



PLAN

Signature électronique

Evolutions de la réglementation

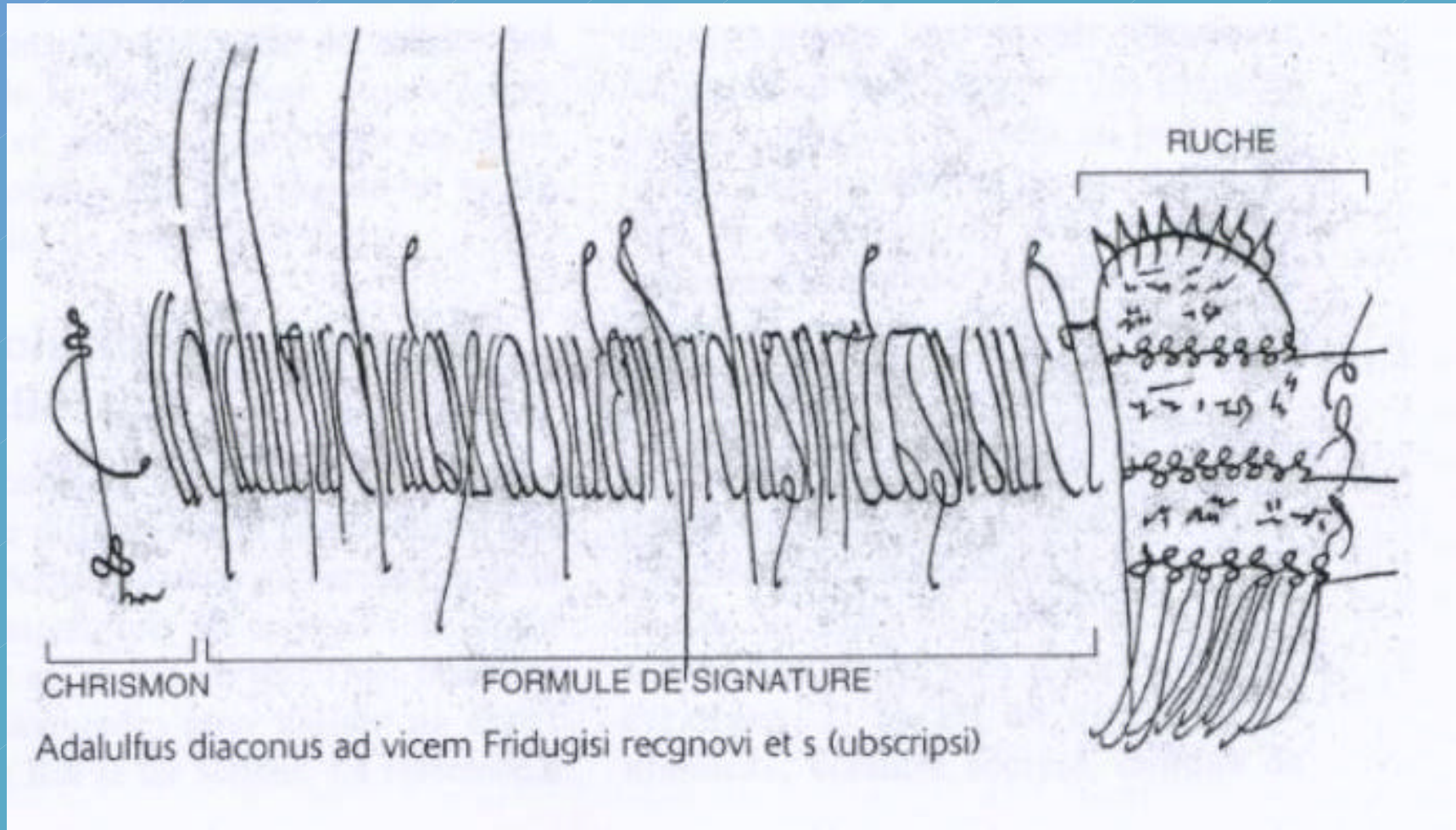
SEE – 25 avril 2002

Problématique

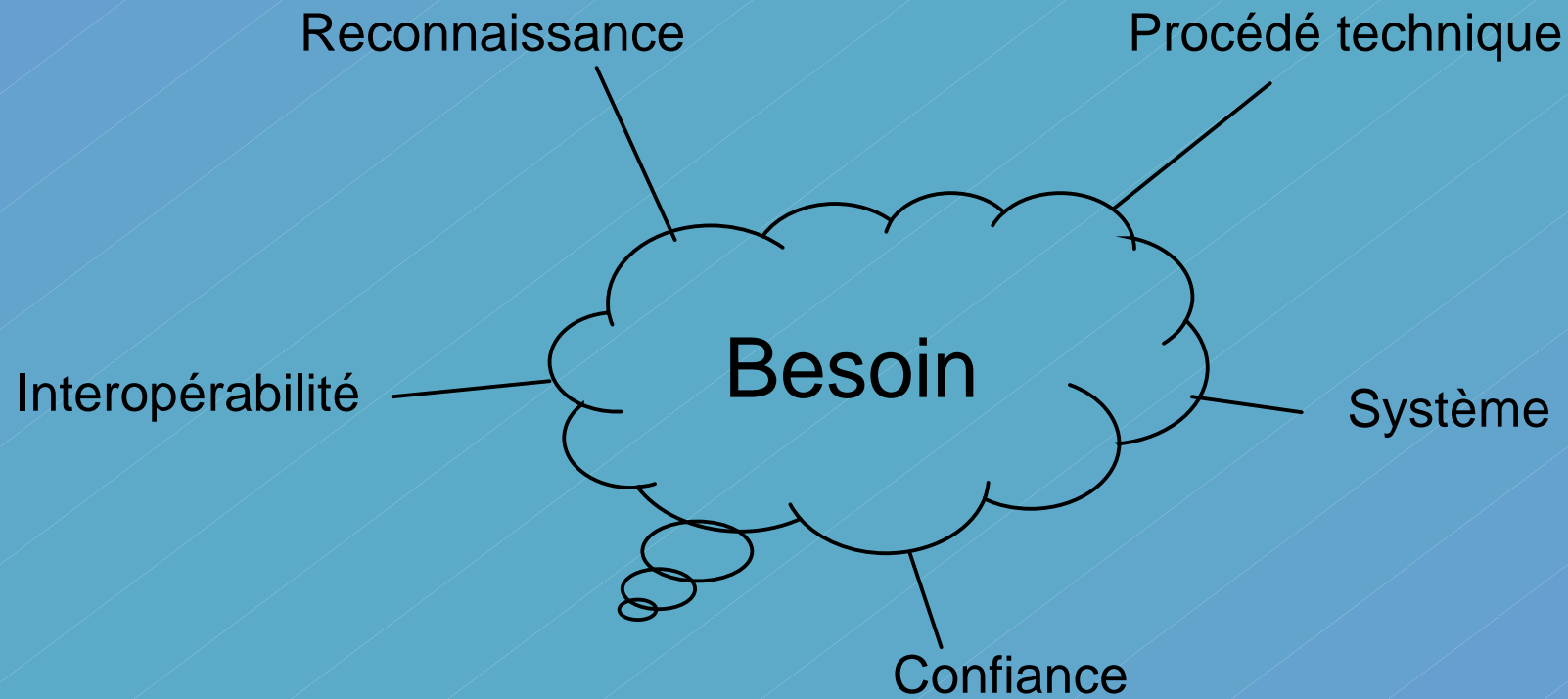
LA SIGNATURE

Transformer un document en
acte juridique qui engage
et authentifie les parties
intéressées

