Under Construction
En Construction

# Infrastructure à Clé Publique (PKI Public Key Infrastructure)

Didier DONSEZ
Université Joseph Fourier
IMA –IMAG/LSR/ADELE
**Didier.Donsez@imag.fr**

# Rappel sur la certification

- Besion de confiance sur ce que pretend être le correspondant
- Solution
  - Une autorité de confiance signe un certificat contenant l'identité et la clé publique après avoir vérifier l'identité du porteur du certificat.

# Quelques termes

- Certification Authority (CA)
  - Une entité de confiance qui émet et révoque des certificats à PK
- Registration Authority (RA)
  - Une entité en qui le CA a confiance pour vérifier l'identité d'un utilisateur
- Certificate Revocation List (CRL)
  - Liste de certificats révoqués.
  - Les raisons peuvent être la corruption de la clé privée, le licenciement d'un employé, …
- Certificate Repository
  - Un site electronique qui detient et rend publique les certificats et les listes de revocation
- Certificate User
  - Une entité qui utilise les certificats pour connaître la clé publique d'autres entités

# Motivation

- Usage
  - IPSec
  - SSL
  - S/MIME (PGP)
  - Code Signing (Java, JavaScript, ActiveX, …)
  - Form Signing…
- Formats et Types de certificat
  - X509 PKIX
  - PGP
  - SPKI/SDSI

# Que contient un Certificat ?

- Numéro de Série
- Identité du porteur (owner)
- Identité du certifieur émetteur (issuer)
- Période de validité
- Classe du certificat
- Clé Publique du porteur
  - Algorithme utilisé, longueur des clés, …
- Signature
  - Algorithme utilisé, longueur des clés, …
- Auto-Certification
  - Certificat signé par le porteur (cas de RootCA)

# Gestion des certificats

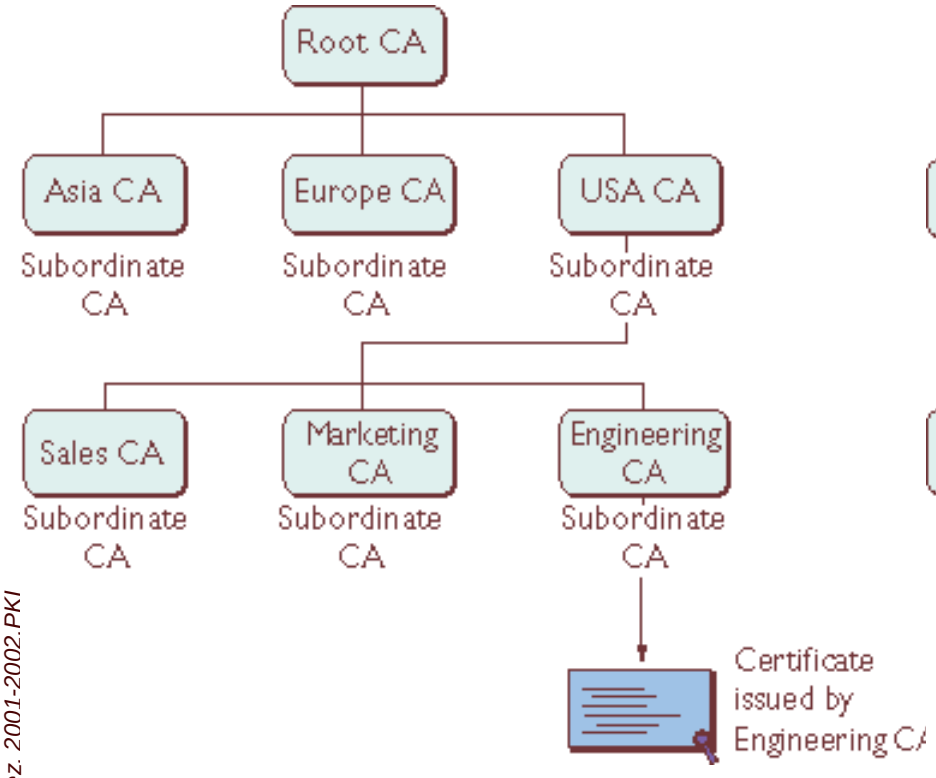
- Génération
  - CPS
  - Hiérarchie de CA
  - Certification croisée
- Publication
  - Annuaire LDAP (*RFC2251)*
- Vérification
  - Chaîne de Certificats
- Renouvellement
- Suspension
- Révocation
  - Clé privée corrompue, Employé licencié, …
  - CRL : listes de révocation

