

**Fonctionnement des PKI**

**- 3 -**

**Architecture PKI**



# Plan

Introduction

Architecture et composantes

Analogie : carte d'identité nationale

Entités et rôles respectifs

Gestion/Cycle de vie des certificats

Demande de certificat

Signature de demande de certificat

Publication de certificat

Révocation de certificat

Politique et énoncé des pratiques de certification

Démonstrations



# **Introduction**

# **Architecture et composantes**



# Analogie : Carte d'identité Nationale

## Procédure

- × Retrait d'un formulaire type
  - × <http://www.interieur.gouv.fr/cerfa/formulaires/20-3252.pdf>
- × Dépôt du formulaire accompagné de pièces justificatives (à la mairie)
  - × Acte de naissance, justificatif de domicile, photos d'identité, empreintes digitales etc.
- × Validation (Formulaire + Pièces) par un service émetteur
  - × Mairie, commissariat de Police par exemple
- × Demande transmise à la préfecture/sous-préfecture, pour délivrance de la carte
- × Mise à disposition de la carte d'identité
  - × Mairie
  - × Commissariat de Police
  - × Préfecture/sous-préfecture



## Authentification et autorisation (1/4)

**Par analogie avec la carte nationale d'identité, le certificat X509v3 offre uniquement un service d'authentification**

- × Ne pas confondre authentification et autorisation !

**Authentification** : n.f. Action d'authentifier

**Authentifier** : v.tr. Certifier authentique, conforme, certain

**Autorisation** : n.f. Action d'autoriser

**Autoriser** : v.tr. Accorder à quelqu'un la permission de (faire quelque chose)

- Le certificat X509v3 certifie le lien entre DN et clef publique
- Seul un service d'*authentification* est rendu
  - × Au sein d'une même communauté d'intérêt, considérant l'autorité de certification racine comme une autorité « *de confiance* »



## Authentification et autorisation (2/4)

### *Authentification et autorisation dans Apache/mod\_ssl*

- × Service d'authentification assuré via les directives suivantes :
  - × `SSLCACertificateFile/SSLCACertificatePath File|Path`
    - × Fichier ou chemin pointant vers les fichiers, au format PEM, contenant les certificats des autorités considérées comme étant dignes « *de confiance* » par le serveur.
      - Les clefs publiques de ces certificats servent à la validation, au sens cryptographique (vérification d'une signature) de l'éventuel certificat présenté par un client lors de la phase *handshake* des protocoles SSLv3 et TLSv1.
      - À la vérification, au sens cryptographique, d'une signature s'ajoute la composante fondamentale qu'est la *confiance*
  - × `SSLVerifyClient none|require|optional|optional_no_ca`
    - × Directive spécifiant le caractère obligatoire de la présentation d'un certificat client.
    - × Des variables d'environnement sont initialisées suite à la présentation d'un certificat client.
      - × Dépendantes de l'implémentation SSL/TLS employée : `mod_ssl`, `apache-ssl` ?
      - × Permettent l'accès, en lecture, aux paramètres du certificat par une application





## Authentification et autorisation (3/4)

- \* Service d'autorisation assuré via la directive `SSLRequire`
  - \* `SSLRequire` Expression
    - \* Accorde ou refuse l'accès à un répertoire sur la base de l'évaluation de l'expression booléenne `Expression`, exprimée en fonction des variables d'environnement dérivées du certificat client présenté
      - \* Exemple d'utilisation ( extrait de la documentation de référence de `mod_ssl` ) :

```
SSLRequire (    %{SSL_CIPHER} !~ m/^(EXP|NULL)-/      \  
    and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd."      \  
    and %{SSL_CLIENT_S_DN_OU} in {"Staff", "CA", "Dev"}  \  
    and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5      \  
    and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20      \  
    or %{REMOTE_ADDR} =~ m/^192\.76\.162\. [0-9]+$/    )  \  
)
```