Histoire



Besoins



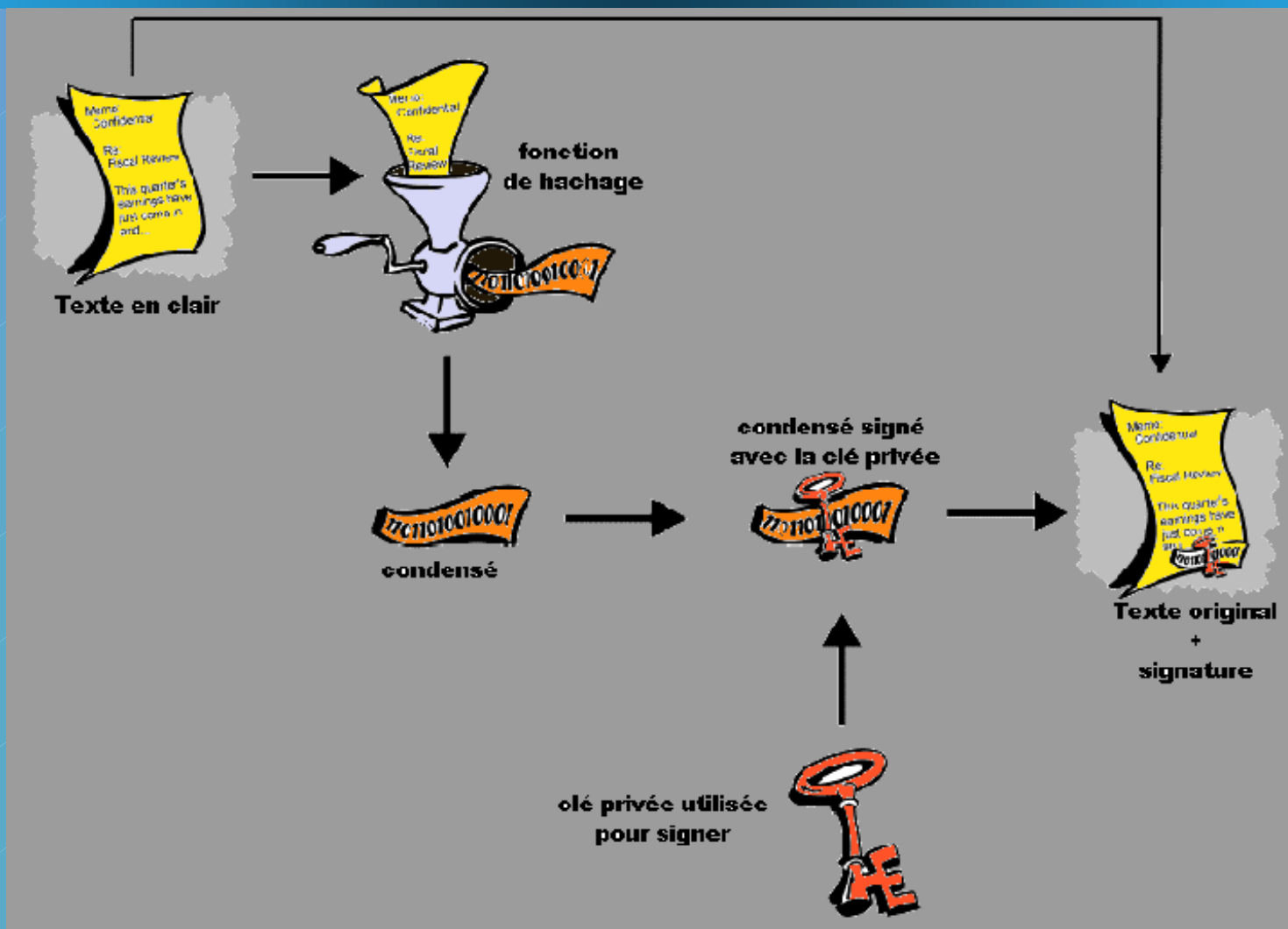
Procédé technique

Principes

- Généralement basée sur l'utilisation d'algorithmes cryptographiques.
- Algorithmes généralement de type asymétriques (RSA pour le plus connu) plus algorithmes de hachages.
- Disponible depuis 1978

Procédé technique

Principes



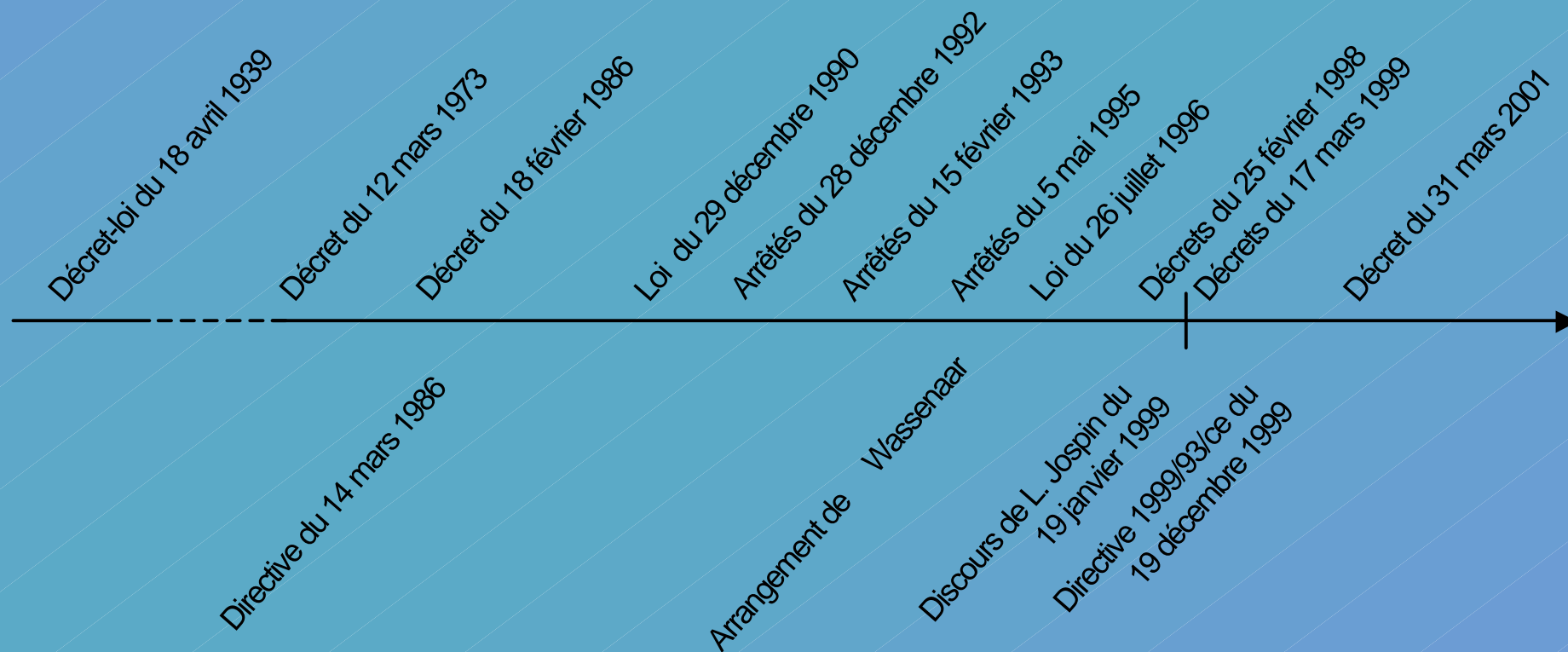
Procédé technique

Principes

- En résumé :
 - Chaque signataire dispose d'une clé privée pour signer et d'une clé publique permettant aux vérificateurs de vérifier la signature.
 - Clé privés et clés publiques sont liées.