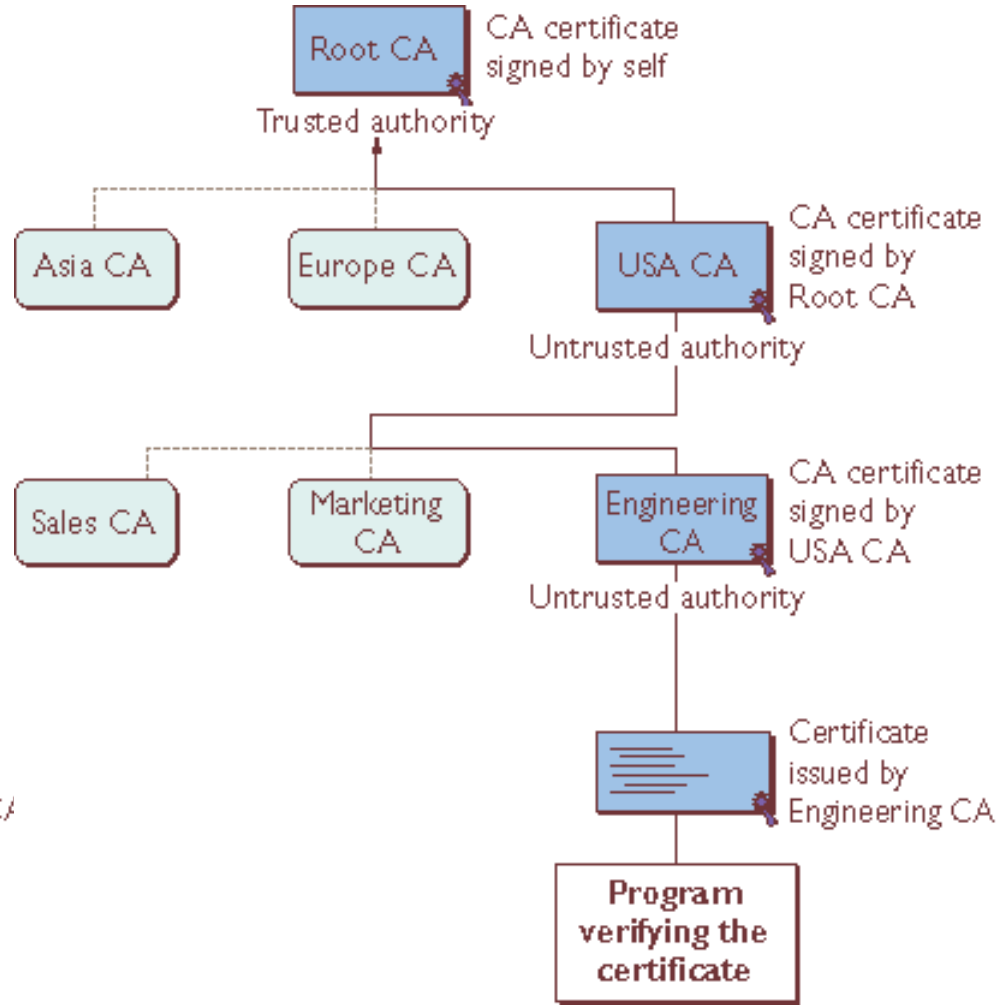
# CSP (Certification Practices Statement)

- Procédure d'établissement de l'identité du porteur
  - Pièce juridique demandée, …
- Dépend de la classe de certificat