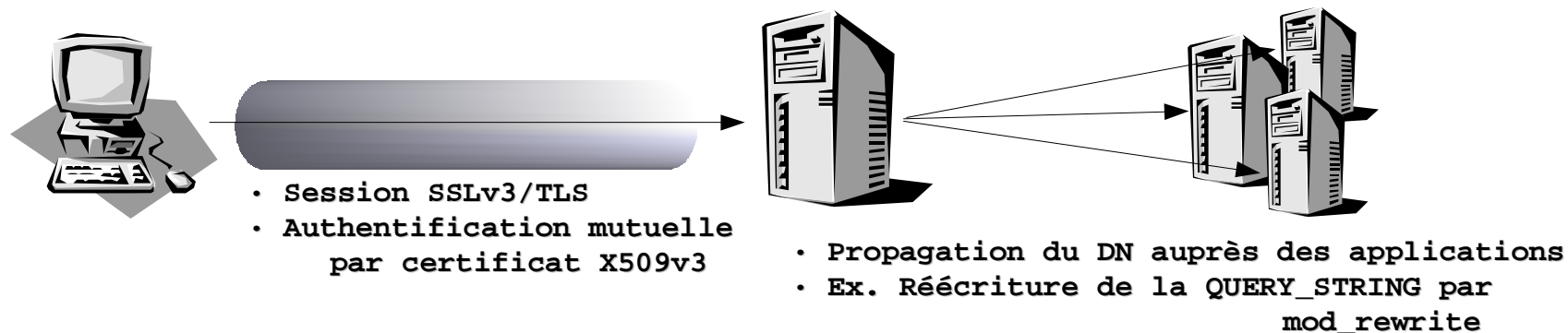
- Nécessite une authentification préalable du client
  - \* Incompatible avec l'utilisation de la directive `optional_no_ca` !



## En pratique :

1. **Authentifier** les utilisateurs sur la base des certificats des autorités « *publiques* » et/ou « *privées* », mais toujours considérées comme « *dignes de confiance* »
  - \* Exemple : base de certificats de Windows 2000
    - \* <http://www.hsc.fr/~davy/certs/trustees.pem>
2. **Autoriser** les utilisateurs sur la base des variables d'environnement dérivées du certificat client

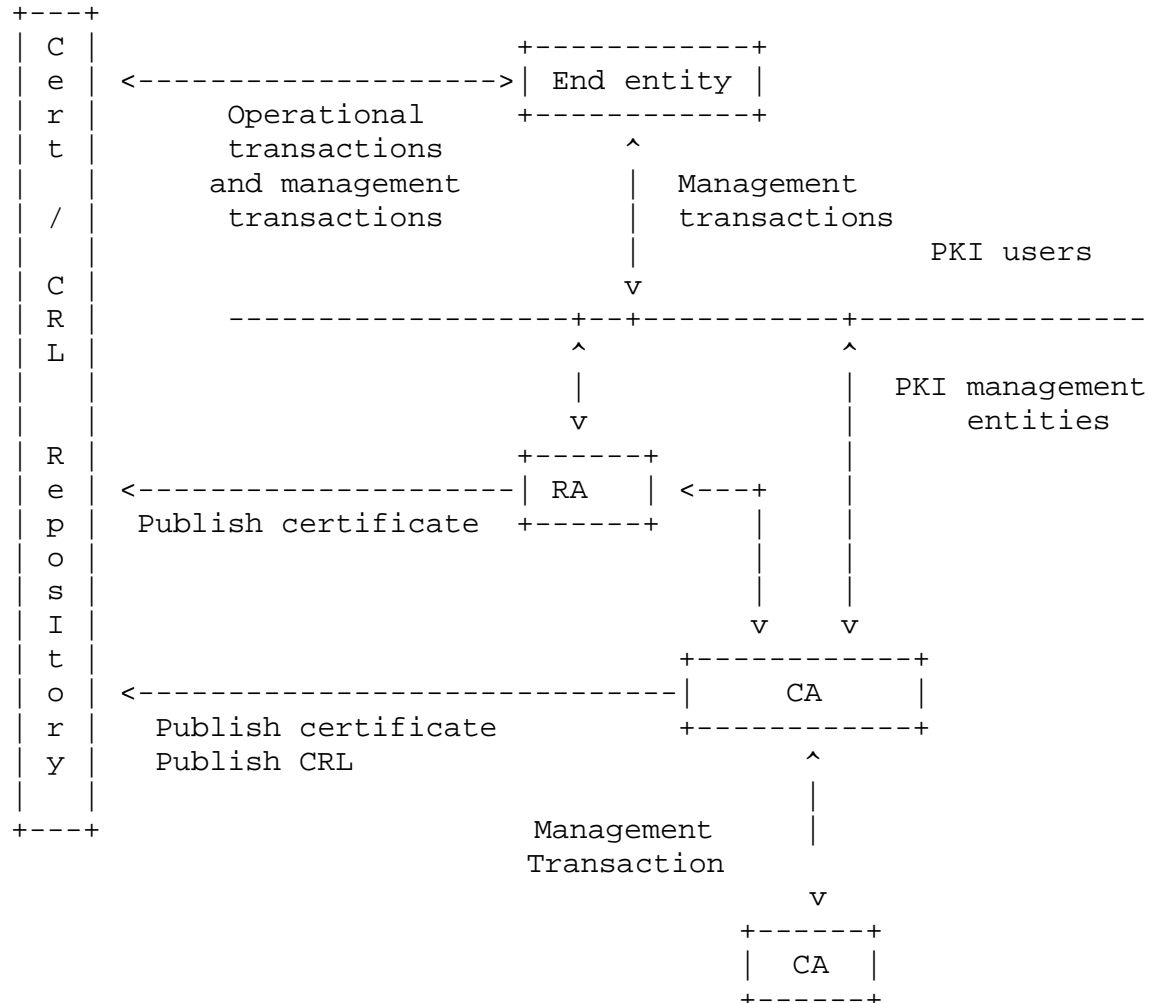
## Exemple d'utilisation : architecture de type SSO