Procédé technique

Réglementation (crypto)



Procédé technique

Réglementation (crypto)

- Décret du 12 mars 1973

Les équipements de cryptographie et de cryptophonie sont considérés comme des armes de guerre de 2ème catégorie (comme les chars de combats, navires de guerre, aéronefs militaires...) et sont donc soumis aux règles propres à ces équipements en matière de détention, fabrication, utilisation, importation et exportation.

- Décret du 18 février 1986

Moyens de cryptologie : matériels ou logiciels conçus, soit pour transformer à l'aide de conventions secrètes des informations claires ou des signaux en informations ou signaux inintelligibles, soit pour réaliser l'opération inverse

Régime dit « d'autorisation » avec particularités selon que l'on est fabricant ou utilisateur.

Procédé technique

Réglementation (crypto)

- Loi du 26 juillet 1996 et décrets du 25 février 1998

Utilisation libre si le moyen de cryptologie n'assure pas la confidentialité

Utilisation libre si le moyen de cryptologie assure la confidentialité et n'utilise que des conventions secrètes gérées selon des procédures et par un organisme agréé. Introduction des Tiers de Séquestre.

Régime déclaratif si longueur de clé inférieur ou égal à 40 bits (pour les fournisseurs). Utilisation libre.

Soumise à autorisation dans les autres cas.

- Arrêtés du 5 mai 1995

contrôle de l'exportation vers des pays tiers et vers les États membres de la CEE (biens à double usage).

Procédé technique

Réglementation (crypto)

Décret du 17 mars 1999

Fait suite au discours de L. Jospin du 19 janvier 1999.

Fourniture de moyen et prestations de cryptologie

Authentification, signature intégrité : Soumise à déclaration simplifiée

Chiffrement inférieur ou égal à 128 bits : soumise à déclaration

Chiffrement supérieur à 128 bits : soumise à autorisation

- Les longueurs de clés concernent des algorithmes de chiffrement de type symétriques (A.E.S., D.E.S., IDEA, RCx...)

Procédé technique

Réglementation (crypto)

Utilisation de moyen et prestations de cryptologie

Authentification, signature, intégrité : Libre

Chiffrement inférieur ou égal à 128 bits : Libre (1)

Chiffrement supérieur à 128 bits : autorisation (ou TdC) (2)

- Sous réserve que le moyen ou la prestation aient fait l'objet d'une déclaration ou si uniquement pour usage privé d'une personne physique. Sinon déclaration d'utilisation personnelle à adresser à la DCSSI
- Si autorisé en fourniture, alors autorisé d'office en utilisation.

Procédé technique

Réglementation (crypto)

Importation de moyen et prestations de cryptologie

Authentification, signature, intégrité : Libre (1)

Chiffrement inférieur ou égal à 128 bits : Libre (2)

Chiffrement supérieur à 128 bits : autorisation

- libre dans tous les cas si provenance d'un état membre de la CEE ou ayant signé les accords instituant l'espace économique européen
- Sous réserve que le moyen ou la prestation aient fait l'objet d'une déclaration ou si uniquement pour usage privé d'une personne physique. Sinon déclaration d'utilisation personnelle à adresser à la DCSSI

Systeme

Rappel

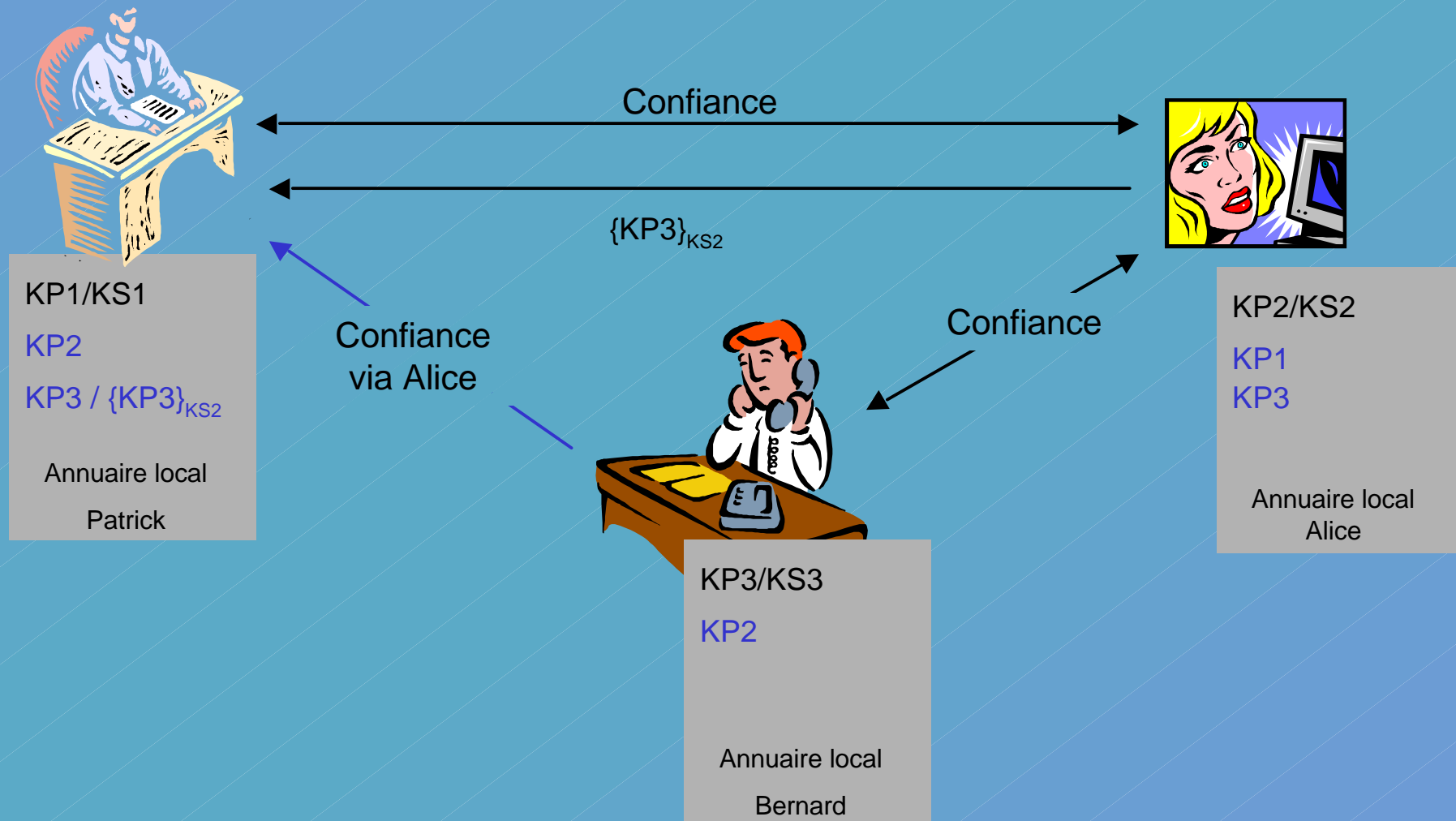
Chaque signataire dispose d'une clé privée pour signer et d'une clé publique permettant aux vérificateurs de vérifier la signature.

Comment lier signataire et clé publique ?

- En la faisant certifier (i.e. signer) avec la clé d'une personne en qui a confiance le destinataire final (principe de PGP ou « les amis de nos amis sont nos amis »).
- En la faisant certifier avec une clé privée dont la clé publique correspondante est connue de tous.

