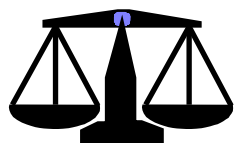




Garantir l'identité de l'internaute par...

LE CERTIFICAT ELECTRONIQUE

juin 2009



Thierry PIETTE-COUDOL

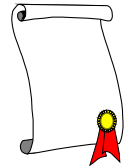
avocat, associé du cabinet André Bertrand (Paris)

Président de l'association IALTA (www.ialtafrance.org)

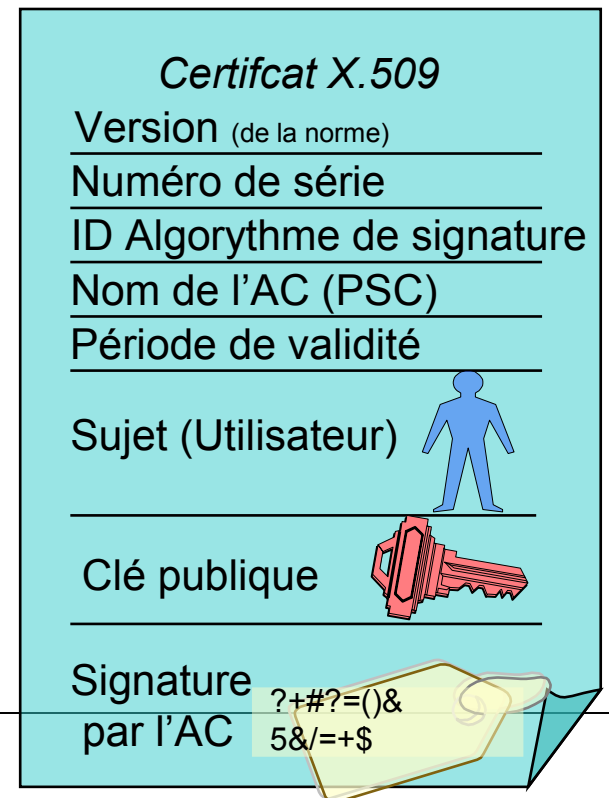
email: piettecoudol@free.fr



Le certificat X 509



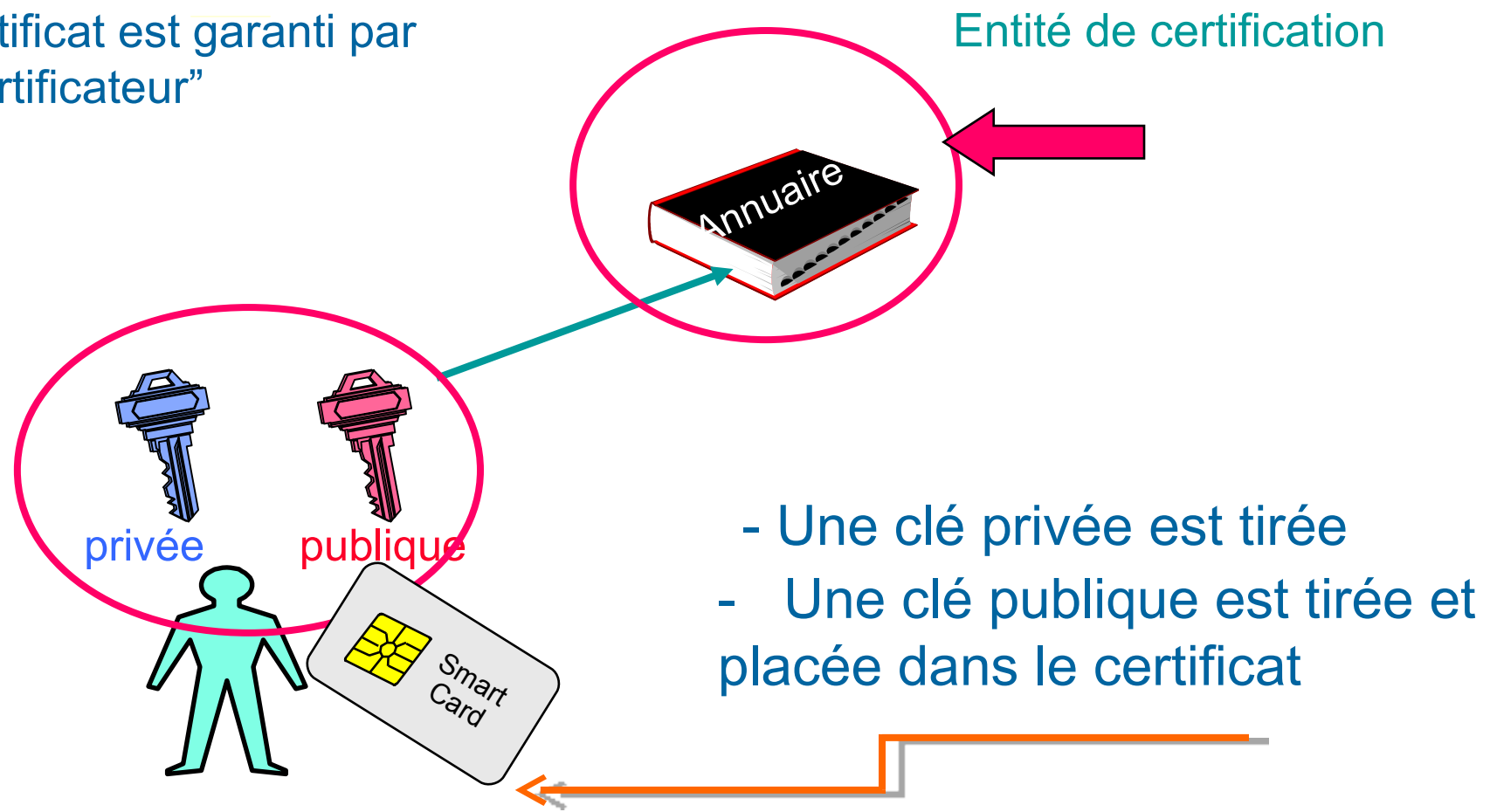
- Les certificats électroniques sont signés par une entité de certification et publiés sur un annuaire accessible en ligne
- Ils sont normalisés (X.509)





Principe du certificat électronique

Le certificat est garanti par un "certificateur"



- Une clé privée est tirée
- Une clé publique est tirée et placée dans le certificat



-
- L'identification repose sur l'utilisation de deux clés cryptographiques, chargé des opérations de chiffrement (clef privée du signataire) et de déchiffrement (clé publique du signataire)



