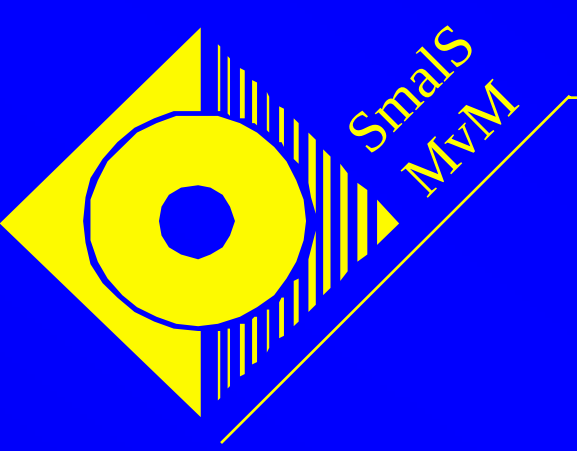


SIGNATURE DIGITALE ET AUTHENTIFICATION FORTE

Michel Laloy

18/06/2002

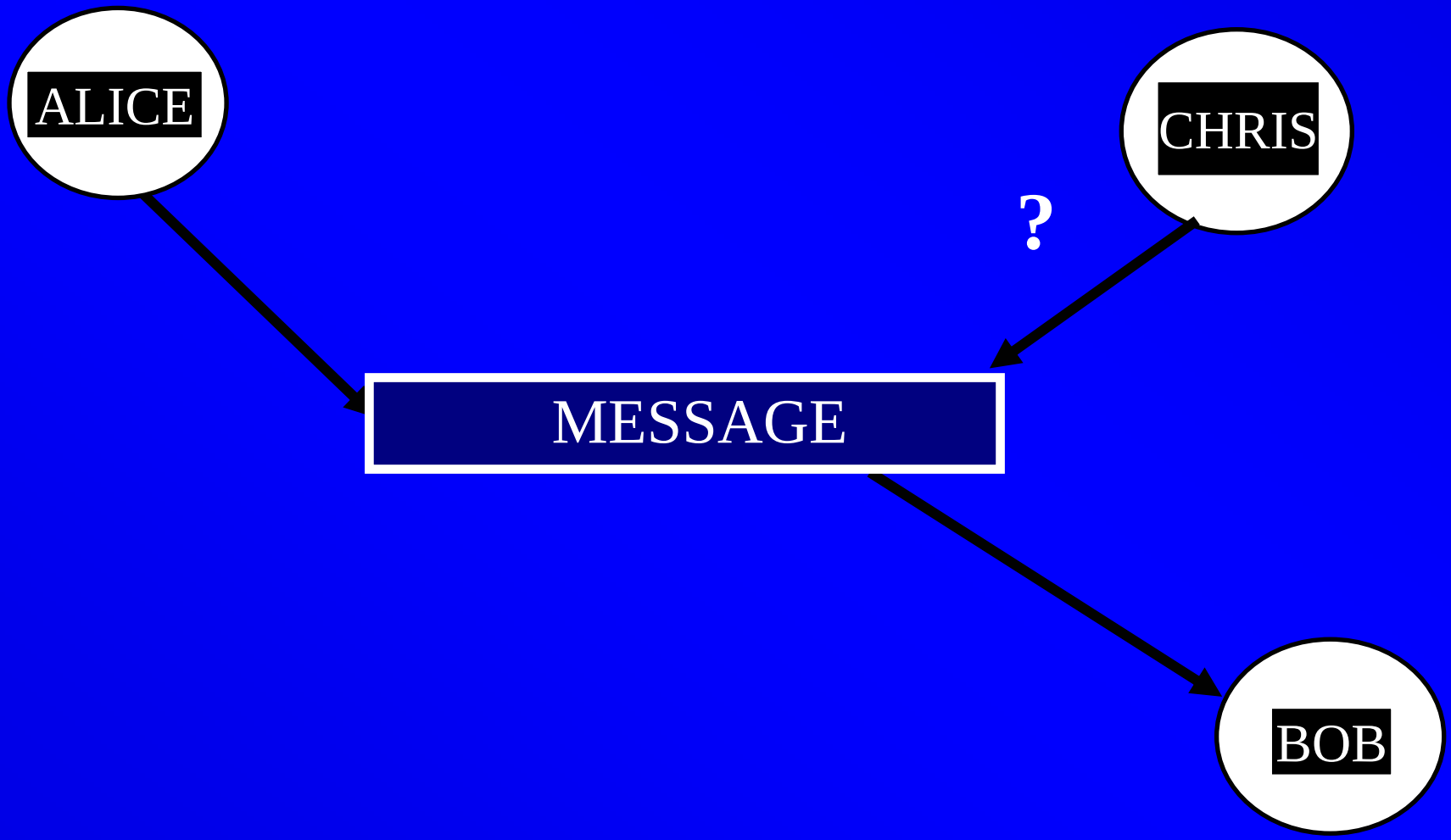
Objectifs

- Expliquer les mécanismes de la signature digitale et de l'authentification forte
- Montrer comment ces mécanismes s'appliquent dans le contexte de l'e-government

Contenu

- Concepts et méthodes. Rôle de la cryptographie
- Les certificats digitaux et les systèmes PKI
- Applications sur Internet
- Le contexte de l'e-government et de la sécurité sociale en Belgique
- Conclusions