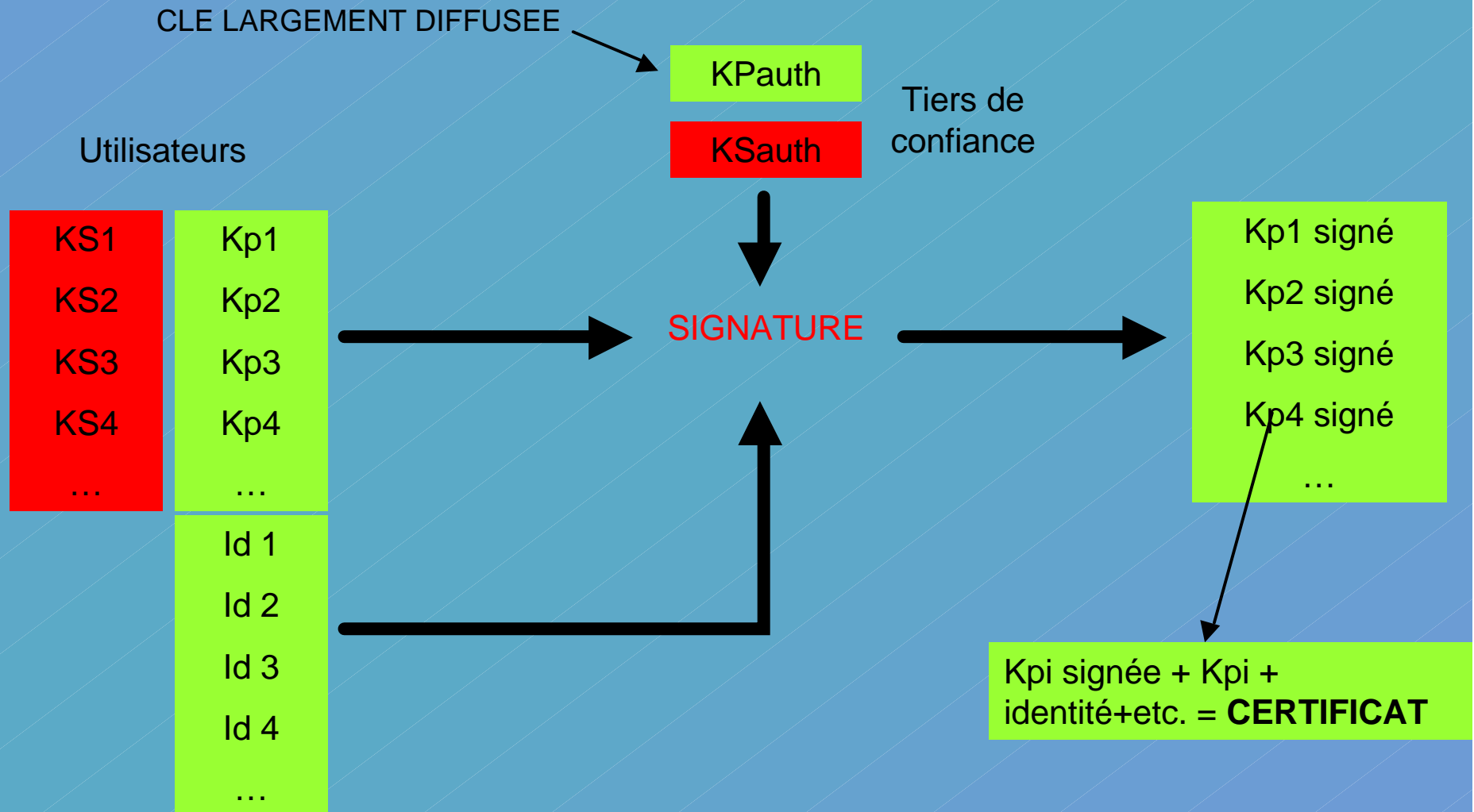
Systeme

Comment faire connaître sa clé publique ?



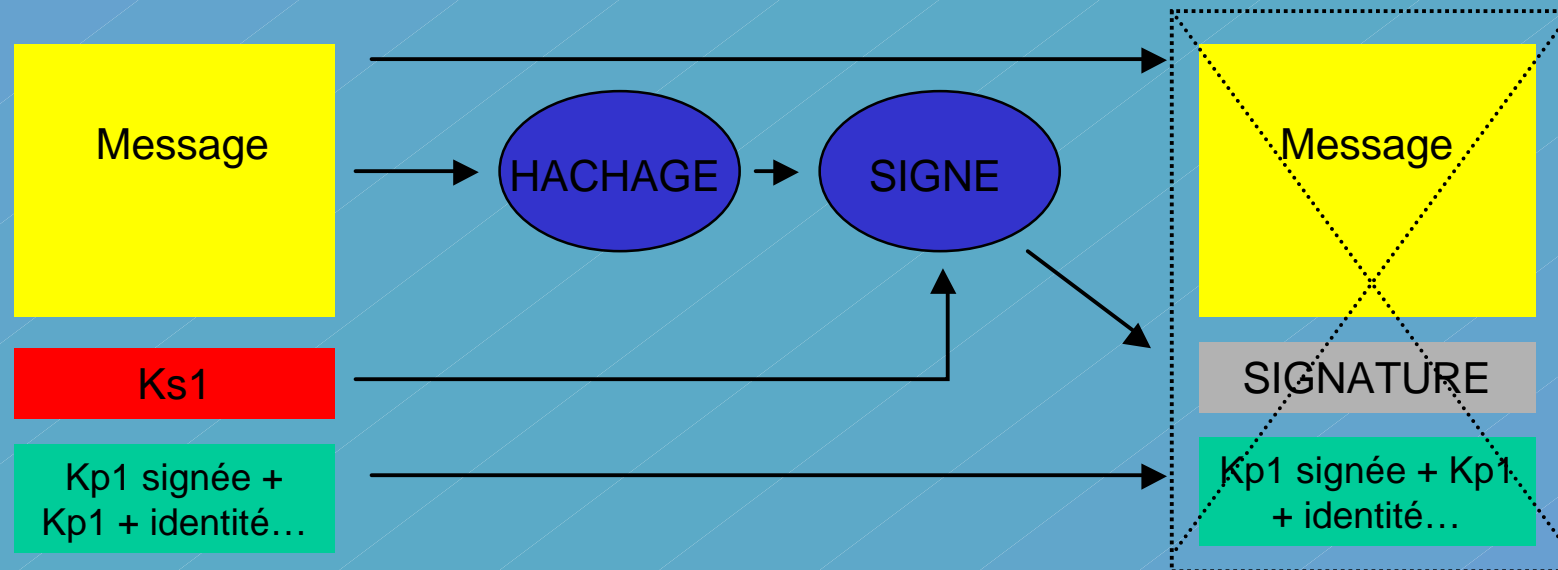
Systeme

Comment faire connaître sa clé publique ?



