Utilisation des certificats d'attribut pour accélérer l'usage de la signature électronique

Paul Axayacatl FRAUSTO BERNAL

EMA-LGI2P
URC EMA-CEA
ENST Paris

JRES 2003

ICare: Internet du Futur

Projet RNRT ICare:

Infrastructure de Confiance sur des Architectures de Réseaux -Internet & Mobile-

Objectif:

Développer des services évolués de signature et de contrôle d'accès basés sur de nouveaux concepts de certificats

ICare: 8 Partenaires

- Industriels Grandes Entreprises
  - Thales Communications (responsable du projet)
  - CEA - LETI
- Industriels PME
  - Opérateur de Services de Sécurité: FranCert
  - Cabinet d'avocats A. Bertrand
- Académiques
  - Ecole des Mines d'Alès (LGI2P)
  - ENST Paris
  - Institut Eurécom
  - Université Technologique Compiègne

Le déploiement d'une PKI et des services associés:
25% Technique 50% Organisation 25% Juridique

PKI : (Publique Key Infrastructure) - Infrastructure à clé publique

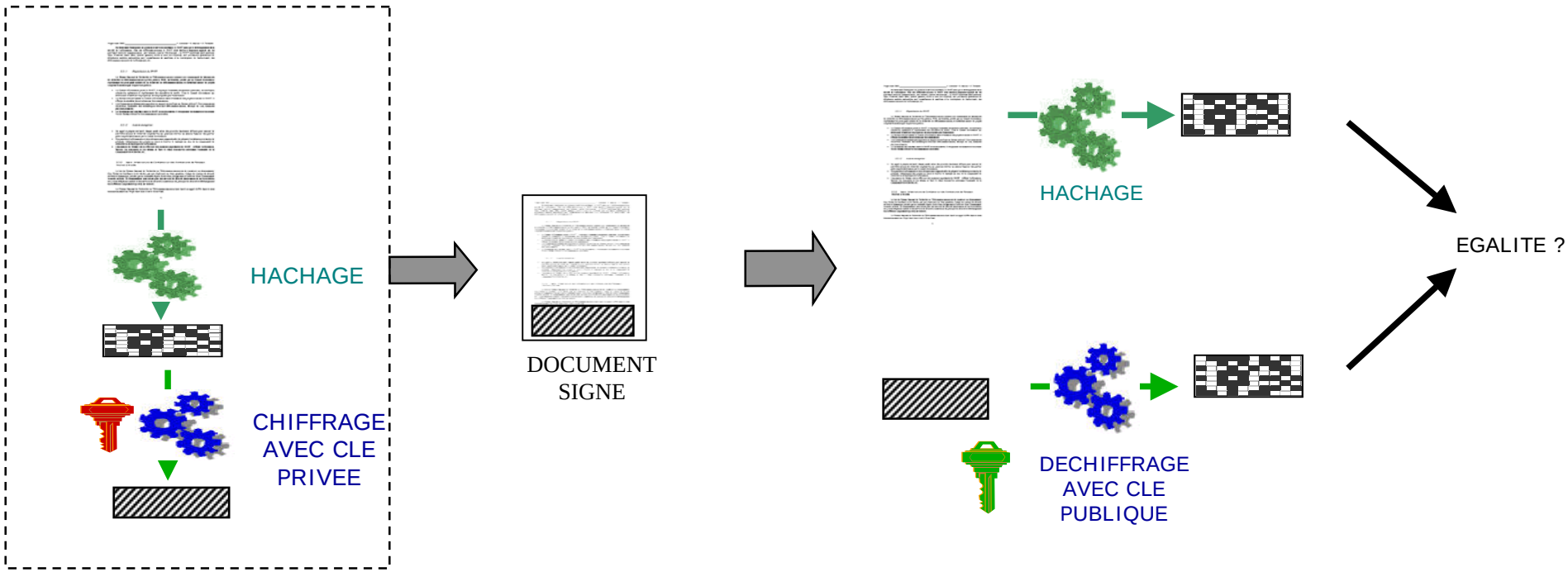
Plan

- Introduction
  - la signature électronique,
  - les certificats d'identité, la PKI.
- Usages de la Signature électronique
- Certificats électroniques
- Infrastructure de confiance
- Conclusion

Qu'est que ce la signature électronique ?

- Définit par ISO 7498-2

"*Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple)".*



Le certificat d ’identité

Le certificat d’identité est le document émis et signé par une autorité de confiance, associant une clé publique à des informations relatives au propriétaire du certificat.

Autorité de Confiance

Gestion des certificats

PKI

Certificat d ’identité X. 509 v3

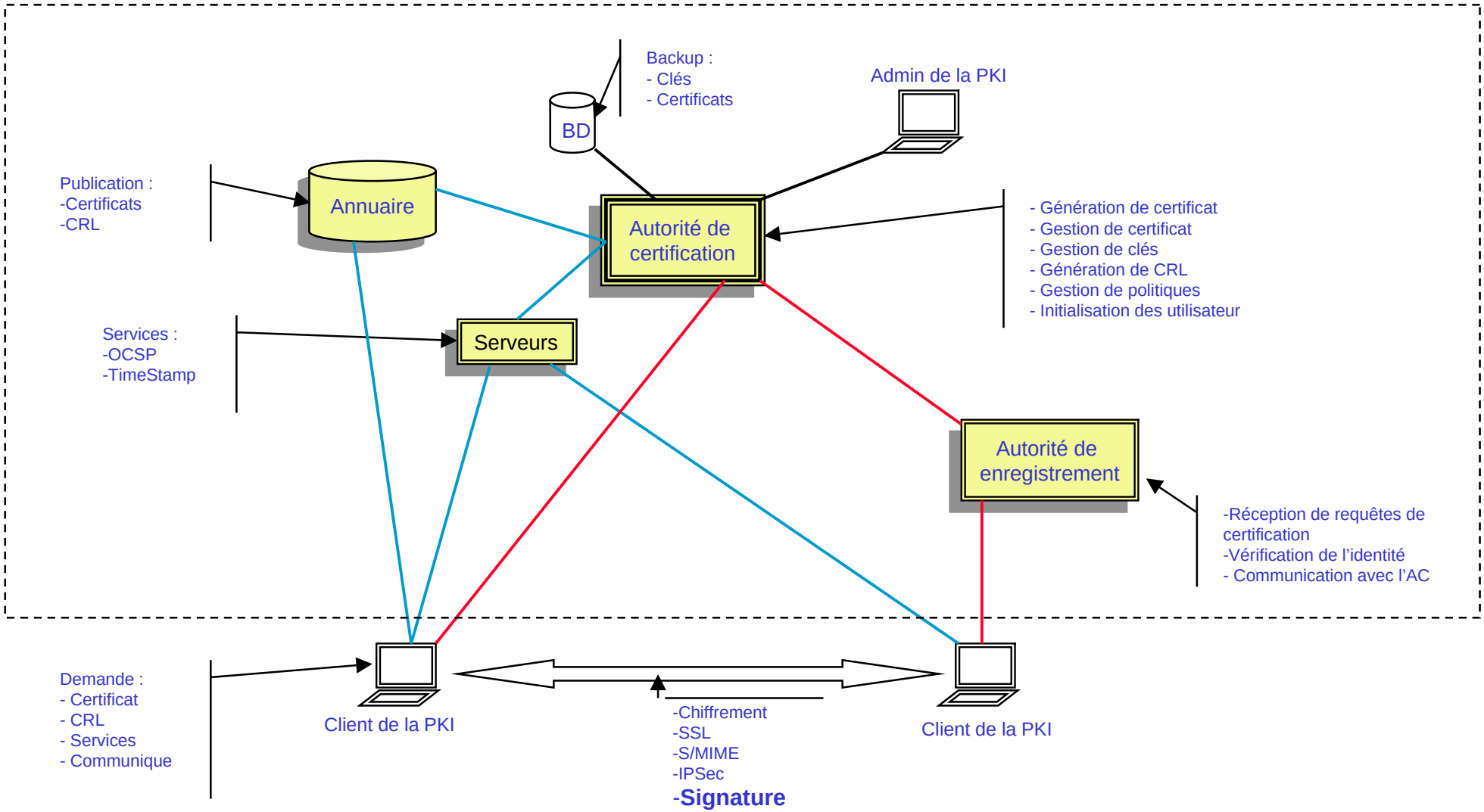
Certificate format version	version 3
Certificate serial number	12345678
Signature algorithm identifier for CA	RSA with MD5
Issuer X.500 name	c=US, o=ACME
Validity period	start=01/08/96, expiry=01/08/98
Subject X.500 name	c=US, o=ACME, cn=John Smith + …
Subject public key information	RSA with MD5
version 2 Issuer unique identifier	
version 2 Subject unique identifier	
version 3 Type / Criticality / Value	Extensions
version 3 Type / Criticality / Value	
version 3 Type / Criticality / Value	
CA Signature	

Qu'est ce que ce PKI ?