Sécurité des transferts électroniques



Transfert de données : garanties attendues (1)

1. **Authentification de l'émetteur (par le destinataire)**
2. **Authentification du destinataire (par l'émetteur)**
3. **Intégrité du message**
4. **Confidentialité**
5. **Non répudiation par l'émetteur**
6. **Non répudiation par le destinataire**

! Indépendamment du mode de transport

Transfert de données : garanties attendues (2)

- **Authentification** :
  on vérifie si l'émetteur (le destinataire) est bien celui qu'il prétend être

- **Non répudiation par l'émetteur** :
  Alice ne peut pas prétendre :
  a. qu'elle n'a pas envoyé de données à Bob
  b. que les données que Bob affirme avoir reçues sont différentes des données qu'elle a envoyées

Transfert de données : garanties attendues (3)

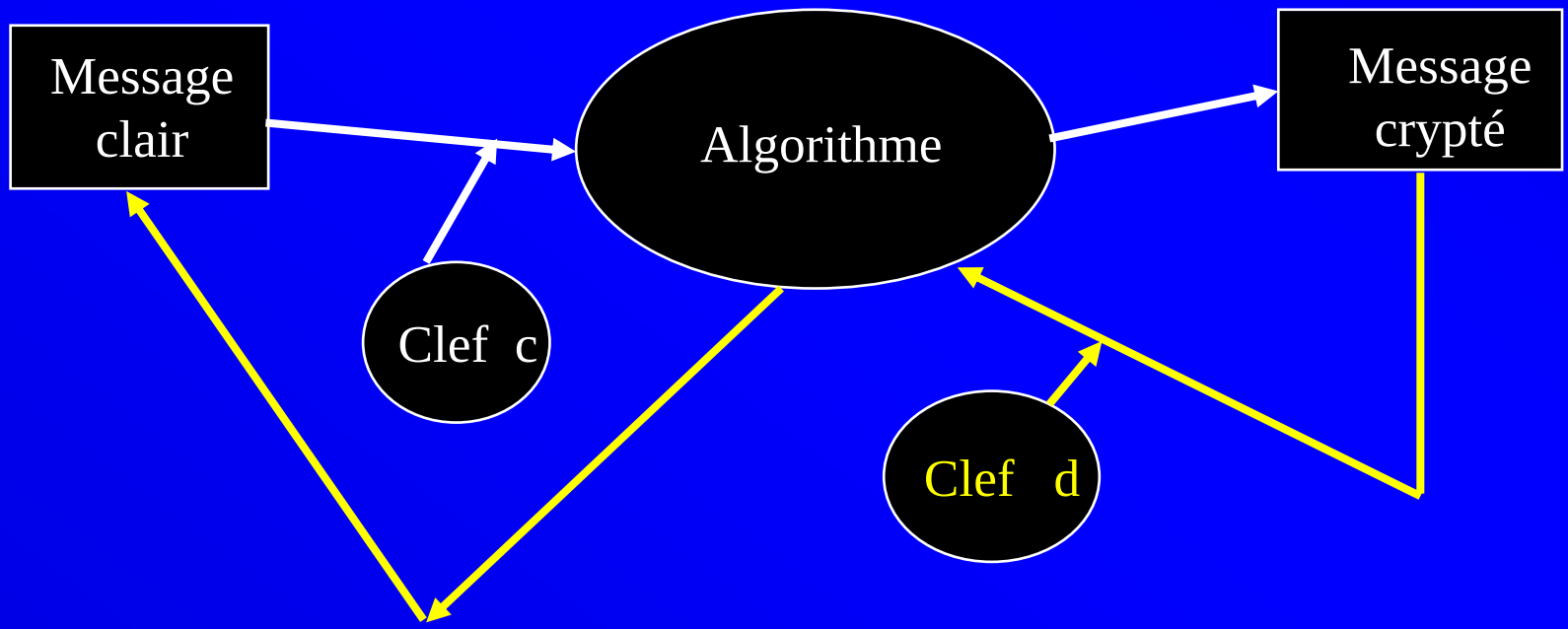
Moyens d'assurer les garanties pour les transfert 'papier' :

- authentif. de l'émetteur : signature (manuelle)
- authentif. du destinataire : lettre recommandée
- confidentialité : lettre scellée
- contrôle d'intégrité :
  paraphes des sections modifiées
- non-répudiation par l'émetteur : sign. manuelle
- non-répudiation par le destinataire :
  lettre recommandée avec avis de réception