Systeme

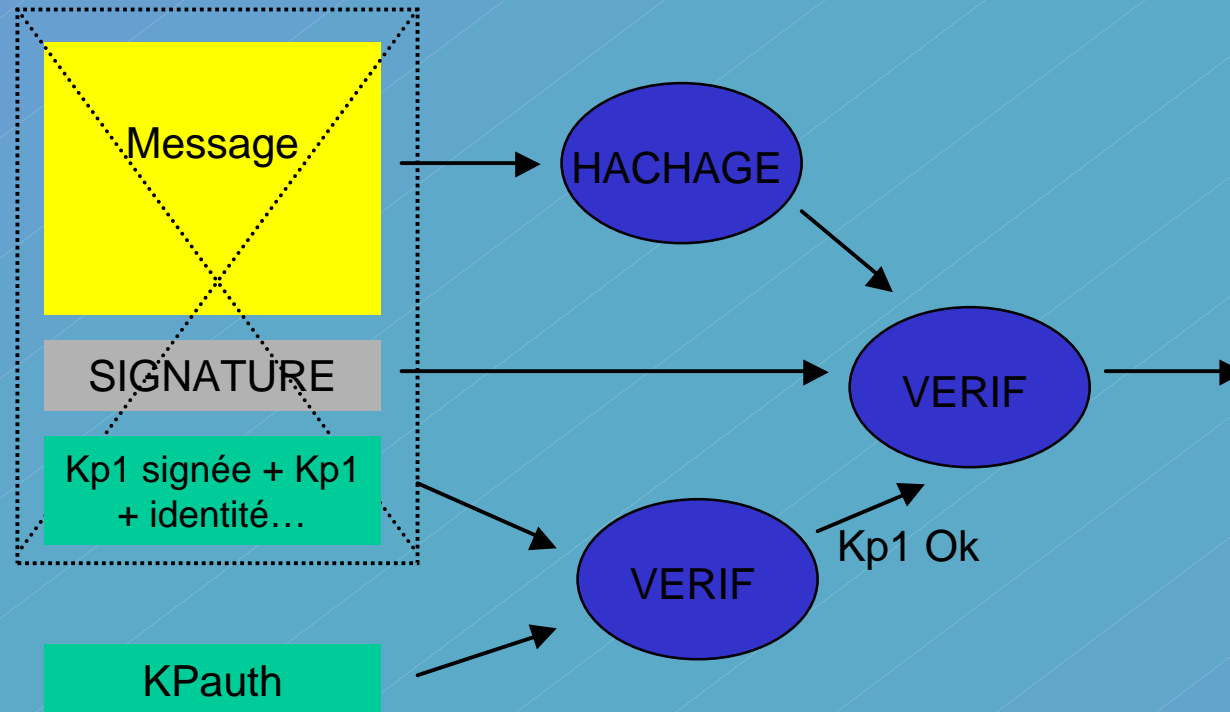
Comment faire connaître sa clé publique ?



EMISSION D'UN MESSAGE

Systeme

Comment faire connaître sa clé publique ?



Si Hash calculé = Hash signé, alors :

Document intègre,
Signature intègre,
KP1 signée intègre,
Kp1 intègre
Identité Ok (Ks1 Ok)

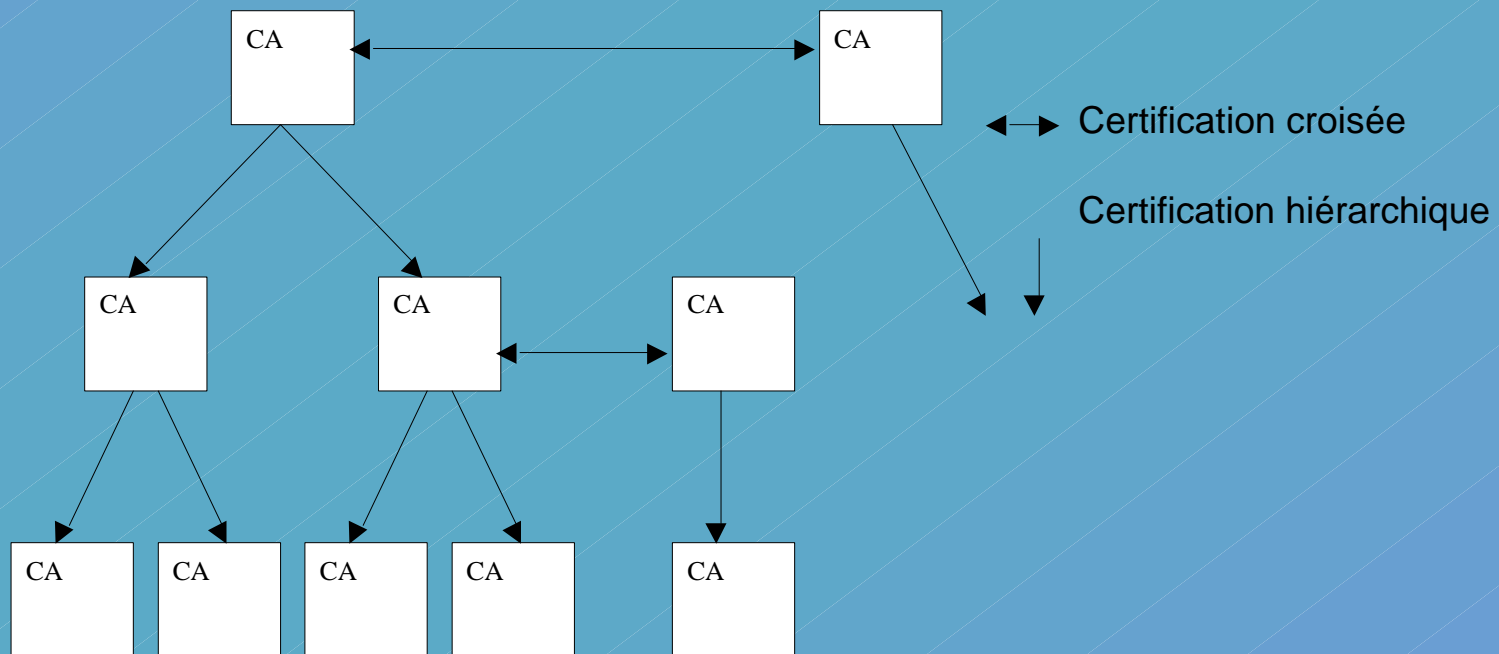
Note : pas besoin
d'annuaire
(théoriquement)

RECEPTION D'UN MESSAGE

Systeme

Comment faire connaître sa clé publique ?

AUTORITES DE CERTIFICATION (AC)



Systeme

Comment se faire connaître de l'AC ?

- En fournissant des éléments de preuve de son identité
- En montrant que l'on connaît la clé privée de la clé publique que l'on fait certifier

Création d'autorités d'enregistrement (AE)

Systeme

Comment disposer d'une clé ?

- En la générant soit même. Mais avec quoi, dans quel environnement, avec quelle confiance ?
- En la faisant générer par un Tiers de Confiance (l'AC par exemple). Comment avoir confiance dans le Tiers de Confiance ?