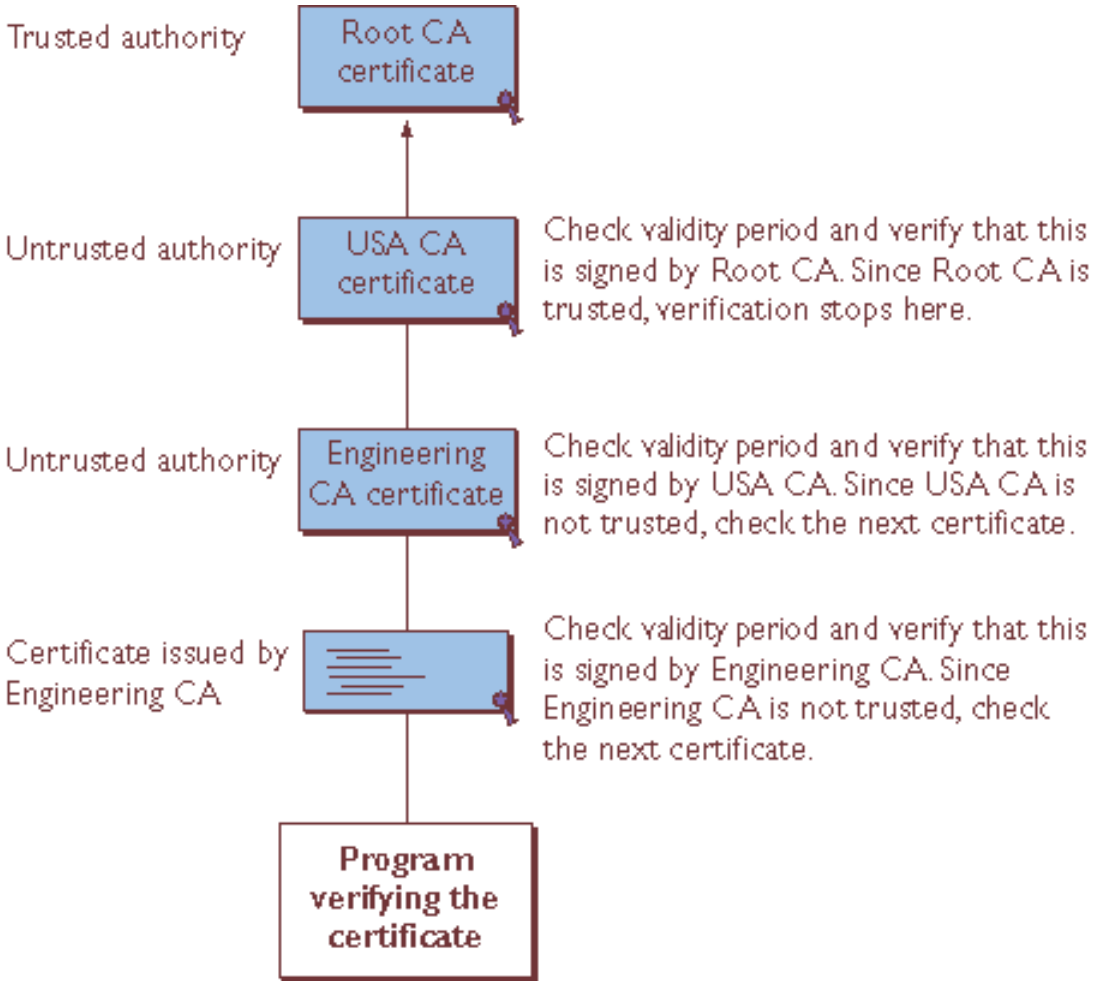
# Hiérarchie de CA

- Délégation de la certification

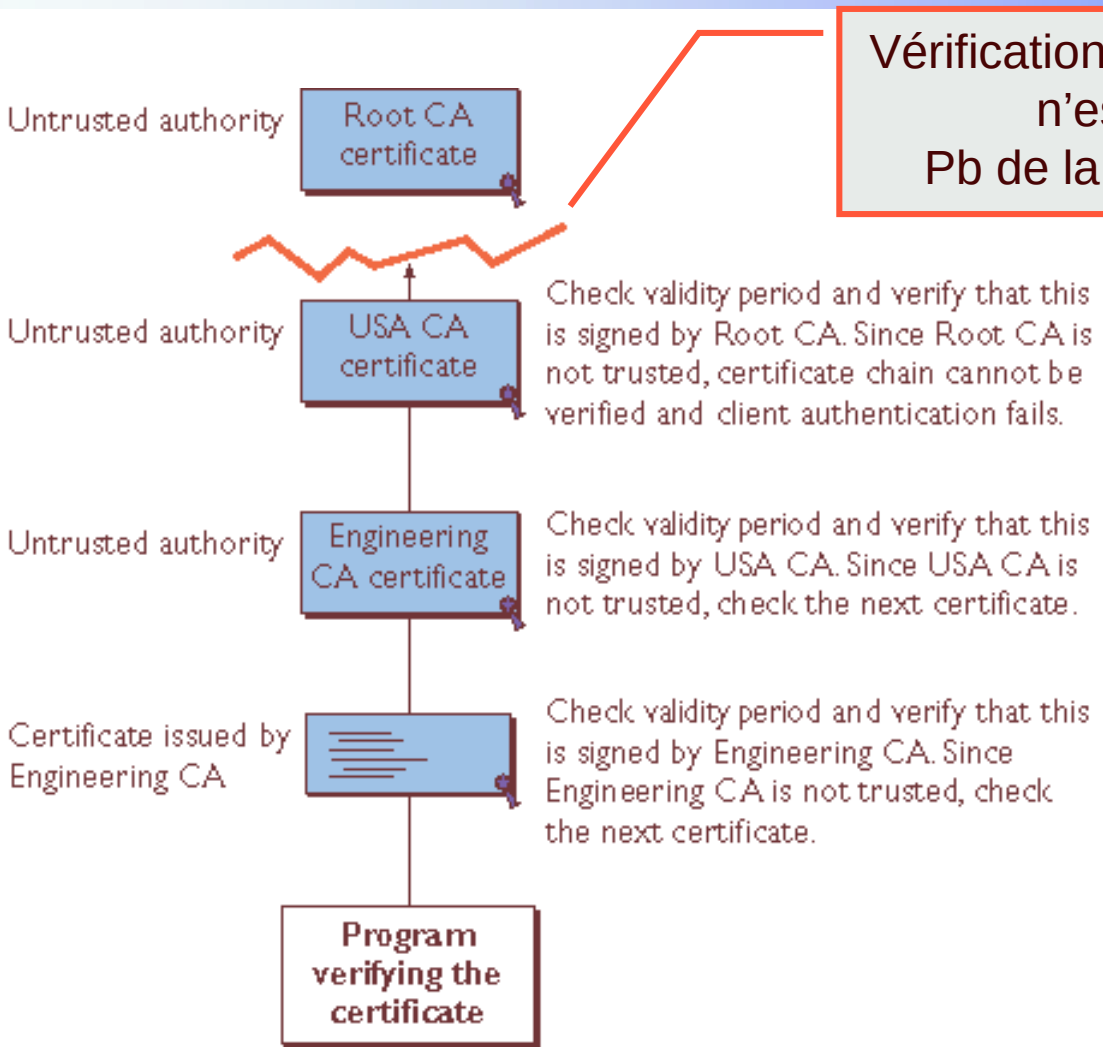


# Chaîne de Certificats et Vérification



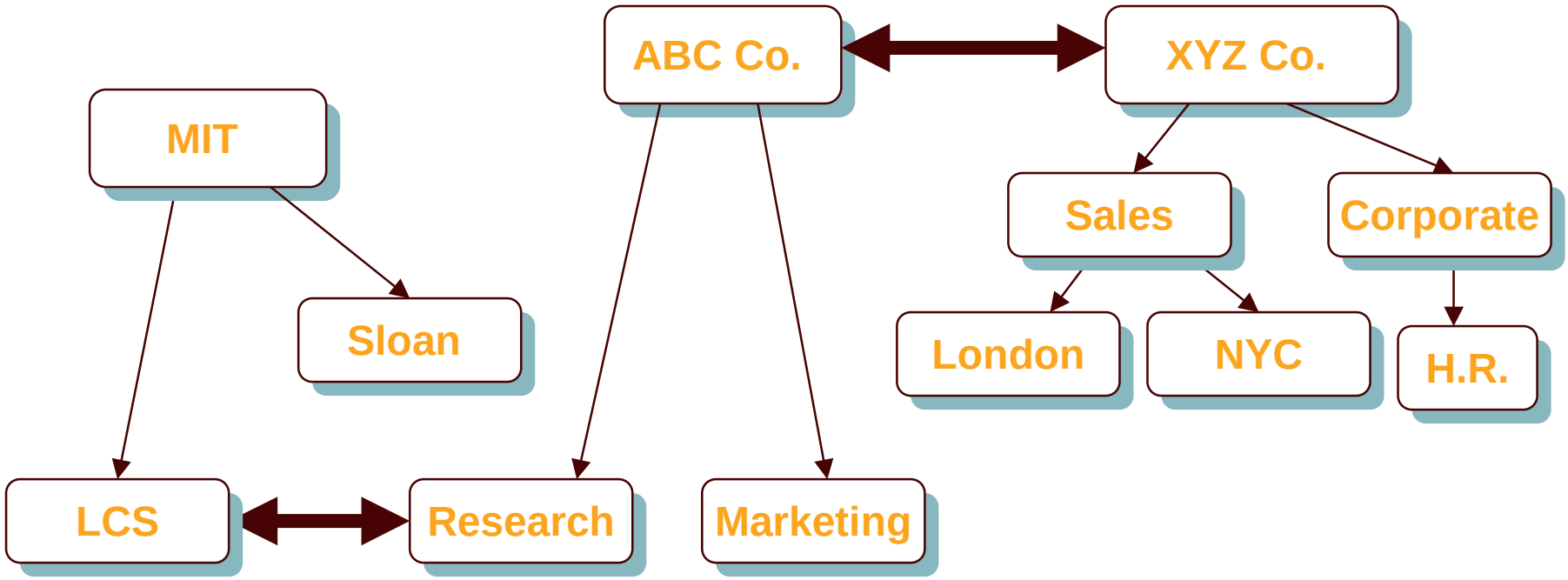
# Chaîne de Certificats et Vérification




Vérification impossible si le RootCA n'est pas joignable :
Pb de la tolérance aux pannes

# Cross-Certification

- CAs (Sub ou Root) qui se font mutuellement confiance dans leur domaine de confiance



# Génération de la paire de clé

- Par le client
  - Le CA ne connaît la PrivKey
    - Perte de la clé, Départ d'un employé

      On ne peut plus lire les mails reçus chiffrés
  - Proof-of-Possession
    - Le client dialogue avec le CA pour prouver qu'il détient la clé privée du certificat à signer
- Par le CA
  - Génération plus sûre du nombre aléatoire pour la fabrication de la paire de clés
  - Archivage (ou *Séquestre*) de la clé privée
  - Historique des paires de clés
  - Transfert sécurisé de la paire de clés vers le client

# Certifying Authority

- Public
  - Moyennant rémunération ;-)
  - Verign, Thawte, Entrust, Baltimore …
  - En France :
    - Certinomis (la Poste, les chambres de commerce, SAGEM)
    - Certplus (Verisign, Matra, France Telecom, Gemplus)
- Privé
  - Motivation : une société est sa propre autorité de certification pour ses employés et ses applications dans les échanges intranet.
  - iPlanet Certificate Management Server (developer.iplanet.com) , OpenCA (www.openca.org), IDX-PKI (idx-pki.idealx.org)