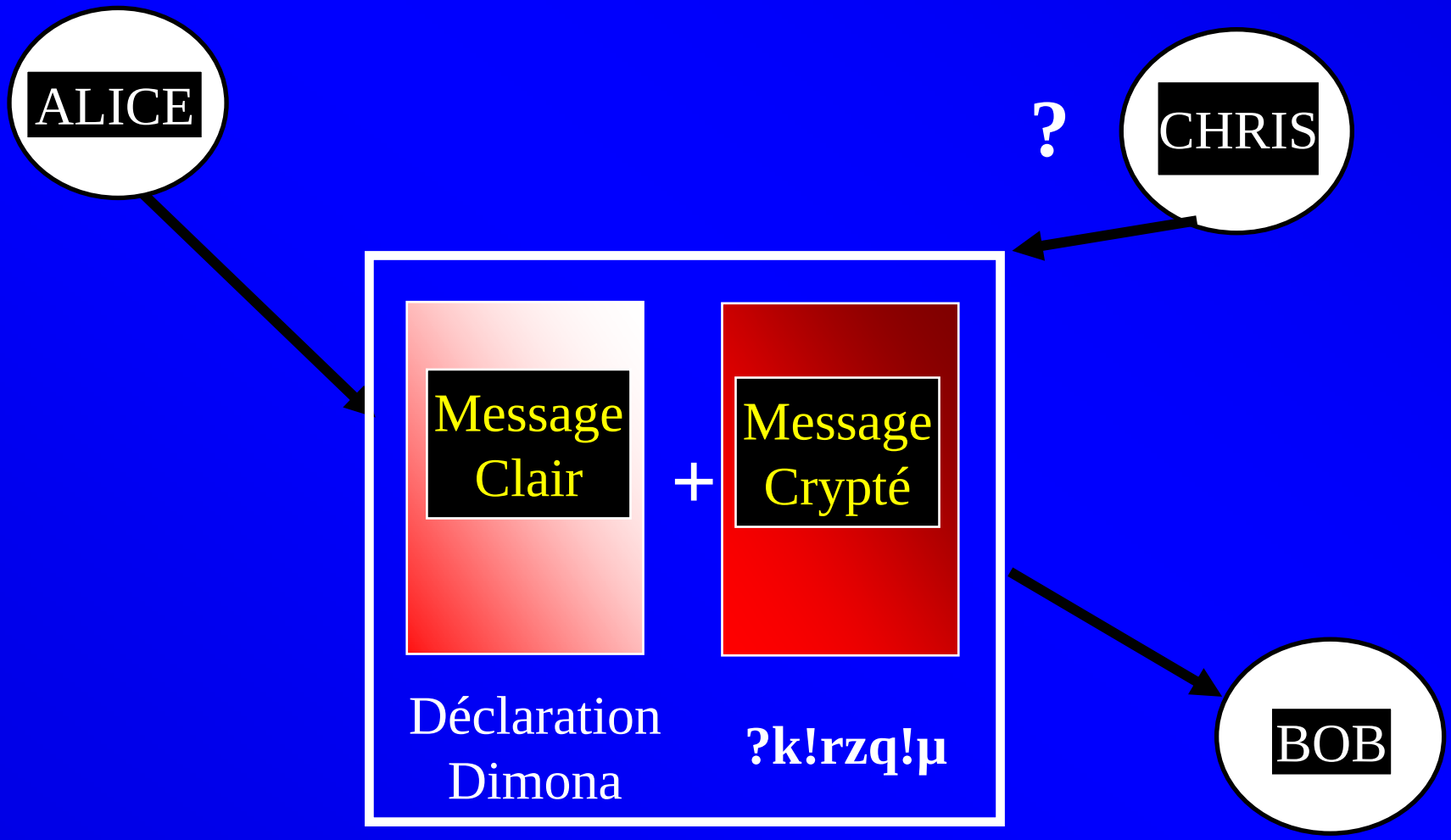
Transfert de données : garanties attendues (4)

Moyens d'assurer les garanties pour les transferts électroniques :

La cryptographie



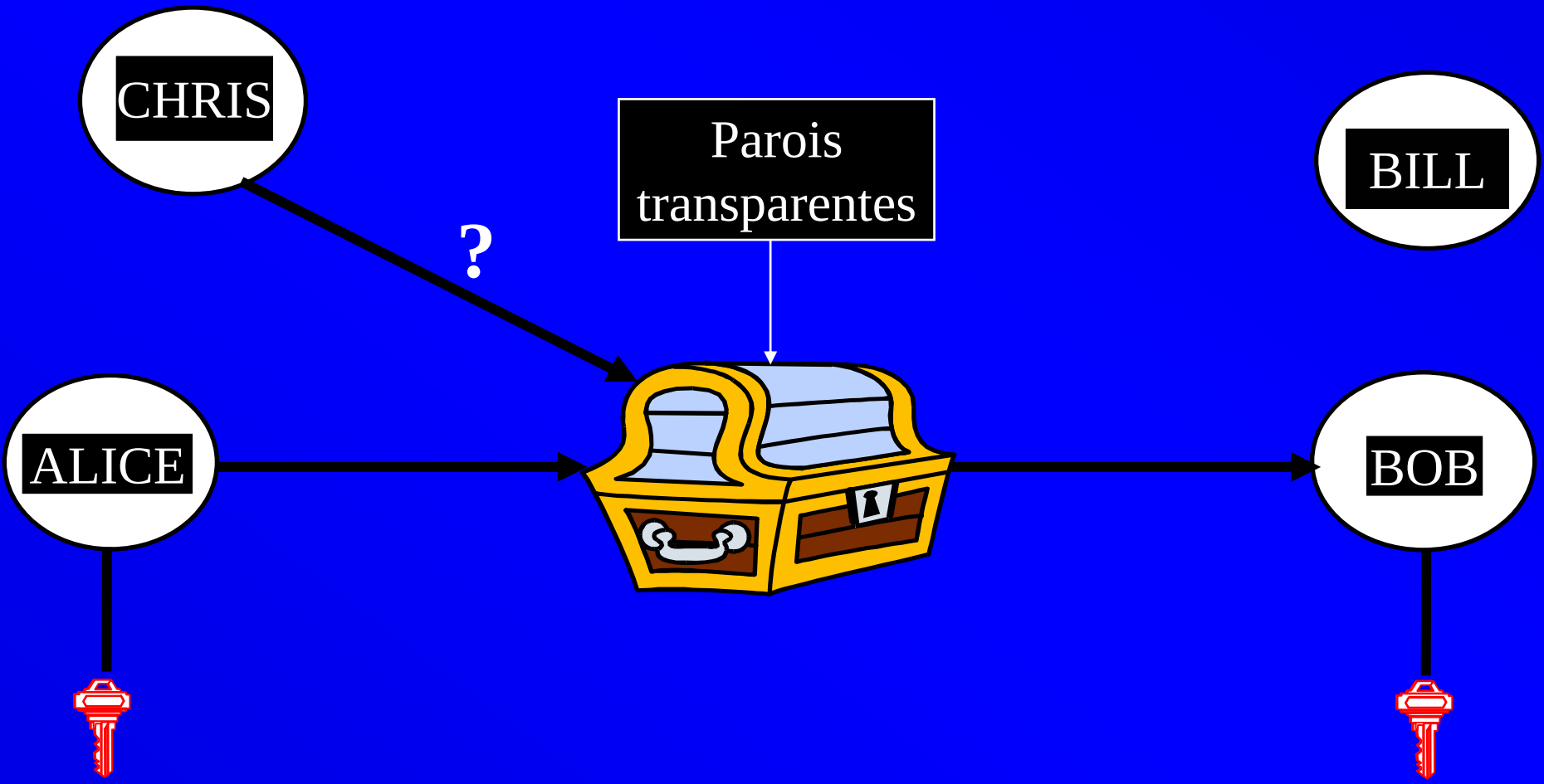
Méthodes cryptographiques (1)