La signature électronique à clefs asymétriques

Les 3 concepts à **RETENIR** :

- 1 - La clé privée ne sort jamais de son support non reproductible,
(actuellement, une puce cryptographique). Elle est secrète et confinée.
- 2 - La clé publique est certifiée par l'entité de certification (dans le certificat).
- 3 - Le certificat qui contient la clé publique est signée par l'entité de certification. Il est téléchargeable sur un annuaire en ligne par tout le monde ou envoyé avec la signature.



La signature électronique à clefs asymétriques

Une clé Publique, c'est quoi

?

Bi-clé RSA de 512 bits (1978, «A method for obtaining digital signature and public-key cryptosystems», Rivest, Shamir, Adleman)

Clé publique, (modulo + exposant public) :

- modulo $n = p * q$

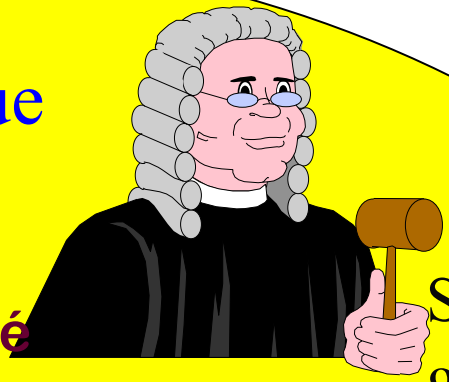
e0 78 c8 f9 2a c3 d7 b1 6a eb 66 00 15 ed 54 28 91 81
35 9f 6f 8a b3 6a ac 9d 0a 75 12 df 9e 77 f0 d3 3c 30
f4 ad 33 6a 9a 65 24 20 89 8b f7 95 9d be 9a bd 31 77
80 ac 14 0f a4 90 e6 0d 0a 29