PKI est l'acronyme anglais d'Infrastructure de Gestion de Clés mieux connu comme *Public Key Infrastructure.* La PKI est l'ensemble d'algorithmes, protocoles et services pour protéger les échanges d'information. Elle s'appuie notamment sur la cryptographie, la manipulation de la signature électronique et les certificats électroniques. Quatre services de base sont assurés :

- **l'authentification**
- **la non-répudiation**
- **la confidentialité**
- **l'intégrité**

Principaux Composant d'un PKI



Plan

- Introduction
- Usages de la signature
  - intérêts
  - nouveaux services
- Certificats électroniques
- Infrastructure de confiance
- Conclusion

Intérêts de la signature électronique

- Évolution vers une économie « paperless »
- Réalisation des transactions électroniques en tout sécurité
  - Authentification de la source
  - Intégrité des données
- Élargissement de l'environnement de travail
- Augmentation des échanges électroniques sensibles
- Automatisation des procédures de travail

Les usages de la signature électronique aujourd'hui

- Intégrité/authentification du courrier électronique(S/MIME)
- Authentification de serveurs dans l'Internet (SSL)
- Cartes EMV
- Télédéclaration des impôts sur le revenu
- Carte de Vie Quotidienne (expérimentation)

} Applications personnelles

- Télédéclaration/télépaiement de la TVA (TéléTVA)
- Actes médicaux : carte Santé Professionnelle
- Dématérialisation des appels d'offres (expérimentation)

} Applications professionnelles

Pourquoi un développement limité ?

- La maturité des architectures PKI
- L'interprétation vague du décret de loi
- Les services liée à la signature (Pas de rentabilité de l'infrastructure sans services)

Différents types de signature électronique

- La Signature Numérique des techniciens (ISO 7498-2)
- La Signature Électronique « Ordinaire » (de la Directive Européen)
- La Signature Électronique « Ordinaire » (du Décret du 30 mars 2001)
- La Signature Électronique Avancée (de la Directive Européen)
- La Signature Électronique Sécurisée (du Décret du 30 mars 2001)

Les usages de la signature électronique aujourd'hui

- Intégrité/authentification du courrier électronique(S/MIME)
- Authentification de serveurs dans l'Internet (SSL)
- Cartes EMV
- Télédéclaration des impôts sur le revenu
- Carte de Vie Quotidienne (expérimentation)

} Applications personnelles

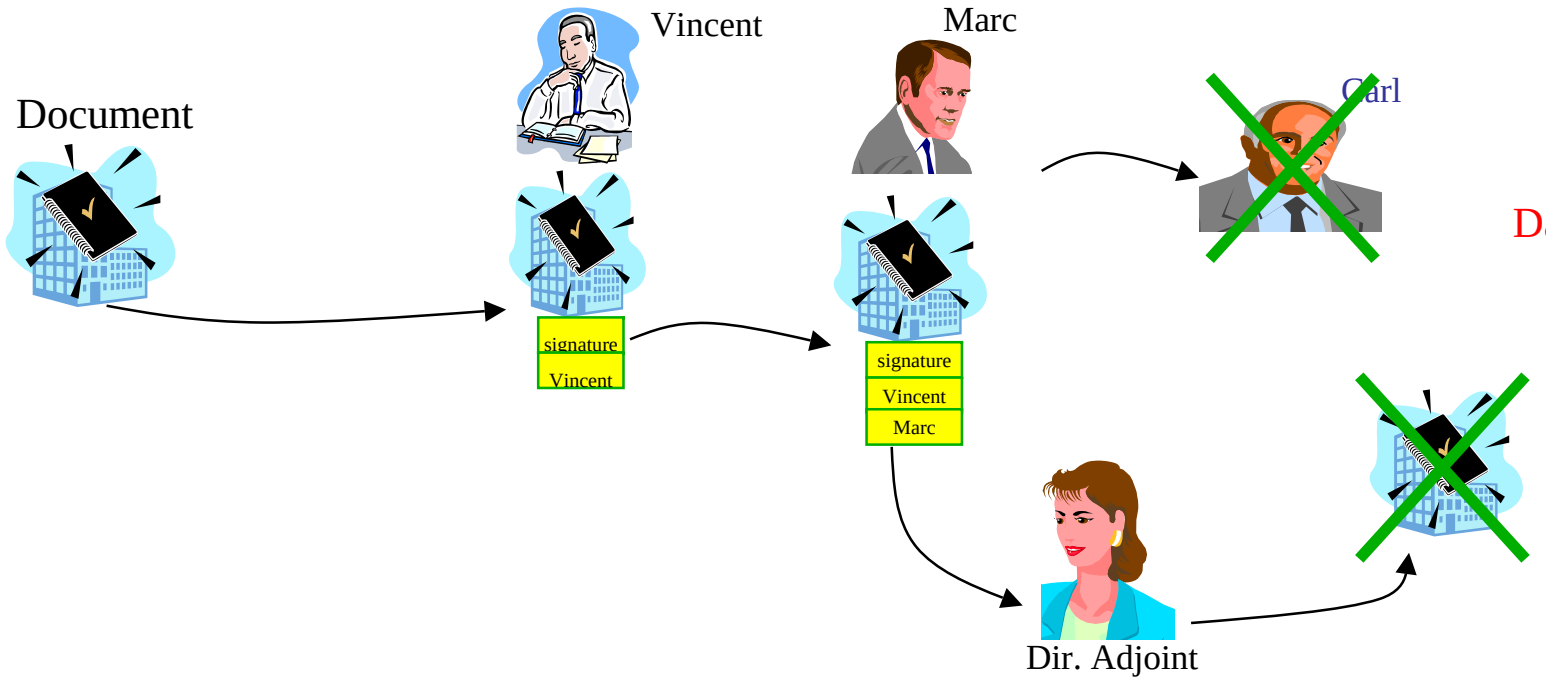
- Télédéclaration/télépaiement de la TVA (TéléTVA)
- Actes médicaux : carte Santé Professionnelle
- Dématérialisation des appels d'offres (expérimentation)

} Applications professionnelles

Pourquoi un développement limité ?

- La maturité des architectures PKI
- L'interprétation vague du décret de loi
- Les services liée à la signature (Pas de rentabilité de l'infrastructure sans services)

Pourquoi de nouveaux services ?



Le processus de signature n'est pas vérifiable.

Parce que :

Qui est autorisé à signer ?

Avec quelle qualité?

Dans quel ordre doivent ils signer ?