Méthodes cryptographiques (2)

- ALICE crypte le message clair
  (ALICE utilise une clef de cryptage)
- BOB décrypte le message crypté
  (BOB utilise une clef de décryptage)
- BOB réussit le décryptage s'il obtient le message clair envoyé par ALICE
- Si clef de cryptage = clef de décryptage : cryptographie symétrique
- Sinon : cryptographie asymétrique

Cryptographie symétrique (1)



Cryptographie symétrique (2)

Authentification de l'émetteur et contrôle d'intégrité :

La clef dont dispose BOB ne permet d'ouvrir le coffret que s'il a été fermé au moyen de la clef d'ALICE

Donc :

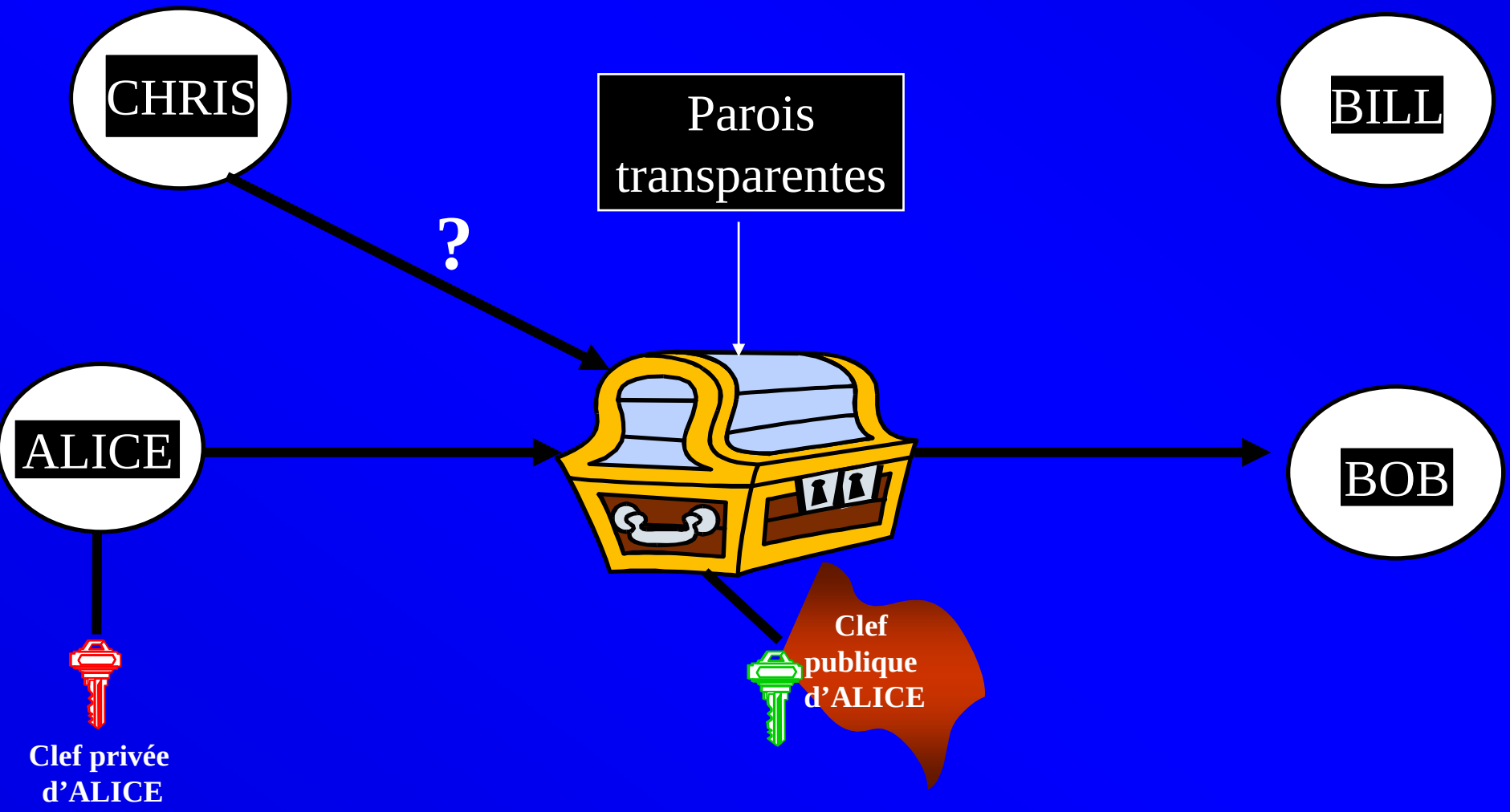
- **si BOB réussit à ouvrir le coffret, il authentifie ALICE**
- **si CHRIS ouvre le coffret pour modifier le message, il ne pourra pas le refermer avec la clef d'ALICE (clef qu'il ne possède pas), et donc BOB ne pourra pas ouvrir le coffret**

