Public Key Infrastructure (PKI)
-
Infrastructure de Gestion de Clé (IGC)

Ahmed Serhrouchni & Mounira MSAHLI

Sommaire

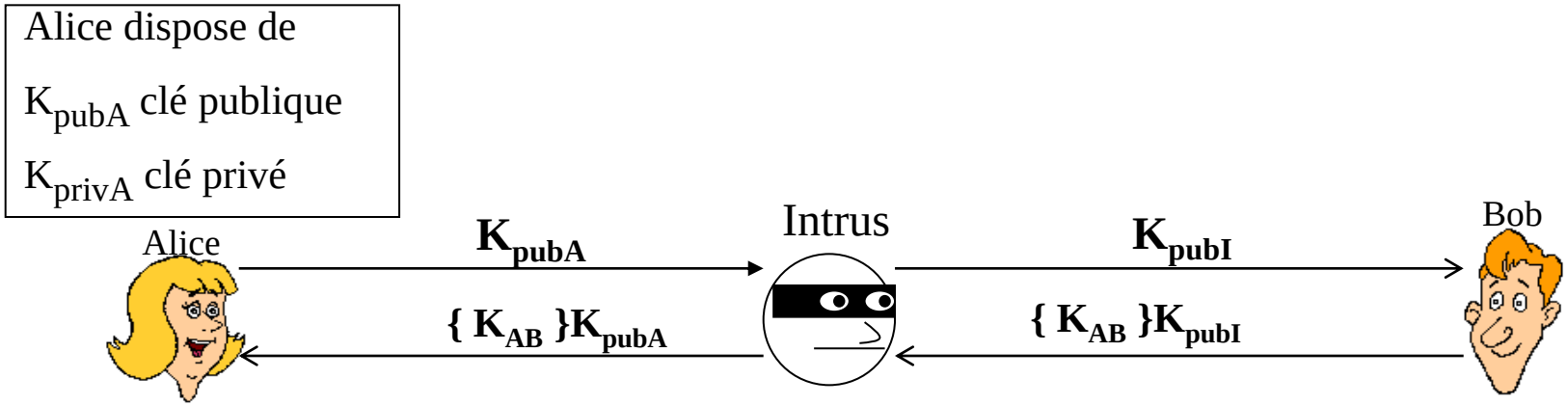
- Rappel des problèmes de la cryptographie
- Services de sécurité cryptographique
- Signature numérique
- Codage et standards
- Certificats X509
- Infrastructures de gestion de clés (PKI)
- Les solutions de sécurité à base de PKI
- La régulation

Rappel des problèmes de la cryptographie

- Problèmes liés au chiffrement symétrique :
  - L'échange des clés
    - Nécessite souvent de la personnalisation
    - Modèle statique
  - La taille de la clé dépend de la législation
    - Dans tous les pays il existe une législation qui limite la taille pour certaines finalités (4 finalités: usage, fourniture, import et export)
  - La taille de la clé dépend des algorithmes
    - Avec DES la taille est limitée à 56 bits, c'est le plus répandu actuellement.
  - Les générateurs de clés manquent de fiabilité
    - Nécessite l'usage de composants physiques
      - Besoin de rafraîchissement des clés ou renvouvellement

Rappel des problèmes de la cryptographie

- Problèmes liés au chiffrement asymétrique :



Nécessité d'authentifier les clés publiques

Services de sécurité cryptographique

Service de confidentialité

- Caractère réservé d'une information dont l'accès est limité aux personnes admises à la connaître
- ISO 7498-2 :
  - la propriété qu'une information n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés.
- Une information échangée entre deux ou plusieurs entités n’est accessible que par celles-ci.

Services de sécurité cryptographique

Service d'intégrité

- Propriété garantissant qu'une information n'a pas été modifié sans autorisation
- ISO 7498-2 :
  - la propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée
- Une information échangée entre deux ou plusieurs entités est reçue par tous telle qu'elle a été émise.
  - Dans un contexte d'échange l'authentification de l'origine accompagne le service d'intégrité.

Services de sécurité cryptographique

Service d’authentification

- Confirmation de la véracité de l'identité ou d’un élément spécifique à une entité déclarée
- ISO/IEC 2382/8:
  - Assure que l'identité de l'origine des données est bien l'identité revendiquée
- Dans la pratique l’authentification
  - consiste à relier des informations entre elles avec généralement un élément permettant de spécifier une entité

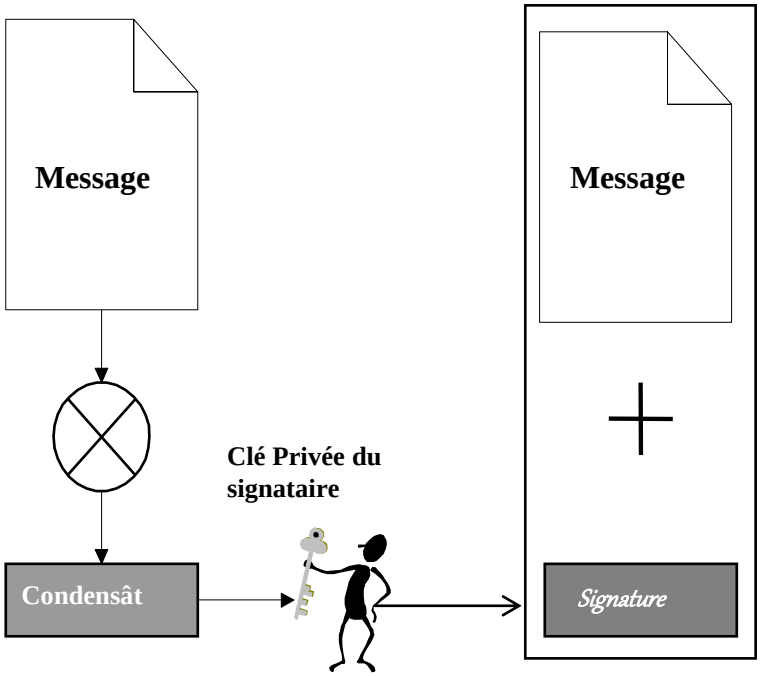
Services de sécurité cryptographique

Service de non répudiation

- La répudiation consiste:
  - au fait que dans un échange où sont impliqués deux ou plusieurs entités , l'une de celles renie d'avoir participé à tout ou partie de l'échange
- La non répudiation consiste:
  - Au fait qu'aucune entité ne puisse répudier d'avoir participé à l'échange
- La non répudiation dans le contexte d'un émetteur et d'un récepteur:
  - Consiste donc à ce que ni l'émetteur et/ou le destinateur ne puisse répudier l'émission et/ou la réception d'un message
- La non répudiation relève de la notion de preuve au sens juridique du terme

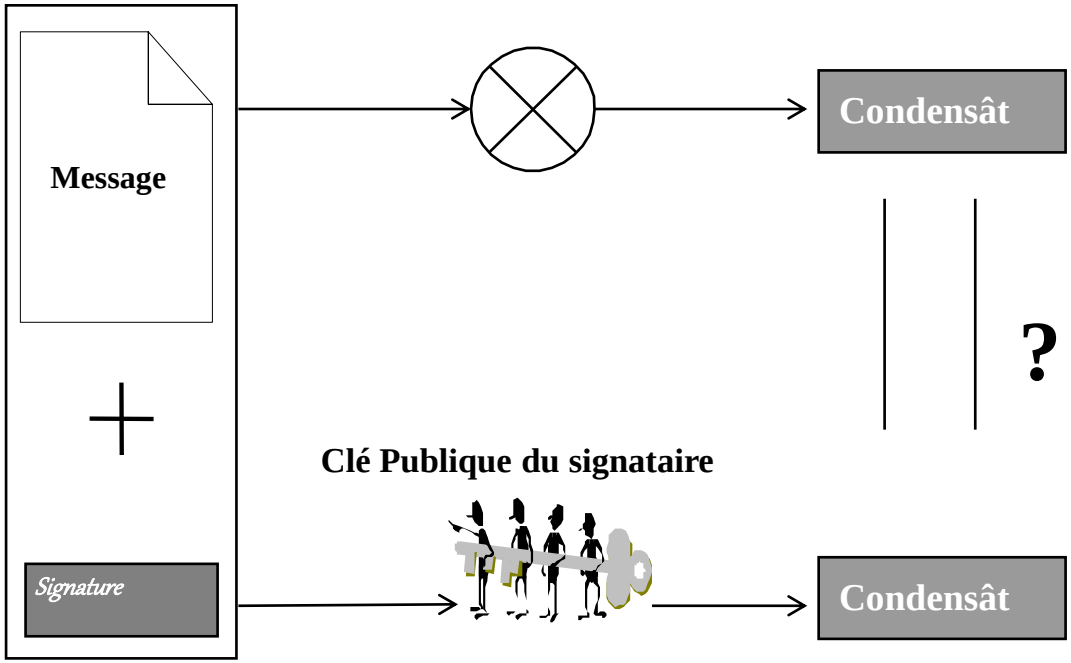
Signature numérique

- Signer un message



Signature numérique

- Vérifier la signature d'un message



Formats et standards
Codage ASN1

- Plusieurs langages de représentation de données: C, Pascal, Lisp, ADA, Java, …
  - Pouvoir d'expression de données différents
- Nécessité d'un formalisme abstrait pour la représentation de données
  - Avec une capacité de pouvoir d'expression extensible
- Nécessité d'une représentation interne indépendante machine

Formats et standards
Codage ASN1

- Langage de représentation des données applicatives.
  - Schéma conceptuel à propos desquels les applications coopèrent
- Deux composantes : syntaxe abstraite et syntaxe de transfert
  - Pouvoir d'expression de toute structure de données ou de ressources
  - La syntaxe abstraite permet la définition de tous types de "type"
  - Indépendance de toute représentation interne

Formats et standards
Codage ASN1

- Langage abstrait pour **la représentation** externe de données
  - Aucune hypothèse sur un langage de typage
- Aucune contrainte sur la taille des ensembles de valeurs ou des valeurs
  - Entier et réel de tailles quelconques
- Pouvoir d’expression de tous types de ressources
  - Système de fichiers, protocoles
- Intègre tous les langages de représentation des données actuels
- Indépendance de la représentation interne

Formats et standards
Codage ASN1

- ASN1 n’est pas une technique formelle
  - Pas de modèle mathématique
  - Pas de vérification
- ASN1 nécessite un compilateur
- ASN1 est plus compacte que XML
  - Codage spécifique pour réduire la taille des données interne
- Le codage interne est ***généralement*** binaire
  - Les objets binaires sont codés en base64 pour le transport par les applications TCP/IP
- ASN1 évolue par le codage et aussi la syntaxe

Formats et standards
Codage ASN1

```
Age  ::= INTEGER (12..25)
Usager ::= SEQUENCE {
        nom   IA5String (SIZE(1..50)),
        age     Age,
        adresse IA5String OPTIONAL,
        ...
    }
```