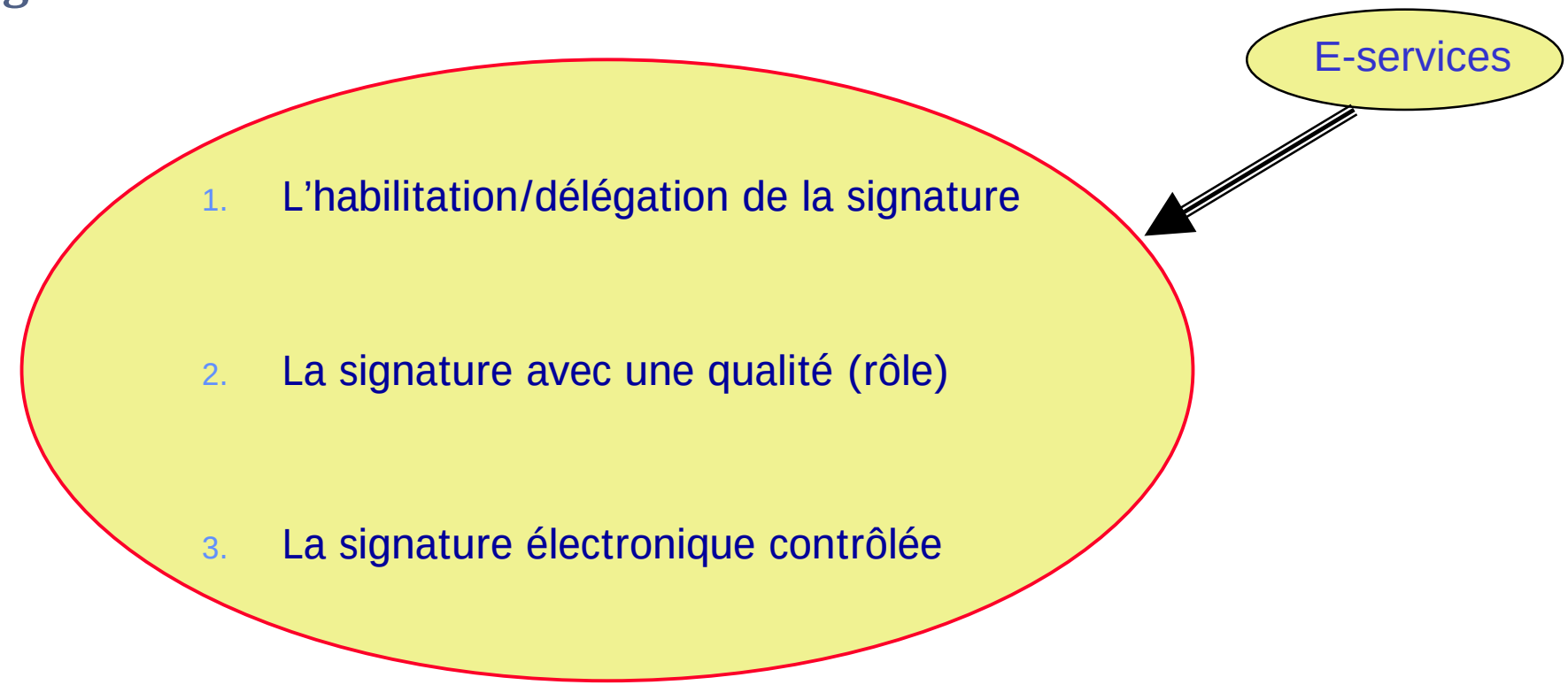
Comment habiliter ?

donc

Nouveaux e-services sont nécessaires

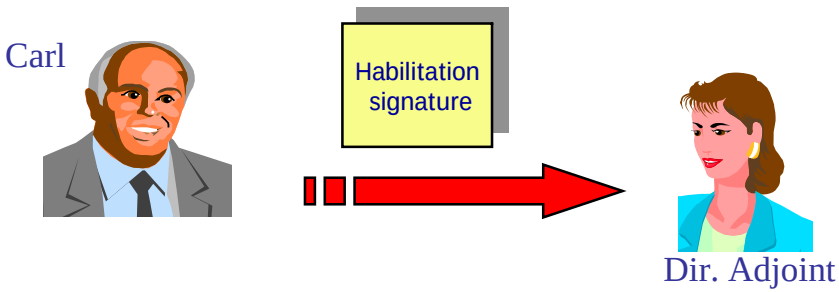
Les services autour de la signature électronique demain

La dématérialisation des échanges est en marche et la signature doit rester



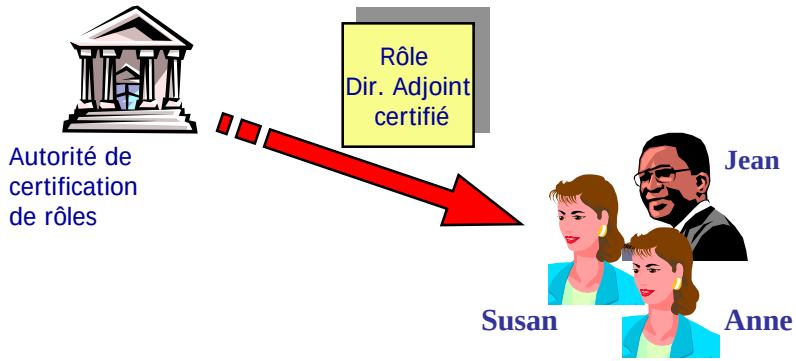
L'habilitation/délégation de la signature

- Certification de l'habilitation
  - L'habilitation donne l'autorisation à quelqu'un d'exercer un pouvoir à sa place.
  - La délégation donne l'autorisation de transférer ce pouvoir à un tiers.
  - La délégation d'une partie de ce pouvoir.
    - Habiliter un tiers à signer un type de document.



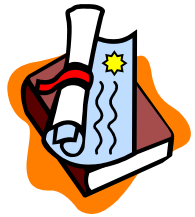
La signature avec un rôle

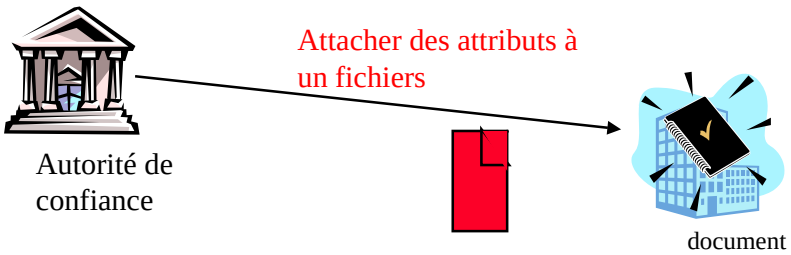
- Certification de rôles
  - Identifier le rôle plutôt que la personne : de nombreux professionnels signent *en qualité* (par exemple en qualité de directeur de laboratoire, directeur commercial, avocat, expert-comptable pour une téléprocédure, etc.), cette qualité est le rôle que le signataire porte.
  - Assigner les rôles de manière dynamique.
  - Associer :
    - Un rôle à une identité.
    - Plusieurs rôles à une identité.
    - Plusieurs identités à un rôle.
    - Aucun rôle à une identité



La signature électronique contrôlée

- Certification des attributs de fichiers
  - Ajouter des contraintes à la signature électronique pour :
    - indiquer les entités autorisées à signer le document,
    - donner l'ordre dans lequel ils doivent signer le document, ...
  - Ajouter des informations pour valider la signature
  - Vérifier automatiquement la signature





Plan

- Introduction
- Usages de la signature
- Certificats électroniques
  - Le certificat d'identité
  - Le certificat d'attribut
  - Proposition de certificat d'attribut
  - Exemples
- Infrastructure de confiance
- Conclusion

Les certificats électroniques

- Certificat d'identification (X.509 v3)
  - Lier clé – entité
  - Authentification
- Certificat d'attribut
  - Lier permission – entité
  - Permission

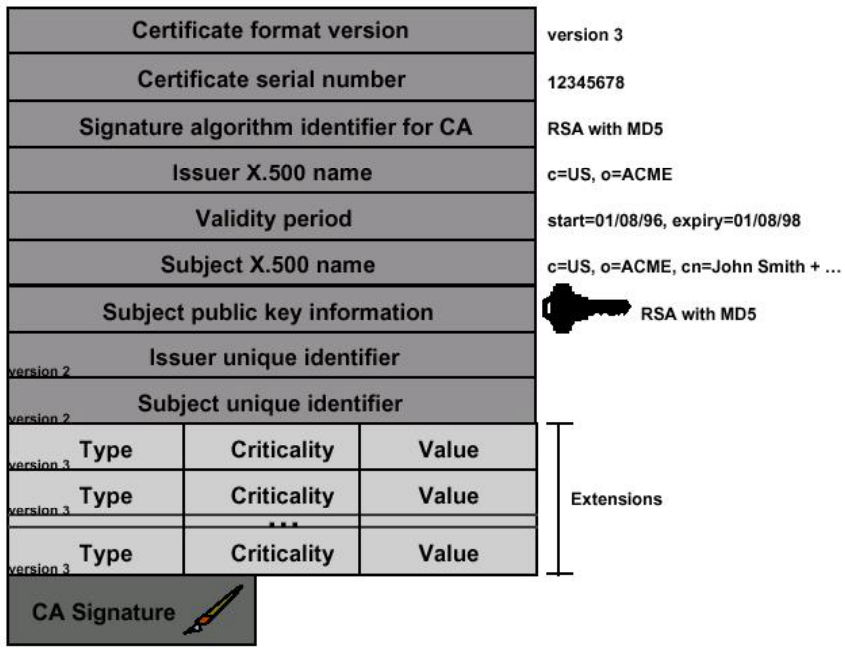
→ complémentaires

Le certificat d ’identité

Le certificat d’identité est le document émis et signé par une autorité de confiance, associant une clé publique à des informations relatives au propriétaire du certificat.