Cryptographie symétrique (3)

Garantit l'authentification de l'émetteur et l'intégrité. Mais :

1. Point faible : ALICE doit communiquer au préalable la clef secrète à BOB (et à lui seul)
2. Point faible : Multiplication des secrets ALICE a besoin d'un secret pour chaque destinataire
3. Point faible : comme BOB connaît la clef secrète, il peut modifier le message à posteriori. **Alice peut répudier le message !**

Cryptographie asymétrique (1)



Cryptographie asymétrique (2)

Authentification de l'émetteur :

- **La clef publique d'ALICE ne permet d'ouvrir le coffret que s'il a été fermé au moyen de la clef privée d'ALICE :**
- **donc, si BOB réussit à ouvrir le coffret au moyen de la clef publique d'ALICE, il authentifie ALICE**

Cryptographie asymétrique (3)

Garantit l'authentification de l'émetteur et de plus :

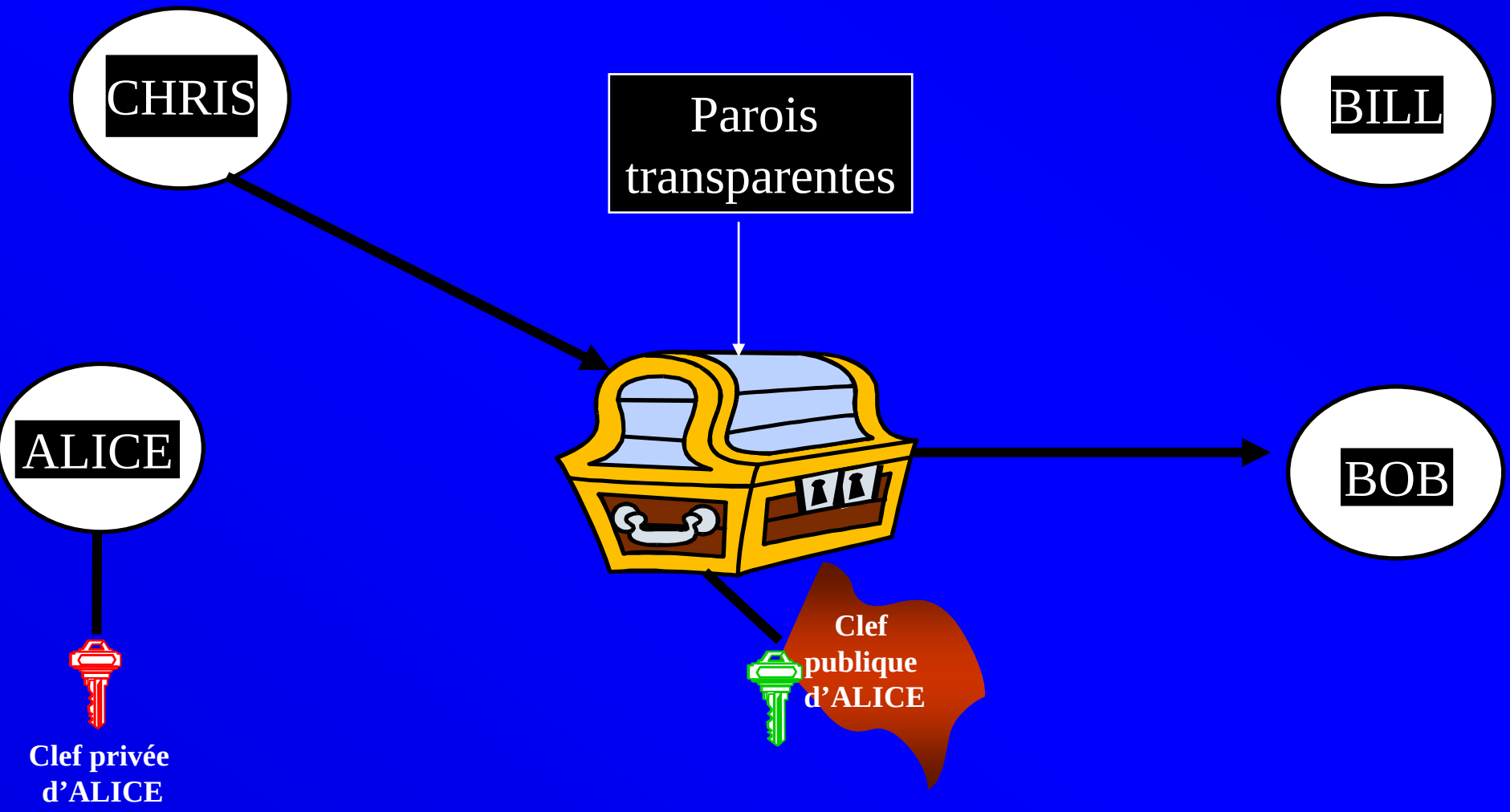
1. **Le secret (la clef privée) ne quitte pas ALICE : authentification FORTE**

