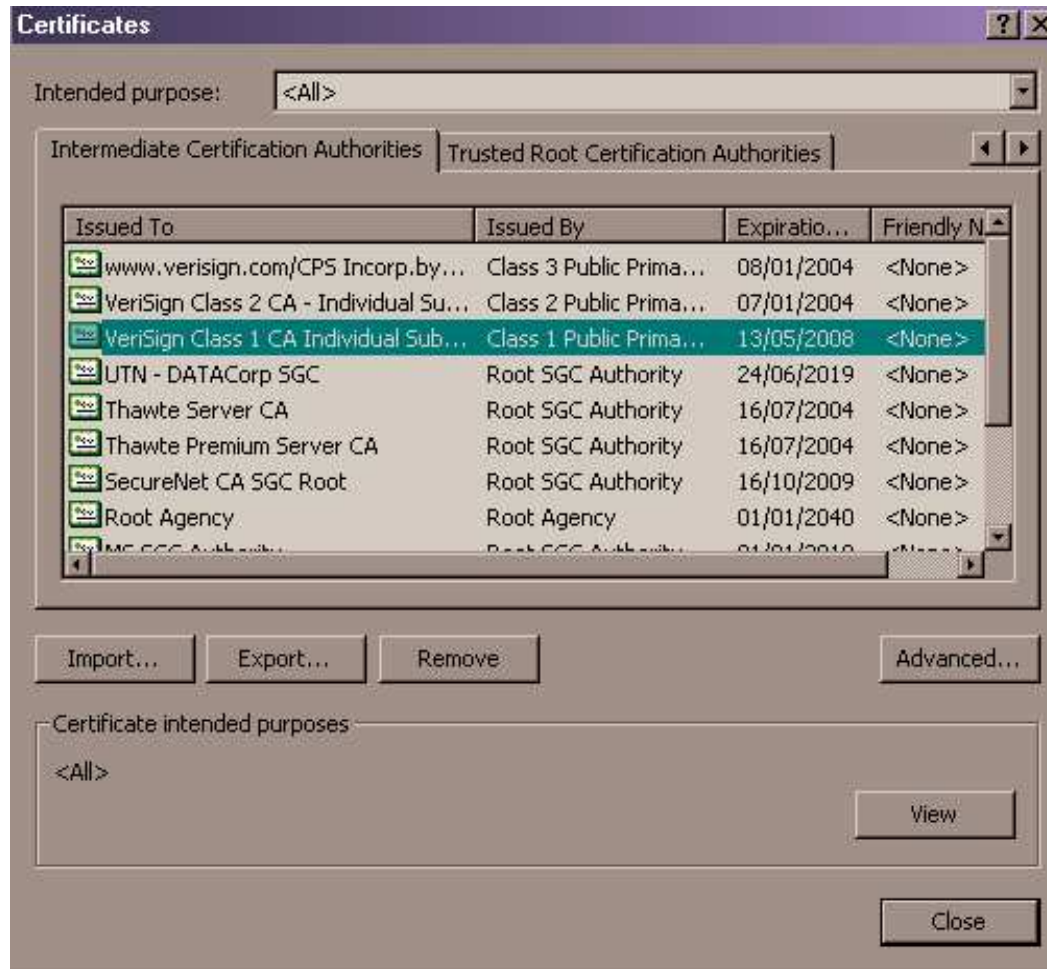


# IE 5.0 : Autorités de certification (3/3)



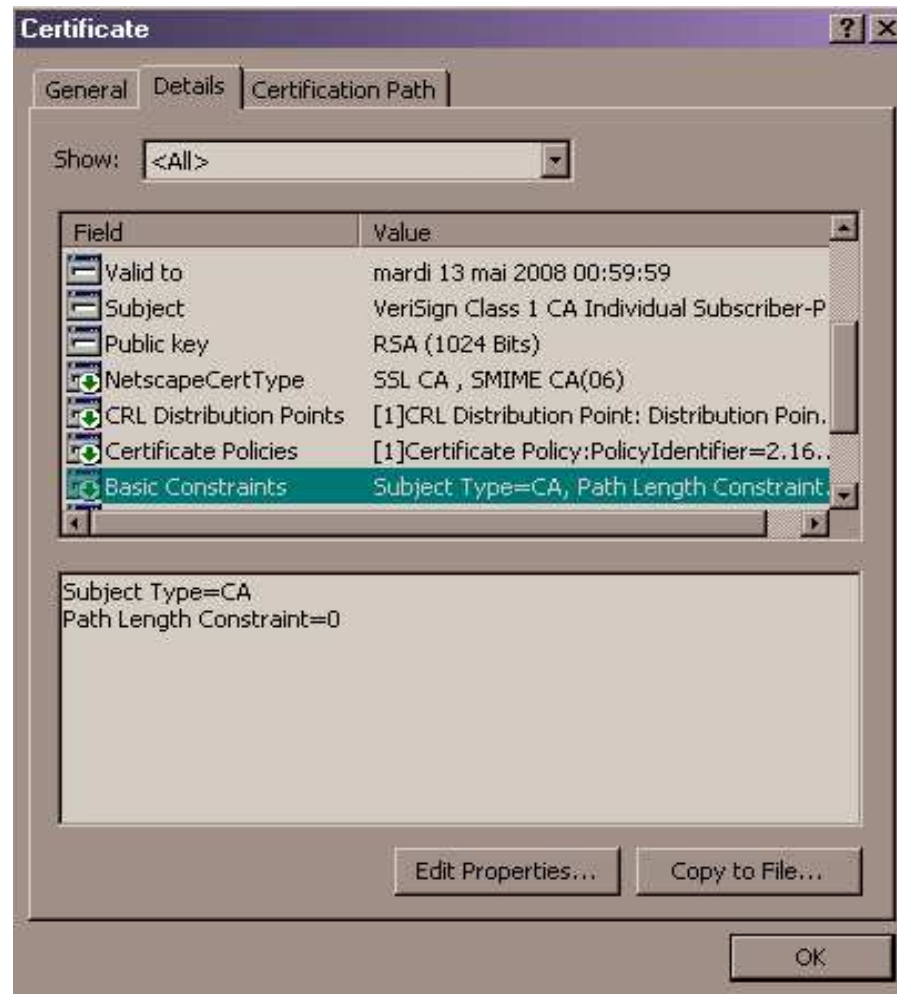


# IE 5.0 : Autorités intermédiaires (1/3)



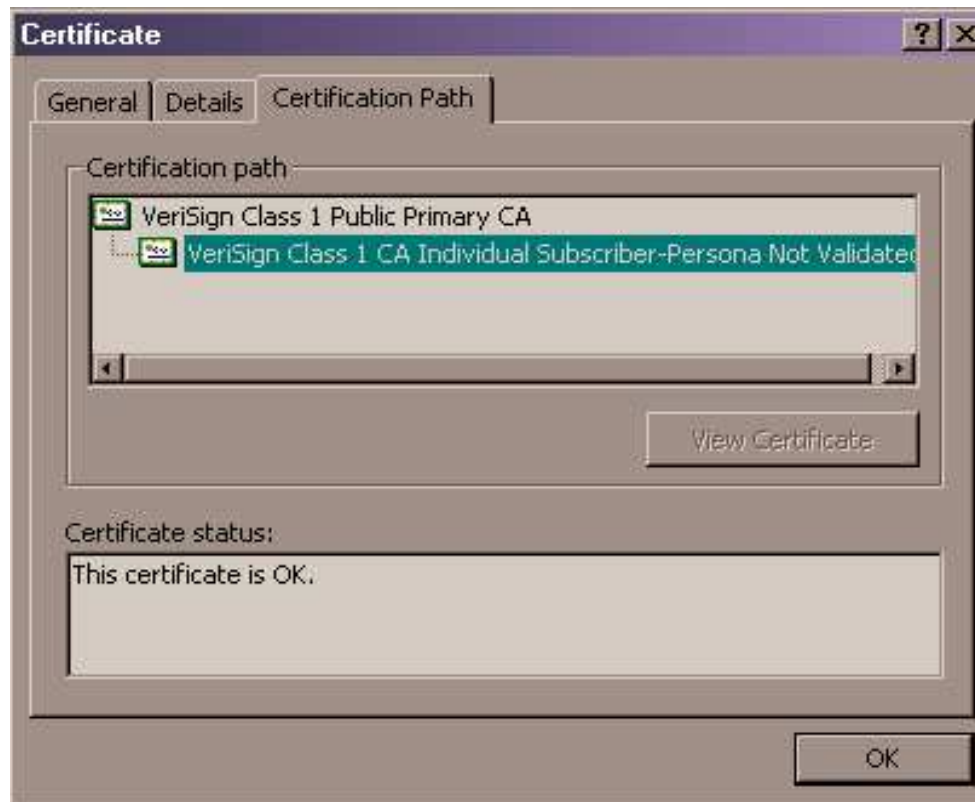


# IE 5.0 : Autorités intermédiaires (2/3)





## IE 5.0 : Autorités intermédiaires (3/3)





# Quelques chiffres... (1/2)

## Champs Standards

- \* Nombre de certificats (racines) référencés : 106
- \* Répartition par pays

| Pays | AU | BE | BR | CH | DE | ES | FI | FR | GB | HK | HU | IT | JP | MX | NL | US | UY | ZA | Ind. |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
|      | 4  | 2  | 4  | 1  | 7  | 4  | 2  | 7  | 1  | 4  | 3  | 2  | 3  | 2  | 1  | 41 | 1  | 6  | 11   |

- \* Version des certificats
- | Version | 1  | 2 | 3  |
|---------|----|---|----|
|         | 44 | 0 | 62 |

- \* Taille des clefs
- | Taille (RSA) | 1000 | 1024 | 2046 | 2048 |
|--------------|------|------|------|------|
|              | 1    | 62   | 2    | 41   |

- \* Les racines possédant ces clefs exotiques étant :

