Projet RNRT ICare: Services évolués de signature et de contrôle d'accès basés sur de nouveaux concepts d certificats

Refik Molva

Institut EURECOM

Octobre 2002

Partenaires du Projet

- Thales Communications (responsable du projet)
- CEA - LETI
- Cabinet d’avocats A. Bertrand

- ENST Paris
- Institut Eurécom
- Université de Technologie de Compiègne
- Ecole des Mines d’Alès

Axes du Projet

- Expérimentation
  - Infrastructure de Clés Publiques (ICP)
  - Choix du logiciel et déploiement
- Recherche et Développement
  - Contrôle d’accès distribué
  - Services de signature
  - Certificats d’attributs
- Etudes et Méthodologie
  - Etude des Usages
  - Critères de certification
  - Législation

Expérimentation

- Choix logiciel
  - solution open source IDX-PKI (IdealX)
  - solution propriétaire UniCert (Baltimore)
- Déploiement au sein du consortium
  - Communautés académiques (ENST, EMA, Eurécom) et industrielle (Thalès)
  - Test d'interopérabilité / applications

- URL PKI Icare: https://icaresrv.eurecom.fr/ https://194.167.202.113/EE

Etude Usages

- Sites non équipés :
  - 2 écoles (14 et 7 entretiens avec grille et observations)

- Sites équipés en ICP (avec grille et observations):
  - une grande entreprise en phase pilote (8 entretiens)
  - un réseau logiciel libre utilisateur courant (4 entretiens plus observation participante)
  - une entreprise de solution de sécurité (1 entretien)

Etude Usages - Conclusions

Etat actuel

- Sécurité suffisante
- Langage obscur
- Tolérance pour une déviance “normale”

Impossible

- Formalismes stricts
- Garanties absolues (biométrie, Etat)

Solution

- Partir des applicatifs
- Ergonomie basée sur ontologies ordinaires
- Délégation entre Autorités distribuées – Modes et Principes
- Viser larges populations (non-limitées aux informaticiens)
- Tolérance négociée – espaces de régulation

Axe R&D

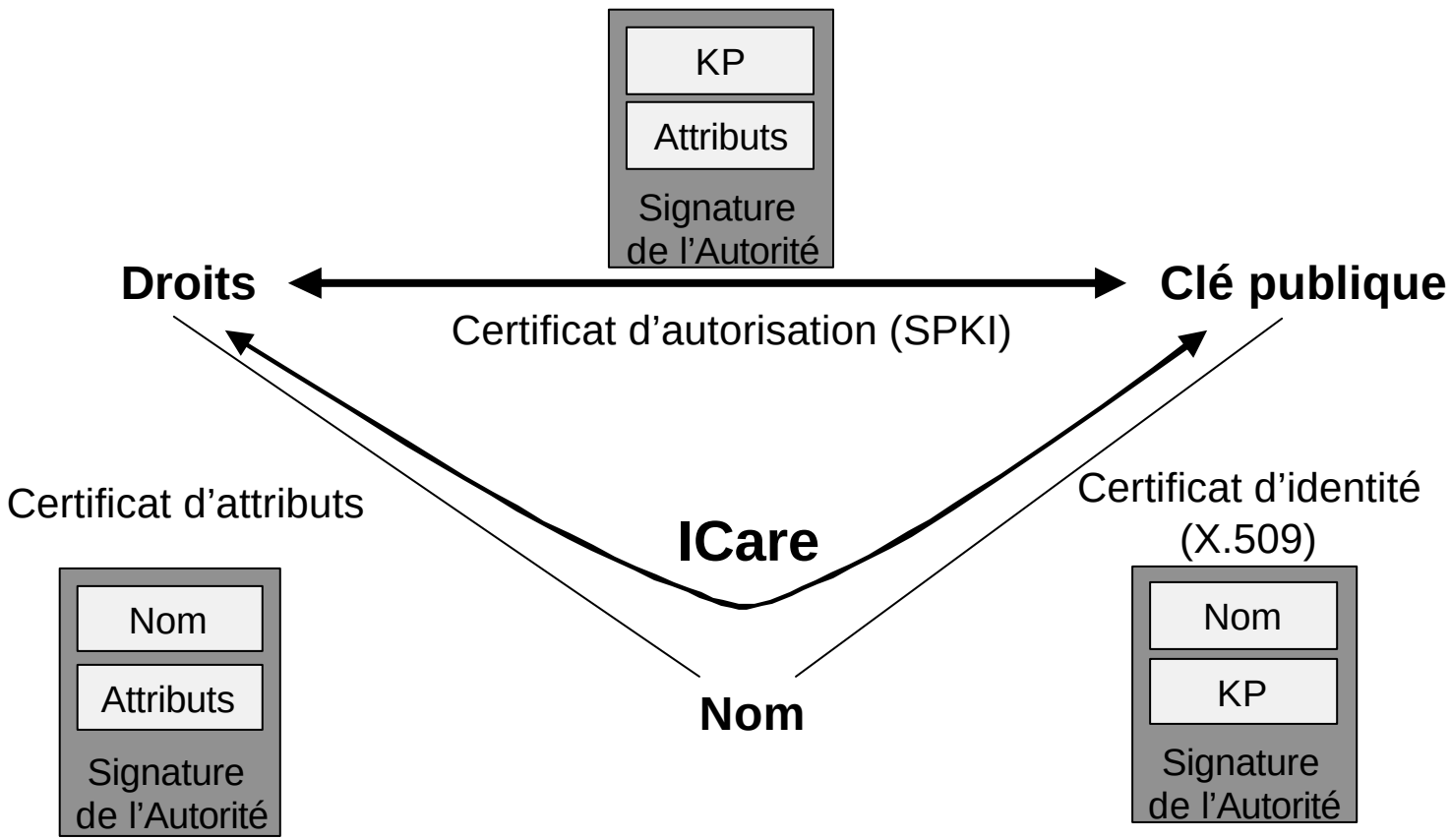
Limitations de l'ICP basé sur les certificats d'identité X509 :

