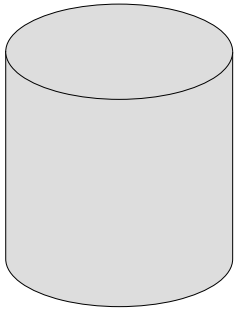
Cryptographie
Certificats et PKI

Chiffrement asymétrique

stockage



magasins de clés des OS
magasins de clés des navigateurs
fichiers PKCS12 .pfx ou .p12
fichiers .jks (Java)
PKCS#11 clés USB, smartcard

Comment être sûr que c'est bien Bob ?

Faire signer par un/plusieurs tiers de confiance

CA

Certificat X509

plusieurs tiers

Certificat PGP

Format de fichiers

- PEM - Privacy Enhanced Mail
  - peut contenir le certificat et la clé privée
    - mais en général séparés dans deux fichiers distincts
  - encodés en Base64
    - commence par : "-----BEGIN CERTIFICATE-----"
    - fini par : "-----END CERTIFICATE-----"
  - extensions : *.pem*, *.crt*, *.cer*, *.key*
  - utilisation courante : serveur Apache

Format de fichiers

- DER
  - format binaire du fichier PEM
  - extensions : *.der*, *.cer*
  - utilisation courante : serveurs Java

Formats de fichier

- PKCS#7 et PB7
  - contient uniquement des certificats et des certificats de chaînes CA
    - pas de clé privée
  - encodage en Base64
    - commence par : "-----BEGIN PKCS7-----"
    - fini par : "-----END PKCS7----"
  - extensions : *.pb7*, *.p7c*
  - utilisation courante : Windows, Tomcat

Formats de fichier

- PCSK#12 et PFX
  - contient le certificat et la clé privée, les certificats CA
  - extensions : *.p12*, *.pkcs12*, *.pfx*
  - utilisation courante : Microsoft, navigateurs

Extensions courantes

- *.csr* : demande de signature de certificat (PKCS#10)
- *.pem* : peut inclure
  - certificat, certificats CA, clé privée
- *.key* : clé privée (format PEM) d'un certificat
- *.pkcs12*, *.pfx*, *.p12* : contient une paire certificat et clé privée
  - conteneur chiffré par mot de passe
- *.der* : fichier *.pem* binaire

Extensions courantes

- *.cer*, *.crt*, *.cert* : fichier au format .pem
  - reconnu par Windows
- *.p7b*, *.keystore*, *.truststore* : fichier au format PKCS#7
  - reconnu nativement par Java
  - *.keystore* et *.truststore* sont utilisés sur les serveurs Java
- *.crl* : liste de révocation de certificats

PKI

- Public Key Infrastructure
  - infrastructure à clé publiques (ICP)
  - infrastructure de gestion de clés (IGC)
- Deux familles principales
  - architecture hiérarchique
    - basées sur le Autorité de Certification (AC)
    - PKI for X.509 certificates (PKIX)
  - architecture non hiérarchique
    - chaque utilisateur gère son réseau de confiance
    - conçu à l'origine pour PGP

Fonctions d'un PKI

- Création d'une paire de clés
- Authentification de la clé publique et génération du certificat
- Remise du certificat au porteur
- Publication des certificats
- Vérification des certificats
- Révocation des certificats

Fonctions d'une PKI

- Autres fonctionnalités
  - service de protection de la clé privée
    - protection logicielle ou support matériel
  - journalisation des actions
  - séquestre des clés privées
  - gestion du recouvrement des clés privées
  - archivage des certificats

Éléments de l'infrastructure

- Plusieurs acteurs communs aux deux architectures
  - détenteur d'un certificat - entité qui possède la clé privée
  - utilisateur d'un certificat - entité qui récupère le certificat et utilise la clé publique
  - AC - Certificate Authority (CA) - qui contrôle l'identité du détenteur de la clé privée
  - émetteur de CRL (Certificate Revocation List)

Éléments de infrastructure

- Entités propres aux architectures hiérarchiques
  - autorité d'enregistrement (AE) - intermédiaire entre le détendeur de la clé et l'AC
  - dépôt (repository) qui est chargé
    - de distribuer les certificats et les CRL
    - d'accepter les certificats et CRL des autres CA
    - connu par son adresse et son protocole
      - LDAP, X.500
  - archive - stockage des informations pour une CA