Lier clé - entité

Certificat d ’identité X. 509 v3

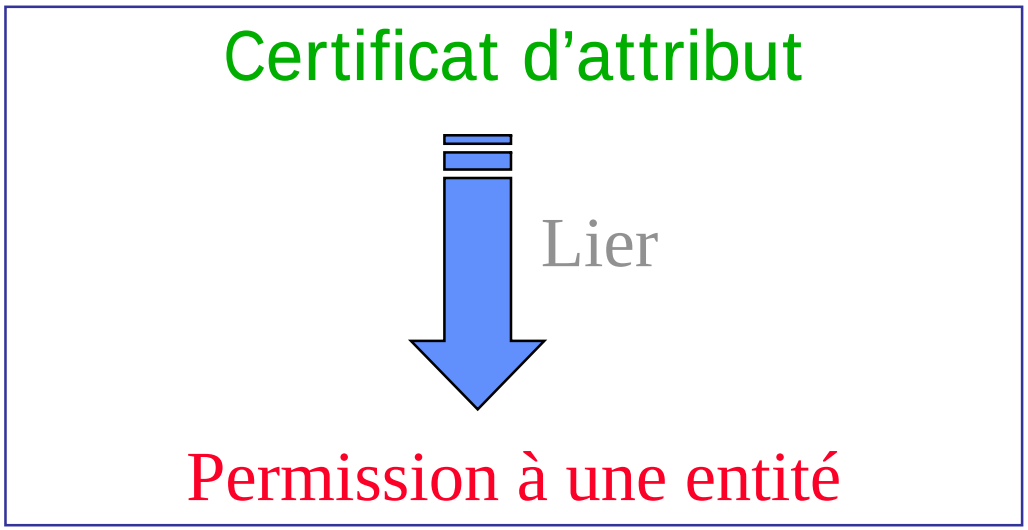


Problèmes du certificat d ’identité

- Certificat X. 509 v3 utilisé par l’IETF
  - L’évolution, une fois signé, le certificat ne peut pas être modifié:
    - La durée de vie des attributs n'est pas forcement la même de celle du certificat d'identification.
    - les attributs peuvent être donnés par une entité différente de l‘autorité de certification émettrice du certificat d'identité.
    - Les attributs ne sont pas nécessairement demandés au même moment que la demande du certificat d'identité.
  - Le rôle, le certificat permet d’authentifier une entité et ne permet pas de donner l’accès à une ressource.
  - L’encodage ASN 1. -> difficulté d’intégrer des nouveaux attributs.
  - L’infrastructure centralisée, infrastructure hiérarchique difficile à démarrer.
  - L’association avec les CRLs. Association très coûteuse et dans beaucoup de cas peu fiable.
  - La durée de vie. Un document signé par une autorité telle qu’une banque ou un notaire avec un certificat qui a une durée de validité de 3 ans alors que ce même document peut servir pour une durée supérieure

PKIX : (Public Key Infrastructure X.509) Infrastructure à Clé Publique X;509
ASN. 1 : (Abstract Syntax Notation One) Notation de syntaxe abstraite 1
CRL : (Certificates Revocation List) Liste de Révocation de Certificats

Le certificat d'attribut



Nous utilisons le **certificat d'attribut** pour ajouter des fonctionnalités à la signature conventionnelle.

Approches des certificats d'attribut

- X.509 v3 (ITU-T ISO/IEC - 1997)
- **SPKI/SDSI** (IETF/MIT RFC 2693 - 1999)
- **X.509 v 2000** (ITU-T ISO/IEC 9594-5 - 2000)
- **PKIX** (IETF RFC 3280 - 2002)
- Keynote (IETF RFC 2704, 2792 - 1998)
- Akenti (Berkeley National Laboratory - 2001)

SPKI : (Simple public Key Infrastructure) Infrastructure à clé publique simplifie
SDSI : (Simple Distributed Security Infrastructure) Infrastructure de sécurité distribuée simple
X.509 v 2000 : Norme du certificat numérique propose par l'ITU-T, ISO

SPKI/SDSI

MIT/IETF RFC 2693

But: Définir une PKI simple à utiliser.

- Le certificat est l'instrument qui habilite le propriétaire à réaliser des actions.
- Le certificat d'autorisation:
  - Autorisation (autorisation, clé)
- Le certificat identifie un individu par sa clé, et non par son nom. Permet l'anonymat.
- La délégation de pouvoir est pris en compte.
- L'infrastructure de gestion est décentralisée (chaîne de certification).
- Le système d'authentification est basé sur les «local names » SDSI
- L'autorisation est vérifiée par une liste de contrôle d'accès (ACL).
- L'encodage des certificats est fait en S-expressions

Remarques de SPKI/SDSI

- L'absence de spécification des protocoles de services (génération, revalidation, révocation, validation en temps réel, envoi de CRL, etc)
- L'infrastructure est orientée vers l'autorisation.
- Pas de profiles pour implémenter le certificat.
- L'interprétation des autorisations du certificat est complexe.
- Les « local names » SDSI limitent la représentation globale de certificats.
- Le système d'authentification n'est pas fiable.
- L'encodage en S-expressions limite l'expressivité des autorisations.
- Le support des listes de contrôle d'accès est coûteuse et peu fiable.

CRL : (Certificat Revocation List) Liste de révocation de certificats.

X.509 version 2000

ITU-T ISO/IEC 9594-5 – IETF RFC 3280

But : Définir un PKI et PMI pour la gestion de certificats à clé publique et de certificats d'attributs

- L'autorité d'attribut de la PMI est centralisée et ses attributs son uniques.
- Le certificat est principalement utilisé pour le contrôle d'accès (FRC 3281)
- Le certificat d'attribut:
  - Attribut (attribut, DN)
- Le certificat identifie un individu par son nom (X.500 – DN)
- L'Infrastructure de gestion est centralisée.
- L'encodage de certificat est fait en ASN. 1
- Le système de révocation utilise ACRL.

PMI : (Privileges Manager Infrastructure) Infrastructure de gestion de privilèges.
DN : (Distinguished Name) Nom distinctive.
ACRL : (Attribute Certificate Revocation List) Liste de révocation de certificats d'attribut

Remarques X.509 v2000 (PKIX)

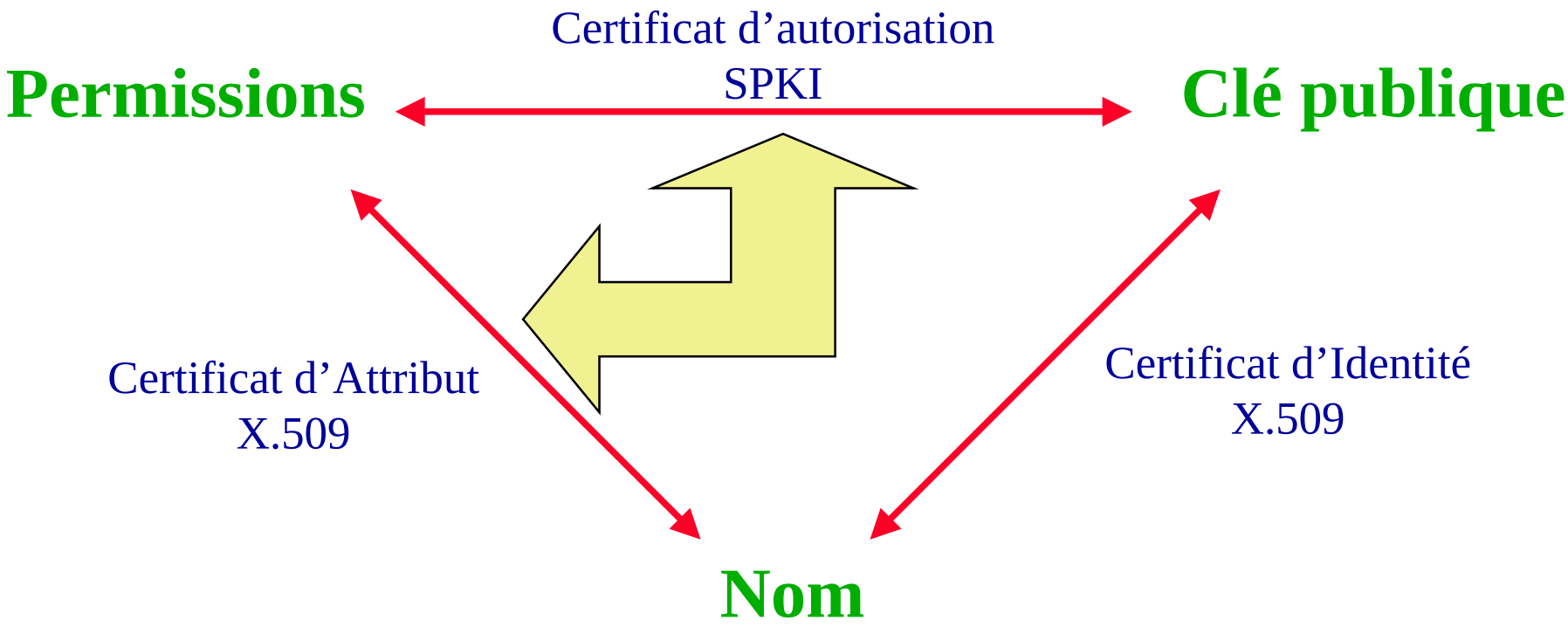
- La complexité du déploiement des certificats d'attribut. Une part de cette complexité est attribuable à l'encodage des certificats X.509 en format ASN.1.
- Les certificats sont limités au contrôle d'accès et à l'authentification.
- L'infrastructure est centralisée.
- L'utilisateur du certificat d'attribut est toujours identifié, donc pas d'anonymat.
- La délégation de pouvoir n'est pas pris en compte.
- La PMI dépend de la PKI.