- absence support pour le contrôle d'accès
- complexité et codage inadéquat (DN, ASN.1)

Solutions :

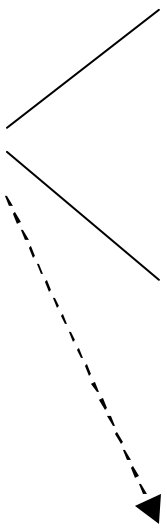
- Certificats d'attributs
- Codage XML

Certificat d'attributs



Certificats d’Attributs - Applications

- Certificat d’attribut

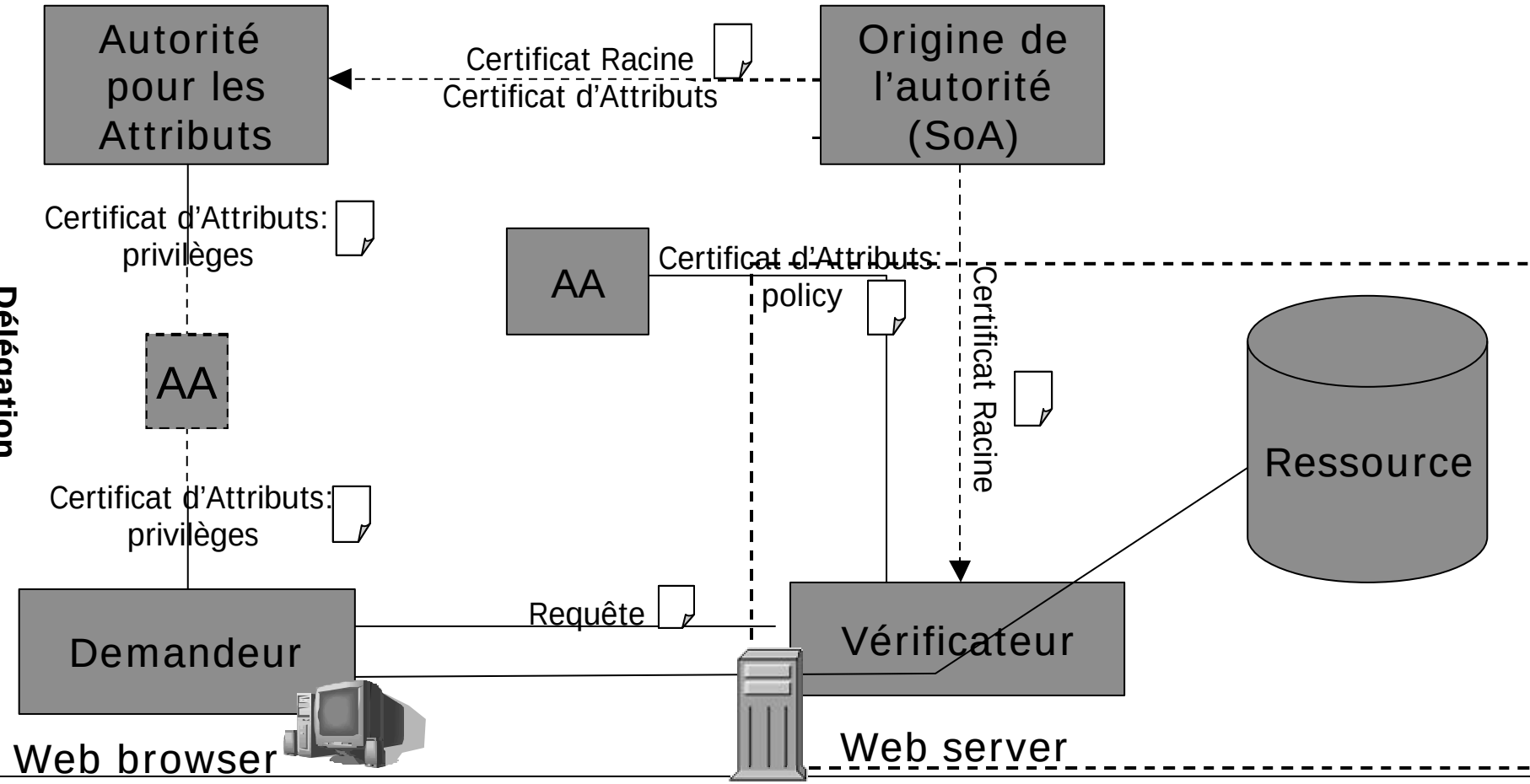


Contrôle d’accès

Services évolués de Signature

Gestion d’identités

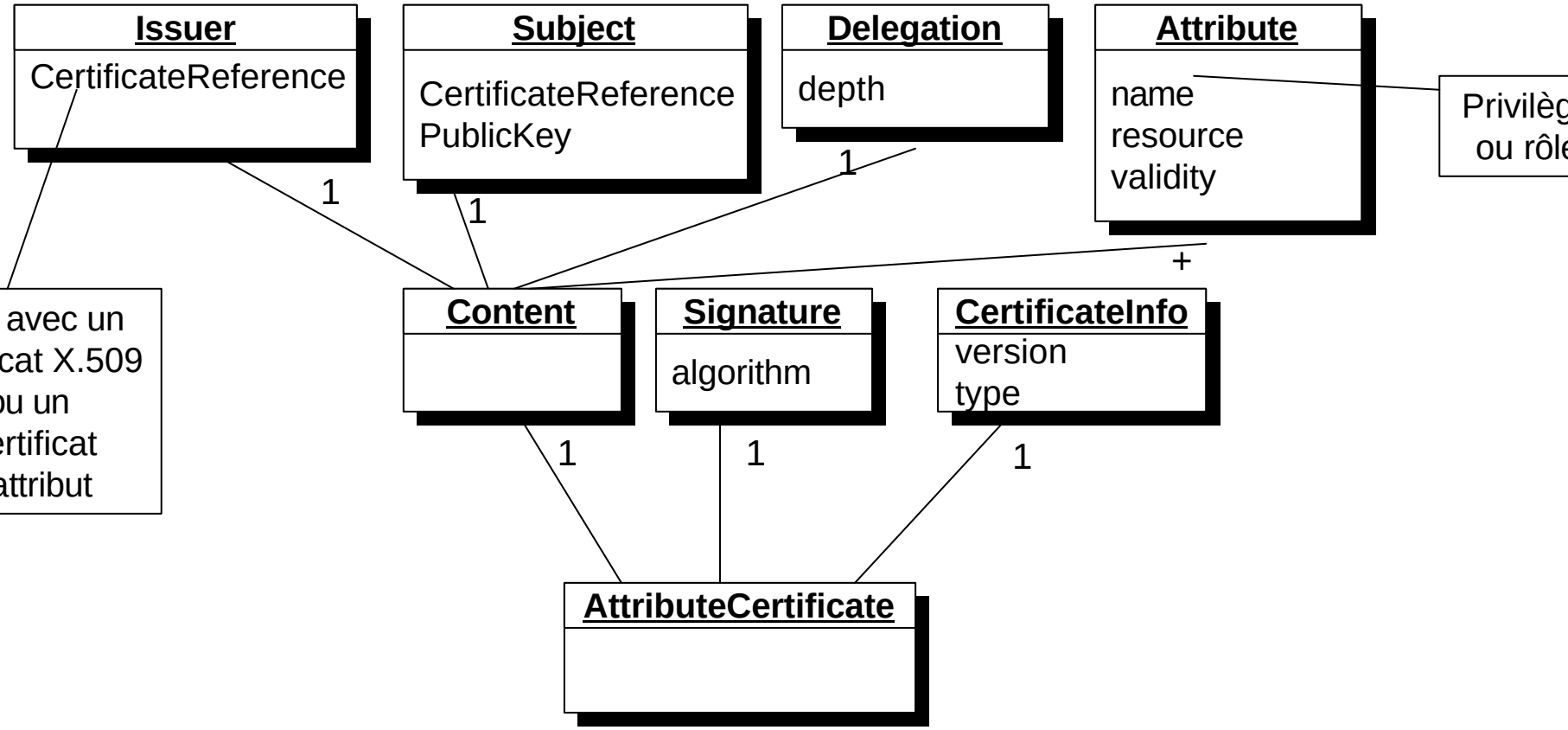
Architecture



Certificats d’Attributs

- Choix du format
- Lien avec certificat d’identité