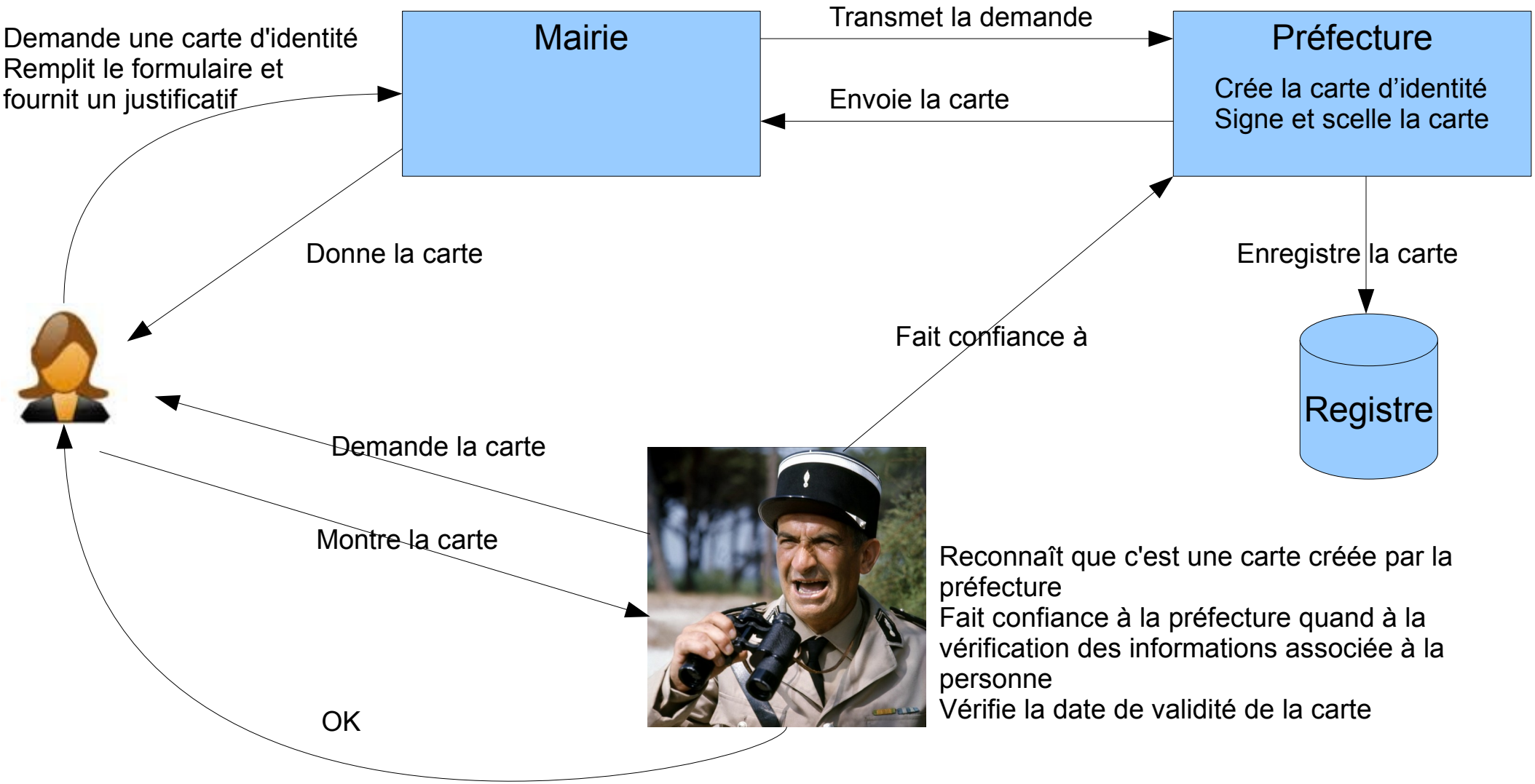
PKI

Une PKI est une infrastructure formée de certificats et de serveurs pour créer, gérer et mettre à disposition des certificats numériques dont l'authenticité est certifiée par l'autorité de certification représentant cette PKI