# Certificats

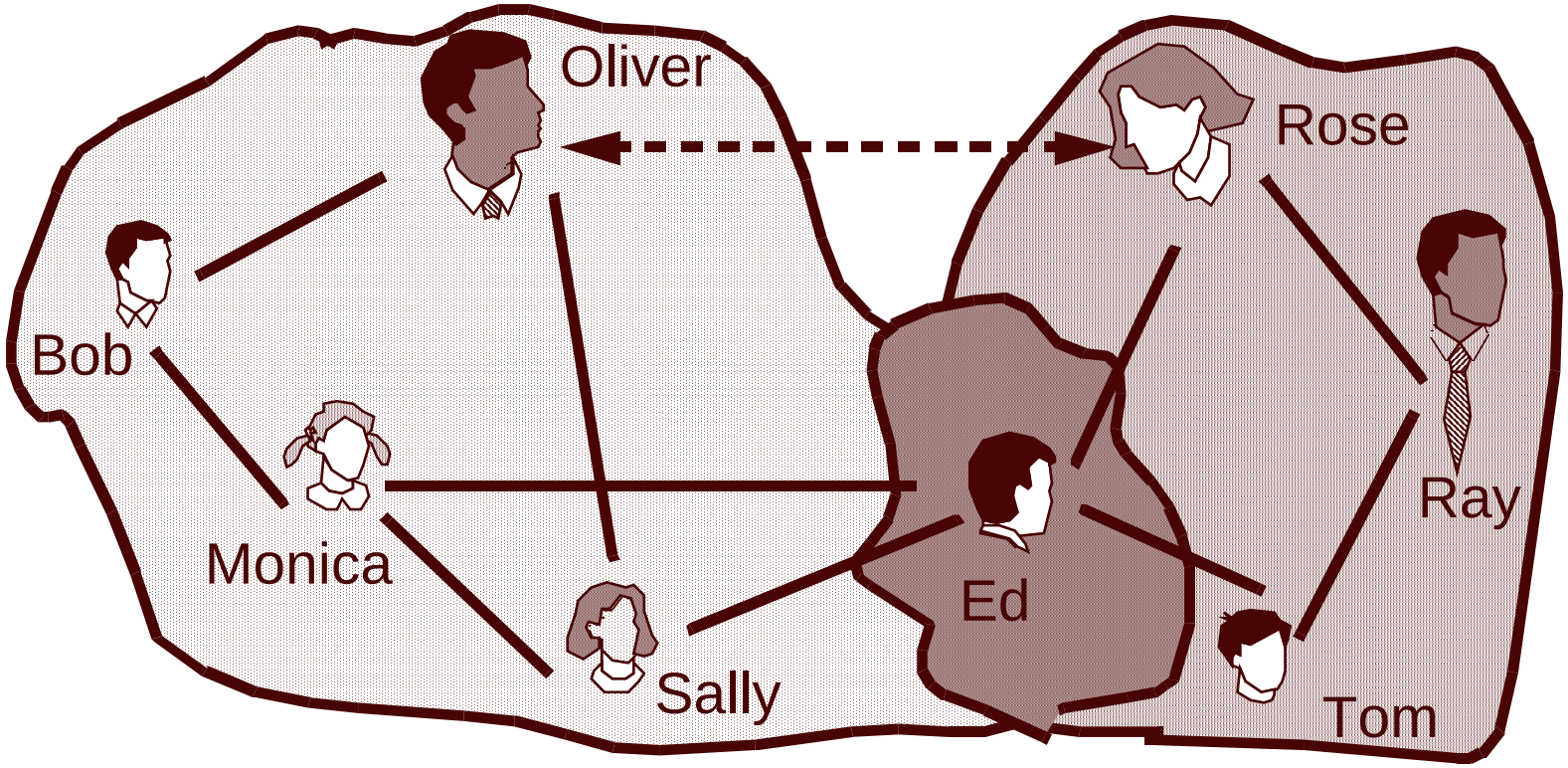
- X509
  - Naming authority hierarchies
  - Cross-certification
  - ID = X500 DN (global sur le principe)
  - CSP (Certification Practices Statement)
- PGP
  - « Web of Trust » = multiple paths of certification (tolerance aux fautes)
    - Un certificat peut être signé par plusieurs détenteurs de clé (keyHolder)
  - ID = adresse email (global grace au DNS mais peut être non persistante)
- SPKI/SDSI
  - Single Naming authority
  - ID = Local (arbitraire, significatif pour le seul émetteur)
  - Pas de CSP (non nécessaire)
- SPKI without name (anonymat)
  - Authorization authority hierarchies, optional k-of-n subjects
  - ID = public key ou hash de PK (très probablement unique)
- SPKI/SDSI k-of-n Subject
  - Listes de n sujets (nom+clé)
  - Verification nécessite un minimun de k chemins (redondance)

# Key Recovery

- M of N
  - N managers connaissent un fragment de la clé
  - Il faut au minimum M managers pour reconstruire la clé

# PGP : Web of Trust

- La confiance sur l'identité est établie par plusieurs utilisateurs reconnus de confiance
  - Probléme de passage à l'échelle



# SPKI (*Simple PKI*) et SDSI (*Simple Distributed Security Infrastructure*)

- Motivation
  - Simplifier le PKI
  - IETF RFC 2692
- Doc
  - http://www.syntelos.com/spki/
  - http://theory.lcs.mit.edu/~rivest/sdsi11.html