SPKI vs X.509

- SPKI
  - Lie permission – clé ou nom
  - Permet anonymat et délégation
  - Gère une infrastructure décentralisée
  - Encode en S-expressions
  - Support ACLs et noms SDSI

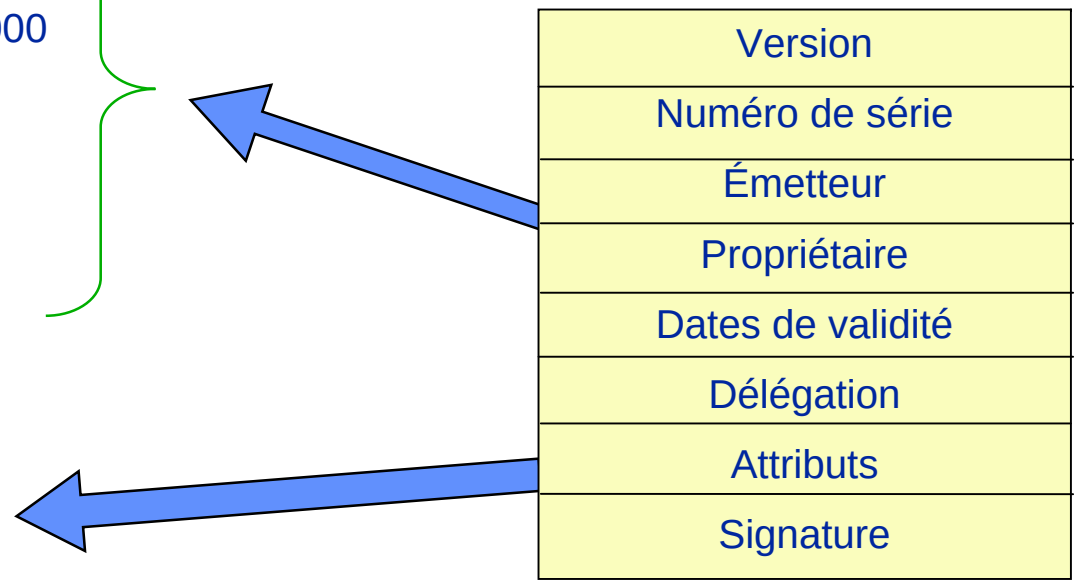
- X.509 version 2000
  - Lie permission – entité
  - Permet le contrôle d'accès
  - Gère une infrastructure centralisée
  - Encode in ASN.1
  - Support ACRL et noms X. 500

Les certificats pour les e-services



Format du certificat d'attribut

- Lier permissions à :
  - Clé publique
  - Rôle ou nom du groupe
  - Un Nom valide pour X.509 v. 2000
    - BaseCertificatId
    - EntityName
    - ObjectDigestInfo
- Structure des attributs :
  - `AttributeName`
  - `AttributeValue`
  - `AttributeDescription`
- Encode en XML, signature XMLDSIG



Format XML

```
<Signature >
    <SignedInfo>
    <SignatureValue>
    <Object>
       <AttributesCertificate>
                <CertificateInfo>
                        <Version>v1.0</Version>
                        <Id>1</Id></CertificateInfo>
                <Content>
                        <Issuer>
                        <Holder>
                        <Validity NotBefore="1023374591054" NotAfter="1023374591054" />
                        <Delegation Depth="0" />
                        <Attribute>
                                <AttributeName>SignatureDelegation</AttributeName>
                                <AttributeValue></AttributeValue>
                                <AttributeDescription></AttributeDescription>
                        </Attribute>
                </Content>
        </AttributesCertificate>
    </Object>
</Signature>
```

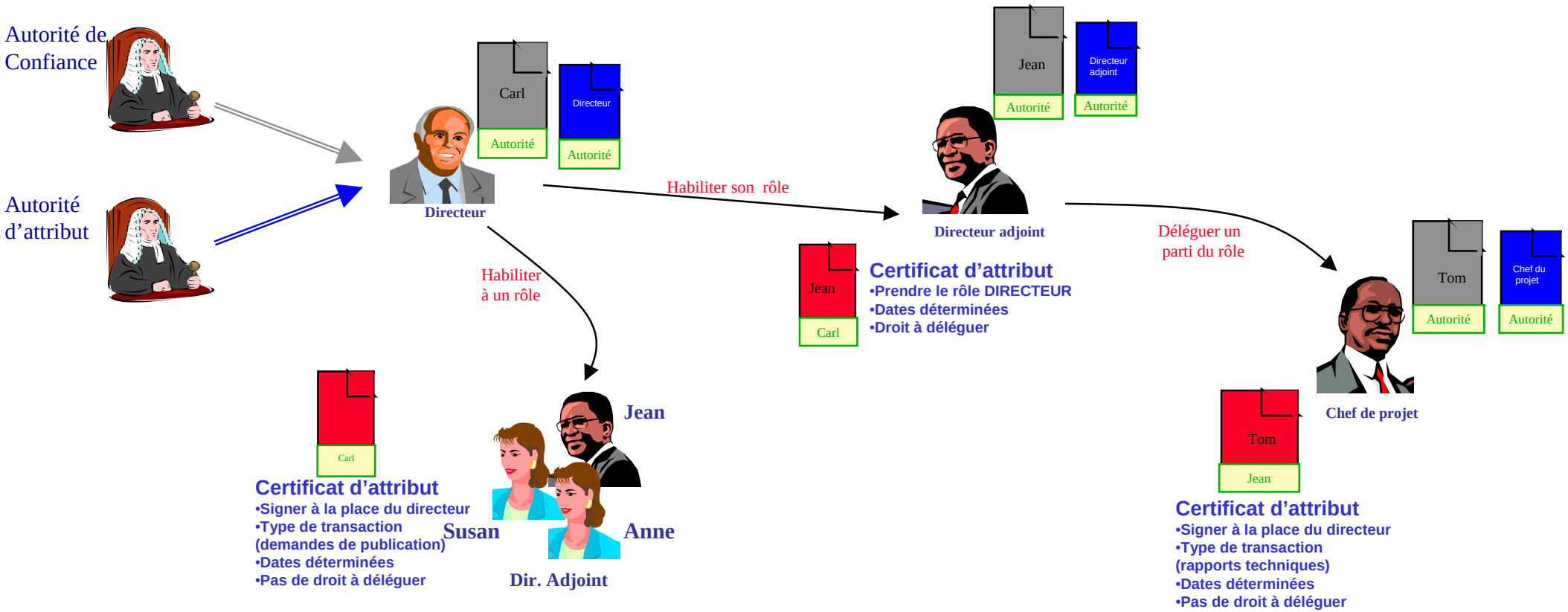
Nouveaux attributs

- SignatureDelegation
  - Donner le droit de signer

- SignaturePath
  - Indiquer les signataires
  - Indiquer la séquence de signatures
  - Permettre certificats d'habilitation