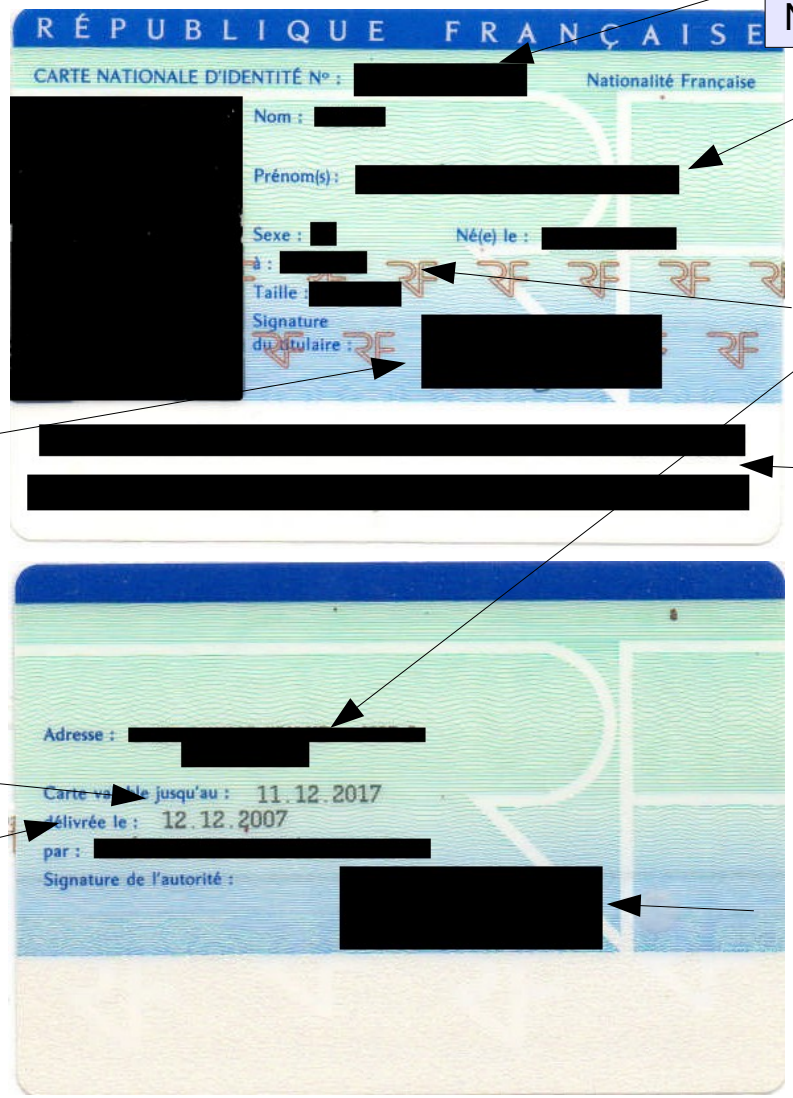
Certificat

- Les algorithmes de chiffrements asymétriques sont basés sur le partage d'une clé publique
- Rien de garantit que la clé partagée soit bien celle de l'utilisateur à qui elle est associée
  - comment prouver l'identité de celui qui partage sa clé ?
- L'objectif du certificat est de prouver que l'utilisateur qui émet la clé publique est bien celui qu'il prétend être
- Le certificat est émis par une autorité de certification
  - CA - Certificate Authority

Analogie : délivrance d'une carte d'identité



Analogie : Carte Nationale d'Identité (CNI)



N° CNI

Identité (nom, prénom, ...)

Description (sexe, taille, adresse)

Signature

Bande de lecture optique (synthèse des informations)