# Standards PKCS

## *« Public-Key Cryptography Standards »*

- ensemble de standards pour la mise en place des IGC, coordonné par RSA
- définissent les formats des éléments de cryptographie :
  - En général les formats sont basés sur ASN.1
  - PKCS #1:RSA Cryptography Standard
    - Inclut PKCS #2 et PKCS #4
  - PKCS #3:Diffie-Hellman Key Agreement Standard
  - PKCS #5:Password-Based Cryptography Standard
  - PKCS #6:Extended-Certificate Syntax
  - PKCS #7:Cryptographic Message Syntax
  - PKCS #8:Private-Key Information Syntax
  - PKCS #9:Selected Attribute Types Standard
  - PKCS #10:Certification Request Syntax Standard
  - PKCS #11:Cryptographic Token Interface Standard
  - PKCS #12:Personal Information Exchange Syntax Standard
  - PKCS #13: Elliptic Curve Cryptography Standard
  - PKCS #15: Cryptographic Token Information Format Standard
- Voir http://www.rsa.com/rsalabs/pkcs/

# Trusted Web Services

- Motivation
  - Gestion des PKI par des échanges basés sur des messages XML transportés sur SOAP.
    - En évitant d'utiliser la syntaxe ASN.1
- Standards
  - XKMS XML Key Management Specification
    - http://www.xmltrustcenter.org/xkms
    - Basé sur

      XML Digital Signature http://www.w3.org/TR/xmldsig-core/

      XML Digital Encryption http://www.w3.org/TR/xmlenc-core/

# XKMS - XML Key Management System

- Motivation
  - Replacer les formats et protocoles PKI (PKIX, Card Management Services, OCSP, etc.) par des documents XML transportés par SOAP.
- Définit les messages de requête et de réponse pour
  - Requérir (request) un certificat
  - Renouveler (renew) un certificat
  - Valider (validate) un certificat (expiration, CRL, OCSP, etc.)
  - Révoquer (revoke) un certificat (CRL)
- Basé sur XML Signature & XML Encryption
- W3C
  - Initié
  - XKMS XML Key Management Specification
    - http://www.xmltrustcenter.org/xkms
  - API Java
    - JSR 104 XML Trust Service APIs

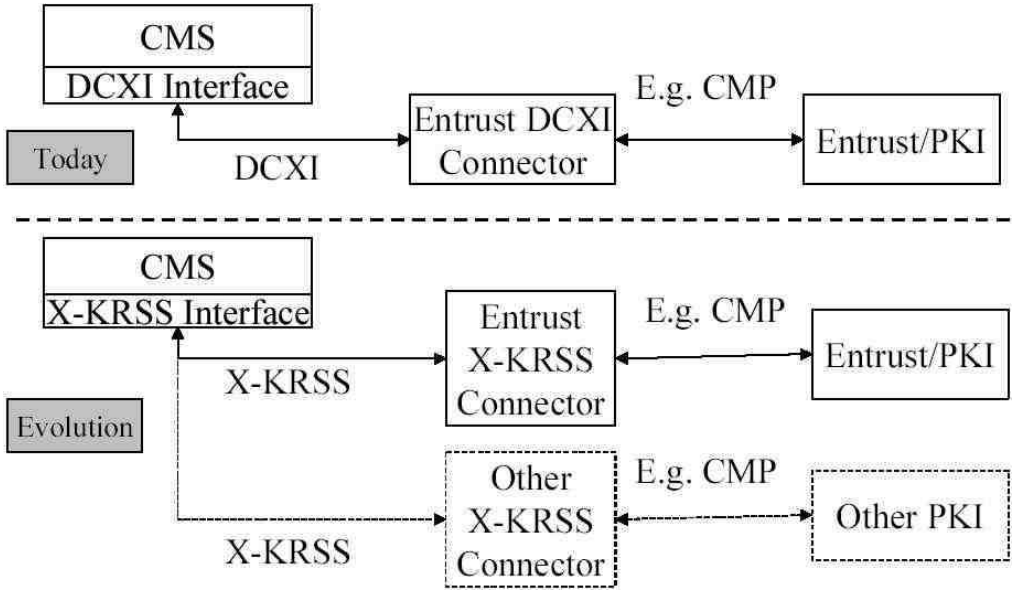
# XKMS
# Exemple de message de révocation

A request to revoke the key specified by <KeyID>

```
<?xml version="1.0"?>
<Request>
    <Prototype>
        <AssertionStatus>Invalid</AssertionStatus>
        <KeyID>unique_key_identifier</KeyID>
        <ds:KeyInfo>……</ds:KeyInfo>
    </Prototype>
    <AuthInfo>
        <AuthUserInfo>
            <ProofOfPossession>[RSA-Sign]</ProofOfPossesion>
        </AuthUserInfo>
    </AuthInfo>
    <Respond>
        <string>KeyName</string>
    </Respond>
</Request>
```

# XKMS Extension

- X-KRSS et CMS




- X-BULK (Baltimore)
  - gestion des clés pour des cartes SIM, des modems Cable, …
  - Motivations : batchs

# Java et PKI

- API Java
  - Java Cryptography Extension (JCE)
    - voir cours JCE
  - Java Secure Socket Extension (JSSE)
    - SSL/TLS
- API Java for XML
  - JSR 104 XML Trust Service APIs
  - JSR 105 XML Digital Signature APIs (javax.security.xml.dsig)
  - JSR 106 XML Digital Encryption APIs