2. **La même clef privée permet à ALICE de s'authentifier auprès de n'importe quel BOB (il suffit à BOB de disposer de la clef publique d'ALICE)**

Garantit l'intégrité et la non-répudiation par l'émetteur : voir plus loin...

Cryptographie asymétrique (4)

Possibilité de fraude ?



Cryptographie asymétrique (5)

PROBLEME ET SOLUTION

- Fraude possible : CHRIS envoie un coffret et sa propre clef publique en prétendant que c'est la clef publique d'ALICE
- Résultat : CHRIS se fait passer pour ALICE auprès de BOB
- Solution : **LES CERTIFICATS**

Cryptographie asymétrique (6)

Un certificat établit un lien entre la clef publique et l'identité du titulaire

CA = Autorité de Certification

Cryptographie asymétrique (7)

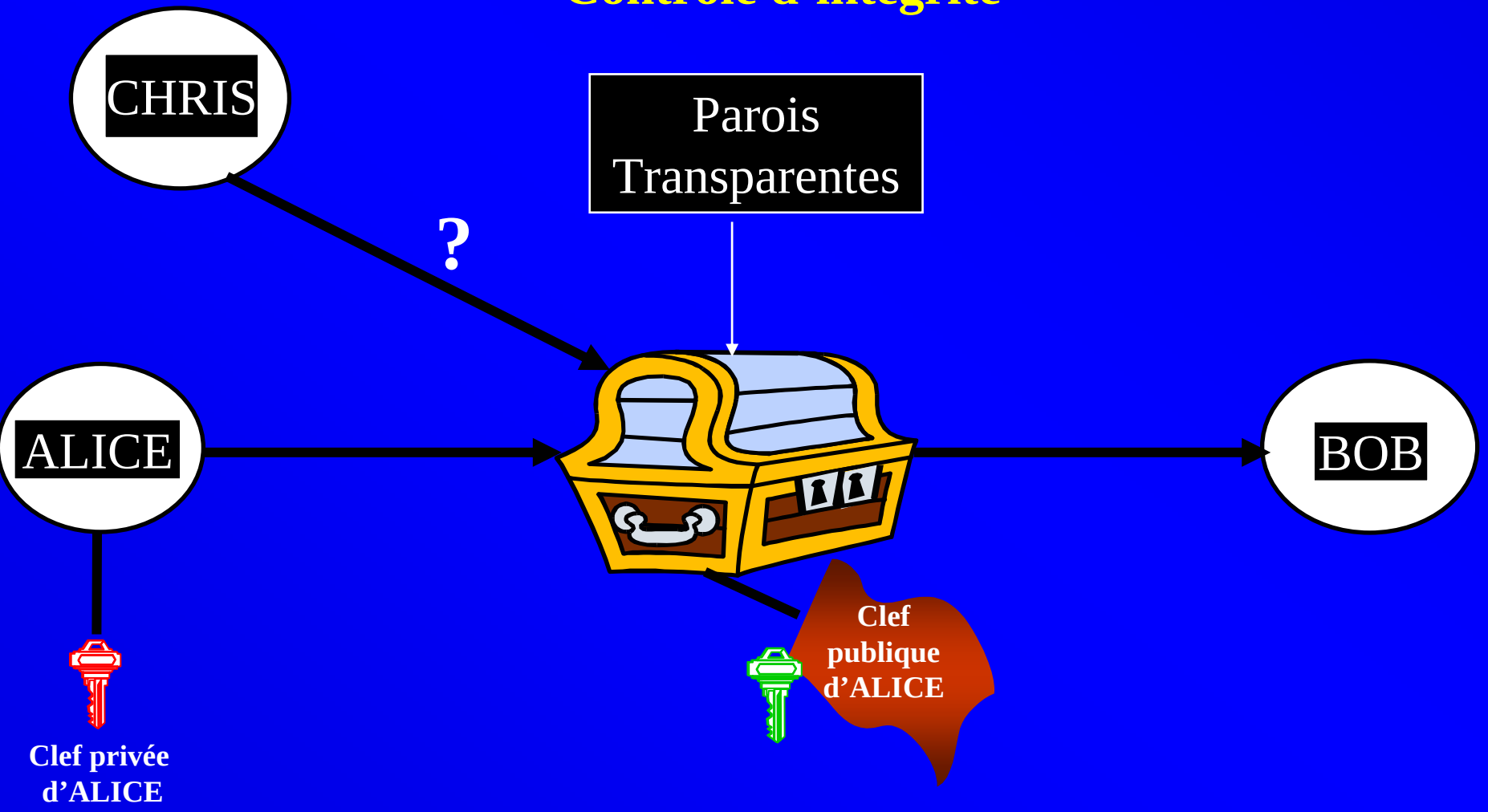
PROBLEME : Un certificat est-il falsifiable ?