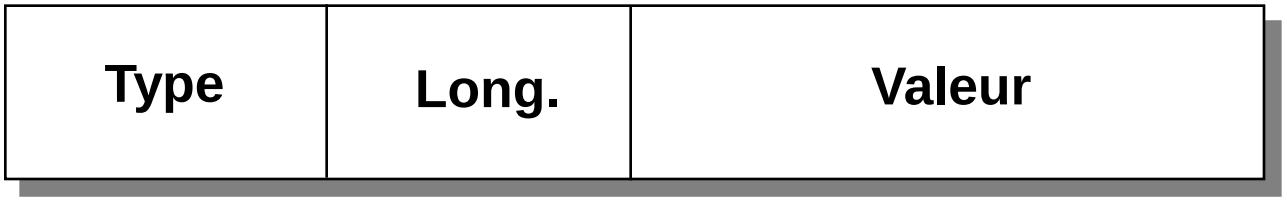
- Capacité de décrire des types simple et complexe.
- Les types peuvent avoir des contraintes sur la taille et/ou la valeur.
- Plusieurs contraintes sont disponibles.
- Des champs peuvent être marqués OPTIONAL.
- Des valeurs peuvent être assignées par DEFAULT.
- Les types peuvent être étendues pour atteindre divers ensembles de données

Formats et standards
Codage ASN1

- ITU-T Rec. X.680 | ISO/IEC 8824-1 - Basic ASN.1 Notation

- ITU-T Rec. X.690 | ISO/IEC 8825-1
  Basic Encoding Rules (BER)
  Distinguished Encoding Rules (DER)
  Canonical Encoding Rules (CER)
- ITU-T Rec. X.691 | ISO/IEC 8825-2
  Packed Encoding Rules (PER)
- ITU-T Rec. X.692 | ISO/IEC 8825-3
  Encoding Control Notation (ECN)
- ITU-T Rec. X.693 | ISO/IEC 8825-4
  XML Encoding Rules (XER)
- ITU-T Rec. X.694 | ISO/IEC 8825-5
  Encoding XML-Defined Data Using ASN.1

- Basic Encoding Rules (BER)
- Décrit une méthode pour l'encodage des valeurs ASN.1
- Basé sur une structure de type: Type, Longueur, Valeur (TLV)
- La structure TLV est récursive



Formats et standards
Codage ASN1

- Des avantages de ASN.1
- Le concepteur de protocole d'application se focalise sur l'information et non sur les besoins d'échanges
- Fournit aux implémenter une description plus précise des messages à échanger
- Indépendant d'un langage particulier
- La technologie a fait ses preuves
- Largement adopté en tant que Standard International

Formats et standards
Standards PKCS

- Des standards pour la cryptographie à clé publique
- PKCS (Public Key Cipher System) sont des standards définis initialement par la compagnie RSA pour activer l'usage de l'algorithme asymétrique RSA.
- Principale objectif: interopérabilité entre les applications.
- Pour la plupart ils sont standardisés à l'IETF. Certains sont obseletes.
- Ils couvrent la réalisation de tous les services de sécurité.
- Ils définissent des formats pour tous les objets liés à la réalisation de ces services. Ils définissent également des interfaces entre certains composants (logiciel et matériel) de sécurité
- ASN1 et DER sont utilisés pour la représentation abstraite et interne de ces objets
- Une description de ces standards avec des exemples et donnée sur le site de RSA (http://www.rsa.com)

Formats et standards
Standards PKCS

PKCS #1: RSA Cryptography Standard
PKCS #3: Diffie-Hellman Key Agreement Standard
PKCS #5: Password-Based Cryptography Standard
PKCS #7: Cryptographic Message Syntax Standard
PKCS #8: Private-Key Information Syntax 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 #14: Pseudorandom Number Generation Standard
PKCS #15: Cryptographic Token Information Format Standard

Formats et standards
Standards PKCS#1

- Défini dans le RFC3447
- Spécifie les primitives RSA de chiffrement, de déchiffrement de signature (selon un principe décrit dans PKCS #7) et de vérification
- Spécifie les schémas de chiffrement et de signature
- Spécifie les méthodes d'encodage de ces schémas
- Spécifie la syntaxe ASN.1 pour:
  - les clés publiques
  - les clés privées
  - les schémas mentionnés ci-dessus

Formats et standards
Standards PKCS#1

- Syntaxe des clés en ASN1 :
- **RSAPublicKey ::= SEQUENCE {**

```
    modulus             INTEGER,    -- n
    publicExponent      INTEGER     -- e }
```

- **RSAPrivateKey ::= SEQUENCE {**

```
  version               Version,
  modulus               INTEGER, -- n
  publicExponent        INTEGER, -- e
  privateExponent       INTEGER, -- d
  prime1                INTEGER, -- p
  prime2                INTEGER, -- q
  exponent1             INTEGER, -- d mod (p-1)
  exponent2             INTEGER, -- d mod (q-1)
  coefficient           INTEGER
                        -- (inverse of q) mod p }
```

- **Le processus de chiffrement RSA (**quatre étapes)
  - ***Le formatage du bloc de chiffrement***
    - *D* représente les données à chiffrer,
    - *EB* (Encryption Block) bloc à chiffrer

      EB = 00 || *BT* || *PS* || *00* || *D*
      - *BT* : représente le type du bloc (00 ou 01 pour une clé privée, 02 pour une clé publique).
      - *PS* représente les octets de bourrage (*k-3*||*D*)
      - permettant d'avoir une longueur *k* pour *EB*.
  - ***Conversion chaîne d'octets/entier***
    - Conversion de *EB* (chaîne de caractères) en un entier *x*.
  - ***L'opération de chiffrement RSA***
  - ***Conversion entier/chaîne d'octets***

Formats et standards
Standards PKCS#5

- Description d'une méthode pour chiffrer une chaîne d'octets avec une clé secrète dérivée d'un mot de passe.
  - Password-Based Cryptography Standard
- Standard destiné au chiffrement de clés privées (réfère PKCS #8).
- Définition de deux algorithmes de chiffrement de clé
  - MD2 avec DES-CBC
  - MD5 avec DES-CBC

Formats et standards
Standards PKCS#5

- Le processus de chiffrement de la clé privé suit trois étapes:
  - la génération de la clé secrète K et d'un IV
  - le formatage du bloc de chiffrement
  - le chiffrement
- La génération de la clé secrète K et d'un IV
  - En entrée on a:
    - un message M (chaîne d'octets)
    - un mot de passe P (chaîne d'octets)
    - une salt value S (chaîne d'octets)
    - un compteur c (entier)
  - la chaîne P || S est condensée c fois
  - les huit premiers octets constituent la clé secrète K
  - Le vecteur d'initialisation IV sera lui constitué des huit derniers octets du résultat de condensation

Formats et standards
Standards PKCS#7

- Standard d'une syntaxe pour application aux données de processus cryptographique:
  - Chiffrement, signature, enveloppe
- Syntaxe récursive:
  - une enveloppe peut être enveloppée
- La syntaxe inclut des attributs optionnels tels la date, les certificats, les CRLs.
- Conversion de PKCS#7 vers PEM (RFC1422).

Formats et standards
Standards PKCS#7

- La syntaxe supporte six types de données (***Content Info***):
  - les données (data),
  - les données signées (signed data),
  - les données « encapsulées » (envelopped data),
  - les données signées et encapsulées (signed-and-envelopped data),
  - les données hachées (digested data)
  - les données chiffrés (encrypted data).
- 2 classes de contenues de *basic* et *enhanced*
  - Les deux premiers sont de la classe ***basic***
    - Pas de chiffrement ni de hachage
  - Les quatre autres de classe ***enhanced***
    - Peuvent contenir d'autres content type

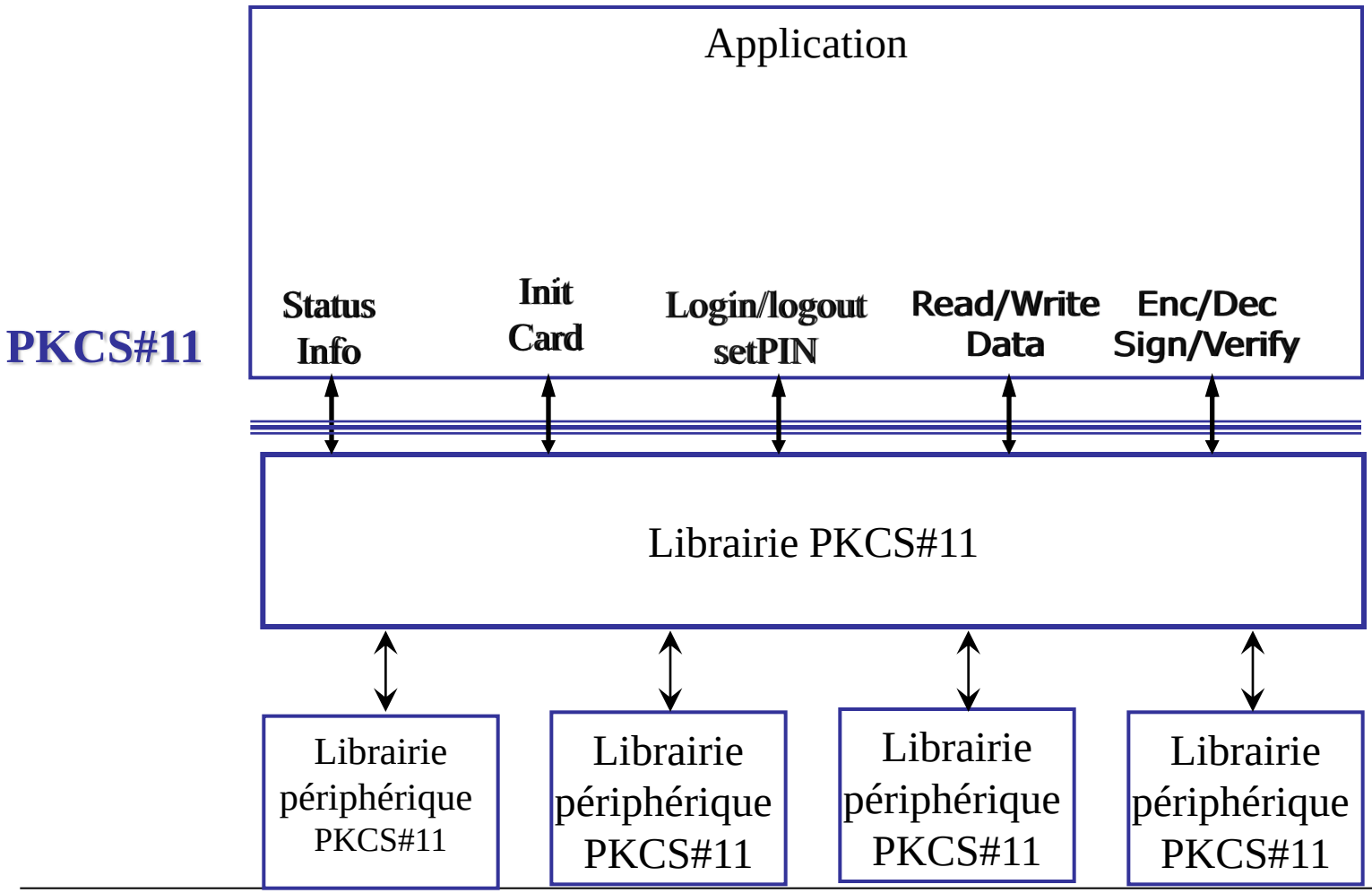
Formats et standards
Standards PKCS#7

```
SignedData ::= SEQUENCE {
    version             Version,
    digestAlgorithms    DigestAlgorithmIdentifiers,
    contentInfo         ContentInfo,
    certificates        [0] IMPLICIT Certificates OPTIONAL,
    crls                [1] IMPLICI CertificateRevocationLists
                        OPTIONAL,
    signerInfos         SignerInfos }

DigestAlgorithmIdentifiers ::= SET OF
                                    DigestAlgorithmIdentifier

SignerInfos                 ::= SET OF SignerInfo
```