# Carte à puce PKI et CMS

- Cartes PKI
  - Cartes à puce pourvue de fonctions cryptographiques
    - (logicielles ou matérielles)
  - Cartes dédiées: GemSafe, CryptoSafe, …
  - Card Applets PKI pour des JavaCard implémentant les packages `javacard.security.*` `javacardx.crypto.*`
- OCF
  - PKICardService
- CMS (Card Management Services)
  - Interfacage avec les CA
  - Extension à XKMS (Entrust)

# ISAKMP

- ISAKMP « *Internet Security Association and Key Management Protocol* »
  - Négociation pour les algorithmes et les clefs
  - Échange des clefs et authentification
  - Protocole d'échange Oakley
  - À donné naissance à IKE « *Internet Key Exchange* »

# Outil : OpenSLL

- Génération de la paire de clé et d'un certificat

  openssl genrsa 1024 > server.key

  openssl req –new -key server.key –out server.csr

  openssl req –x509 -key server.key –in server.csr –out server.crt

- Directives pour mod_ssl d'Apache

  SSLCertificateFile /usr/local/apache/conf/ssl.crt/server.crt

  SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/server.key

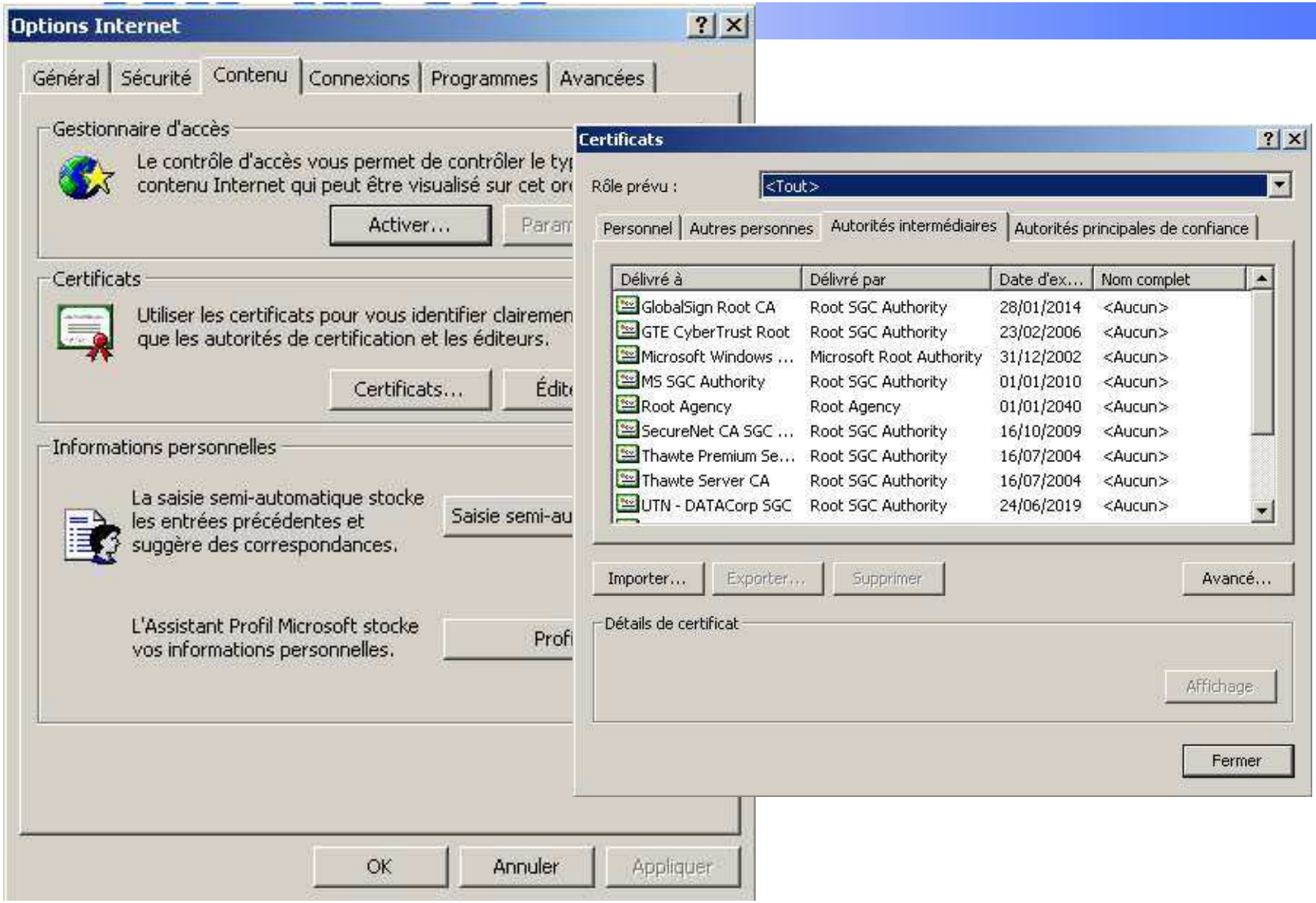
# Outil : GnuPGP

- Génération, Signature, Chiffrage

  gpg –gen-key