Comment empêcher CHRIS de fabriquer un faux certificat (qui contiendrait sa propre clef publique mais indiquerait ALICE comme titulaire) ?

Réponse : voir plus loin

Cryptographie asymétrique (8)

Contrôle d'intégrité



Cryptographie asymétrique (9)

Contrôle d'intégrité :

- **La clef publique d'ALICE ne permet d'ouvrir le coffret que s'il a été fermé au moyen de la clef privée d'ALICE : si CHRIS ouvre le coffret pour modifier le message, il ne pourra pas le refermer avec la clef privée d'ALICE (clef qu'il ne possède pas), et donc BOB ne pourra pas ouvrir le coffret**

Cryptographie asymétrique (10)

La cryptographie asymétrique garantit aussi la non-répudiation par l'émetteur :

Si BOB a reçu un message d'ALICE, ALICE ne peut pas prétendre ne pas avoir envoyé de message ou avoir envoyé un message différent du message reçu par BOB. En effet :

Cryptographie asymétrique (11)

Comme BOB ne possède pas la clef privée d'ALICE, il ne peut pas créer un message, ou modifier un message après réception, et présenter ce message créé ou modifié comme étant un message envoyé par ALICE

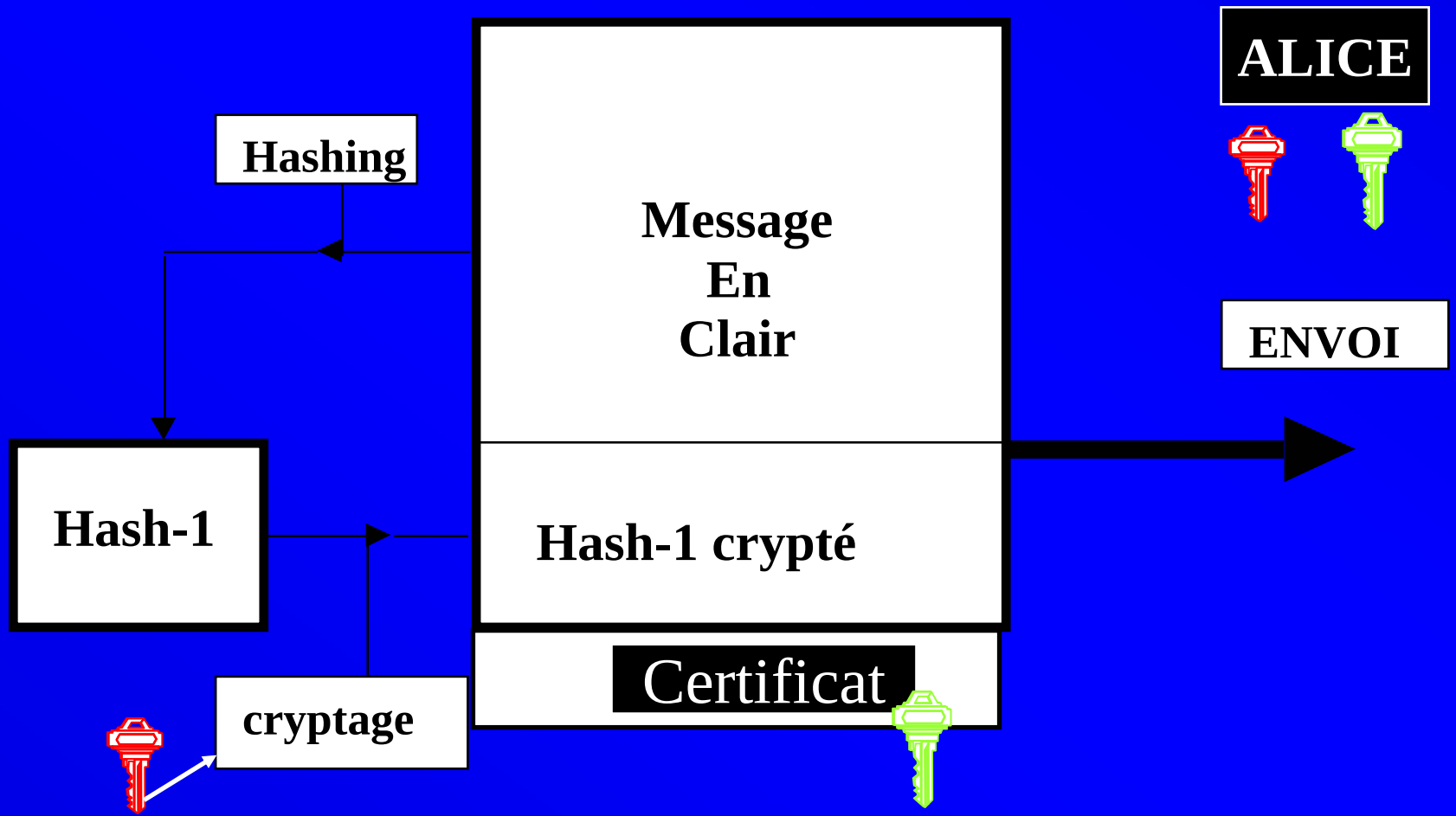
Cryptographie asymétrique (12)