(1000) Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server Certification Authority

(2046) Issuer: C=FR, O=Certiposte, CN=Certiposte Classe A Personne

Issuer: C=FR, O=Certiposte, CN=Certiposte Serveur





## Quelques chiffres... (2/2)

### Extensions v3

- \* X509v3 Key Usage : 40 (14 critical)
  - \* Certificate Sign : 40
  - \* CRL Sign : 38
  - \* Digital Signature : 11
  - \* Non Repudiation : 7
- \* X509v3 Basic Constraints : 60 (33 critical)
  - \* CA:TRUE : 60
  - \* Pathlen : 15

|         |   |   |   |   |   |    |
|---------|---|---|---|---|---|----|
| Pathlen | 1 | 3 | 4 | 5 | 8 | 10 |
|         | 1 | 3 | 3 | 2 | 1 | 5  |
- \* X509v3 CRL Distribution Points : 22
  - \* URI : 13
  - \* DirName : 10
- \* Disponibilité des CRL :
  - \* 404 Not Found : 6
  - \* 503 Service Unavailable : 2
  - \* 200 OK : 5





# Démonstrations : HTTPS (1/8)

## Le protocole HTTPS

- × Authentification du serveur par certificat X.509
- × Authentification du client par certificat X.509 (SSLv3/TLSv1 uniquement)
- × Importation de la paire certificat/clef privée via PKCS#12
- × Suivi de session authentifiée et gestion des autorisations au niveau du serveur
  - Restriction d'accès selon :
    - × DN (Organisation, pays etc.)
    - × Plages horaires
- × Configuration
  - × Serveur Apache + Mod\_SSL
  - × OpenSSL, pour la génération des certificats





## Démonstrations : HTTPS (2/8)

### Limitations :

#### incompatibilité entre les protocoles SSL/TLS et HTTP/1.1

- × Problématique
  - × Entête 'Host:' introduite en HTTP/1.1
    - × Extension HTTP/1.0 dans les navigateurs modernes
  - × Hébergement de plusieurs sites pour une même instance de serveur WEB
    - × Distinction et distribution des requêtes suivant :
      - × L'adresse IP
      - × Le nom référencé par l'entête Host
- × Limitation
  - × Utilisation des protocoles SSL/TLS
    - Protocole SSL/TLS se déroulant avant tout dialogue HTTP
- × Problème de validation d'un certificat
  - × Le nom présenté via le RDN 'CN' dans le certificat X.509 ne coïncide pas forcément avec le nom de domaine pleinement qualifié (FQDN) par lequel le serveur HTTPS est accédé