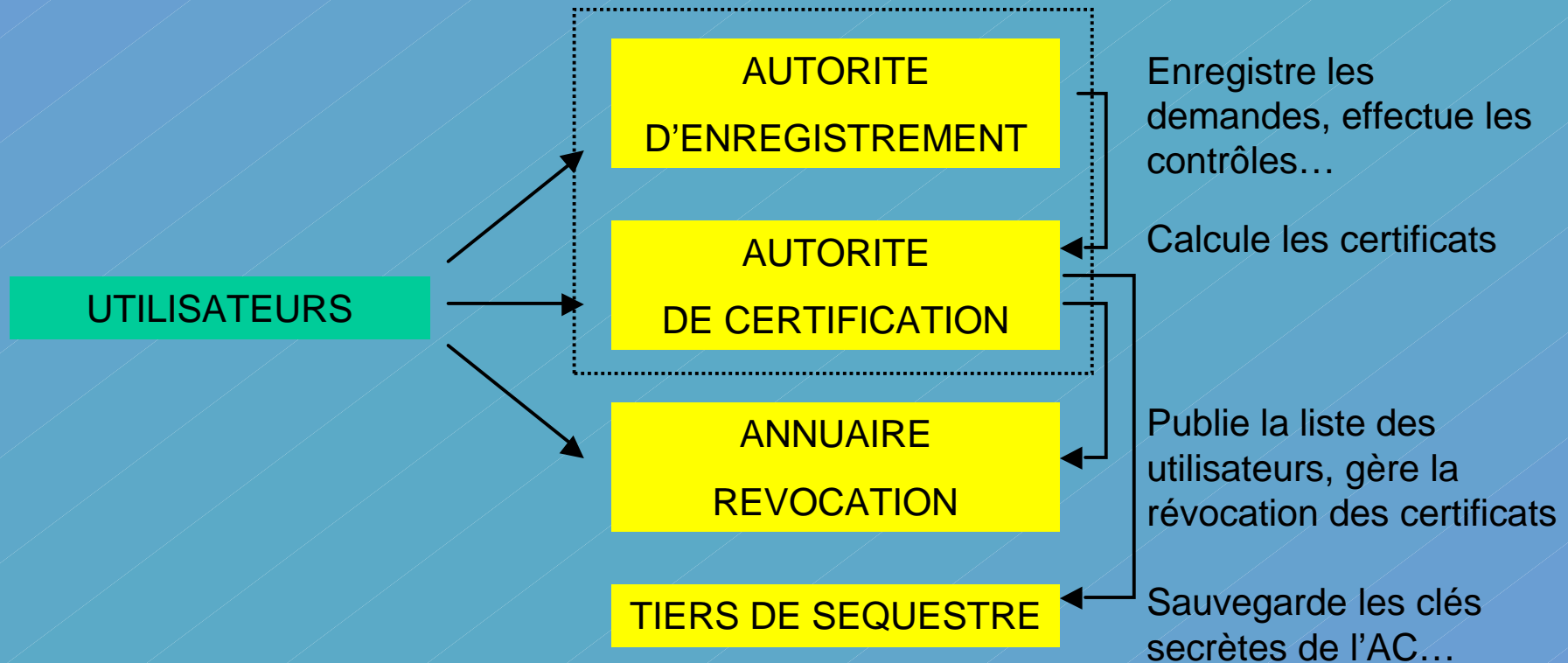
Systeme

Comment faire savoir que sa clé est révoquée ?

- En prévenant soit même tous ses correspondants.
- En publiant cette information sur un serveur (typiquement, un annuaire). Encore faut-il qu'il soit consulté.
- La révocation doit être datée précisément. Il faut faire appel à un Tiers de Confiance d'horodatage.

Systeme

Infrastructure de clés publiques



Reconnaissance

Quelle reconnaissance ?

Contractuelle ?

(carte bancaire, Véridial, Cerdial...)

Légale ?

Reconnaissance

Directive européenne 1999/93/CE

- « **signature électronique** », une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ;
- « **signature électronique avancée** », une signature électronique qui satisfait aux exigences suivantes :
 - a) être liée uniquement au signataire ;
 - b) permettre d'identifier le signataire ;
 - c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
 - d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

Reconnaissance

Directive européenne 1999/93/CE

Les états membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au motif que :

- La signature se présente sous une forme électronique.

Ou

- Qu'elle ne repose pas sur un **certificat qualifié**.

Ou

- Qu'elle ne repose pas sur un certificat qualifié délivré par un **prestataire accrédité de certification**.

Ou

- Qu'elle n'est pas créée par un **dispositif sécurisé de création de signature**.

Reconnaissance

Directive européenne 1999/93/CE

- « **Certificat qualifié** » il comporte les informations disant qu'il est qualifié, il doit comporter l'identité du prestataire de service, le nom ou pseudo du signataire, la possibilité d'inclure la qualité du signataire, l'identification des dates de début et fin de validité du certificat, etc.
- « **Autorités qualifiées (AC qualifiées)** », utilisent des moyens fiables pour la certification, ont une organisation ad'hoc, emploient du personnel qualifié, ont un service d'annuaire rapide, utilisent des ressources crypto sûres, vérifient l'identité du signataire, produisent des certificats qualifiés, etc.
- « **Dispositif sécurisé de création de signature** » : il doit répondre à des exigences de sécurité décrites dans l'annexe III de la directive (génération des clés, confidentialité des clés privées, droits d'accès à la création de la signature, garanties sur l'intégrité des données à signer, etc.).

Reconnaissance

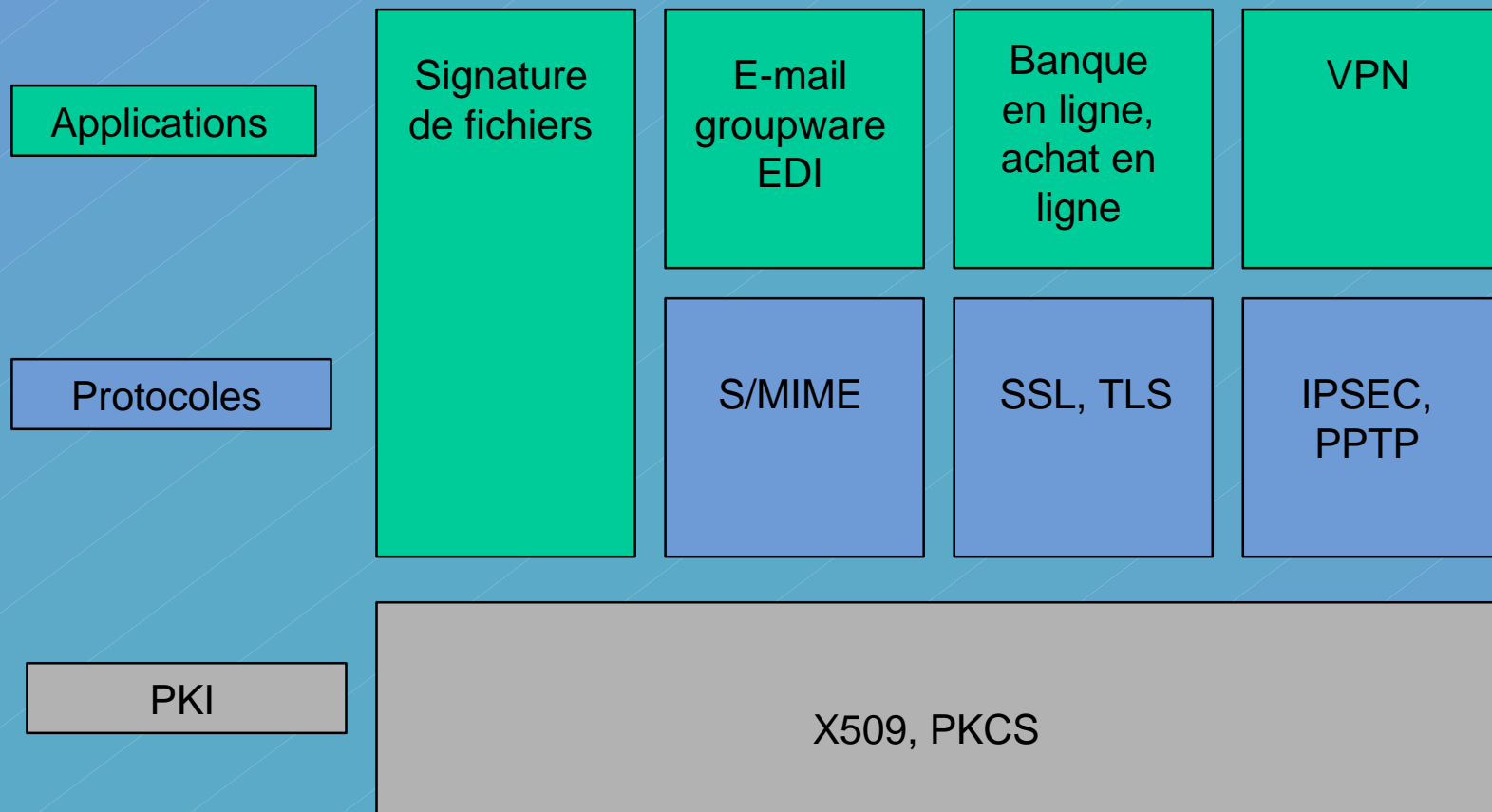
Dans le droit français

« **Décret 2001-272 du 30 Mars 2001** » : il reprend dans les grandes lignes les éléments de la directive européenne.