Formats et standards
Standards PKCS#11

- Définit une API
  - Connu sous le nom de CRYPTOKI
  - Cryptoki isole une application des détails associés à un périphérique cryptographique patrticulier.
- Permet l'accès à des « tokens » cryptographiques
  - les cartes à puce
  - les « token USB ».
- Fournit les services suivants de:
  - Stockage des clés publiques/privée, des certificats, des valeurs d'authentification (PIN), et d'autres type de données.
  - chiffrement/déchiffrement
  - Signatures et de vérification
  - génération des clés
  - génération des nombres aléatoires
- La plupart des browsers supporte cette API

Formats et standards
Standards PKCS#11



Formats et standards
Standards PKCS#15

- Standardisation du format des fichiers et répertoires pour le stockage d’éléments cryptographiques.
  - Cryptographic Token Information Format Standard

- Ne standardise pas le calcul RSA

Les certificats
Motivations

- Problème de la cryptographie asymétrique
  - La distribution des clés publiques
  - L'authentification des clés publiques
    - Une clé publique appartient bien à celui qui prétend en être le détenteur
  - L'usage associé à la clé publique
- La cryptographie asymétrique:
  - Pour les services orienté preuve
  - La distribution des clés de session
  - Pour une durée de vie plus conséquente
    - Nécessité de les révoquer si nécessaire
- La réponse est le certificat et une infrastructure associée pour leur gestion

Les certificats
Motivations

- « Certificat » = relève d'une autorité ou institution
- Le contenu = information « authentique »
- Mise en place d'un état de confiance en présence d'un certificat
- Dico: « Acte écrit qui rend témoignage de la vérité d 'un fait, d'un droit »
- Présence d'une autorité « reconnu » qui atteste de la véracité du contenu.
- Certificat = document « signé »

Les certificats
Motivations

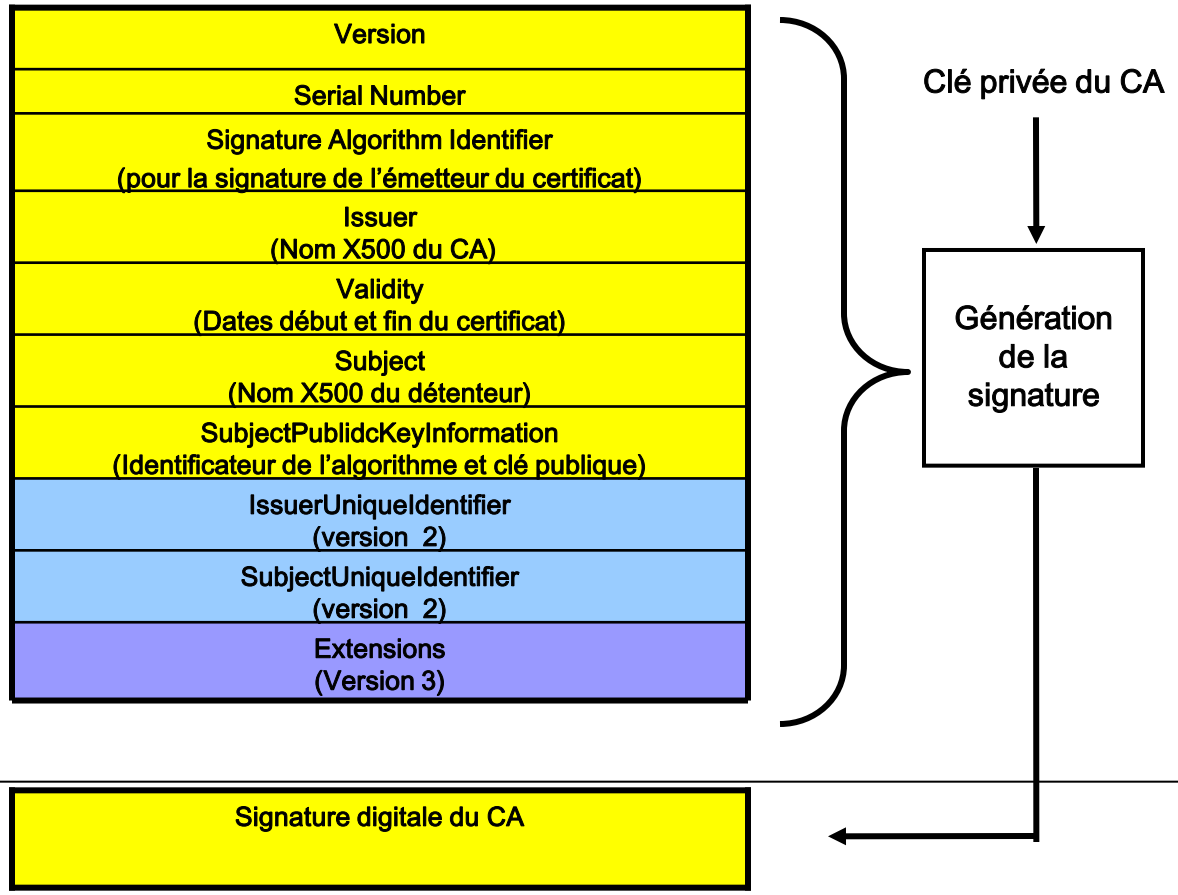
- Certificat personnel
  - permet d'authentifier un utilisateur.
- Certificat serveur
  - permet d'authentifier un serveur
- Certificat développeur
  - permet de signer et d'authentifier les programmes et macros développés.
- Certificat d'autorité de certification
  - permet de signer des certificats.

Les Certificats
Standard X.509

- Un seul standard en lice: Certificats X509
- Standard:
  - ITU-T X.509(03/2000), ou ISO/IEC 9594-8
    - Certificats de clé publique et d'attribut
  - RFC 3280: (définition de profil fonctionnel basé sur X509)
- Versions successives:
  - 1988 : v1
  - 1993 : v2 = v1 + 2 nouveaux champs
  - 1996 : v3 = v2 + extensions

Les Certificats
Standard X.509

- Structure de données permettant de lier différents éléments au moyen d'une signature
  - Le sujet ,la clef, l'émetteur du certificat, conditions de validité,…



Les Certificats
Standard X.509

Certificat ::= SEQUENCE {

version[0] Version DEFAULT v1,

serialNumber CertificateSerialNumber,

signature AlgorithmIdentifier,

issuer Name,

validity Validity,

subject Name,

subjectPublicKeyInfo SubjectPublicKeyInfo,

issuerUniqueIdentifier[1] IMPLICIT UniqueIdentifier OPTIONAL,

-- si ce composant est présent, la version doit être v2 ou v3

subjectUniqueIdentifier[2]IMPLICIT UniqueIdentifier OPTIONAL,

-- si ce composant est présent, la version doit être v2 ou v3

extensions[3] Extensions OPTIONAL

-- si ce composant est présent, la version doit être v3 --

}

Les Certificats
Standard X.509

```
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER
Validity ::= SEQUENCE {
    notBefore    Time,
    notAfter     Time }

SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm            AlgorithmIdentifier,
    subjectPublicKey     BIT STRING }

Extensions ::= SEQUENCE OF Extension

Extension ::=   SEQUENCE {
        extnId           Object Identifier,
        critical         BOOLEAN DEFAULT FALSE,
        extnValue        OCTET STRING}
```

Les Certificats
Standard X.509

Certificate:

Version: 1 (0x0)

Serial Number: 1f:42:28:…:b3:ab:1f:1c

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, **O=**VeriSign, Inc., **OU=**Class 2 Public Primary Certification Authority - G2, **OU=** (c) 1998 VeriSign, Inc. - For authorized use only, **OU=**VeriSign Trust

Validity

Not Before: May 18 00:00:00 1998 GMT

Not After : May 18 23:59:59 2018 GMT

Subject: C=US, **O=**VeriSign, Inc., **OU=**Class 2 Public Primary Certification Authority - G2, **OU=** (c) 1998 VeriSign, Inc. - For authorized use only, **OU=**VeriSign

Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:a7:…:7f:77

Exponent: 65537 (0x10001)

Signature Algorithm: sha1WithRSAEncryption

11:45:….:ce:ef:

Les Certificats
Standard X.509

Certificate:

Version: 3 (0x2)

Serial Number: d0:1e:40:90:00:00:27:4b:00:00:00:01:00:00:00:04

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Utah, L=Salt Lake City, **O=**Xcert EZ by DST, **CN=**Xcert EZ by …

Validity

Not Before: Jul 14 16:14:18 1999 GMT

Not After : Jul 11 16:14:18 2009 GMT

Subject: C=US, **ST=**Utah, L=Salt Lake City, **O=**Xcert EZ by DST, **CN=**Xcert EZ

Subject Public Key Info: Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit): 00:...:ee:71

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical **CA:**TRUE

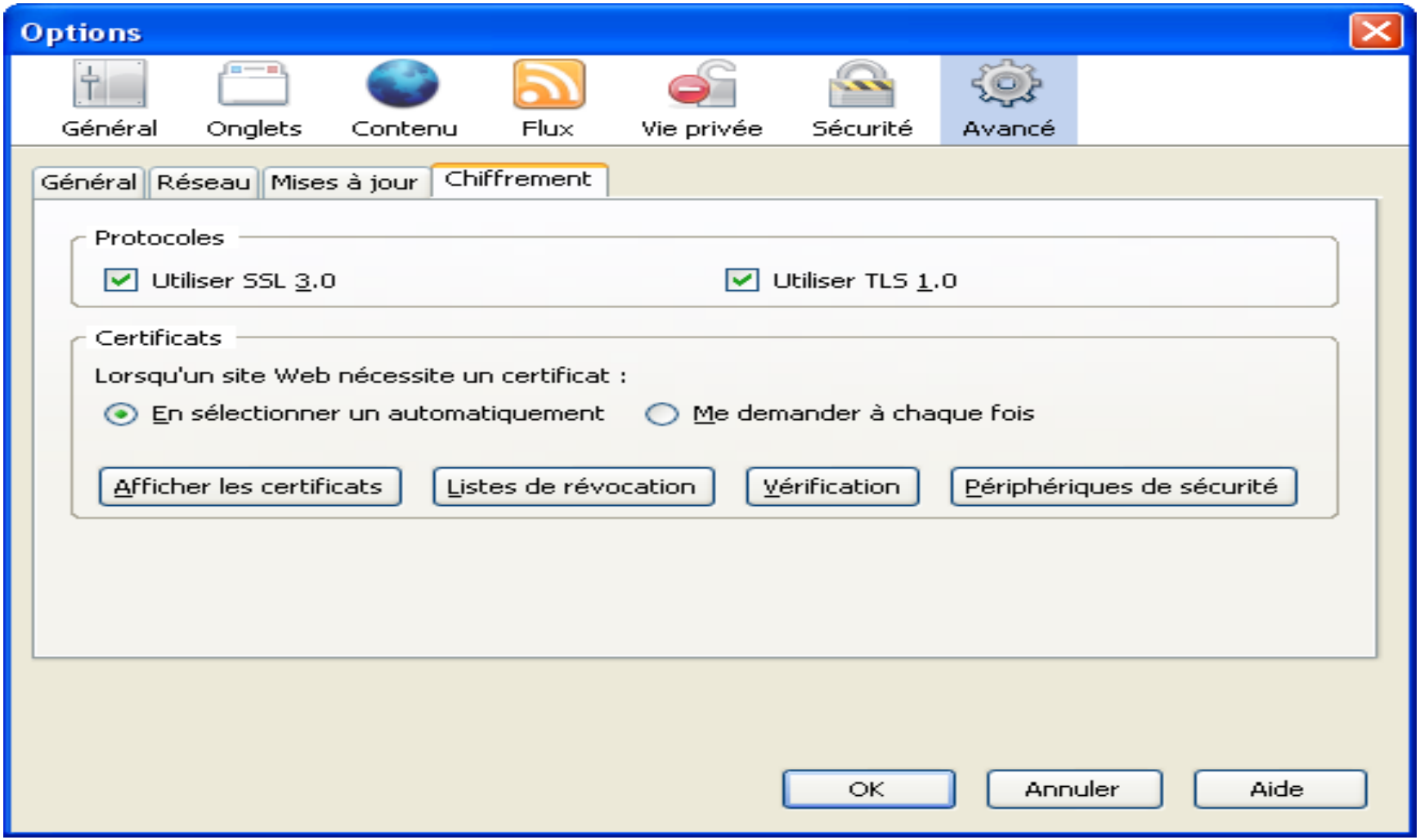
X509v3 Authority Key Identifier:

keyid:08:20:...:27:77

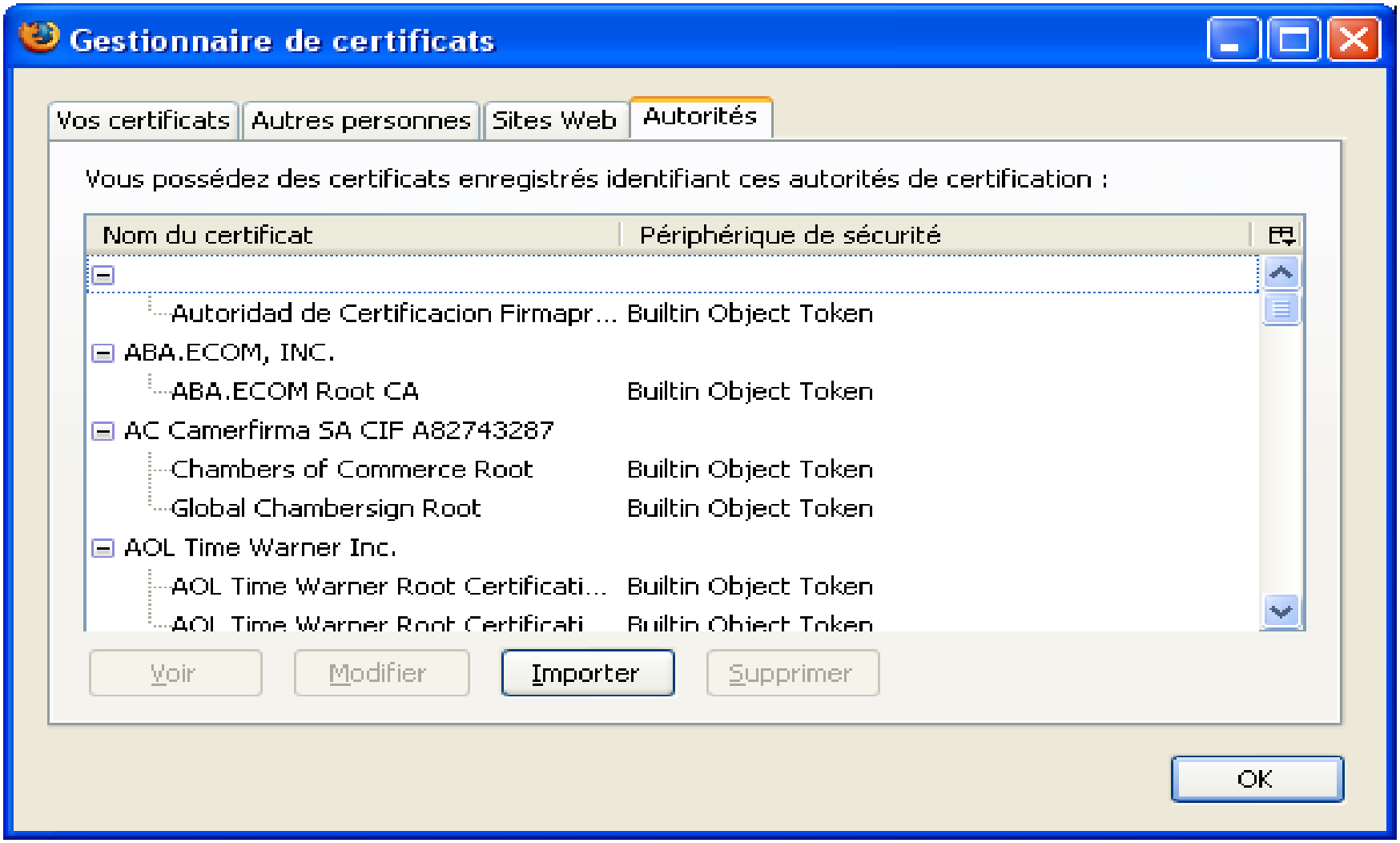
X509v3 Subject Key Identifier: 08:20:...:27:77

Signature Algorithm: sha1WithRSAEncryption 5a:87:...:79:7c

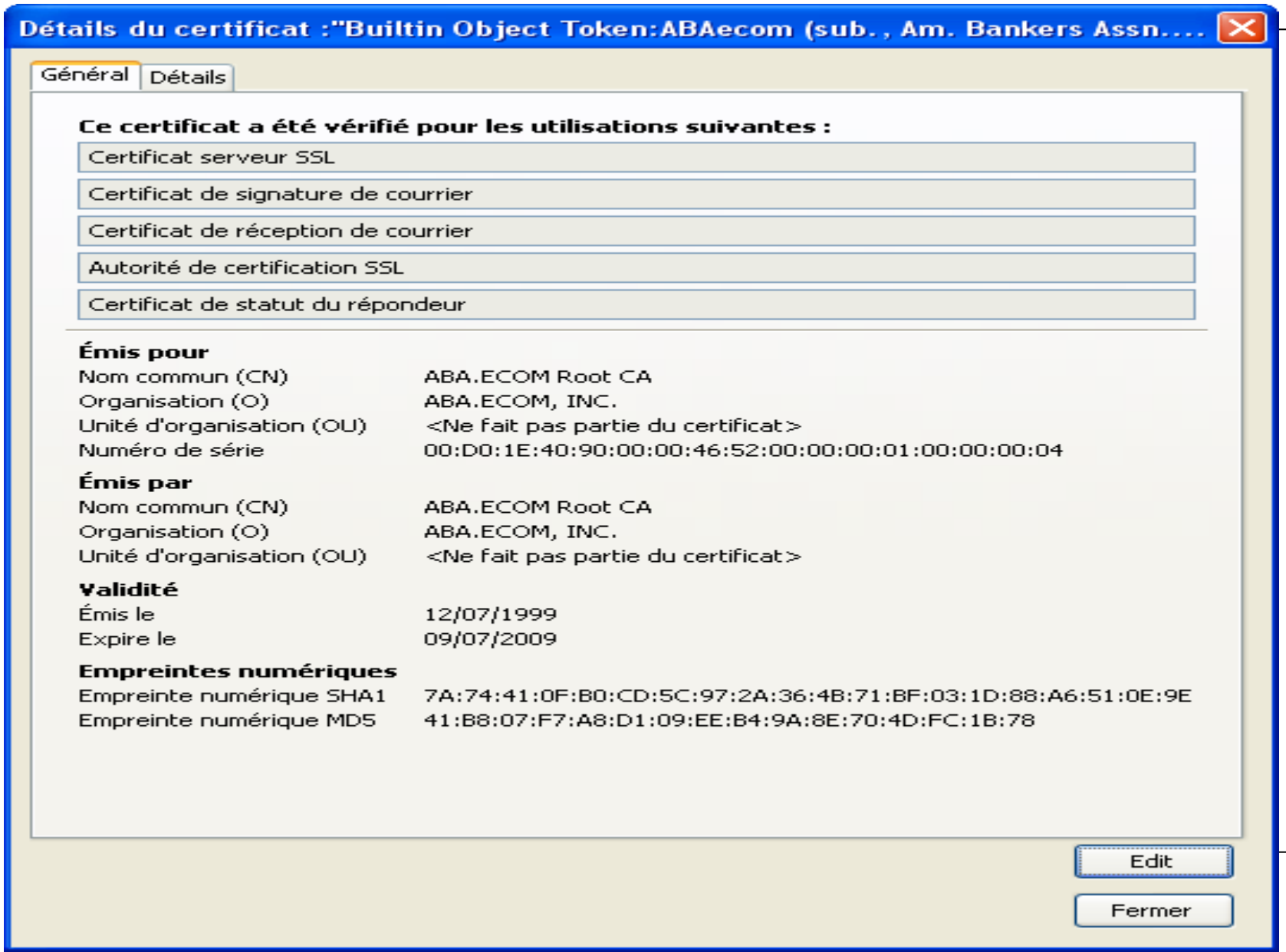
Les Certificats
Standard X.509



Les Certificats
Standard X.509



Les Certificats
Standard X.509

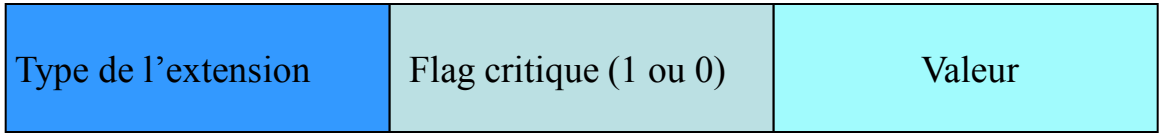


Les Certificats
Standard X.509: les extensions

- Le but initial des certificats est de lier:
  - identité et clé publique par la signature d'un tiers de confiance
- Pour couvrir des services plus étendus
  - Nécessaire d'associer d'autres informations à la clé publique
- L'extension consiste à ajouter de nouveaux champs aux certificats
- L' extension est défini dans ITU-T Rec. X.660 et ISO/IEC 9834-1
- Des extensions sont standardisées,
  - possibilité de définir des extensions spécifiques
- Si l'application ne supporte pas une extension critique, elle abandonne le certificat.

Les Certificats
Standard X.509: les extensions

- Structure de l'extension



- Type est unique pour chaque extension: le type est un type de base ASN1 Object Identifier (OID)
- Avec un flag critique
  - Si l'application:
    - ne supporte pas cette extension, elle refuse le certificat
    - supporte cette extension et la valeur est conforme elle l'accepte sinon elle le rejette
- Avec un flag non critique
  - Si l'application
    - ne supporte pas cette extension: elle accepte le certificat
    - supporte cette extension et la valeur est conforme elle l'accepte sinon elle le rejette.