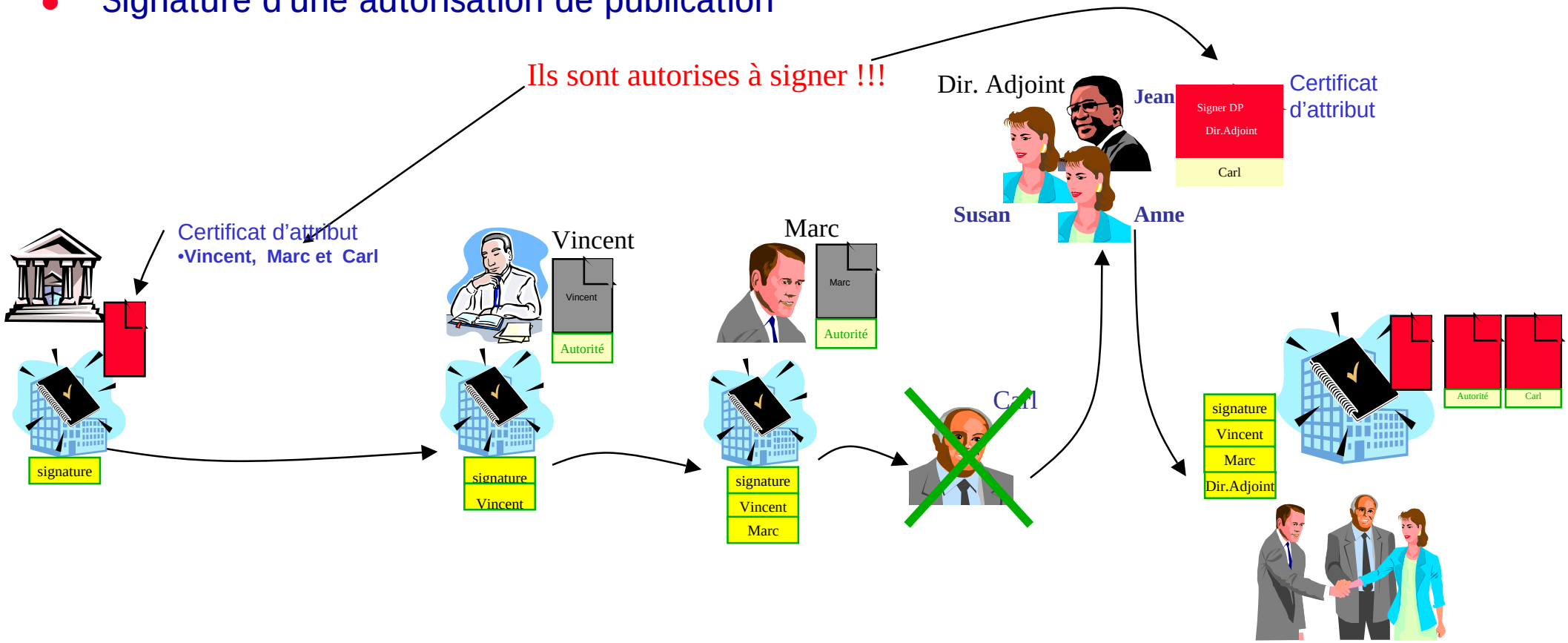
Applications (1)

- L'identification, l'habilitation, la délégation et le rôle



Applications (2)

- Signature d'une autorisation de publication

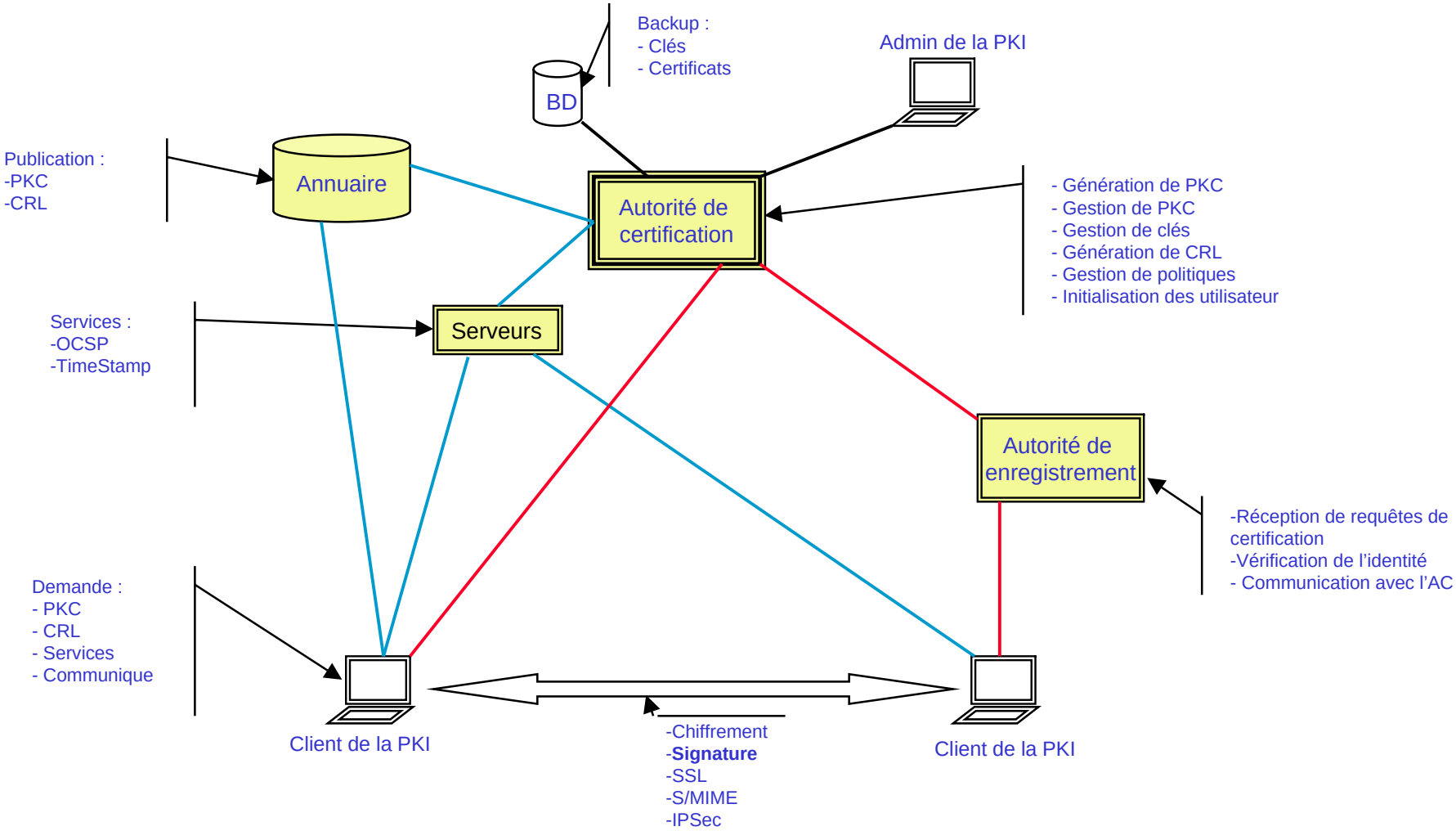


La Multisignature est valide !!!