Il devait être complété par 5 arrêtés. En fait, deux textes devraient voir le jour :

- Un décret lié à la certification des produits qui devrait également se substituer à l'avis de septembre 1995 sur le schéma d'évaluation (*décret du 18 avril 2002 paru au JO du 19 avril 2002*)
- Un arrêté pour la qualification des prestataires de certification

Interopérabilité



Source RSA sécurité

Interopérabilité

PKCS1 : recommandations pour l'implémentation de systèmes crypto utilisant RSA

PKCS3 : échange de clés par Diffie Hellman

PKCS5 : utilisation de mot de passe en cryptographie

PKCS6 : syntaxe pour des certificats étendus

PKCS7 : syntaxe de messages cryptographiques (certificat...)

PKCS8 : syntaxe pour des données mémorisant des clés privés

PKCS10 : syntaxe pour une requête de certification

PKCS11 : API "Cryptoki" pour des équipements qui contiennent des informations cryptographiques et réalisent des fonctions cryptographiques

PKCS12 : syntaxe d'échange d'informations personnelles

etc.

Interopérabilité

Certificat X509

- N° de version du certificat (correspondant à la version de la norme : valeur 2 pour X509V3)
- N° de série : n° de série du certificat pour une AC donnée
- Signature : signature de l'AC pour authentifier le certificat
- Emetteur : nom de l'AC qui a créé le certificat
- Validité : date de début et date de fin du certificat
- Sujet : nom de l'abonné
- Clé publique : clé publique de l'abonné et identifiant de l'algorithme utilisé
- Extensions...

Interopérabilité

Travaux de l'ETSI

- **TS 101 773** : formats des signatures électroniques et format des politiques de signature.
- **TS 101 861** : profil du protocole d'horodatage (se base sur la RFC correspondante de l'IETF).
- **TS 101 862** : profil d'un format de certificat qualifié
- **TS 101 953** : format de signature en XML
- **TS 101 733** : formats de signature électronique

Interopérabilité

Travaux de l'IETF

- **RFC 3039** : Internet X.509 Infrastructure à clé publique
Profil de certificat qualifié
- **RFC 3126** : Formats de signature électronique pour des signatures électroniques à long terme
- **RFC 31XX** : Protocole d'horodatage

Confiance

produits

Les produits sensibles

- Ressources crypto de la PKI (génération de clés de l'AC (et des utilisateurs éventuellement), génération d'aléas...).
- Ressources crypto de génération de clé des utilisateurs, calcul de la signature.
- Application de création de signature (que signe-t-on ?).

Confiance

Produits – critères d'évaluation

M. Hilarion Lefuneste

4, rue Tillante

66000 Pèse

Cher ami,

J'étais hier chez ton imbécile de voisin qui avait organisé une soirée au profit des comtes et barons nécessaires. Se trouvait là l'inénarrable Virgule de Guillemet qui a organisée la collecte de vieux blasons, titre de noblesses et autres babioles.

Ton voisin Talon a placé un de ses discours pompeux et suffisant dont il a le secret. Je comprends que tu ais quelques difficultés à supporter ce personnage gras et libidineux, au physique comme au moral.

Reçoit toute mon amitié.

Vincent Poursan.

M Achille Talon

2, rue Tillante

66000 Pèse

Monsieur cher ami,

Je tiens à vous remercier pour votre sympathique soirée et souhaite pouvoir vous rendre la pareille prochainement

Dans l'attente de votre présence à notre réunion des voisins de quartier qui se déroulera dans quelques semaines, je vous prie de croire, cher ami, à mes sentiments les meilleurs.

Votre dévoué

Confiance

Produits – critères d'évaluation

Hilarion Lefuneste

4, rue Tillante

66000 Pse

Cher ami,

Jtais hier chez ton imbcile de voisin qui avait organis une soire au profit des comtes et barons ncessiteux. Se trouvait l linnarrable Virgule de Guillemet qui a organise la collecte de vieux blasons, titre de noblesses et autres babioles. Ton voisin Talon a plac un de ses discours pompeux et suffisant dont il a le secret. Je comprends que tu ais quelques difficults supporter ce personnage gras et libidineux, au physique comme au moral.

Reoit toute mon amiti.

Vincent Poursan.

@\$NormalmH2A@2Police par dfautz +,-./BCjkly| :OPQR]^XY&'@AR""Runkno...

XY&'@AR>^tvxz|

M Achille Talon

2, rue Tillante

66000 Pse

Monsieur cher ami,

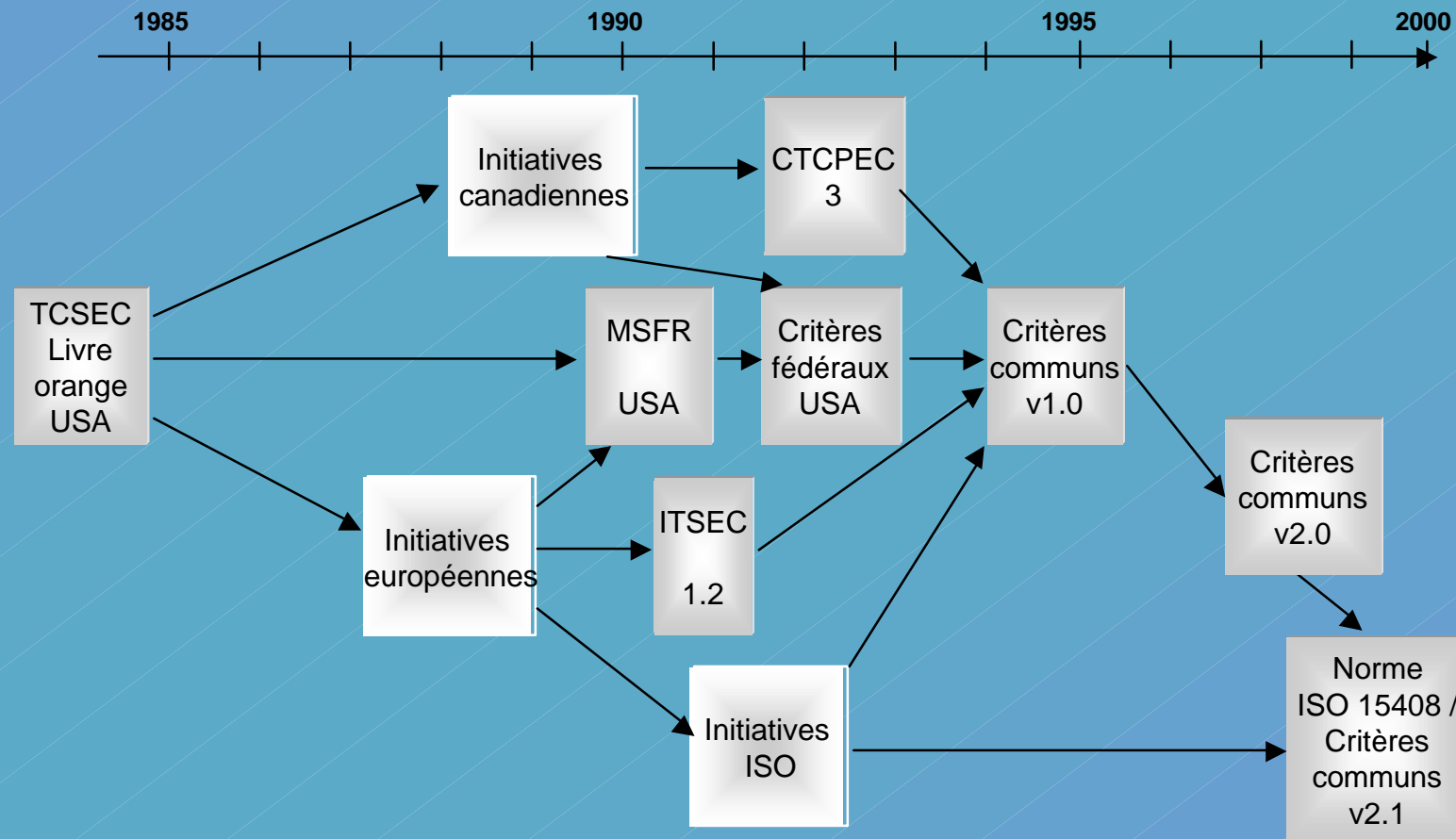
Je tiens vous remercier pour votre sympathique sauterie soire et souhaite pouvoir vous rendre la pareille prochainement Dans l attente de votre prsence notre runion des voisins de quartierqui se droulera dans quelques semaine, je vous prie de croire, cher ami, mes sentiments les meilleurs.