Les Certificats
Standard X.509: les extensions

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
    extnID OBJECT IDENTIFIER,
    critical BOOLEAN DEFAULT FALSE,
    extnValue OCTET STRING }

id-ce OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 29 }

http://asn1.elibel.tm.fr/cgi-bin/oid/display?tree=2.5.29&see=all

Les Certificats
Standard X.509: les extensions

0 - ITU-T plus de 35 OIDs

1 - ISO plus de 2202 OIDs (1.3.6.1 - OID – Internet)

2 - ISO/ITU-T plus de 1172 OIDs

2.5 - X.500 Directory Services

2.5.1 - X.500 modules

2.5.2 - X.500 service environment

2.5.3 - X.500 application context

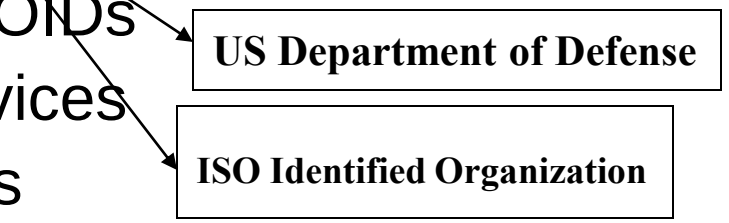
2.5.4 - X.500 attribute types

2.5.5 - X.500 attribute syntaxes

……..

2.5.29 - certificateExtension (id-ce)

2.5.30 - managementObject (id-mgt)



Les Certificats
Standard X.509: les extensions

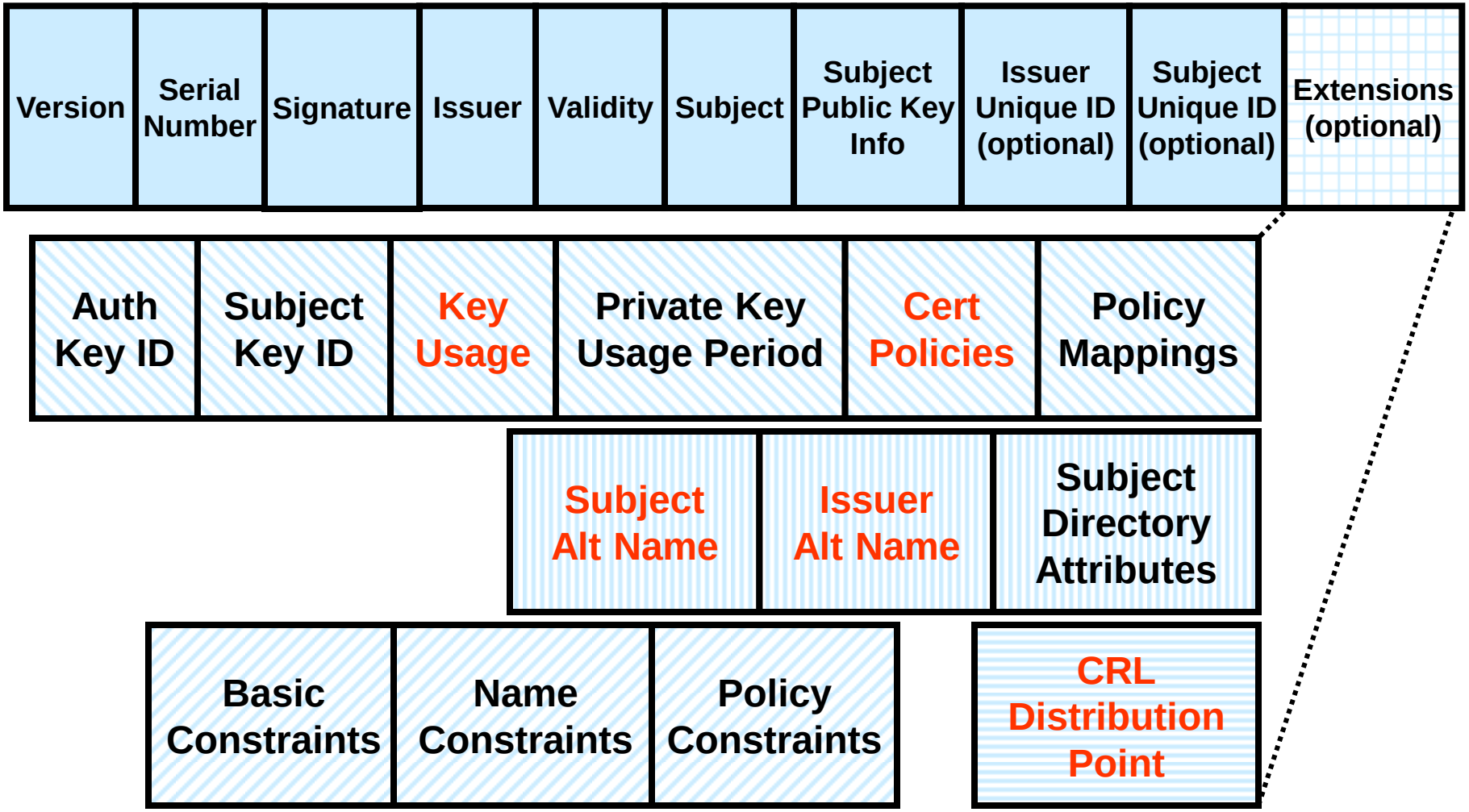
2.5.29 - certificateExtension (id-ce)
2.5.29.1 - old Authority Key Identifier
2.5.29.2 - old Primary Key Attributes
2.5.29.3 - Certificate Policies
2.5.29.4 - Primary Key Usage Restriction
2.5.29.14 - Subject Key Identifier
2.5.29.15 - Key Usage
2.5.29.16 - Private Key Usage Period
2.5.29.17 - Subject Alternative Name
2.5.29.18 - Issuer Alternative Name
2.5.29.19 - Basic Constraints
2.5.29.20 - CRL Number
2.5.29.21 - Reason code

2.5.29.23 - Hold Instruction Code
2.5.29.24 - Invalidity Date
2.5.29.27 - Delta CRL indicator
2.5.29.28 - Issuing Distribution Point
2.5.29.29 - Certificate Issuer
2.5.29.30 - Name Constraints
2.5.29.31 - CRL Distribution Points
2.5.29.32 - Certificate Policies
2.5.29.33 - Policy Mappings
2.5.29.35 - Authority Key Identifier
2.5.29.36 - Policy Constraints
2.5.29.37 - Extended key usage
2.5.29.46 - FreshestCRL
2.5.29.54 - X.509 version 3 certificate extension Inhibit Any-policy

Les Certificats
Standard X.509: les extensions

- Extensions sur:
  - le nomage de l'objet et du signataire
  - les clés publiques/privés
  - la révocation
  - la politique de certification
  - le rôle
  - Autres … logo (RFC 3709: Internet X.509 Public Key Infrastructure:Logotypes in X.509 Certificates)

Les Certificats
Standard X.509: les extensions



Les Certificats
Standard X.509: les extensions

- **SubjectAlternativeName**
  - un nom X.500, une adresse X400, un nom rfc822 (adresse mail), un Directoryname (DNS), un nom EDI, une URL, une adresse IP, un OID… ou toute forme de nom,

SubjectAlternativeName ::= GeneralNames
IssuerAlternativeName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {

otherName	**[0]**	**OtherName**
rfc822Name	**[1]**	**IA5String,**
dNSName	**[2]**	**IA5String,**
x400Address	**[3]**	**ORAddress,**
directoryName	**[4]**	**Name,**
ediPartyName	**[5]**	**EDIPartyName,**
uniformResourceIdentifier	**[6]**	**IA5String,**
iPAddress	**[7]**	**OCTET STRING,**
registeredID	**[8]**	**OBJECT IDENTIFIER }**

OtherName ::= SEQUENCE {
type-id OBJECT IDENTIFIER,
value [0] EXPLICIT ANY DEFINED BY type-id }

Les Certificats
Standard X.509: les extensions

- **IssuerAlternativeName**
  - Toute forme de nom;
- **AuthorityKeyIdentifier**
  - Permet de distinguer plusieurs clés utilisés par le même CA. Identifie la clé publique pour la vérification de la signature apposée au certificat.
- **SubjectKeyIdentifier**
  - Identificateur de clé unique par rapport à toutes les clés en possession du sujet.
- **CertificatePolicies :**
  - liste des politiques de sécurité reconnues par le CA émetteur.
- **KeyUsage** : usage de la clé publique certifiée
  - DigitalSignature, NonRepudiation, KeyEncipherment, keyCertSign, CRLSign
- **ExtendedKeyUsage :**
  - Indique un ou plusieurs buts pour l'usage de la clé publique: serverAuth, clientAuth, codeSigning, emailProtection, timeStamping, OCSPSigning

    ExtentededKeyUsage ::= SEQUENCE OF KeyPurposeId

    KeyPurposeId ::= OBJECT IDENTIFIER

Les Certificats
Standard X.509: les extensions

- **BasicConstraints:**
  - indique si le détenteur d'un certificat peut agir comme un CA, si oui, donne aussi la longueur de chemin de certification
- **Extensions sur la révocation:**
  - indique la méthode à utiliser pour vérifier la révocation

BasicConstraints ::= SEQUENCE {
cA BOOLEAN DEFAULT FALSE,
pathLenConstraint INTEGER (0..MAX) OPTIONAL }

Exemple: X509v3 extensions:

Basic Constraints: critical **CA:**TRUE

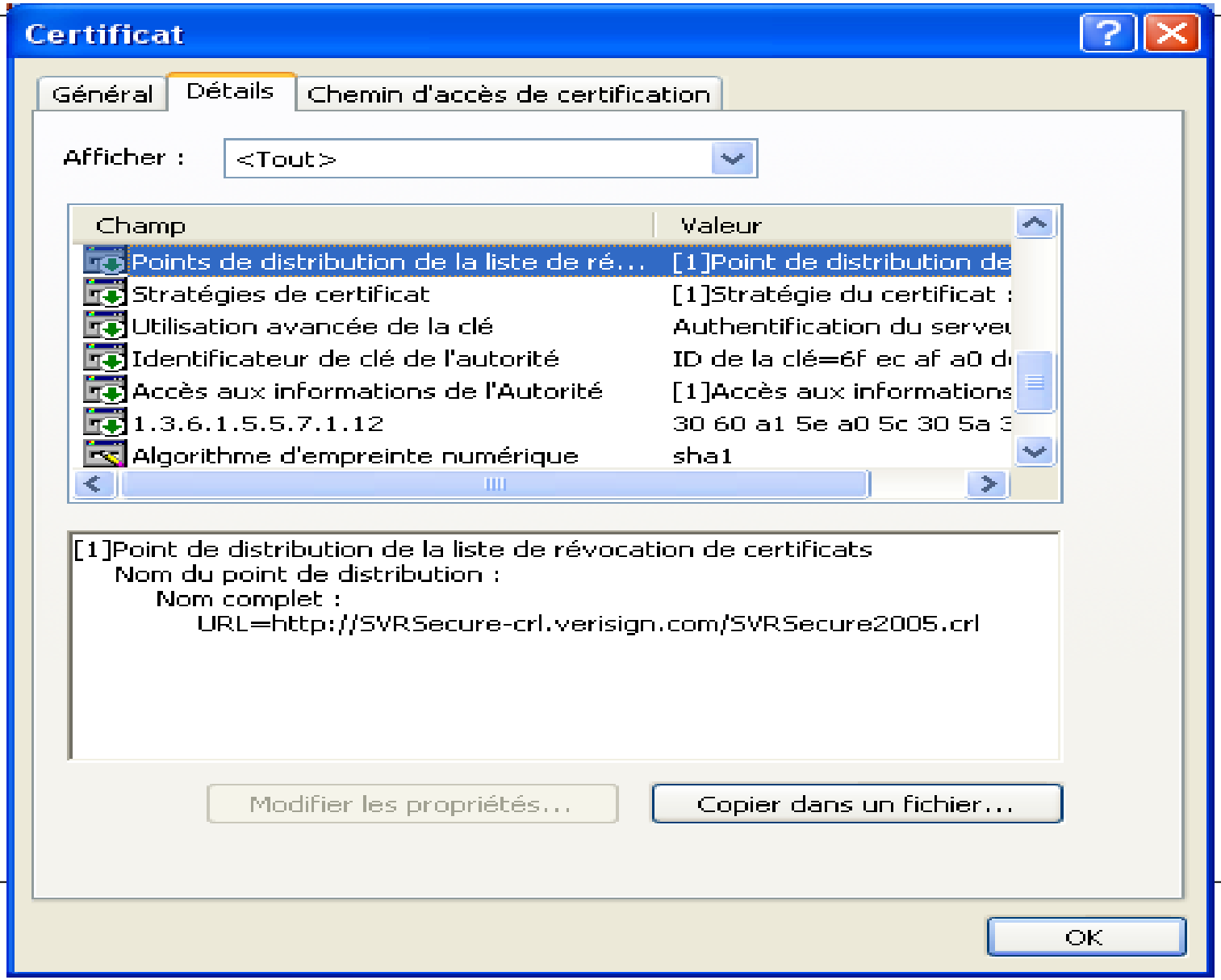
Les Certificats
Standard X.509 : Révocation

- **Un certificat peut être révoqué quand:**
  - La clé privé de l'autorité est compromise
  - La clé privée associée au certificat est compromise
  - Changement de statut du détenteur du certificat
  - Suspension du détenteur du certificat
  - Un certificat a été obtenu frauduleusement
  - Un changement intervenu dans l'état du sujet du certificat en tant qu'entité approuvée
- **L'autorité de révocation et l'autorité de certification peuvent être la même entité**

Les Certificats
Standard X.509 : Révocation

- **Différentes méthodes de révocation:**
  - **CRLs (Certficate Revocation List)**
  - **CRL Distribution Points,**
  - **Delta CRLs,**
  - **OCSP (Online Certificat S Protocol)**
    - **Vérification en temps réel**
  - **SCVP (Simple Certificate Validation Protocol)**
    - **Protocole déchargeant un client de la vérification complète d'un certificat**
- **Un certificat comporte dans une extension la ou les méthodes supportées**
  - **Adresse du serveur (ou des serveurs) CRL et nom du fichier contenant la liste des CRLs, …**
  - **http://SVRSecure-crl.verisign.com/SVRSecure2005.crl**

Les Certificats
Standard X.509 : Révocation



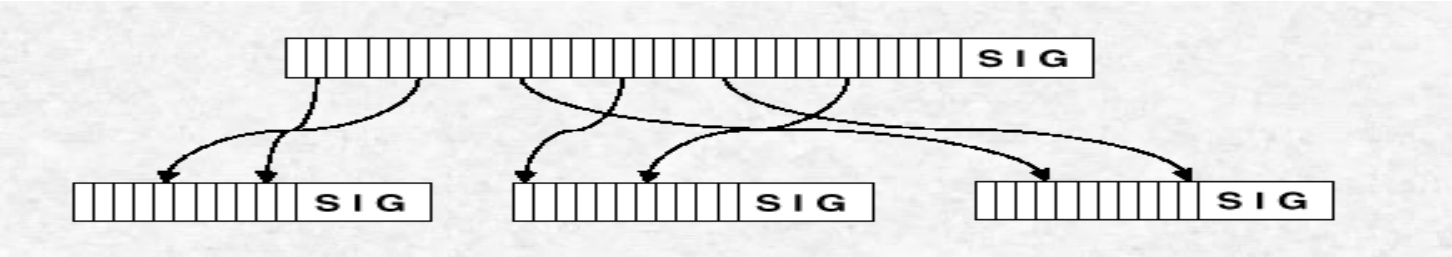
Les Certificats
Standard X.509 : Révocation

- **CRL**
  - **Modèle traditionnel , supporté par toutes les plateformes.**
    - **Liste noires des certificats révoqués.**
    - **Signée par l'autorité de certification et publiée dans l 'annuaire**
  - **Chaque entrée contient :**
    - **le numéro de série du certificat**
    - **la date de la révocation**
    - **d 'autres infos comme la cause de la révocation**

Les Certificats
Standard X.509 : Révocation

- **Avantages de la CRL**
  - **Simple**
  - **Compatible avec les applications**
  - **Peut être caché**
- **Inconvénients de la CRL**
  - **Le serveur de révocation doit publier périodiquement une nouvelle CRL**
    - **même si aucun certificat n'a été révoqué durant depuis la dernière publication**
  - **La périodicité de la CRL peut être pénalisante pour certaines applications notamment de paiement**
  - **La taille de la CRL peut grossir ceci implique:**
    - **une surcharge en communication, en calcul et en stockage**
  - **L'expiration à la même date de la CRL, conduit à une implosion de requête**

- **CRL Distribution Points**
  - **Principe : diviser la CRL en des parties plus petites**
  - **Chaque certificat contient les informations permettant à l ’application de vérifier sa validité au bon endroit**



- **CRL Distribution Points:**
  - identifie les points de distribution de la CRL.

id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }

CRLDistributionPoints ::=

SEQUENCE SIZE (1..MAX) OF DistributionPoint

```
DistributionPoint ::= SEQUENCE {
     distributionPoint   [0]DistributionPointName OPTIONAL,
     reasons             [1]ReasonFlags OPTIONAL,
     cRLIssuer           [2]    GeneralNames OPTIONAL }

DistributionPointName ::= CHOICE {
    fullName                        [0]    GeneralNames,
    nameRelativeToCRLIssuer [1]      RelativeDistinguishedName }
```

- **CRL Distribution Points:**
  - **Avantages**
    - **Peut être cachée**
    - **Problème de taille résolu**
  - **Inconvénients**
    - **Endroit de vérification du certificat est en dur dans le certificat**
    - **Introduit une complexité d ’implémentation**

- **Delta CRL**
  - Fournit les informations sur les certificats dont le statut a changé depuis la dernière CRL.
  - Réduit la quantité de données à échanger avec l'autorité de certification et améliore les temps de réponse et la sécurité de la vérification de la validité des certificats.
  - Les usagers maintiennent leurs propres bases de données de CRLs
  - Chaque delta CRL est associée à une CRL de référence

Les Certificats
Standard X.509 : Révocation

- **OCSP: Online Certificate Status Protocol – RFC 2560**
  - **Permet la vérification temps réel de la validité du certificat**
  - **Repose sur un modèle client-serveur (Requête/Réponse)**
    - **Le serveur OCSP peut utiliser la CRL pour répondre**
  - **L ’application héberge un client qui interroge le serveur OCSP sur l ’état du certificat**
  - **le serveur envoi l ’état du certificat dans un message signé**

- **OCSP: Online Certificate Status Protocol**
  - **Avantages**
    - **fourni des informations à jou**
    - **temps de réponse rapide**
    - **réponse peut être cachée**
  - **Inconvénients**
    - **le serveur OCSP a besoin de signer toutes les réponses**
    - **la clé privée du serveur OCSP doit être hautement sécurisée => engendre une vulnérabilité au système => augmente les coûts**
    - **Nécessite une très haute disponibilité du serveur et du service**

Les Certificats
Standard X.509 : Révocation

- **SCVP (Simple Certificate Validation Protocol)**
  - **Draft de l'IETF**
- **Modèle Client/Serveur**
- **Le client SCVP décharge la vérification du certificat sur un serveur**
- **Le serveur SCVP fournit:**
  - **Les informations sur la validité, le chemin de certification, la révocation**
  - **La validation du certificat**

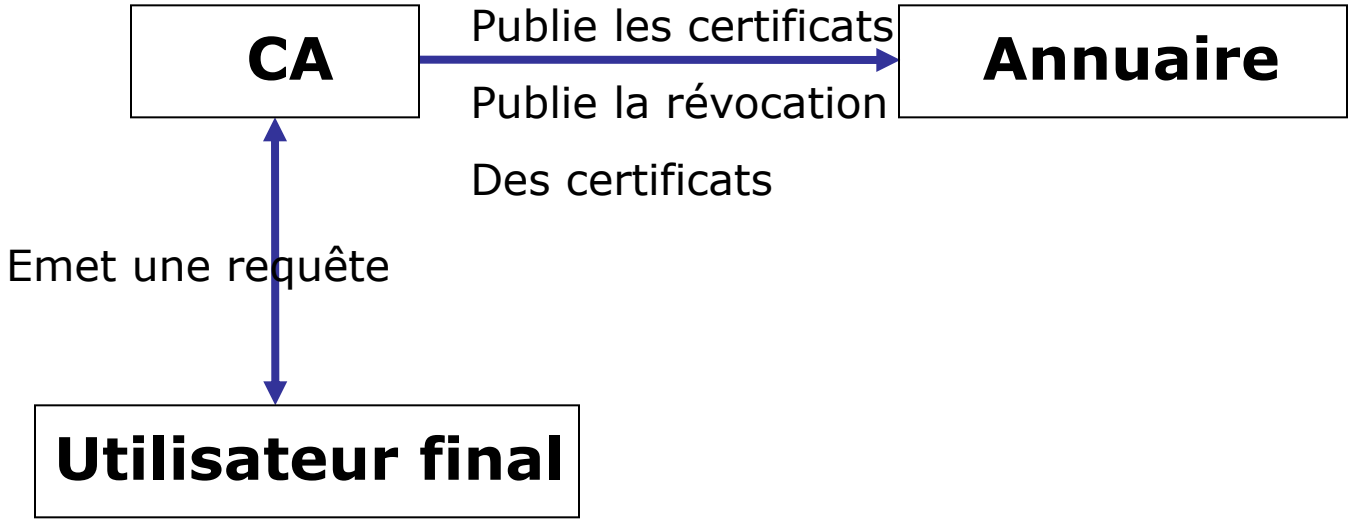
- **SCVP (Simple Certificate Validation Protocol)**
  - **Inconvénient**
    - **État de draft**
    - **Nécessite un serveur sur site**
  - **Avantages**
    - **Décharge les postes clients légers**
    - **Centralise les politiques de validation**
    - **Simple du côté client**

Infrastructure de Gestion de clés ou PKI

- Opérations de base de la PKI:
  - Fournit et gère les éléments de sécurité qui permettent la mise en œuvre des services de sécurité à base de cryptographie asymétrique:
    - authentification, identification, non répudiation, signature
  - Instaurer une tierce partie de confiance entre les acteurs.
  - **Pour: la vérification, la certification, la révocation, la publication des clés publiques**

Infrastructure de Gestion de clés ou PKI
L'autorité de certification

- Comment être sûr qu'une clé publique est bien associé à un sujet?
- L'autorité de certification répond à cette question.
- Le CA vérifie l'authenticité de la requête, signe et publie le certificat.