- exposant public, PK : $(2^{16} + 1 = 65.537)$

01 00 01



Infrastructure à Clé Publique



**Système d'enregistrement
des membres d'une communauté**

**Système de
gestion et de
pilotage**



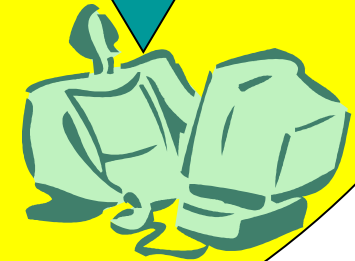
Constitution de
l'annuaire des
clefs publiques
certifiées



**Génération
des bi-**



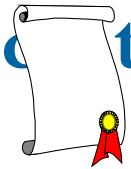
**Système de stockage
des clés publiques,
de vérification de la**



Constitution de la liste des {
certificats révoqués { **signature par diffusion des
certificats**




La confiance est dans le certificat



Certificat [?] [X]

Général | Détails | Chemin d'accès de la certification

 **Informations sur le certificat**

Ce certificat est destiné à :


- Assurer que le courrier électronique provenait de l'expéditeur
- Protéger le courrier électronique contre toute modification
- Assurer que le contenu de courriers électroniques ne peut pas être vu par d'autres personnes
- Garantir votre identité auprès d'un ordinateur distant

* Consultez la déclaration de l'émetteur du certificat pour plus de détails.

Délivré à : ERIC CHAMBRIN

Délivré par : AC Le Chainon Manquant Classe 3Plus

Valide à partir du 25/10/01 **jusqu'au** 25/04/03

 Vous avez une clé privée qui correspond à ce certificat.

Declaracion de l'emetteur...

OK





Quelle niveau de confiance dans le certificat ?



- **Classe 1: confiance faible**
 - Une adresse email est nécessaire. Le certificat est envoyé à l'adresse email
 - Risque : Qui est derrière l'adresse e-mail ?
- **Classe 2: confiance moyenne**
 - vérification sur dossier papier (par exemple Kbis, lettre entête, photocopie certifiée conforme)
- **Classe 3: bonne confiance**
 - Délivrance selon une procédure stricte avec présence physique et justificatifs
- **Classe 3+: haute confiance**
 - Délivrance selon une procédure stricte avec présence physique et justificatifs. Génération des clés dans une carte à puce.

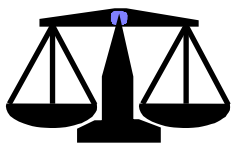
Dans tous les cas, la délivrance du certificat est liée la Politique de Certification



Du certificat électronique à...

LA SIGNATURE ELECTRONIQUE

juin 2009



Thierry PIETTE-COUDOL

avocat, associé du cabinet André Bertrand (Paris)

Président de l'association IALTA (www.ialtafrance.org)