## Démonstrations : HTTPS (3/8)

### Illustration

```
$ openssl s_client -connect 192.70.106.69:443
CONNECTED(00000003)

Server certificate
-----END CERTIFICATE-----
subject=/C=FR/ST=Ile-de-France/L=Levallois-Perret/O=Herve Schauer Consultants/CN=www.webserver.com
issuer=/C=FR/ST=Ile-de-France/L=Levallois-Perret/O=Herve Schauer Consultants/CN=CA SSL

No client certificate CA names sent

SSL handshake has read 3360 bytes and written 320 bytes

New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
Server public key is 1024 bit
SSL-Session:
Protocol : TLSv1
Cipher : EDH-RSA-DES-CBC3-SHA
Session-ID: 399FF3BB460AE2A297079497F1BE7A0DB73973F99808ED12569C571B59FEF525
Master-Key:
94B3A8FFCEA690E35AA138AFC496AF803CD8F3C70C1617E44AF5AB0919D5F6DB2630C9F1AFB0D6C53FA7F0107E38DFF3
Verify return code: 0 (ok)

GET / HTTP/1.0
Host: UnAutre.webserver.com

HTTP/1.0 200 ok
Content-type: text/html
```





## Démonstrations : HTTPS (4/8)

### Hôtes virtuels par adresse IP

- × Génération des certificats
  - × Champ CN égal au FQDN
  - × Génération « classique »
  - × Mécanisme transparent pour l'utilisateur
- × Utilisation de plusieurs adresses IP
- × Alternative similaire : utiliser des ports différents

### Hôtes virtuels par nom

- × Une et une seule adresse IP
- × Utilisation d'alias DNS (CNAME)
  - × Un seul certificat X.509 est présenté pour les 2 hôtes hébergés...



# Démonstrations : HTTPS (5/8)

## Hôtes virtuels par nom



## Hôtes virtuels par adresse IP





## Démonstrations : HTTPS (6/8)

### Méthodes de validation des certificats

- × Netscape
  - × Gestion des wildcards et expressions rationnelles dans le champ CN
  - × Gestion des CN multivalués
  - × Spécification Netscape (SSLv3) :
    - × [http://www.netscape.com/eng/security/ssl\\_2.0\\_certificate.html](http://www.netscape.com/eng/security/ssl_2.0_certificate.html)
- × Internet Explorer
  - × Gestion des subjectAltName multivalués de type dNSName
  - × En cas de subjectAltName non présent :
    - × Gestion du CN avec wildcards
    - × Conformité partielle à la RFC2818 [HTTP/TLS]





## Démonstrations : HTTPS (7/8)

### Problématique

- × Internet Explorer 5.01 ne gère pas les wildcards
  - × <http://support.microsoft.com/support/kb/articles/Q258/8/58.ASP>
  - × <http://www.thawte.com/support/server/wildcards.html>
- × Application de correctifs nécessaire
  - × Peu envisageable à grande échelle, et face à une population cliente non identifiée

### Solution

- × Certificat « hybride »
  - × Valeur du commonName
    - × `(foo|bar).webserver.com` ou `*.webserver.com`
  - × X509v3 Subject Alternative Name:
    - × `DNS:foo.webserver.com, DNS:bar.webserver.com`

## Pour aller plus loin...

- × « SSL and TLS – Designing and Building Secure Systems » (Eric Rescorla)
  - × Addison-Wesley, 2001 ISBN 0-201-61598-3
  - × <http://www.rtfm.com/sslbook/>
- × « SSL/TLS : du concept à la pratique »
  - × <http://www.hsc.fr/~davy/ssl-tls.pdf>