# PKI : entités et rôles respectifs (1/2)

Internet X509 PKI : Certificates Management Protocols (RFC2510)





## PKI : entités et rôles respectifs (2/2)

- × Autorité de certification privée
  - × Gestion de la PKI et des clefs de l'autorité de certification racine
- × Autorité de certification publique
  - × Délivrance de certificat X.509v3 aux utilisateurs finaux
  - × Infogérance de PKI ( Verisign, GTE Cyber Trust, Certplus, Chambersign etc.)
- × Modèle hybride
  - × Côté client : Autorité Locale d'Enregistrement
    - × Contrôle du contenu des informations certifiées
      - × Génération des bi-clefs
      - × Enregistrement des demandes
      - × Authentification des entités terminales
  - × Côté prestataire de services : autorité de certification
    - × « Fabrication » des certificats
      - × Signature des demandes de certificat
      - × Publication et archivage des certificats
        - × Gestion des listes de révocation ?
      - × Fourniture de services (horodatage etc.)



# **Cycle de vie des certificats X.509**



# Demande de certificat (1/6)

## Génération du bi-clef

- × Décentralisée
  - × Génération du bi-clef à l'enregistrement sur le poste client
    - × Support : carte à puce, disque dur, dongle USB, carte pcmcia etc.
    - × Demande de certificat pouvant être émise par un client léger (Cf. Netscape)
    - × Suivant le niveau de sécurité associé à la classe du certificat :
      - × Adresse électronique valide suffisante
      - × Présence physique requise
- × Centralisée
  - × Dé-corrélation des phases d'enregistrement et de génération du bi-clef
  - × Bi-clef généré dans un site « sécurisé », puis délivrance du certificat (sur carte à puce, par exemple) à l'utilisateur
- × Recouvrement des clefs
  - × Exigences de sécurité différentes
    - × Problème de la non-répudiation pour la clef privée de signature
  - × CA Publiques : sauvegarde des certificats X.509 seuls
  - × CA Privées : sauvegarde du certificat de signature et du bi-clef de chiffrement





## Demande de certificat (2/6)

### Génération d'une demande de certificat

- \* Demande de certificat au format PKCS#10
  - \* « *Certificate Request Syntax Standard* »
  - \* <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/>
  - \* Utilisation de l'utilitaire req(1ssl)
- \*

```
$ openssl req -new -config ./openssl.cnf -newkey rsa:1024 -nodes \  
-keyout private_key.pem -out req.csr
```
- \* Exemple de formulaire de demande de certificat

```
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.  
-----  
Pays [FR]:  
Departement [Ile-de-France]:  
Localite (e.g. Ville) [Levallois-Perret]:  
Organisation [Herve Schauer Consultants]:  
Nom ou URL []:Franck Davy  
Adresse Email []:Franck.Davy@hsc.fr  
Challenge []:secret
```





## Demande de certificat (3/6)

### Format de la demande de certificat

Certificate Request:

Data:

Version: 0 (0x0)

Subject: C=FR, ST=Ile-de-France, L=Levallois-Perret,

O=Herve Schauer Consultants, CN=Franck DAVY/Email=Franck.Davy@hsc.fr

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit): [...]