- Intégration dans l’ICP
- Intégration avec logiciels applicatifs

Certificat d'attributs en XML



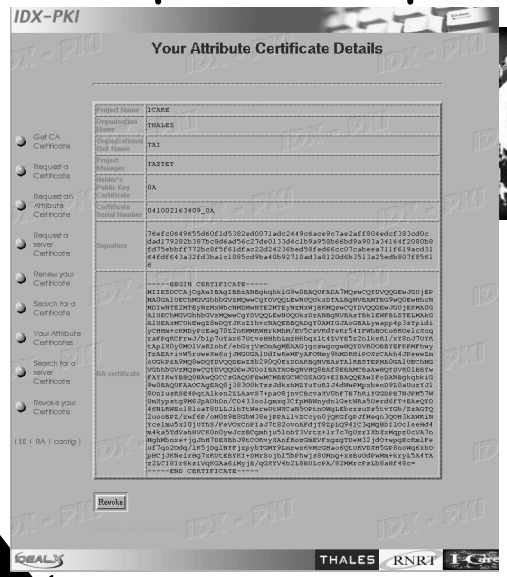
Grammaires DTD:

Accounting

<Name>
<Organization Unit >
<Office>
<Phone>

Project

<Project Name>
<Organization>
<Organization Unit>
<Project Manager>



Script CGI

Formulaires HTTP:

Compatabilite

* Name:
* Organization Unit:

Project

* Project Name:
* Organization:
* Organization Unit:
* Project Manager:
Send
Reset

Script CGI

Nom de la grammaire

Fichier XML:

<xml….