Plan

- Contexte
- Usages de la signature
- Certificats électroniques
- Infrastructure de confiance
  - Besoins
  - Modèle de confiance
  - Acteurs de l'infrastructure
  - Choix techniques
- Conclusion

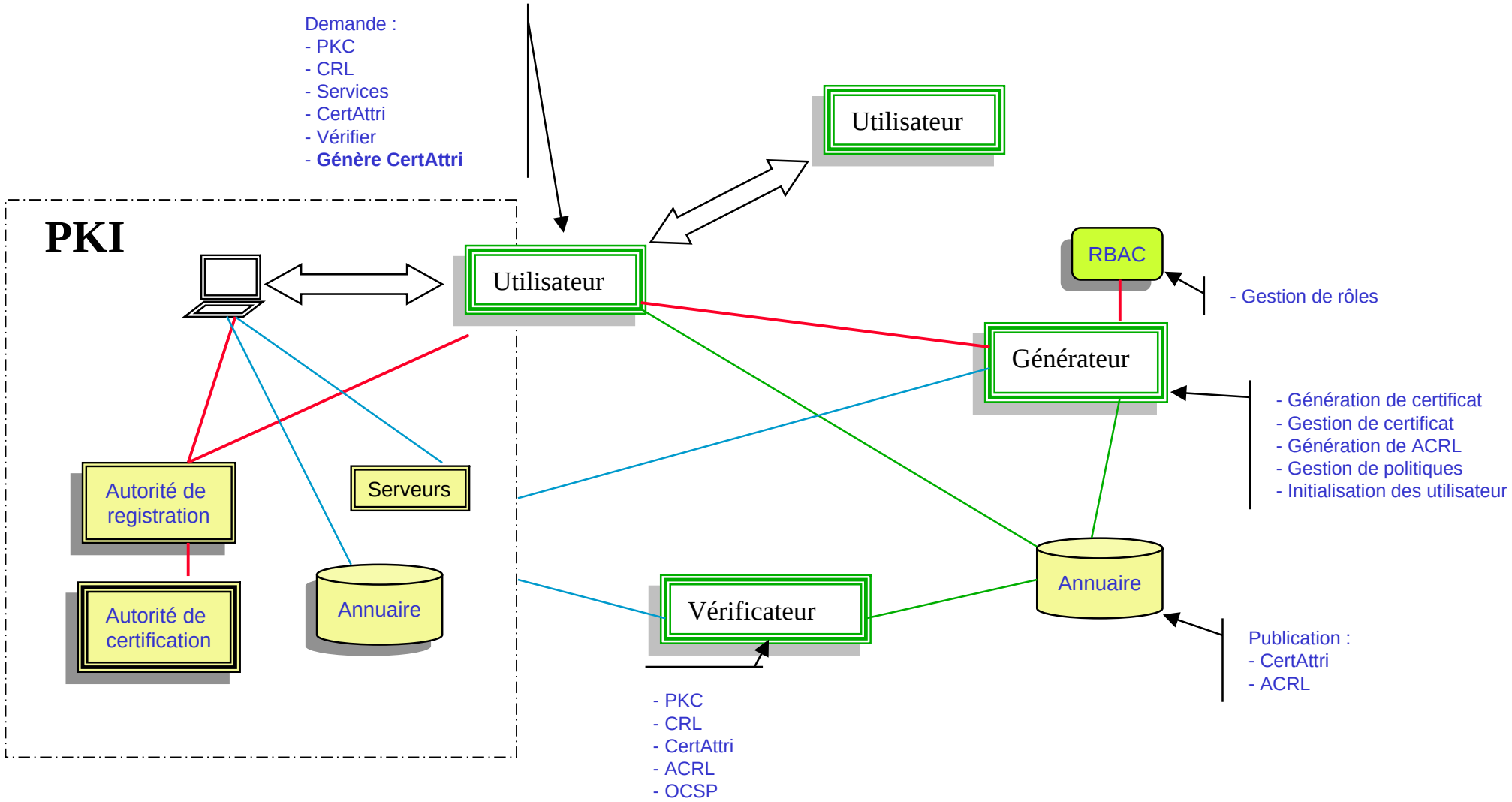
Principaux Composant d'un PKI



Besoins de notre infrastructure

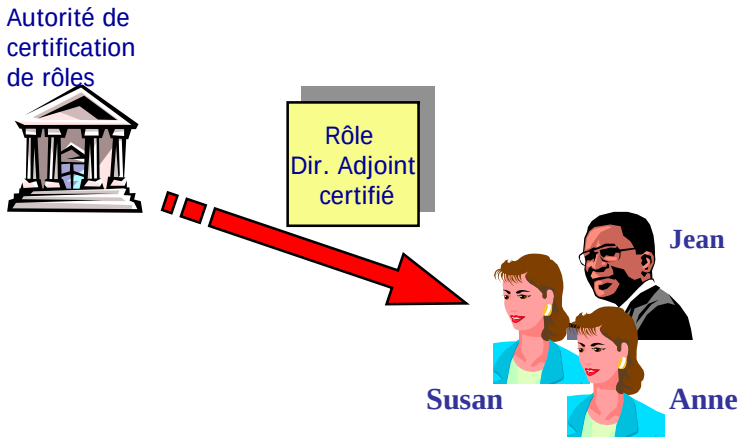
- L'infrastructure doit supporter l'émission décentralisée des certificats d'attribut.
- L’infrastructure doit assurer la compatibilité vers d’autres infrastructures.
- L’infrastructure doit être indépendante de la PKI.
- L'infrastructure doit gérer les privilèges des utilisateurs, notamment leurs rôles.
- Le modèle de confiance doit être adaptable aux besoins et services des utilisateurs
- Les utilisateurs de l’infrastructure doivent accéder aux services de la PKI.

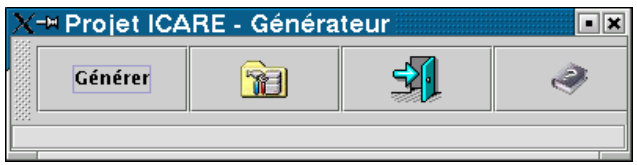
Modèle de confiance



Générateur

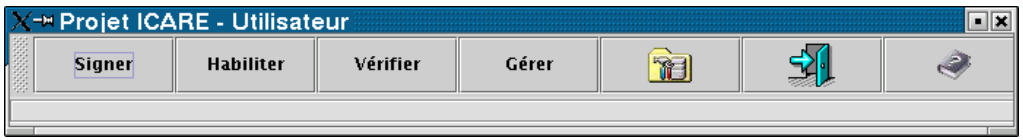
- Générer les certificats d'attribut
- Gérer les différentes rôles.
- Gérer les politiques de signature.
- Gérer les politiques de certification.
- Définir la route des signatures.
- Générer ACRL
- Initialiser les utilisateur

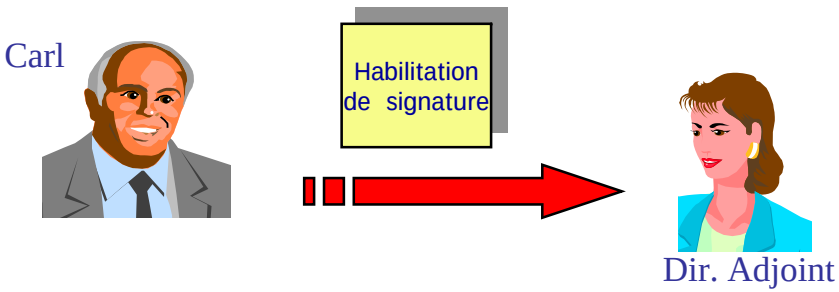




Utilisateur

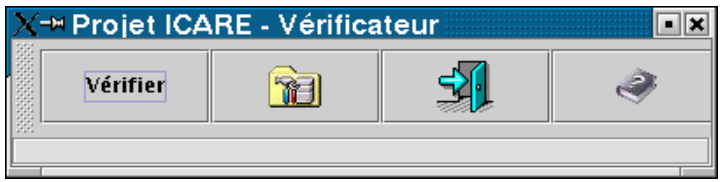
- Signer des objets (simple et multiple)
- Émettre des certificats d'habilitation
- Vérifier les signatures
- Interagir avec la PKI