Exponent: 65537 (0x10001)

Attributes:

a0:00

Signature Algorithm: md5WithRSAEncryption [...]

#### \* Champ Data

- \* Ensemble des données « administratives » entrées via un formulaire
- \* Clef publique RSA générée (au format PKCS#1 !)

#### \* Champ Signature

- \* Structure ASN.1 'Data:' (encodée suivant la syntaxe de transfert DER) signée
- \* Signature avec la clef privée correspondant à la clef publique (champ 'RSA Public Key' figurant dans le certificat (la clef privée n'est pas divulguée à l'autorité signataire !))



# Demande de certificat : carte à puce (4/6)

## Utilisation d'openssl-engine

- × Carte PCMCIA
  - × Carte Chrysalis-ITS Luna2 PC Card
- × Procédure décrite :
  - × « *Using a Cryptographic Hardware Token with Linux* »
    - × <http://www.linuxjournal.com/article.php?sid=4744>
- × Initialisation

```
$ openssl req -engine luna2 -keyform engine -text -key DSA-public:1:1234 \  
                                                    -out request.csr  
  
-engine : spécifie le token  
-key    : Nom de la clé : Slot de la carte PCMCIA : Code PIN
```

- × Après réception du certificat certificate.pem

```
$ openssl smime -sign -engine luna2 -in email.txt -out signed.email.txt \  
                -signer certificate.pem -keyform engine -inkey DSA-Public:1:1234
```

# Demande de certificat : client léger (5/6)

## Client léger : Netscape Navigator (version > 3.0)

- × Utilisation d'une extension pour la génération de clef  
<http://wp.netscape.com/eng/security/ca-interface.html>
- × Tag HTML 'KEYGEN'  

```
<KEYGEN NAME="name" CHALLENGE="challenge string">
```
- × Une clef RSA de 512 (export), 768 ou 1024 bits est générée
- × La clef privée RSA est conservée dans la base de donnée locale des certificats
- × La clef publique et le challenge sont signés par la clef privée
  - × Protection contre le rejeu (les données soumises ne sont pas signées !)
- × Encodage DER de la structure PublicKeyAndChallenge

```
PublicKeyAndChallenge ::= SEQUENCE {  
    spki SubjectPublicKeyInfo,  
    challenge IA5STRING  
}  
SignedPublicKeyAndChallenge ::= SEQUENCE {  
    publicKeyAndChallenge PublicKeyAndChallenge,  
    signatureAlgorithm AlgorithmIdentifier,  
    signature BIT STRING  
}
```



# Demande de certificat : client léger (6/6)

## Données soumises par formulaire

```
commonname=John+Doe&email=doe@foo.com&org=Foobar+Computing+Corp.&orgunit=Bureau+of+Bureaucracy&locality=Anytown&state=California&country=US&key=MIHFMHEwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAnX0TILJrOMUue%2BptwBRE6Xfv%0AWtKQbsshxk5ZhcUwcyvcnIq9b82QhJdoACdD34rqfCAIND46fXKQUnb0mvKzQID%0AAQABFhFNb3ppbGxhSXNNeUZyaWVuZDANBgkqhkiG9w0BAQQFAANBAAKv2Eex2n%2FS%0Ar%2F7iJNroWlSzSMtTiQTEB%2BADWHGj9ulxrUrOilq%2Fo2cuQxIfZcNZkYAkWP4DubqW%0Ai0%2F%2FrgBvmco%3D
```