Infrastructure de Gestion de clés ou PKI
L'autorité de certification

- L'autorité de certification:
  - Entité qui conçoit/signe les certificats électroniques
    - Lien entre identité, clé publiques, et autres attributs
    - Utilise sa clé privé pour signer les certificats conçus après vérification
    - Peut révoquer ou suspendre les certificats
  - Entité ayant le rôle de tiers de confiance
- L'autorité de certification est en possession d'un certificat propre
  - autosigné
  - ou délivré par une autre CA
- Pour certaines architectures le CA n'est pas relié au « réseau en entrée ».

Infrastructure de Gestion de clés ou PKI
L'autorité de certification

Certificat racine de ABA: ISSUER == Subject

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d0:1e:40:90:00:00:46:52:00:00:00:01:00:00:00:04
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=DC, L=Washington, O=ABA.ECOM, INC., CN=ABA.ECOM
    Root CA/Email=admin@digsigtrust.com
        Validity
            Not Before: Jul 12 17:33:53 1999 GMT
            Not After : Jul  9 17:33:53 2009 GMT
        Subject: C=US, ST=DC, L=Washington, O=ABA.ECOM, INC., CN=ABA.ECOM
    Root CA/Email=admin@digsigtrust.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b1:d3:11:e0:79:55:43:07:..............
                    Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:8
    Signature Algorithm: sha1WithRSAEncryption
        04:6f:25:86:e4:e6:96:27:b4:d9:42:……..
```

Infrastructure de Gestion de clés ou PKI
L'autorité de certification

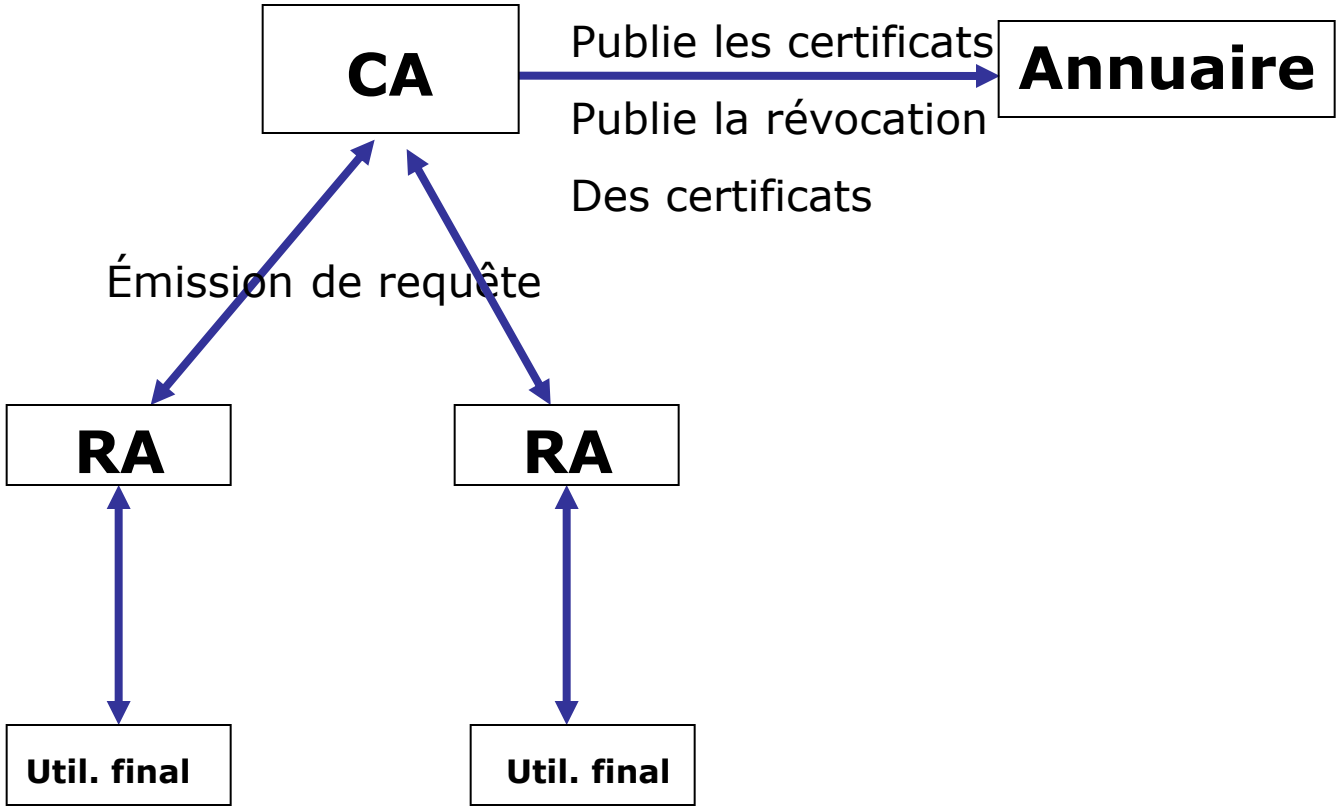
- L'autorité de certification peut être sous la responsabilité:
  - d'une organisation (Verisign)
  - d'un corps de métier (Avocat: ABA)
  - d'une institution (DGI)
- L'autorité de certification peut être administré par un ou plusieurs administrateurs qu'on appelle des opérateurs
  - CAO: Certificate Authority Operator
  - Opérateur dispose d'un certificat signé par le CA pour son authentification

Infrastructure de Gestion de clés ou PKI
L'autorité de certification

- Opérateur de certification:
  - Peut être aussi un organisme qui a la responsabilité:
    - technique de l'élaboration des certificats, leur distribution, leur révocation,…
  - Exemples : Verisign, twathe, …etc.
  - Il gère en collaboration avec la RA les cycles de vie des certificats

Infrastructure de Gestion de clés ou PKI
L'autorité d'enregistrement

- L'autorité d'enregistrement (RA) vérifie les demandes de certificat de l'usager



Infrastructure de Gestion de clés ou PKI
L'autorité d'enregistrement

- Autorité d 'enregistrement (RA)
  - Rôle de décharger le CA de la phase lourde de vérification
    - Vérification de l 'identité de l 'utilisateur en se référant aux exigences de la politique de certification
  - exécute la politique de sécurité
  - traite uniquement les enregistrements,
  - Ne traite pas la révocation.
- Fonctionne sous l'autorité du CA
  - Interface de type PKCS#10 entre RA et CA
- Comprend en général deux interfaces :
  - une permettant aux utilisateurs de faire leurs demandes
  - une de gestion réservée aux opérateurs de la RA permettant de valider les demandes

Infrastructure de Gestion de clés ou PKI
L'autorité d'enregistrement

- Les requêtes du RA vers le CA sont signées
- Les RAO sont les opérateurs des Ras
  - Un RA peut avoir plusieurs opérateurs
- Plusieurs RA peuvent être reliés au même CA
  - Avec éventuellement des politiques différentes
- L' enregistrement peut être:
  - Local: le RA se trouve sur le même site, on l'appelle le LRA (Local RA)
  - Externalisé: le RA se trouve sur un site distant

Infrastructure de Gestion de clés ou PKI
L'annuaire de publication des certificats

- Les certificats sont en général publiques:
  - La publication se fait dans des annuaires « d'accès libre »
- Les annuaires sont en général basés sur LDAP
- Les annuaires publient:
  - Les certificats des entités associés à un CA
  - Le certificat du CA
  - La liste des certificats révoqués
    - Cette liste contient tous les certificats révoqués est signé par la CA émettrice

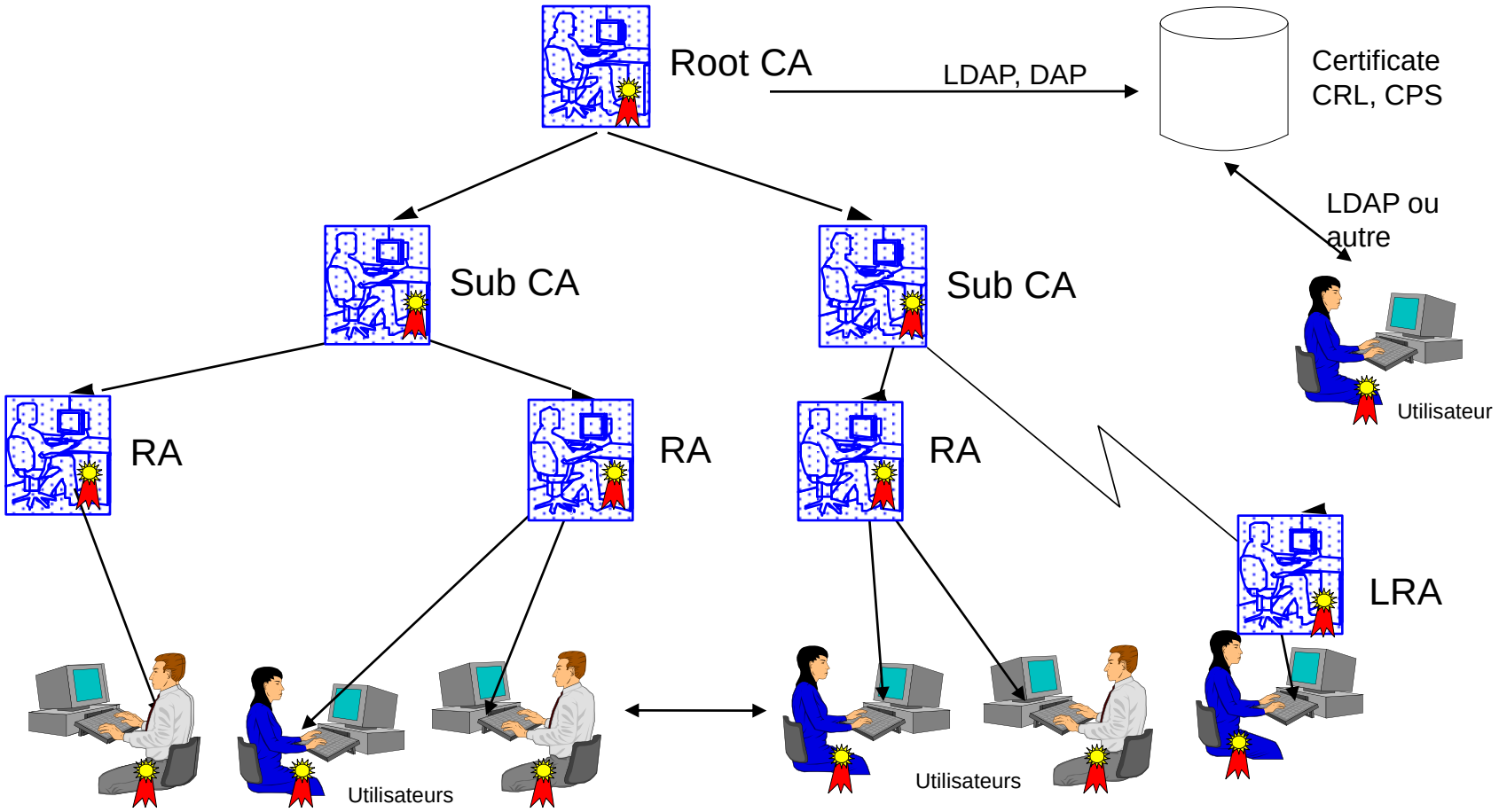
Infrastructure de Gestion de clés ou PKI
L'annuaire de publication des certificats

- Base de stockage d'information standardisé à l'ITU et à l'ISO
  - Interface de communication standard pour récupérer / rechercher une information
    - DAP = Directory Access Protocol (full OSI stack)
    - LDAP = Lightweight Directory Access Protocol (TCP/IP stack)
- Optimisé pour les opérations de lecture et de recherche