# Exemple de PKI : télédéclaration des impôts (1/9)

## Service de déclaration des impôts en ligne

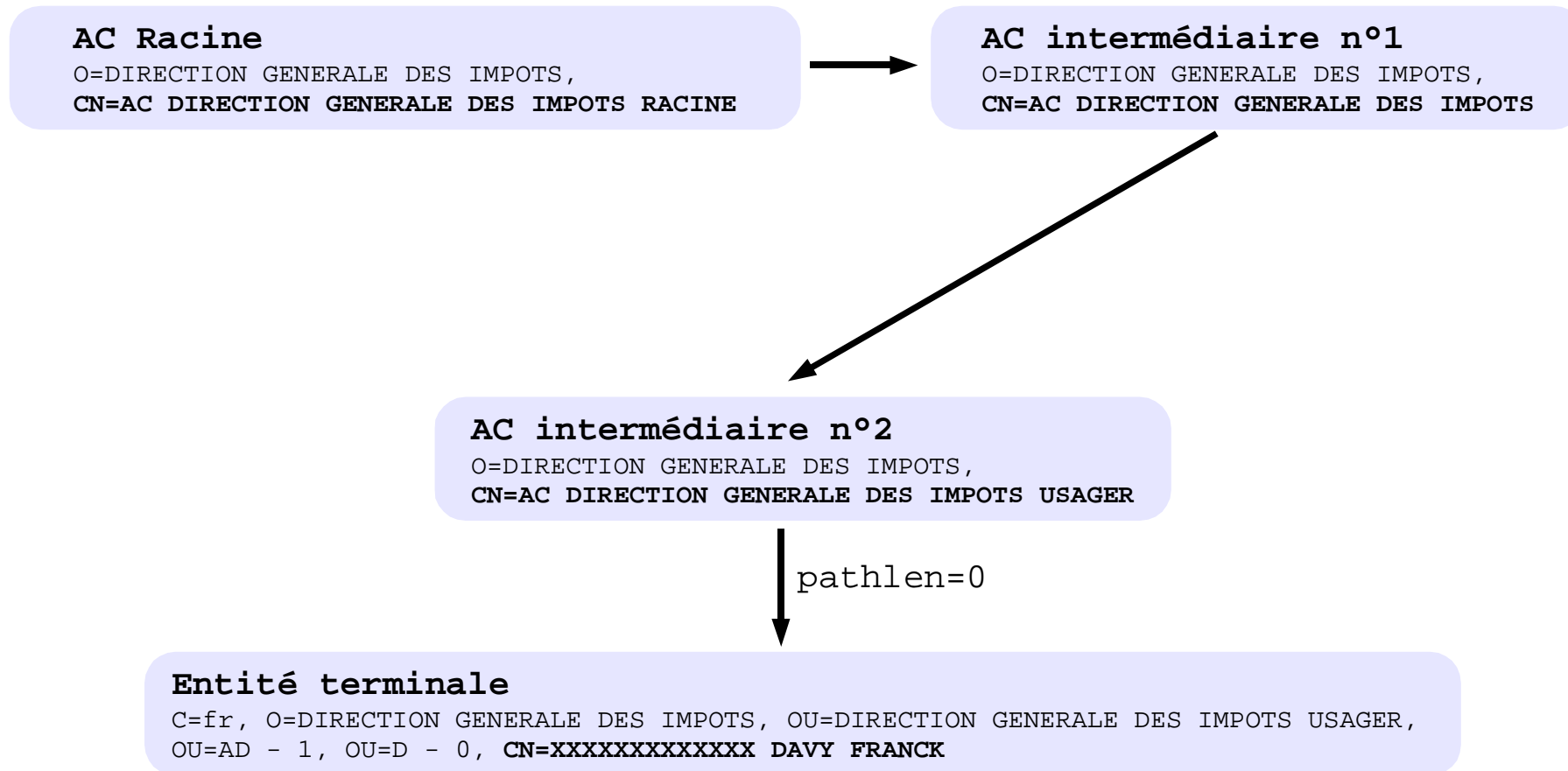
<http://www.ir.dgi.minefi.gouv.fr/>

- × Usage du certificat X.509 client généré
  - × Authentification client SSLv3/TLSv1 (*gérée par le navigateur*)
    - × Restriction de l'accès au site HTTPS
    - × Pour rappel : **il n'y a pas de service de non répudiation en SSL/TLS**  
*La clef utilisée pour « signer » les données applicatives n'est pas celle associée à la clef publique contenue dans le certificat*
  - × Signature numérique de la déclaration au format électronique (*gérée une applet Java*)
    - × À laquelle est associée un service de non-répudiation (« imputabilité »)
- × Clef privée et certificat dans un fichier au format PKCS#12 contenant :
  1. Les certificats des autorités signataires
    - a) Autorité de certification racine
    - b) Autorités de certification intermédiaires
  2. Le certificat client et la clef privée associée (chiffrée en DES-EDE3-CBC)



# Exemple de PKI : télédéclaration des impôts (2/9)

## Télédéclaration des impôts : architecture



# Exemple de PKI : télédéclaration des impôts (3/9)

## AC Racine

Certificate:

Data:

**Version: 3 (0x2)**

Serial Number:

7a:7a:cd:e8:d9:d3:65:ee:00:fb:8f:6b:3a:8b:89:70

Signature Algorithm: sha1WithRSAEncryption

**Issuer: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS RACINE**

Validity

Not Before: Jul 5 00:00:00 2001 GMT

Not After : Jul 4 23:59:59 2013 GMT

**Subject: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS RACINE**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

**RSA Public Key: (2048 bit)**

Modulus (2048 bit): [...]