- \* Champ key encodé en base 64, au format SPKAC
  - \* Acronyme Netscape de « *Signed Public Key and Challenge* »
  - \* Donnée manipulable par l'outil spkac(1ssl)

```
$ openssl spkac -key private.key -challenge 'secret' -out spki.cnf
$ openssl spkac -in spki.cnf
Netscape SPKI:
Public Key Algorithm: rsaEncryption
RSA Public Key: (512 bit)
Modulus (512 bit):
00:df:bd:db:40:b1:cb:28:17:42:c9:57:15:63:f8:
[...]
Exponent: 65537 (0x10001)
Challenge String: secret
Signature Algorithm: md5WithRSAEncryption
-----BEGIN PUBLIC KEY-----
MdwWdQYJKoZIhvcNAQEBBQADKwAwKAIhAN+920CxyygXQslXFWP4JM4B4AqTNmH9
[...]
-----END PUBLIC KEY-----
```





# Signature de demande de certificat

## Signature de la demande de certificat par l'autorité de certification

- × Signature du champ 'data' de la demande de certificat au format PKCS#10, éventuellement modifié (conformité à la politique de certification) et augmenté d'extensions v3
- × Remarques
  - × Version 0 pour la demande de certificat
  - × Possibilité d'inclure des extensions dans la demande de certificat
- × En pratique, avec `ca(1ssl)`
  - × `openssl.cnf` : fichier de configuration openssl
  - × Chargement des extensions à incorporer au certificat final
  - × `keyUsage`, `cRLDistributionPoints`, etc.

```
$ openssl ca -config ./openssl.cnf -extensions SMIME -in smime.csr \  
-out smime.pem
```

- × Cas d'une autorité racine : certificat auto-signé

```
$ openssl req -new -x509 -config ./openssl.cnf -extensions CA -sha1 \  
-newkey rsa:1024 -nodes -days 3650 -keyout ca/ca.key -out ca/ca.pem
```





# Publication de certificat (1/4)

## Éléments publiés

- × Certificats des autorités de certification/révocation
- × Certificats des entités terminales
- × Listes de révocation (CRL)
- × Publication via LDAP
  - × Schéma core
    - × objectClass certificationAuthority (2.5.6.16)
    - × Attributs
      - × authorityRevocationList
      - × cACertificate
      - × certificateRevocationList
  - × Schéma inetOrgPerson
    - × objectClass inetOrgPerson (2.16.840.1.113730.3.2.2)
    - × Attribut userCertificate
- × Liste des OID référencés : « Objects Identifiers Registry »
  - × <http://www.alvestrand.no/objectid/>





## Publication de certificat (2/4)

### Téléchargement des CRL via le protocole LDAP

- \* Extension X509v3 :

```
X509v3 CRL Distribution Points:  
URI:http://crl-acracine.certinomis.com/acracine.crl  
DNS:ldap.certinomis.com  
DirName:/C=FR/O=CertiNomis/OU=AC Racine - Root CA/CN=CertiNomis
```

- \* Recherche par ldapsearch(1) sur ldap.certinomis.com

```
# CertiNomis Classe 2+, CertiNomis ,FR  
dn: cn=CertiNomis Classe 2+, o=CertiNomis ,c=FR  
certificaterevocationlist;binary:: MIIBJjCBkgIBATANBgkqhkiG9w0BAQUFADBBMQswCQY  
[...]  
tsyl7hmtQH/0z2HhJV63yek1hLjuJ4s//53cwNzFyM+607g==  
certificaterevocationlist;base64:: TulJQkpqQ0JrZ0lCQVRBTKJna3Foa2lHOXcwQkFRVUZ  
[...]  
zFoTGp1sJrZLy8KNTNjd056RnlNKzYwN2c9PQo=  
objectclass: top  
objectclass: crlDistributionPoint  
cn: CertiNomis Classe 2+
```

- \* Certificat DER encodé en base 64 (# Format PEM)





# Publication de certificat (3/4)

## Publication via le protocole HTTP

- \* Types MIME (RFC2585)

- .cer      application/pkix-cert
  - .crl      application/pkix-crl

- \* Autres...

- ...spécifiques aux applications

- .cer      application/x-x509-ca-cert
    - .crl      application/pkcs-crl
    - .crt      application/pkix-cert
    - .crt      application/x-x509-ca-cert
    - .crt      application/x-x509-user-cert
    - etc.