Votre dvou

@\$NormalmH2A@2Police par dfaut +,-./BCstu""RUnknownAQLPC148PC1%C:\Me

Confiance

Produits – critères d'évaluation



Confiance

Produits – critères d'évaluation

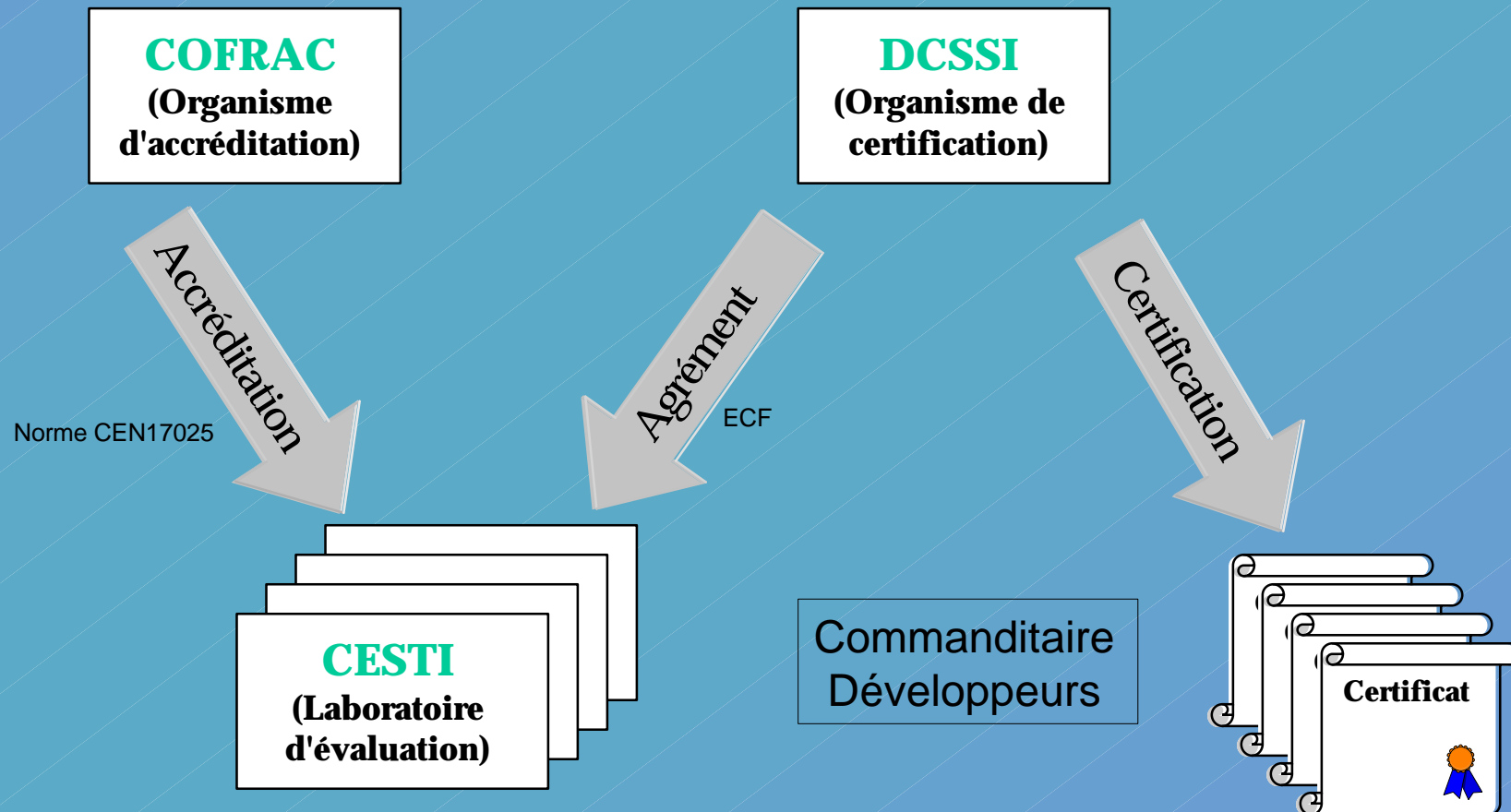
- ◆ Critères normalisés par l'ISO, successeurs des ITSEC (critères européens) et TCSEC (critères américains),
- ◆ Approche connue et normalisée,
- ◆ Schéma garantissant les critères de reproductibilité, impartialité, répétabilité et objectivité

Certification avec reconnaissance internationale

Confiance

Produits – critères d'évaluation

Schéma français d'évaluation



Confiance

Produits – critères d'évaluation

Quelques caractéristiques des CC

- Sept niveaux de confiance (EAL1 à EAL7), 3 niveaux de résistance des mécanismes de sécurité (élémentaire, moyen élevé).
- Possibilité d'avoir des Profils de Protection (PP = spécification de besoin générique)
- Possibilité d'évaluer des produits (carte à mémoire, logiciel de chiffrement, firewall...) et des systèmes (ensemble de produits, évaluation au niveau EAL1 généralement)

La résistance des mécanismes crypto est réalisée à part (en France, par la DCSSI)

Confiance

Produits – critères d'évaluation

Au niveau européen, orientation vers l'utilisation d'un SSCD (Secure Signature Creation Device) pour la production de signatures avancées.

- Doit être évalué EAL4 ou EAL4+
- Ne doit pas autoriser la duplication des clés privées,
- Doit s'inscrire dans un système de production sûre de clés privés (idéalement, le SSCD produit les clés)

CWA 14168 : PP SSCD niveau EAL4

CWA 14169 : PP SSCD niveau EAL4+

Confiance

Services

Les services sensibles

- Tiers de confiance et en particulier, autorités de certification
- Valeur et validité des certificats
- Horodatages
- ...

Confiance

Services

Travaux du CEN/ISSS, ETSI, IETF...

- **CWA 14171** : Procedures for Electronic Signature Verification (normes minimales pour la vérification de signatures avancées ou qualifiées au niveau du logiciel client)
- **TS 101 456** : règles de gestion et des politiques de certification pour des fournisseurs de services de certification délivrant des certificats qualifiés.
- **RFC 3125** : Politiques de signature électroniques
- **CWA 14167** : Security requirements for trustworthy systems & products (fonctionnalités exigées pour les produits cryptographiques des fournisseurs de services de certification)
- Etc.

Confiance

Services

Au niveau européen, orientation vers un schéma de « qualification » des CA (non obligatoire)

- Certification basée sur TS101456 dérivée de BS7799 (ou ISO17799)
 - ⇒ il faut disposer d'un schéma de certification (COFRAC)
 - ⇒ il faut disposer d'organismes de certification
 - ⇒ audit essentiellement organisationnel et assez superficiel
 - ⇒ confiance limitée, coût peu élevé

Confiance

Services



COFRAC
(Organisme
d'accréditation)



?

Schéma de certification prévu

**Organismes
certifiés**

Apporter la preuve de la mise
en œuvre
d'un système de gestion
de la sécurité de l'information
(ISMS)

ISO 45012

Accréditation

Agrement

Audit

**Organismes
certificateurs**



Certificat



Confiance

Schéma global