Exponent: 65537 (0x10001)

**X509v3 extensions:**

**X509v3 Basic Constraints:**

CA:TRUE

**X509v3 CRL Distribution Points:**

URI:[http://icp.dgi.minefi.gouv.fr/teleir/AC\\_DIRECTION\\_GENERALE\\_DES\\_IMPOTS\\_RACINE.crl](http://icp.dgi.minefi.gouv.fr/teleir/AC_DIRECTION_GENERALE_DES_IMPOTS_RACINE.crl)

**X509v3 Key Usage:**

Certificate Sign, CRL Sign

**X509v3 Subject Key Identifier:**

08:F1:F8:CF:BF:01:4F:88:58:D4:9A:7F:5B:BC:ED:C7:69:69:43:DE

**X509v3 Authority Key Identifier:**

keyid:08:F1:F8:CF:BF:01:4F:88:58:D4:9A:7F:5B:BC:ED:C7:69:69:43:DE

# Exemple de PKI : télédéclaration des impôts (4/9)

## AC intermédiaire n°1

Certificate:

Data:

**Version: 3 (0x2)**

Serial Number:

6d:61:71:7a:c0:dc:23:c0:f3:a7:2b:03:ac:21:f0:af

Signature Algorithm: sha1WithRSAEncryption

**Issuer: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS RACINE**

Validity

Not Before: Jul 5 00:00:00 2001 GMT

Not After : Jul 4 23:59:59 2012 GMT

**Subject: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

**RSA Public Key: (2048 bit)**

Modulus (2048 bit): [...]

Exponent: 65537 (0x10001)

X509v3 extensions:

**X509v3 Basic Constraints:**

**CA:TRUE**

**X509v3 CRL Distribution Points:**

**URI:http://icp.dgi.minefi.gouv.fr/teleir/AC\_DIRECTION\_GENERALE\_DES\_IMPOTS\_RACINE.crl**

**X509v3 Key Usage:**

**Certificate Sign, CRL Sign**

X509v3 Subject Key Identifier:

04:6C:AE:8D:DB:03:C7:21:91:EB:5B:61:35:AD:A5:AF:43:5E:2F:DB

X509v3 Authority Key Identifier:

keyid:08:F1:F8:CF:BF:01:4F:88:58:D4:9A:7F:5B:BC:ED:C7:69:69:43:DE

# Exemple de PKI : télédéclaration des impôts (5/9)

## Certificat des autorités de certification racine et intermédiaire n°1

- \* AC Racine : certificat autodélivré/autosigné
  - \* subject == issuer
- \* Version 3
  - \* Présence d'extensions X509v3
- \* Clef publique RSA de 2048 bits
  - Usages :
    - Émission de certificats (Certificate Sign)
    - Émission de listes de révocation (CRL Sign)
  - Liste de révocation associée via l'extension cRLDistributionPoints
  - Autorités **non opérationnelles**

```
$ openssl crl -inform DER \
-in AC_DIRECTION_GENERALE_DES_IMPOTS_RACINE.crl -text -noout
```

```
Certificate Revocation List (CRL):
Version 1 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: /O=DIRECTION GENERALE DES IMPOTS/CN=AC DIRECTION GENERALE DES IMPOTS RACINE
Last Update: Jul 5 00:00:00 2001 GMT
Next Update: Jul 4 23:59:59 2013 GMT
No Revoked Certificates.
Signature Algorithm: sha1WithRSAEncryption
91:9f:54:d7:ad:67:1a:f9:b8:f6:13:09
```

# Exemple de PKI : télédéclaration des impôts (6/9)

## AC intermédiaire n°2

Certificate:

Data:

**Version: 3 (0x2)**

Serial Number:

70:f8:41:2e:35:ab:81:86:b3:ea:6e:77:05:49:2a:1b

Signature Algorithm: sha1WithRSAEncryption

**Issuer: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS**

Validity

Not Before: Jul 5 00:00:00 2001 GMT

Not After : Jul 4 23:59:59 2011 GMT

**Subject: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS USAGER**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

**RSA Public Key: (1024 bit)**

Modulus (1024 bit): [...]