## Points de publication

- \* CRL (Protocole HTTP généralement, méthode GET classiquement)

- \* Extension `cRLDistributionPoints`

- URI:http://bar/crl/foobar.crl

- \* OCSP (Protocole HTTP, méthode POST)

- \* Extension `Authority Information Access`

- OCSP - URI:http://foobar/





## Publication de certificat (4/4)

### Démonstrations

- × Messagerie sécurisée avec S/MIME, avec des certificats clients publiés dans un annuaire LDAP

Powered by  
*Open*LDAP<sup>®</sup>





## Révocation de certificat (1/9)

« Il appartient à l'utilisateur d'un certificat de vérifier qu'un certificat qu'il se destine à utiliser n'a pas été révoqué »

FAQ du DCSSI

[http://www.ssi.gouv.fr/fr/faq/faq\\_igc.html](http://www.ssi.gouv.fr/fr/faq/faq_igc.html)

- × Révocation = suspension d'un certificat avant sa date de fin de validité
  - × Raisons pouvant conduire à la révocation d'un certificat
    - × Changement de statut d'une entité
    - × Arrêt d'activité d'une autorité
    - × Procédure d'émission du certificat non réglementaire
    - × Perte de la clef privée
    - × Compromission de la clef privée
  - × Demande de révocation à l'initiative de
    - × Autorité signataire
    - × Détenteur du certificat
      - × Preuve de possession (par partage de secret)
    - × Tierce partie autorisée
      - × Implication judiciaire par exemple





## Révocation de certificat (2/9)

- × Mise en oeuvre de mécanismes permettant à un utilisateur de s'assurer de la non-révocation d'un certificat
  - × Principaux mécanismes de révocation
    - × (Partiellement) mis en oeuvre dans les navigateurs grand-public
    - Mécanisme de Listes de Révocation
      - × CRL (« *Certificate Revocation List* »)
      - Protocole OCSP (« *Online Certificat Status Protocol* »)
  - × Mécanisme de CRL
    - × Publication d'une liste périodiquement mise à jour des certificats révoqués
      - × Certificats identifiés par
        - × Leur autorité signataire
        - × Leur numéro de série, unique pour une autorité signataire donnée
      - × Liste signée par l'autorité signataire
        - × Ou une autorité déléguée
        - × Présence de l'extension v3 cRLSign dans le certificat de l'autorité émettant la CRL :  
X509v3 Key Usage: CRL Sign



## Révocation de certificat (3/9)

× Exemple de liste de révocation :

```
$ openssl crl -in crl.pem -text -noout -CApath /etc/ssl/trusted
verify OK
Certificate Revocation List (CRL):
  Version 1 (0x0)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: /C=FR/L=Levallois-Perret/O=Herve Schauer Consultants
          /CN=CA ROOT/Email=Franck.Davy@hsc.fr
  Last Update: Aug 27 21:34:33 2001 GMT
  Next Update: Sep 26 21:34:33 2001 GMT
  Revoked Certificates:
    Serial Number: 03
    Revocation Date: Aug 17 21:33:46 2001 GMT
    Serial Number: 06
    Revocation Date: Aug 26 18:10:10 2001 GMT
    Serial Number: 07
    Revocation Date: Aug 26 18:15:12 2001 GMT
  Signature Algorithm: md5WithRSAEncryption
    56:1a:c1:b6:d9:2d:03:8f:4a:aa:dc:1a:46:74:2d:f6:42:ed:
    [...]
    a1:c0:42:e6
```





# Révocation de certificat (4/9)

## Disponibilité des CRL

- \* Nécessité d'indiquer, sur un certificat X.509 destiné à être utilisé, l'URL de la liste de révocation relative au certificat
- \* Ajout d'une extension X509v3 au certificat : `cRLDistributionPoints` (CRLDP)
  - \* Association au certificat de la liste de révocation dont il dépend
  - \* Client qui n'a pas à connaître, au préalable, l'intégralité des adresses où télécharger les CRL relatives à une autorité signataire pour une famille de certificats donnée
  - \* Permet une stratégie de partitionnement des CRL
    - \* Limitation du nombre de certificats émis portant des CRLDP identiques
    - \* Lutte contre la taille croissante des listes de révocation émises

X509v3 extensions:

X509v3 Subject Alternative Name:

DirName:/CN=OCSP 1-4

X509v3 CRL Distribution Points:

URI:http://crl.verisign.com/RSASecureServer-p.crl

- \* Protocoles de distribution utilisés
  - \* HTTP
  - \* LDAP
    - \* Mais à quel annuaire se connecter ?