email: piettecoudol@free.fr



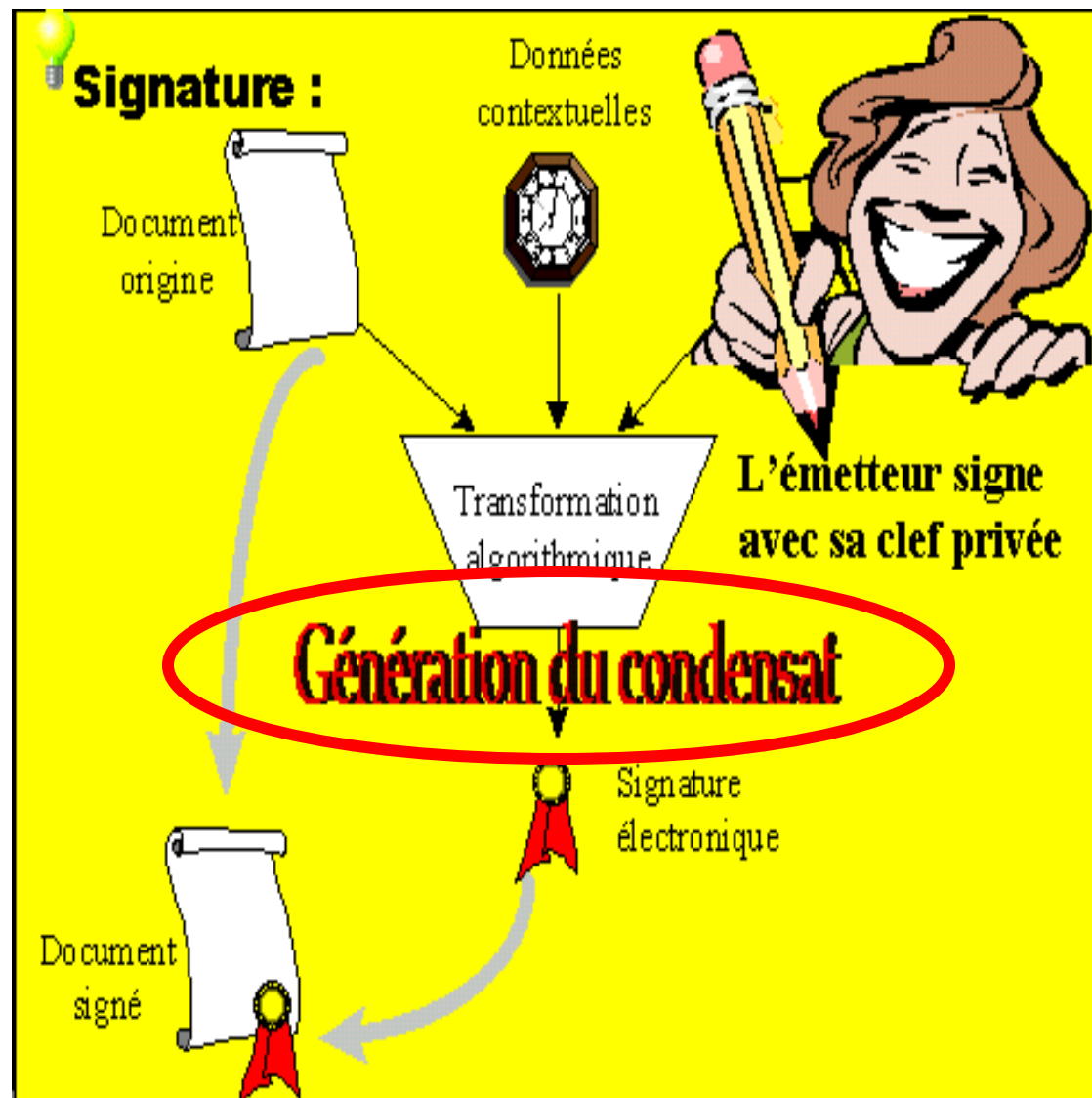
Fonctions de la signature électronique

- Dans le cadre d'un échange d'informations dématérialisées, la signature électronique apporte deux garanties techniques fondamentales :
 - **Authentification** du signataire d'un message électronique,
 - **Intégrité** du message lors de son acheminement électronique.
- ☞ Authentification + Intégrité = Authenticité