Date de fin de validité

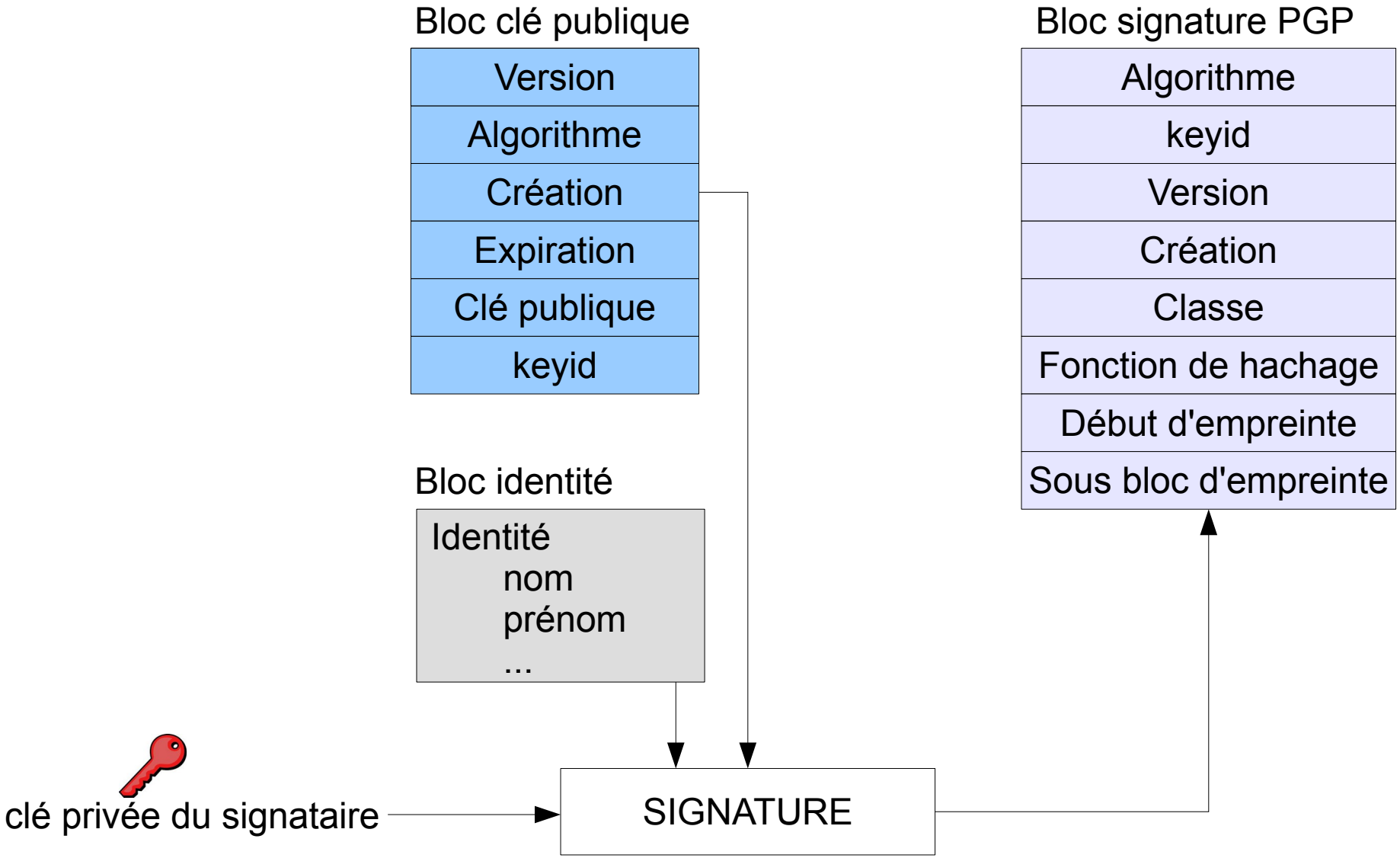
Date d'émission

Nom et signature de l'autorité (préfet)

Certificat PGP

- Un certificat PGP peut contenir plusieurs signatures
  - une signature réalisée avec la clé privée du porteur du certificat
    - auto-signature
  - autres signatures de personnes agissant en qualité d'AC
    - attestent de la confiance dans le fait que la clé appartient bien au propriétaire