<compta>
<name> …
<organizatio
<office> … <
<phone> …
</compta>

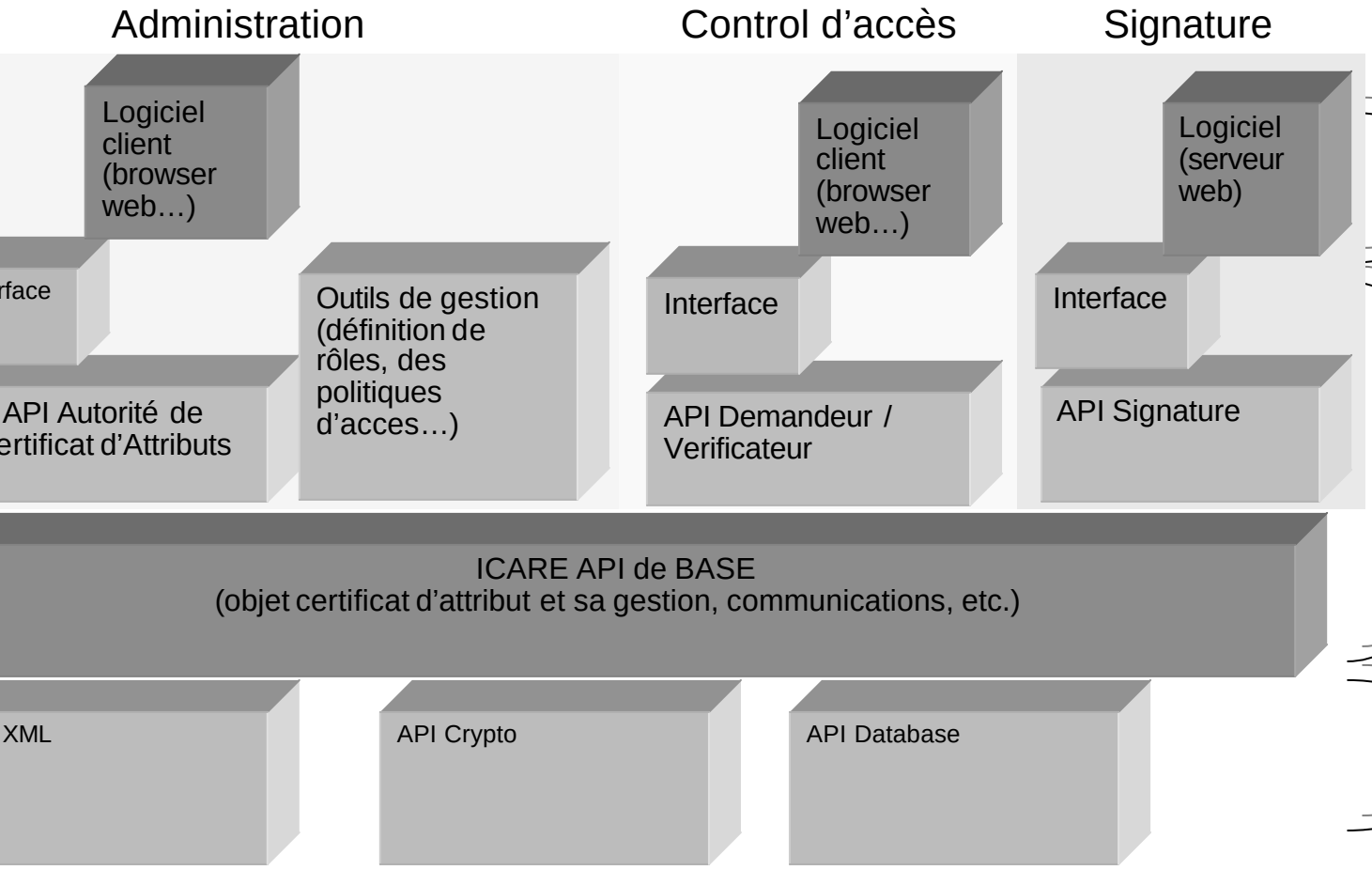
</xml>

<xml….