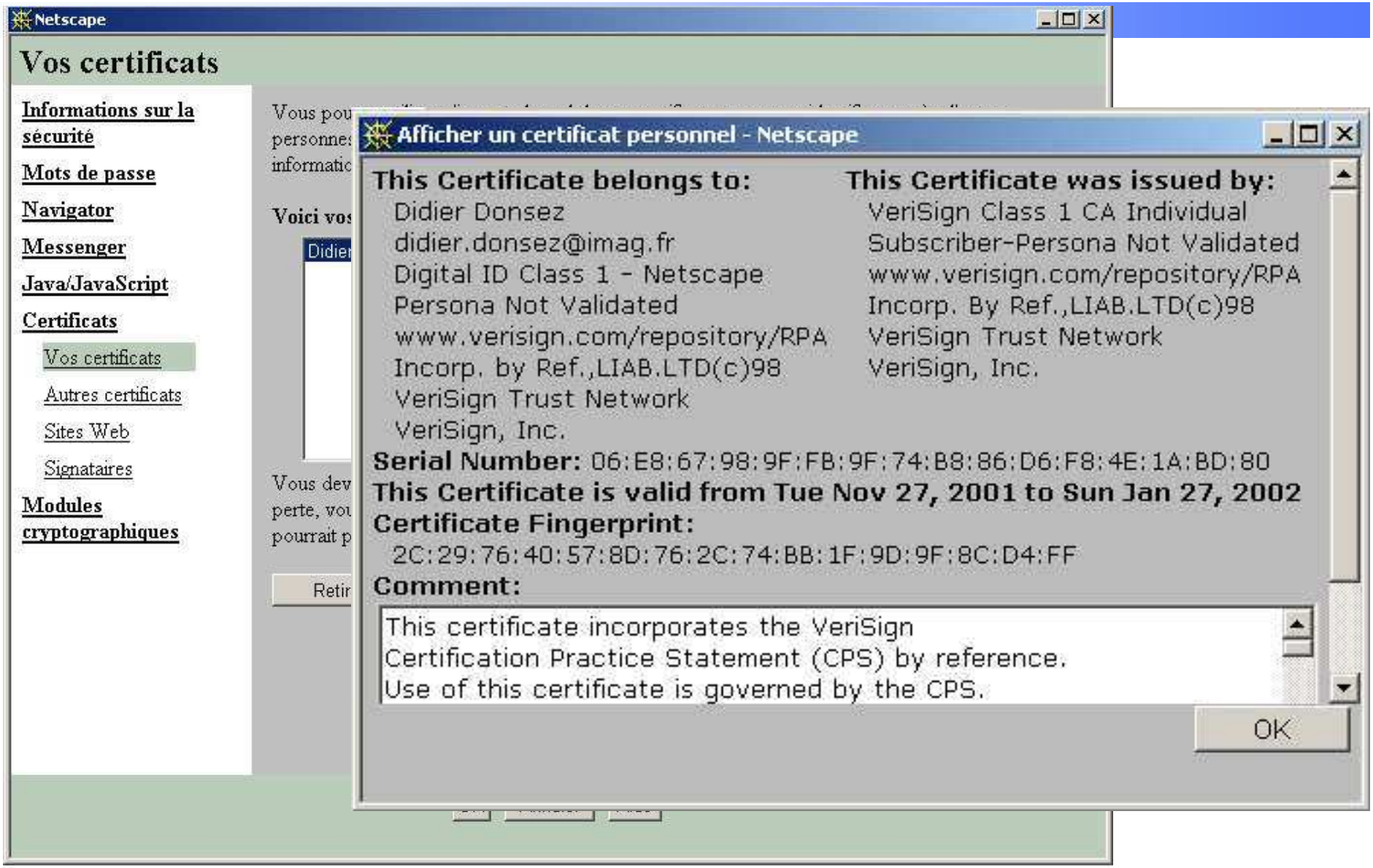
# Import de Certificats dans les Navigateurs

## *MS Internet Explorer*



# Import de Certificats dans les Navigateurs

## *Netscape Communicator (4.x)*



# Import de Certificats dans les Navigateurs *Nokia Mobile Internet Toolkit (WIM)*

# Bibliographie

- PKI : Public Key Infrastructure
  - http://www.iplanet.com/developer/docs/articles/security/pki.html
  - http://docs.iplanet.com/docs/manuals/security.html
  - http://www.verisign.com/resources/wp/index.html
  - http://www.thawte.com/
  - https://www.entrust.com/developer/java/faqs.htm

# Bibliographie


- http://csrc.nist.gov/pki/documents/welcome.html
- http://www.itu.int/
- http://www.itu.int/search/wais/Macbeth/#HowtoSearch
- http://www.mtic.pm.gouv.fr/dossiers/documents/lat/annuaires.shtml
- http://www.ietf.org/rfc/rfc2251.txt
- http://www.certplus.com/
- http://www.matranet.com/products/index.html
- http://www.ii.atos-group.com/francais/
- http://www.gemplus.com/french/index.htm
- http://www.certificat.com/
- http://www.scssi.gouv.fr/
- http://www.mtic.pm.gouv.fr/dossiers/documents/MTIC_certification_et_icp.pdf
- http://www.counterpane.com/pki-risks.html