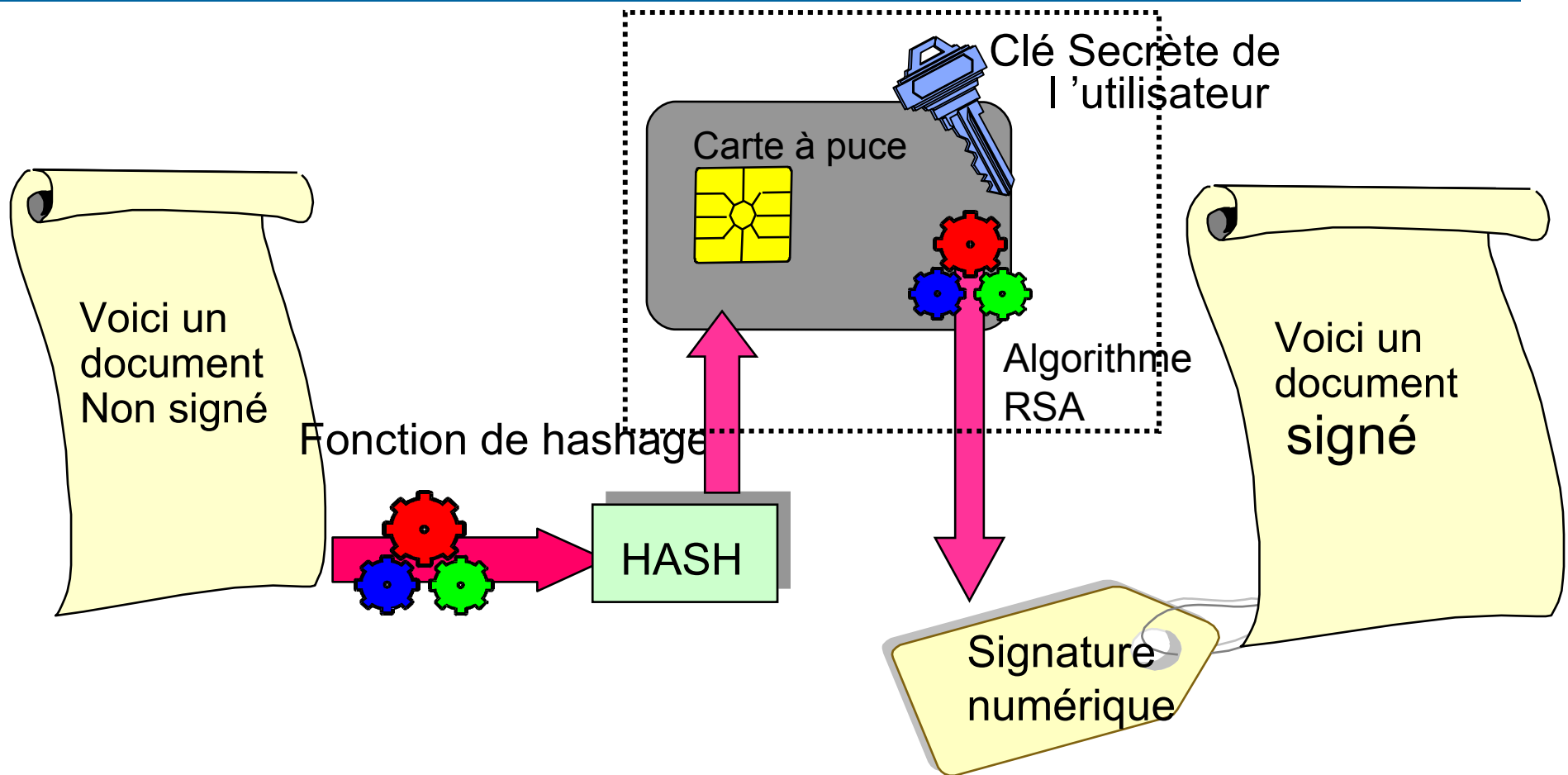
La signature électronique à clefs asymétriques

- Au niveau technique, la signature électronique se présente comme un « condensé chiffré » du message signé. Le condensé est chargé d'assurer l'intégrité