- Pas optimisé pour les opérations d'écriture
- Capacité d'effectuer des requêtes complexes
- Haute performance et évolutivité

Infrastructure de Gestion de clés ou PKI
Les composants d'un PKI

- Terminologie:
  - PKI: Public Key Infrastructure
  - IGC: Infrastructure de Gestion des clés
- Composants de base de la PKI:
  - CA: autorité qui signe les certificats
  - RA: autorité qui vérifie les requêtes des usagers et les soumet au CA
  - Annuaire: contient les certificats et les certificats révoqués.
  - Les usagers.

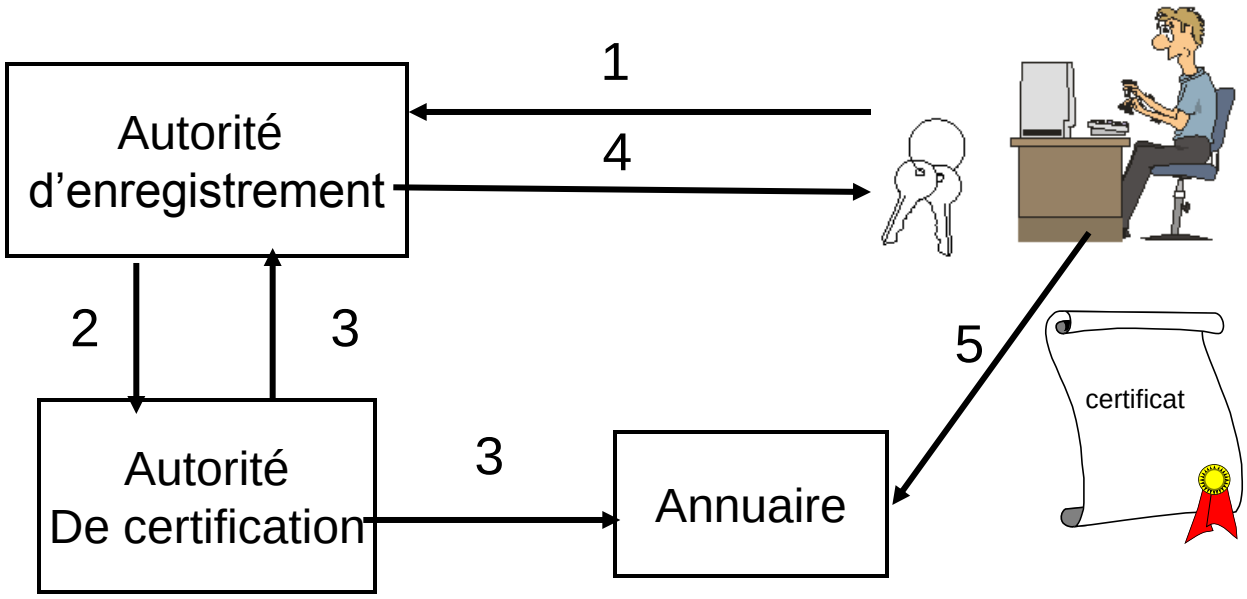
Infrastructure de Gestion de clés ou PKI
Les composants d'un PKI



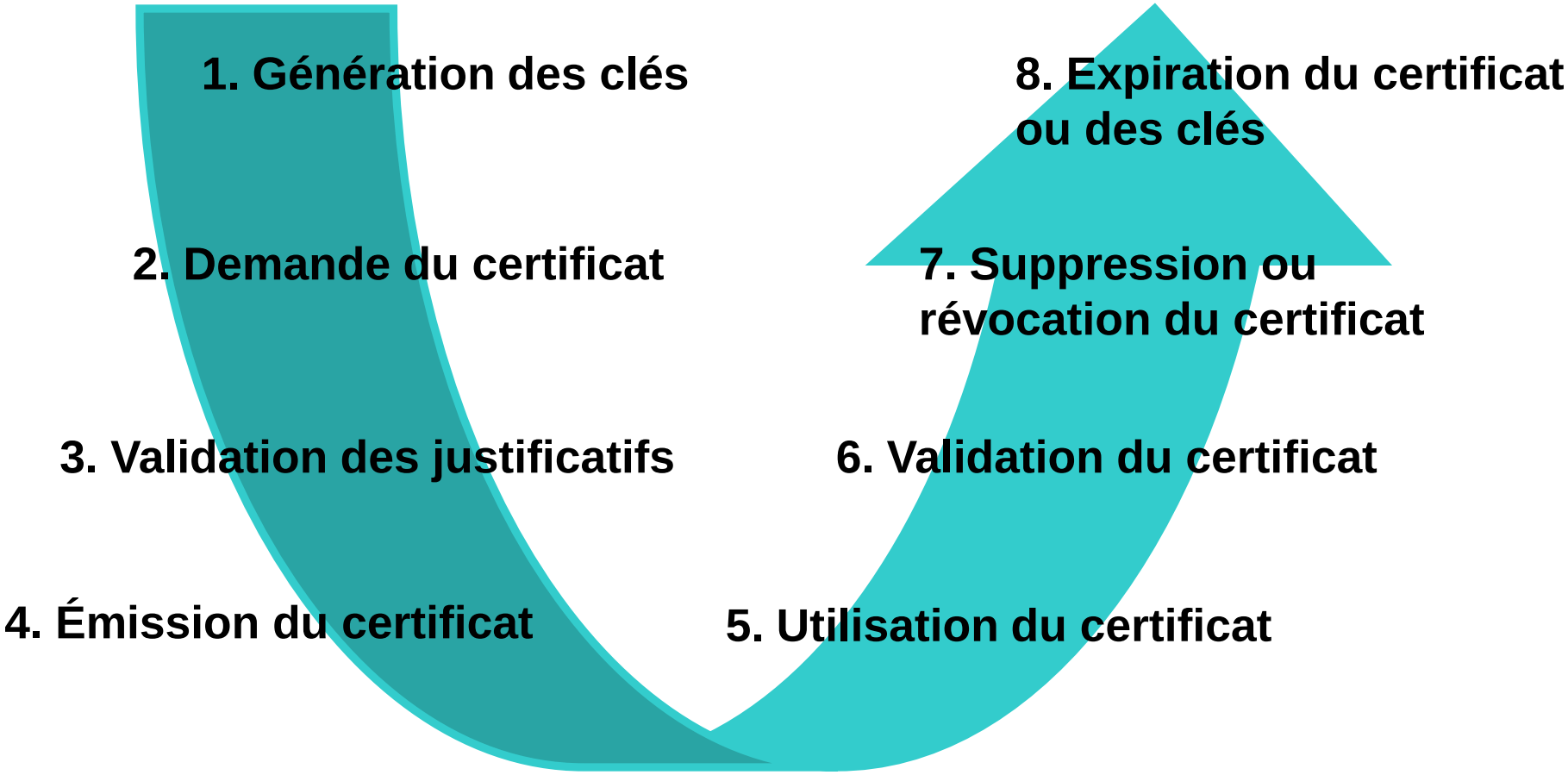
Infrastructure de Gestion de clés ou PKI
Les fonctions principales d'un PKI

- Les fonctions de base :
  - Enregistrement des utilisateurs
  - Valider les modèles de confiance
  - Définir et gérer le Certification Practice Statement (CPS)
  - Gérer les clés et les certificats
  - Révocation et suspension des certificats
  - publication des certificats
  - Création et publication des CRL
  - Archivage et récupération des certificats
  - Maintenance et Responsabilité
- Les fonctions avancées
  - Services d'horodatage
  - Service de récupération des clés privées

Infrastructure de Gestion de clés ou PKI
Scénario de demande d'un certificat



Infrastructure de Gestion de clés ou PKI
Cycle de vie d'un certificat



Infrastructure de Gestion de clés ou PKI
Politique de certification: (CP)

- Dérivée des politiques de sécurité en place
- Un ensemble de règles indiquant les usages du certificat et par qui, et les conditions juridique, administratif et technique de sa mise en œuvre
- Elle détermine :
  - le niveau d'assurance
  - le mode d 'Identification et d 'authentification
  - Durée de validité des certificats
  - période d 'émission de la CRL / révocation des certificats
  - publication des certificats
  - re-génération des certificats
  - les limites de responsabilité
  - le niveau des contrôles de sécurité
  - le niveau des audits
- Toutes ces info sont décrites dans le Certification Practice

Infrastructure de Gestion de clés ou PKI
Politique de certification: (CP)

- Des documents pour aider la rédaction des politiques et de leur application:
  - RFC3647 (RFC2527 obselete): Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
  - Référentiel Général de Sécurité (RGS)
    - Annexe 6:
      - Politique de certification type pour la confidentialité
      - Politique de certification type pour l'authentification
      - Politique de certification type pour la signature électronique
      - …

Infrastructure de Gestion de clés ou PKI
Politique de certification: (CP)

- Précise les règles de gestion des clés et des certificats
  - Support de la clé privée (carte à puce, fichier sur le disque)
  - Gestion des historiques des clés de chiffrement
- Fixe les procédures à appliquer et les cas d'application
  - Identification des cas de gestion des clés et certificats (vol, détérioration, perte)
  - Rédaction des énoncés de pratiques de certification pour chaque cas
  - Audit des outils logiciels pour les failles techniques
  - Certification du code utilisé

Infrastructure de Gestion de clés ou PKI
Énoncé de Politique de certification: (ECP)

- Certification Policy Statement (CPS) ou ECP
- Description complète de la méthode dont la totalité des exigences énoncés dans la PC sont mises en place et appliqués par la CA
- Description détaillée de l'implantation effective des services offerts et des procédures associés à la gestion du cycle de vie des certificats
- Une CA peut avoir un CPS et plusieurs PC
- Plusieurs CAs accepter des CPSs différentes pour une même PC

Infrastructure de Gestion de clés ou PKI
Énoncé de Politique de certification: (ECP)

- Énoncé détaillé des procédures opérationnelles, des standards et des pratiques de la PKI pour atteindre les fonctions de la politique de certification:
  - l ’émission d ’un certificat
  - l ’enregistrement des utilisateurs
  - les durées de vie et la révocation
  - le modèle de confiance et le processus de vérification
  - les modes de publication des certificats
- Conçu dans l’objectif de:
  - Définir les procédures pour le personnel
  - limiter la responsabilité
- Nécessite le plus souvent la participation des conseillers juridiques

Infrastructure de Gestion de clés ou PKI
CP et CPS

- Une CP indique le niveau d'assurance qu'on attribue à un certificat

- Un CPS indique la façon dont une CA établit ce niveau d'assurance