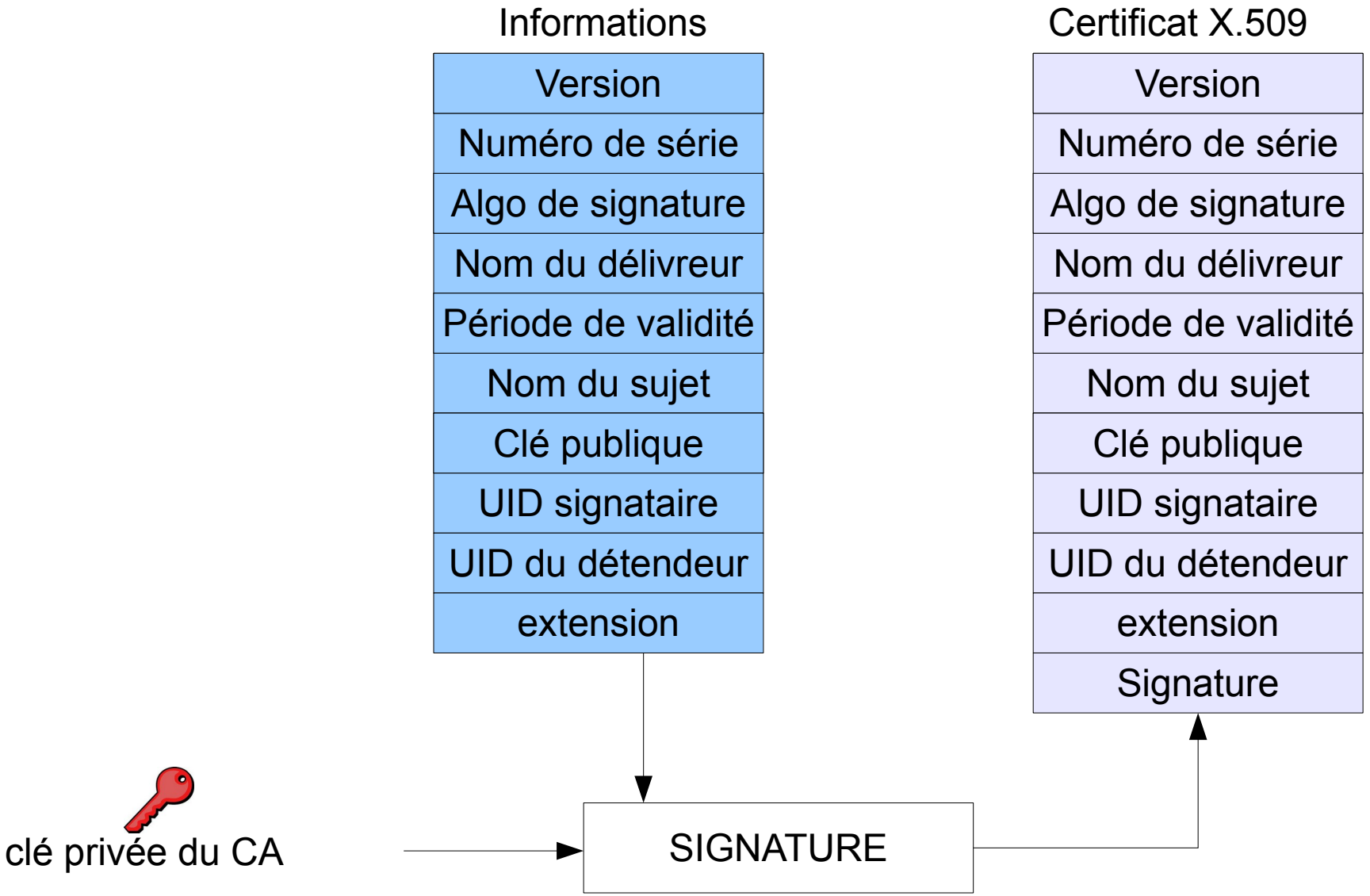
Certificat GPG



Certificat X509

- Le certificat est structuré en deux parties
  - informations sur le certificat lui-même
    - version de la norme X509
    - n° de série du certificat
    - algorithme de chiffrement utilisé
    - dates de début et fin de validité du certificat
    - objet de l'utilisation de la clé publique
    - clé publique du propriétaire du certificat
  - signature du CA
    - chiffrement par la clé privée du CA de l'empreinte des informations précédentes

Certificat X.509



Format des clés

- Binaire encodé DER
  - Definite Encoding Rules
- Encodage PEM
  - Privacy Enhanced Mail
  - base64
- Encodage XML

```
-----BEGIN CERTIFICATE-----
MIICQTCCAaqgAwIBAgIESJm+LDANBgkqhkiG9w0BAQUFADBlMQswCQYDVQQGEwJG
UjEOMAwGA1UECBMFUGFyaXMxDjAMBgNVBAcTBVBhcmlzMRUwEwYDVQQKEwxvcmdh
bmlzYXRpb24xDjAMBgNVBAsTBXVuaXRlMQ8wDQYDVQQDEwZjbGllbnQwHhcNMDgw
ODA2MTUwNzI0WhcNMDgxMTA0MTUwNzI0WjBlMQswCQYDVQQGEwJGUjEOMAwGA1UE
CBMFUGFyaXMxDjAMBgNVBAcTBVBhcmlzMRUwEwYDVQQKEwxvcmdhbmlzYXRpb24x
DjAMBgNVBAsTBXVuaXRlMQ8wDQYDVQQDEwZjbGllbnQwgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAJTLtYpRRKKXvQ1RMtwL134VUtcoQTb+J82Dr9o7bA90nWii
oWhJ+CKwLhGq08BTfiZnsVXadBE5QxLfC/ExB4sb6eXDlGa9fiCFKydSSLfrgtEv
8sNGLMde4zQd6aK6E49watXs9C+pqCs4+3VMpRSi1vlFyeghvrPYQobbwLcbAgMB
AAEwDQYJKoZIhvcNAQEFBQADgYEAY4EVTn8JsPAYZaKZuPBuOriEQSiYchCTzjX3
0xb+YSMwuLBn/S0ajbPdfSx4aUzbnKhwo0df3rn6Nl+sSjRpjeRYoagw+dYpSIta
eRh3eotqP37vkWMMHcZvgwYOcQYocv0ySlI2cDyYFjuvKkUwpJAEHIccDxldQTNY
0BiwJCQ=
-----END CERTIFICATE-----
```