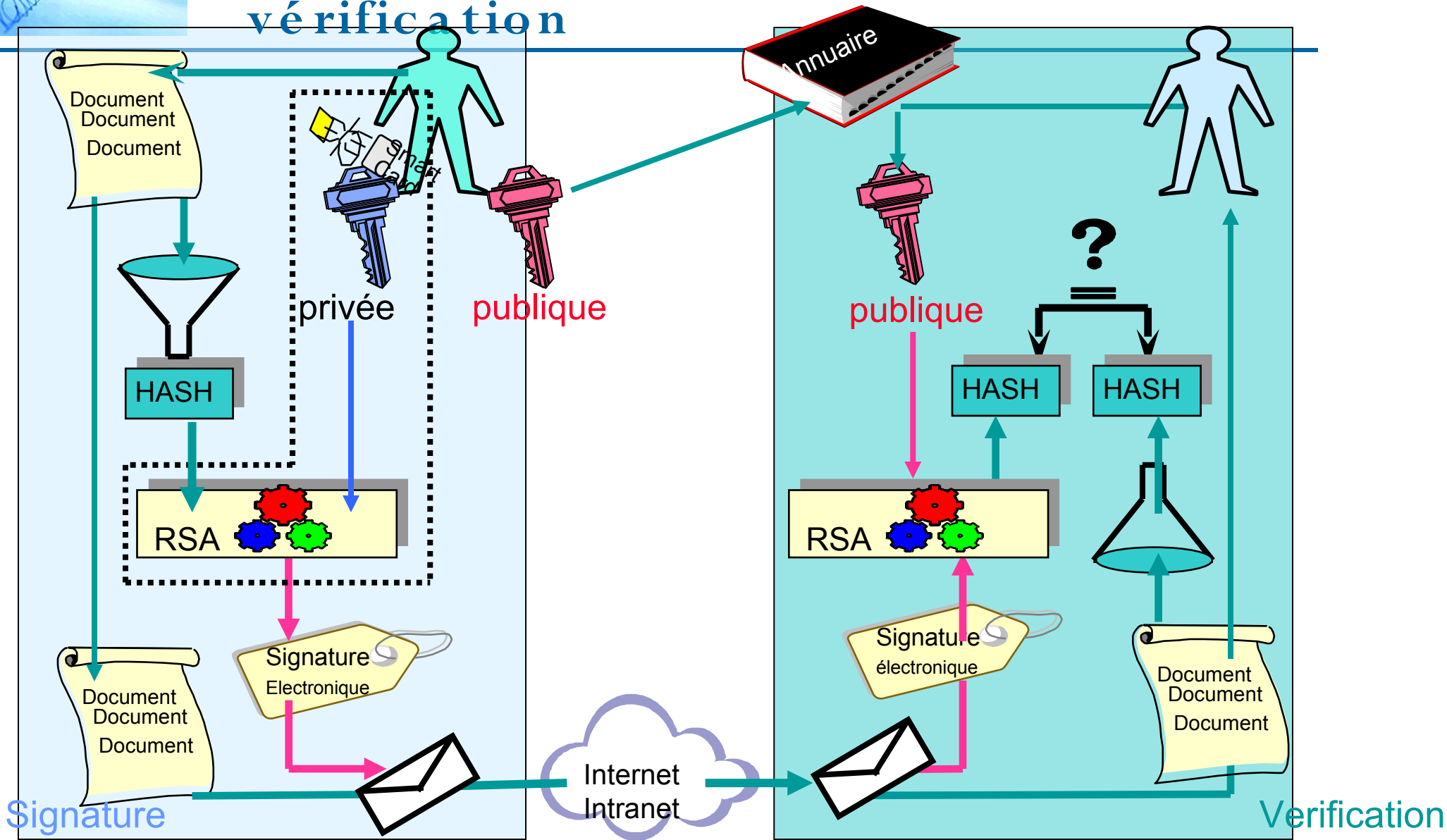




Le processus de signature



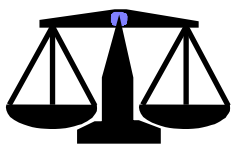
Signature électronique et vérification





Les transactions électroniques, exemple de mise en œuvre en France

Saly - juin 2009



Thierry PIETTE-COUDOL

avocat, associé du cabinet André Bertrand (Paris)

Président de l'association IALTA (www.ialtafrance.org)

email: piettecoudol@free.fr



1 - LA SIGNATURE ELECTRONIQUE

- 11/ La SE garantit l'authenticité du fichier signé (identification + intégrité)

- 12/ La SE peut être utilisée au niveau technique, mais aussi juridique (des agréments et certification sont nécessaires)

- 13/ Trois utilisations de la SE : 1) signature - 2) validation de la dématérialisation – 3) sécurisation des échanges électroniques



2- LE CONTRAT ELECTRONIQUE

21/ Le contrat électronique est valide supporté par messagerie électronique

22/ Les exigences de forme du contrat papier se retrouvent dans le contrat électronique (lisibilité, présentation)

23/ Trois sécurisation du contrat électronique : 1) recommandé électronique – 2) accusé de réception électronique – 3) horodatage



3 - LA PREUVE ELECTRONIQUE

- 31/ La preuve ne se conçoit que pour un "écrit électronique" garanti en intégrité et identifiant son émetteur
- 32/ La preuve s'organise et se maintient pendant tout le cycle de vie, depuis la formation jusqu'à l'archivage électronique.
- 33/ Trois éléments à archiver : 1) le fichier électronique – 2) la signature du fichier – 3) le certificat lié à la signature