## Révocation de certificat (5/9)

### En pratique :

- \* Connexion au site [www.certplus.com](http://www.certplus.com)
- \* Certificat présenté comportant les extensions X509.v3 suivantes :

#### X509v3 extensions:

X509v3 Basic Constraints:

CA:FALSE

X509v3 Key Usage:

Digital Signature, Key Encipherment

X509v3 CRL Distribution Points:

URI:<http://crl.verisign.com/RSASecureServer.crl>

X509v3 Certificate Policies:

Policy: 2.16.840.1.113733.1.7.1.1

CPS: <https://www.verisign.com/CPS>

User Notice:

Organization: VeriSign, Inc.

Number: 1

Explicit Text: VeriSign's CPS incorp. by reference liab. ltd. (c)97 VeriSign

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

Authority Information Access:

OCSP - URI:<http://ocsp.verisign.com>



## Révocation de certificat (6/9)

### Téléchargement de la CRL par Internet Explorer

- \* Téléchargement automatique si présence de l'extension cRLDistributionPoints
- \* Option (avancée) non activée par défaut
  - \* « Vérifier la révocation des certificats »
- \* Connexion sur le site <http://www.certplus.com>
  - \* Sortie de TDIMon
    - \* <http://www.sysinternals.com>

```
28 0.60371751 IEXPLORE.EXE:964 TDI_SEND TCP:0.0.0.0:1183 195.101.88.66:443
42 0.97214981 IEXPLORE.EXE:964 IRP_MJ_CREATE TCP:Connection obj SUCCESS Context:0x80118948
43 0.97217551 IEXPLORE.EXE:964 TDI_ASSOCIATE_ADDRESS TCP:Connection obj SUCCESS TCP:0.0.0.0:1184
44 0.97220513 IEXPLORE.EXE:964 TDI_CONNECT TCP:0.0.0.0:1184 216.168.253.32:80
```

```
195.101.88.66 : www.certplus.com
216.168.253.32 : crl.verisign.net
```





## Révocation de certificat (7/9)

- \* Sortie de FILEMon
  - \* <http://www.sysinternals.com>

```
1731 20:22:08 IEXPLORE.EXE:964 IRP_MJ_CREATE
C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\
Content.IE5\XH7R96CX\RSASecureServer[1].crl
SUCCESS Attributes: N Options: Create
1732 20:22:08 IEXPLORE.EXE:964 IRP_MJ_WRITE
C:\Documents and Settings\Administrateur\Local Settings\Temporary Internet Files\
Content.IE5\XH7R96CX\RSASecureServer[1].crl
SUCCESS Offset: 0 Length: 685
[...]
2535 20:22:23 IEXPLORE.EXE:964 IRP_MJ_CREATE C:\Documents and Settings\Administrateur\
Local Settings\Temporary Internet Files\Content.IE5\4XKXAXPM\certplus[1].htm
SUCCESS Attributes: N Options: Create
```

- \* Téléchargement préliminaire du fichier RSASecureServer.crl
- \* Téléchargement de la page certplus.htm
  - \* Latence importante due à la taille de la CRL  
797ko
- \* Fonctionnalité similaire dans Mozilla et Netscape 6
  - \* Avec la possibilité d'effectuer un téléchargement périodique des CRL, et non simplement ponctuel, à la consultation d'un site





## Révocation de certificat (8/9)

### Protocole OCSP

- × Mis en oeuvre dans Mozilla
- × Exemple avec l'application cliente ocspl(1) d'OpenSSL

```
$ openssl ocspl -url http://ocspl.verisign.com -issuer ./trust/ca.pem \  
                -CAfile ./trust/ca.pem -cert ./certplus.pem -text  
OCSP Request Data:  
  Version: 1 (0x0)  
  Requestor List:  
  Certificate ID:  
  Hash Algorithm: sha1  
  Issuer Name Hash: 0E9290B27AA8BAF65D3C9229AFE8F31DB953B2DA  
  Issuer Key Hash: 034FA3A36BCBEC6D0760176CEC9ABF67C542F26A  
  Serial Number: 47C1C31DC6D28C5C2000373C7F5D90C1  
  Request Extensions:  
  OCSP Nonce:  
  705BFEE68E6F0B631DDF3C57AEDC4AD8
```