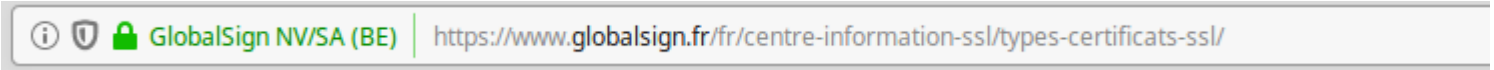
```
<RSAKeyPair>
  <Modulus>...<Modulus>
  <Exponent>...</Exponent>
  <P>...</P>
  <Q>...</Q>
  <DP>...</DP>
  <DQ>...</DQ>
  <InverseQ>... </InverseQ>
  <D></D>
</ RSAKeyPair>
```

Classe de certificat

- Autorité d'enregistrement vérifie l'identité de l'utilisateur
  - 4 classes en fonction des vérifications
  - classe 1 : adresse email
  - classe 2 : preuve de l'identité, photocopie de la CNI
  - classe 3 : présentation physique du demandeur
  - classe 3+ : identique classe 3, le certificat est stocké sur support physique
    - carte à puce par exemple

Types de certificats X.509

- standard : certificat classique
- étendu - EV Extended Validation
  - site de confiance
  - l'AC vérifie que l'organisation possède le droit exclusif d'utilisation du nom de domaine
    - navigateurs récents
      - fond vert selon le navigateur
      - la dénomination légale de l'entreprise est affichée



Types de certificats X.509

- omnidomaines - wildcare
  - domaines et sous domaines
  - *.foo.com → www.foo.com, bar.foo.com, foobar.foo.com
    - RFC 2818
- multisites - subjectAltName
  - plusieurs sites HTTPS sur une seule IP

Types de certificats SSL

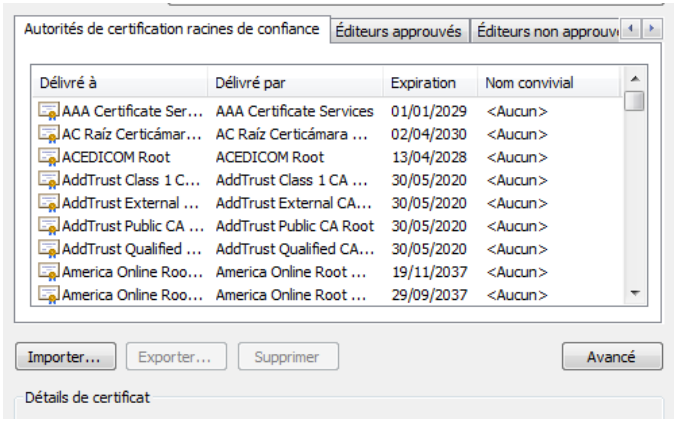
- EV - validation étendue
  - vérification de l'existence légale, physique et opérationnelle de l'organisation
  - vérification de l'exactitude des informations transmises par l'organisation
    - téléphone, adresse
  - vérification du droit exclusif d'utilisation du nom de domaine
  - vérification de l'accord de l'organisation d'émettre un certificat
  - à partir de 600 USD par an

Types de certificats SSL

- OV - validation de l'organisation
  - vérification du droit exclusif d'utilisation du nom de domaine
  - le CA soumet l'organisation à certaines vérification
  - à partir de 350 USD par an
- DV - validation de domaine
  - vérification du droit exclusif d'utilisation du nom de domaine
  - à partir de 250 USD par an

Autorité de certification

- Une AC émet un certificat pour une autre AC
  - elle engage sa responsabilité
  - si on fait confiance à une AC, on fait alors confiance aux AC qu'elle à certifié
- L'AC de départ est l'AC racine
- Les navigateurs possèdent une liste d'AC reconnues
  - il est possible d'en ajouter



Révocation de certificat

- Raisons pouvant à amener à révoquer un certificat
  - perte de la clé privée
  - compromission de la clé privée (piratage)
  - disparition du titulaire
  - ...
- L'AC doit maintenir une liste des certificats révoqués
  - en effet la date du certificat est encore valide