<project>
<project name> … </project name>
<organization> … </organization>
<organization unit> … </organization unit>
<project manager> … </project manager>
</project>

</xml>

APIs


Administration
Control d'accès
Signature
Logiciel client (browser web…)
Logiciel client (browser web…)
Logiciel (serveur web)
rface
Outils de gestion (définition de rôles, des politiques d'acces…)
Interface
Interface
API Autorité de ertificat d'Attributs
API Demandeur / Verificateur
API Signature
ICARE API de BASE
(objet certificat d'attribut et sa gestion, communications, etc.)
XML
API Crypto
API Database
Integration dans produits exista
Développem ICARE
Librairies OpenSource Commercial

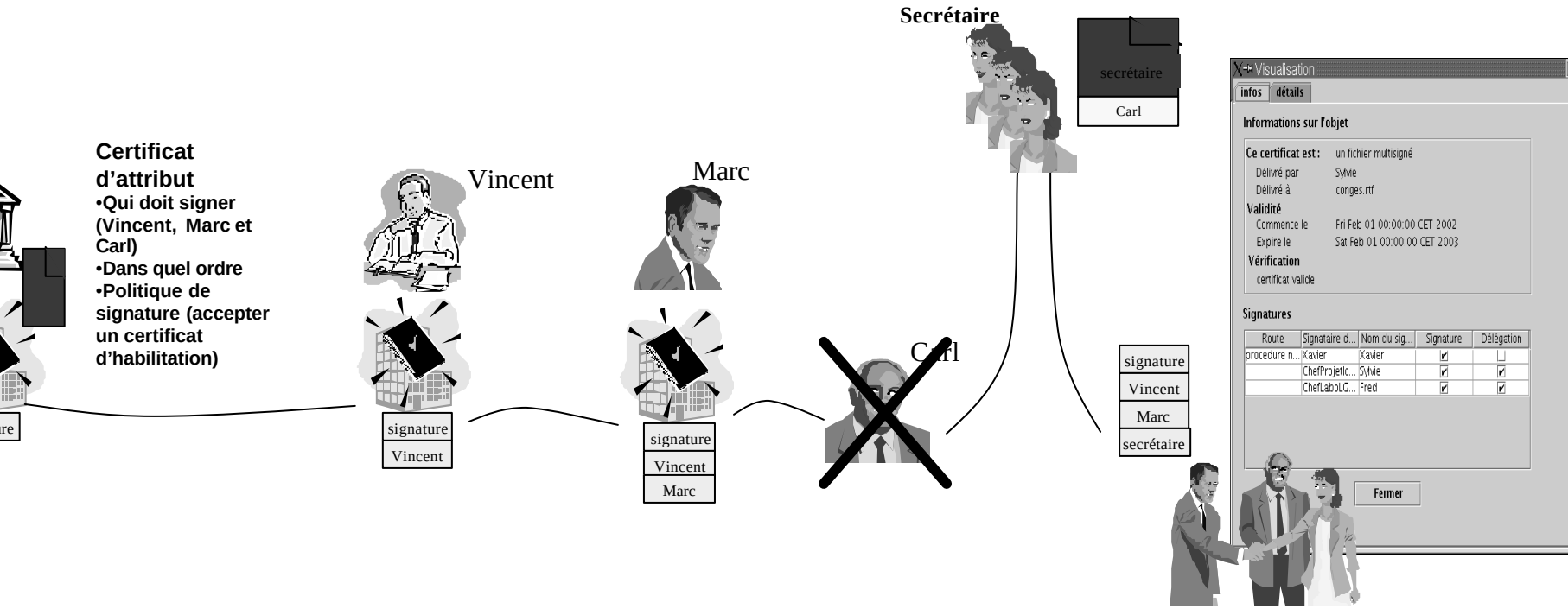
Etat de l’art

X.509

- ASN1 → XML
- Compatibilité avec les Technologies Internet
- ICP(PKI) non-indispensable
- délégation et autorisation sans identification (SPKI)