## Révocation de certificat (9/9)

### \* Réponse du serveur

#### OCSP Response Data:

OCSP Response Status: successful (0x0)

Response Type: Basic OCSP Response

Version: 1 (0x0)

Responder Id: O = "VeriSign, Inc.", OU = VeriSign Trust Network,  
OU = Terms of use at <https://www.verisign.com/RPA> (c)00,  
CN = Secure Server OCSP Responder

Produced At: Jun 16 13:29:56 2002 GMT

#### Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 0E9290B27AA8BAF65D3C9229AFE8F31DB953B2DA

Issuer Key Hash: 034FA3A36BCBEC6D0760176CEC9ABF67C542F26A

Serial Number: 47C1C31DC6D28C5C2000373C7F5D90C1

Cert Status: good

This Update: Jun 16 13:29:56 2002 GMT

#### Response Extensions:

OCSP Nonce:

705BFEE68E6F0B631DDF3C57AEDC4AD8



## Terminologie

### Politique de certification – Certificate Policies

« Ce document décrit l'ensemble des règles qui définissent le type d'application auxquelles un certificat est adapté. Un certificat de clé publique contient l'identifiant de la politique de certification avec laquelle il a été émis, et selon laquelle il est destiné à être utilisé. »

FAQ du DCSSI sur les infrastructures à gestion de clés  
[http://www.scssi.gouv.fr/fr/faq/faq\\_igc.html](http://www.scssi.gouv.fr/fr/faq/faq_igc.html)

- Politique d'émission des certificats, qui précise dans quel cadre le certificat peut être utilisé
  - Vérification est à la charge de l'utilisateur

## Terminologie

### Énoncé des pratiques de certification – Certificate Practice Statement

« Ce document énonce les pratiques utilisées par l'IGC dans la gestion des certificats, pratiques qui dépendent de la politique de certification mise en oeuvre. Une IGC doit publier cette déclaration afin de décrire les modalités de fonctionnement des services qu'elle rend »

FAQ du DCSSI sur les infrastructures à gestion de clés

[http://www.scssi.gouv.fr/fr/faq/faq\\_igc.html](http://www.scssi.gouv.fr/fr/faq/faq_igc.html)

- Énoncé des pratiques employées par l'autorité de certification pour émettre un certificat

## Profil PKIX

« *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* » (RFC2527)

<http://www.ietf.org/rfc/rfc2527.txt>

Description d'un ensemble de spécifications en terme de :

- \* Responsabilités légales, juridiques et financières
- \* Fonctionnalités
- \* Administration

## PC2

« *Procédures et politiques de certification de clés* »

[www.ssi.gouv.fr/fr/documents/pc2.pdf](http://www.ssi.gouv.fr/fr/documents/pc2.pdf)



# Politique et énoncé des pratiques de certifications (4/4)

## En pratique :

### → Extension v3 Certificate policies

```
Issuer: O=VeriSign, OU=VeriSign Class 2 OnSite Individual CA
X509v3 Certificate Policies:
  Policy: 2.16.840.1.113733.1.7.1.1
  CPS: https://www.verisign.com/CPS
  User Notice:
    Organization: VeriSign, Inc.
    Number: 1
    Explicit Text: VeriSign's CPS incorp. by
reference liab. ltd. (c)97 VeriSign
```

### → Autre...

```
Issuer: O=VeriSign Trust Network,
OU=VeriSign, Inc.,
OU=VeriSign International Server CA - Class 3,
OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
```



# Démonstrations





# Questions ?





## Remerciements.

- × à Hervé Schauer, Ghislaine Labouret et à l'ensemble des consultants du cabinet HSC, pour leurs conseils et leur relecture
- × à Ahmed Serhrouchni, pour son encadrement et ses enseignements à l'ENST