CRL Certificate Revocation List

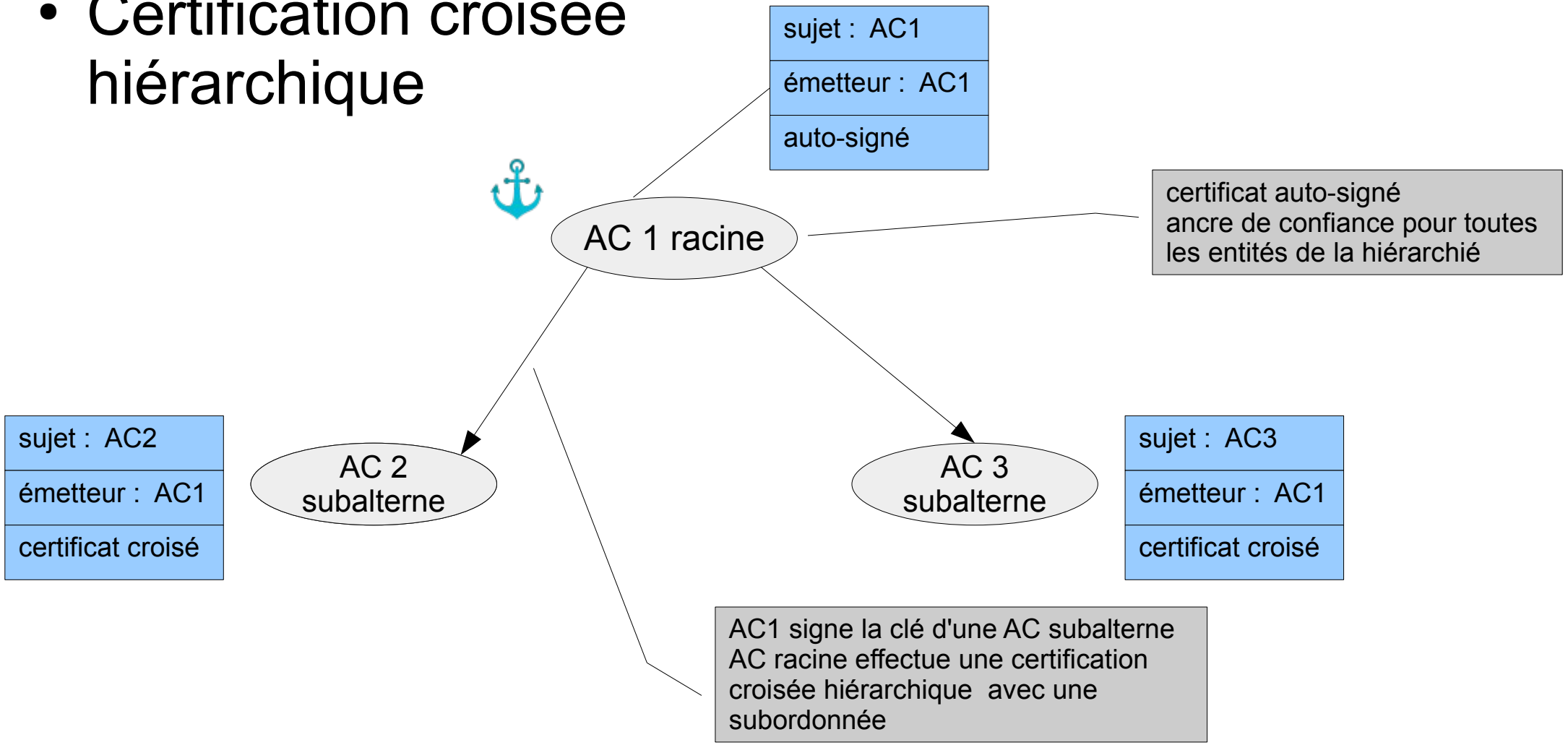
- Liste sous forme de paire
  - numéro de série du certificat - motif de révocation
- Liste envoyée sous format DER ou PEM
  - récupération complexe
- Protocole de vérification en ligne des certificats
  - la liste est hébergée chez une Autorité de Validation
  - serveur OCSP - Online Certificate Protocol

Autorité de certification

- Certification croisée
  - deux opérations
    - 1 - relation de confiances entre deux AC par
      - la signature de la clé publique et du certificat associé d'une AC par une seconde AC
      - le certificat est nommé "certificat croisé" - "cross certificate"
    - 2 - marche dans la chaîne de confiance
      - liste des certificats croisés en partant de l'AC racine
      - cette AC racine est nommée "ancre de confiance" - "trusted anchor"