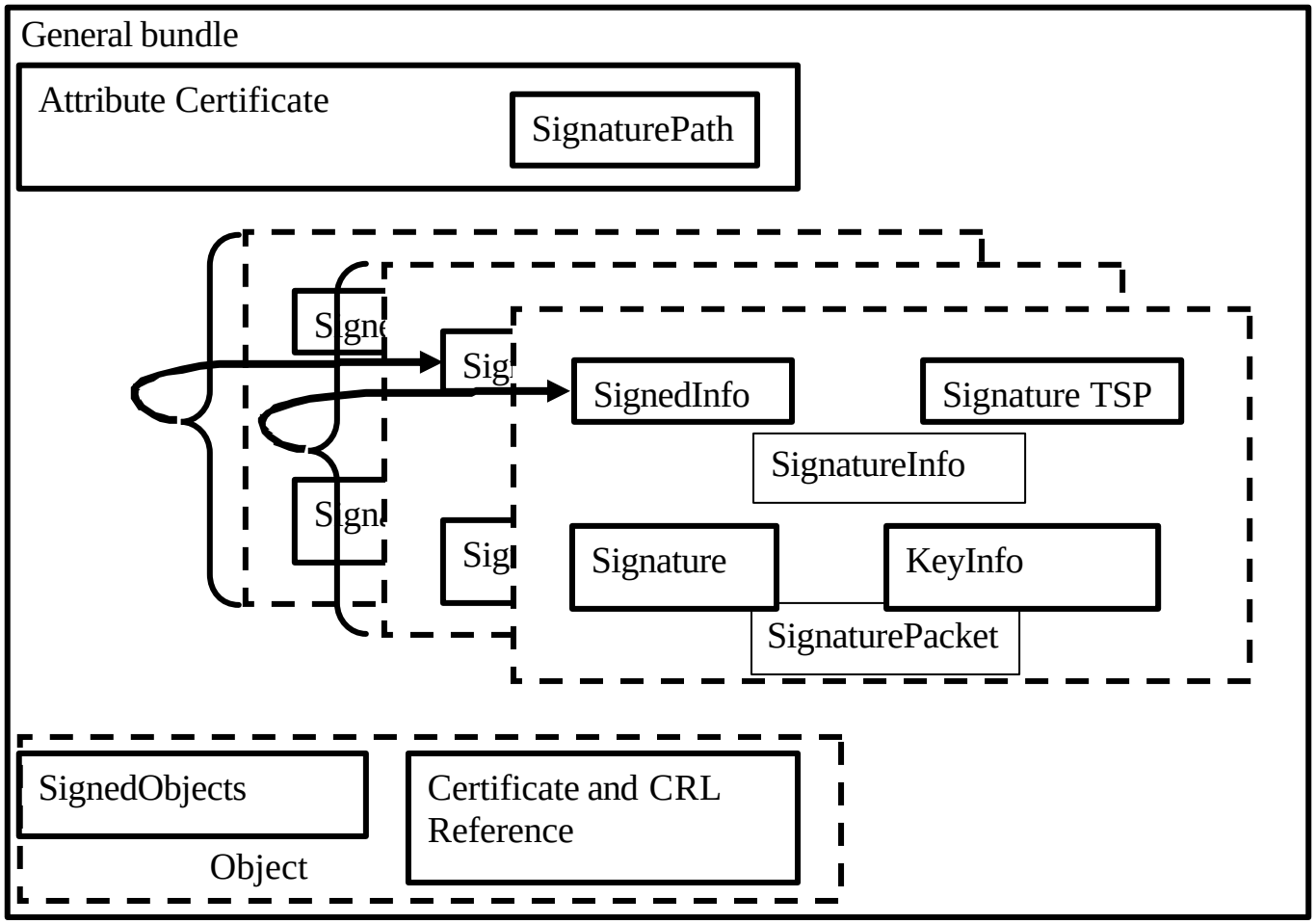
- XACML
  - Orienté Politique de C. A.
- SAML
  - Format d’échange

Application : Multisignature



Multisignature

Variante XAdES-C + Certificat d'attributs



Conclusion

- Expérimentation PKI et Usages

⇒ Introduction par Processus Itératif

- R&D sur Certificats d'Attributs et Services Avancés
  - Développement en cours
  - Niveau comparable aux activités W3C, ETSI
  - Publications en cours
- Précompétitif: Start-up(s)