Exponent: 65537 (0x10001)

X509v3 extensions:

**X509v3 Basic Constraints:**

**CA:TRUE, pathlen:0**

**X509v3 CRL Distribution Points:**

**URI:http://icp.dgi.minefi.gouv.fr/teleir/AC\_DIRECTION\_GENERALE\_DES\_IMPOTS.crl**

**X509v3 Key Usage:**

**Certificate Sign, CRL Sign**

**Netscape Cert Type:**

**SSL CA, S/MIME CA**

X509v3 Subject Alternative Name:

DirName:/CN=DGI-1

X509v3 Subject Key Identifier:

03:71:E1:87:C2:F3:73:26:D0:0A:31:24:A0:34:4E:7A:38:81:7F:8A

X509v3 Authority Key Identifier:

keyid:04:6C:AE:8D:DB:03:C7:21:91:EB:5B:61:35:AD:A5:AF:43:5E:2F:DB

# Exemple de PKI : télédéclaration des impôts (7/9)

## Certificat de l'autorité de certification n°2

- \* AC opérationnelle : délivre des certificats à des entités terminales
  - \* Longueur de l'itinéraire de certification égal à 0
    - Aucune autorité de certification intermédiaire tolérée sous l'autorité CN=AC DIRECTION GENERALE DES IMPOTS USAGER

- \* Version 3

- \* Présence d'extensions X509v3

- \* Clef publique RSA de 1024 bits

Usages :

Émission de certificats clients/serveurs SSL/TLS (SSL CA, Certificate Sign)

Émission de certificats clients S/MIME (S/MIME CA, Certificate Sign)

Émission de listes de révocation (CRL Sign)

Liste de révocation associée à ce certificat via l'extension `cRLDistributionPoints`

Autorité **opérationnelle**

```
$ openssl crl -inform DER \
-in AC_DIRECTION_GENERALE_DES_IMPOTS.crl -text -noout
```

```
Certificate Revocation List (CRL):
```

```
[...]
```

```
Issuer: /O=DIRECTION GENERALE DES IMPOTS/CN=AC DIRECTION GENERALE DES IMPOTS
```

```
[...]
```

```
No Revoked Certificates.
```



# Exemple de PKI : télédéclaration des impôts (8/9)

## Certificat client

Certificate:

Data:

**Version: 3 (0x2)**

Serial Number:

54:df:be:15:c2:49:d7:02:78:47:cf:8c:ac:04:fd:0d

Signature Algorithm: md5WithRSAEncryption

**Issuer: O=DIRECTION GENERALE DES IMPOTS, CN=AC DIRECTION GENERALE DES IMPOTS USAGER**

Validity

Not Before: Mar 17 00:00:00 2003 GMT

Not After : Mar 16 23:59:59 2006 GMT

**Subject: C=fr, O=DIRECTION GENERALE DES IMPOTS, OU=DIRECTION GENERALE DES IMPOTS USAGER, OU=AD - 1, OU=D - 0, CN=XXXXXXXXXXXXX DAVY FRANCK**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

**RSA Public Key: (512 bit)**

Modulus (512 bit): [...]

Exponent: 65537 (0x10001)

X509v3 extensions:

**X509v3 Basic Constraints:**

CA:FALSE

**X509v3 CRL Distribution Points:**

URI:<http://onsitecrl.certplus.com/>

DIRECTIONGENERALEDESIMPOTSDIRECTIONGENERALEDESIMPOTSUSAGER/LatestCRL

**X509v3 Key Usage:**

Digital Signature, Non Repudiation

**Netscape Cert Type:**

SSL Client

2.16.840.1.113733.1.6.9:

...



# Exemple de PKI : télédéclaration des impôts (9/9)

## Certificat d'une entité terminale

- \* Clef publique RSA de 512 bits

Usages :

Utilisation comme certificat client SSL/TLS (SSL Client, Digital Signature)

Utilisation comme certificat de signature, avec service de non répudiation associé (Digital Signature, Non Repudiation)

OID « propriétaire » Verisign : 2.16.840.1.113733.1.6.9

Identifie l'énoncé des pratiques de certification de l'autorité signataire

```
OID value: 2.16.840.1.113733.1.6
```

```
OID description:
```

```
-- VeriSign defined certificate extension sub tree -- (2.16.840.1.113733.1.6) --
id-extensions OBJECT IDENTIFIER ::= {id-pki extensions(6)}
```

```
URL for further info: http://www.verisign.com/repository/CPS/CPSCH2.HTM
```

Liste de révocation associée à ce certificat via l'extension `cRLDistributionPoints`

```
$ date
```

```
lun mar 31 13:43:41 CEST 2003
```

```
$ openssl crl -inform DER -in LatestCRL -text -noout | \
grep "Serial Number" | wc -l
```

```
103405
```