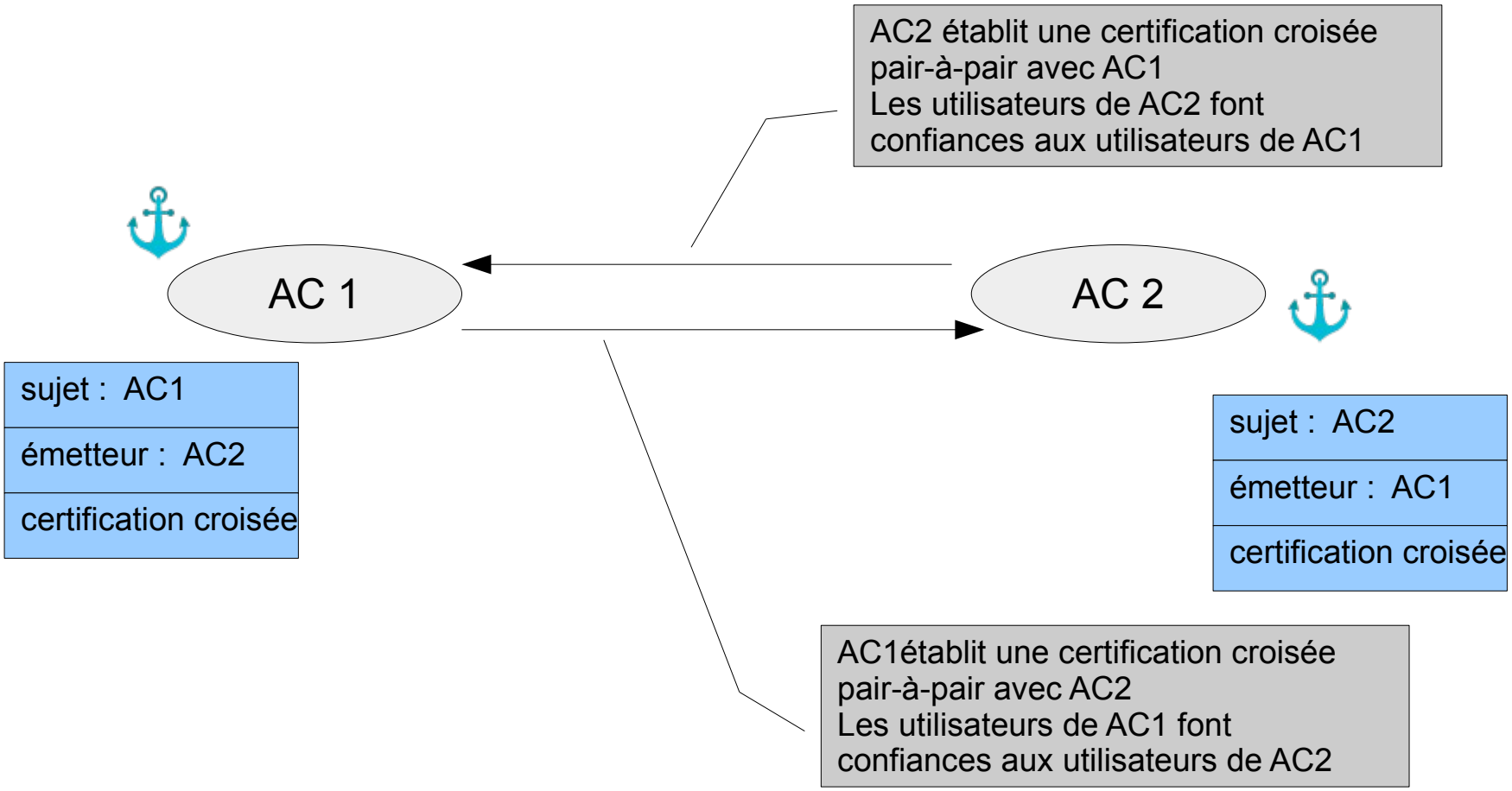
Autorité de certification

- Certification croisée hiérarchique



Autorité de certification

- Certification croisée pair-à-pair



Ressources

- Architectures PKI et communications sécurisées
  - DUNOD
  - auteurs :
    - Jean-Guillaume Dumas
    - Pascal Lafourcade
    - Patrick Redon