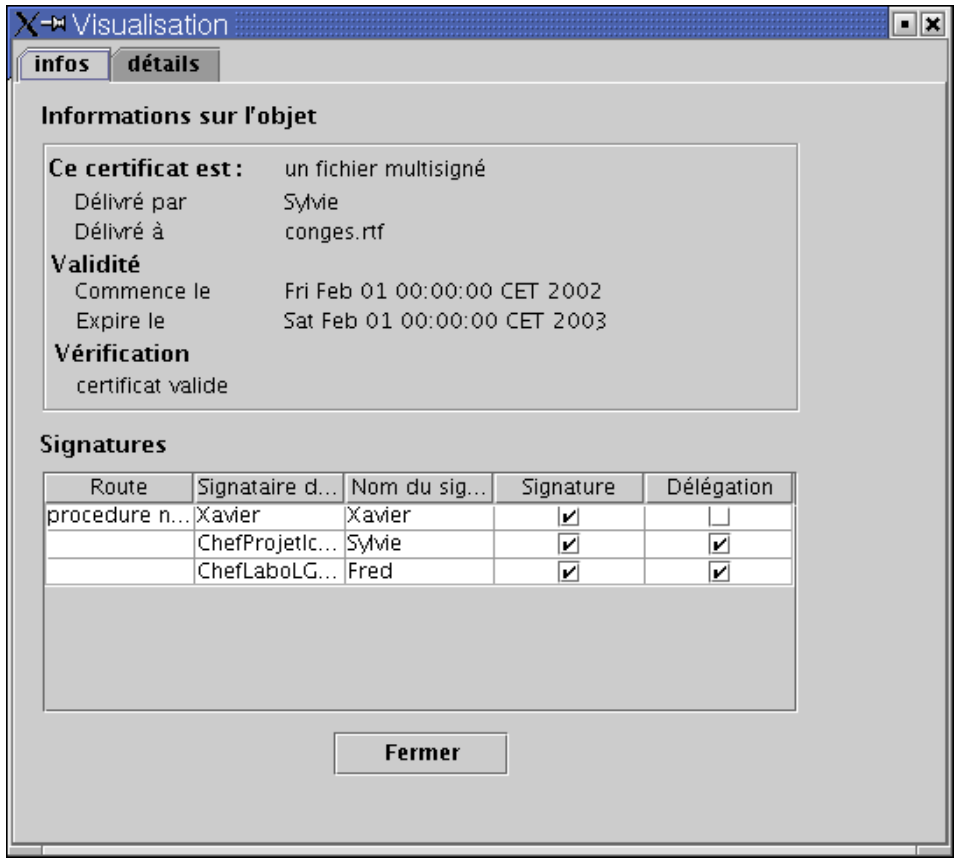




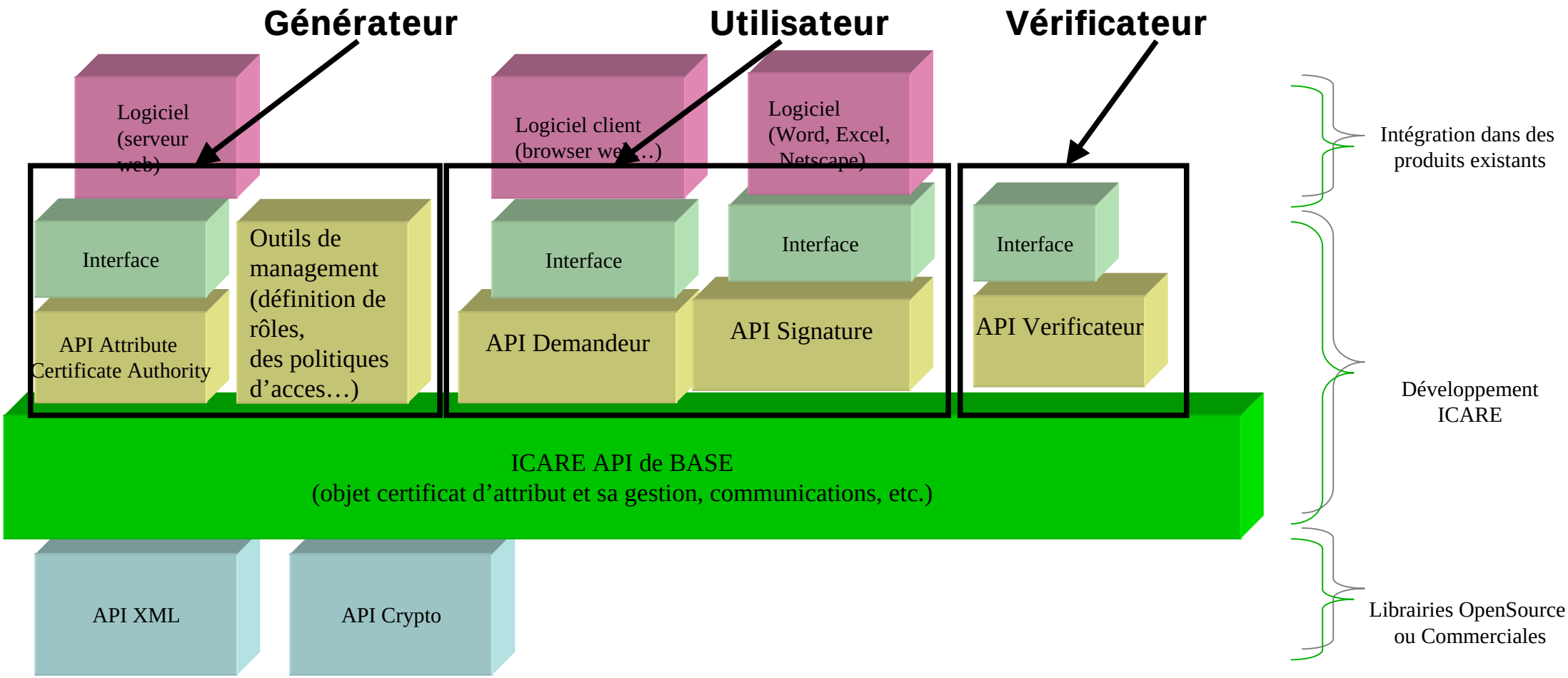
Vérificateur

- Vérifier :
  - l'intégrité des documents
  - la validité des signatures
  - la séquence de signataires
  - les dates de validité
  - la validité des certificats d'attribut
  - la validité des certificats d'identité





Architecture logicielle



Choix technologiques

- CRYPTIX
  - Algorithmes de cryptographie
  - Gestion des clés
  - Librairie open source
- Librairie sécurité SUN
  - Gestion des certificats X.509 v3
  - Librairie incluse dans le jdk 1.4
- JDOM
  - Gestion du langage et des documents XML
  - Librairie open source

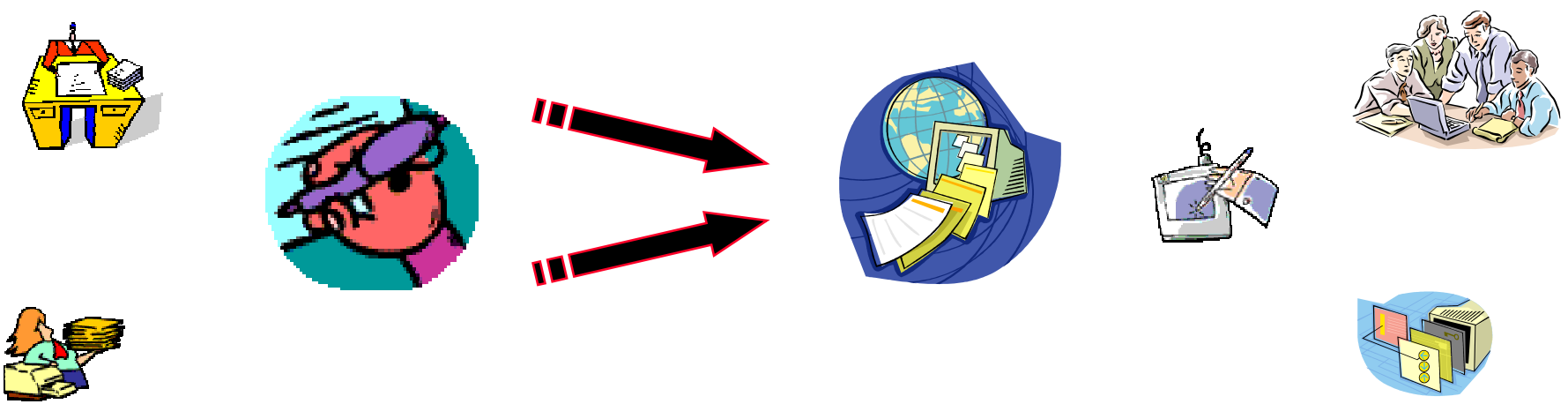
Plan

- Contexte
- Usages de la signature
- Certificats électroniques
- Infrastructure de confiance
- Conclusion

Conclusion

- L'utilisation des Certificats d'Attributs permet de:
  - contrôler la signature électronique
  - habiliter, déléguer la signature
  - signer avec une qualité professionnelle (rôles)

Avec ces nouveaux e-services l'usage de la signature électronique devrait se développer et permettre aux utilisateurs de retrouver dans un environnement électronique le contexte et les contraintes quotidiennes des signatures manuscrites



Questions ?

Paul Axayacatl FRAUSTO BERNAL
Paul.Frausto@ema.fr