- PROBLEME : Il n'est pas possible de mettre un message trop long dans le coffret (traduction : le cryptage asymétrique d'un long message prend trop de temps)
- SOLUTION : Résumer le message avant de le mettre dans le coffret (traduction : on **hashe** le message avant de le crypter = on produit un **digest** de ce message)
- Longueur typique d'un digest : 128 ou 160 bits
- Le hashing joue aussi un autre rôle...

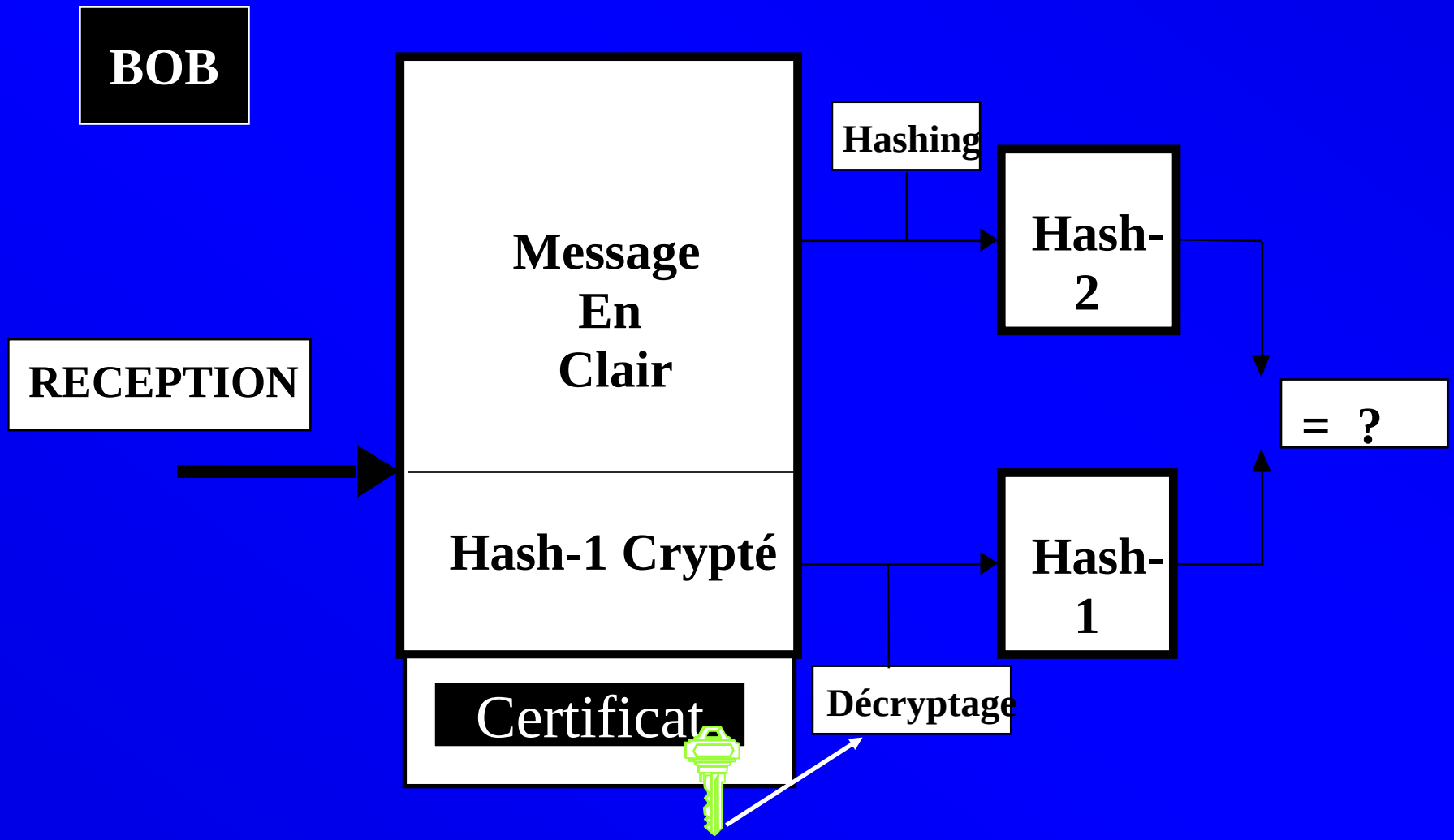
La signature digitale (1)

- La signature digitale d'un message (d'un document) est le résultat du cryptage asymétrique d'un digest du message (du document)
- Pour signer digitalement un document (pour apposer sa signature digitale), ALICE produit un digest de ce document et crypte ce digest avec sa clef privée
- BOB doit vérifier la signature et valider le certificat d'ALICE

La signature digitale (2)



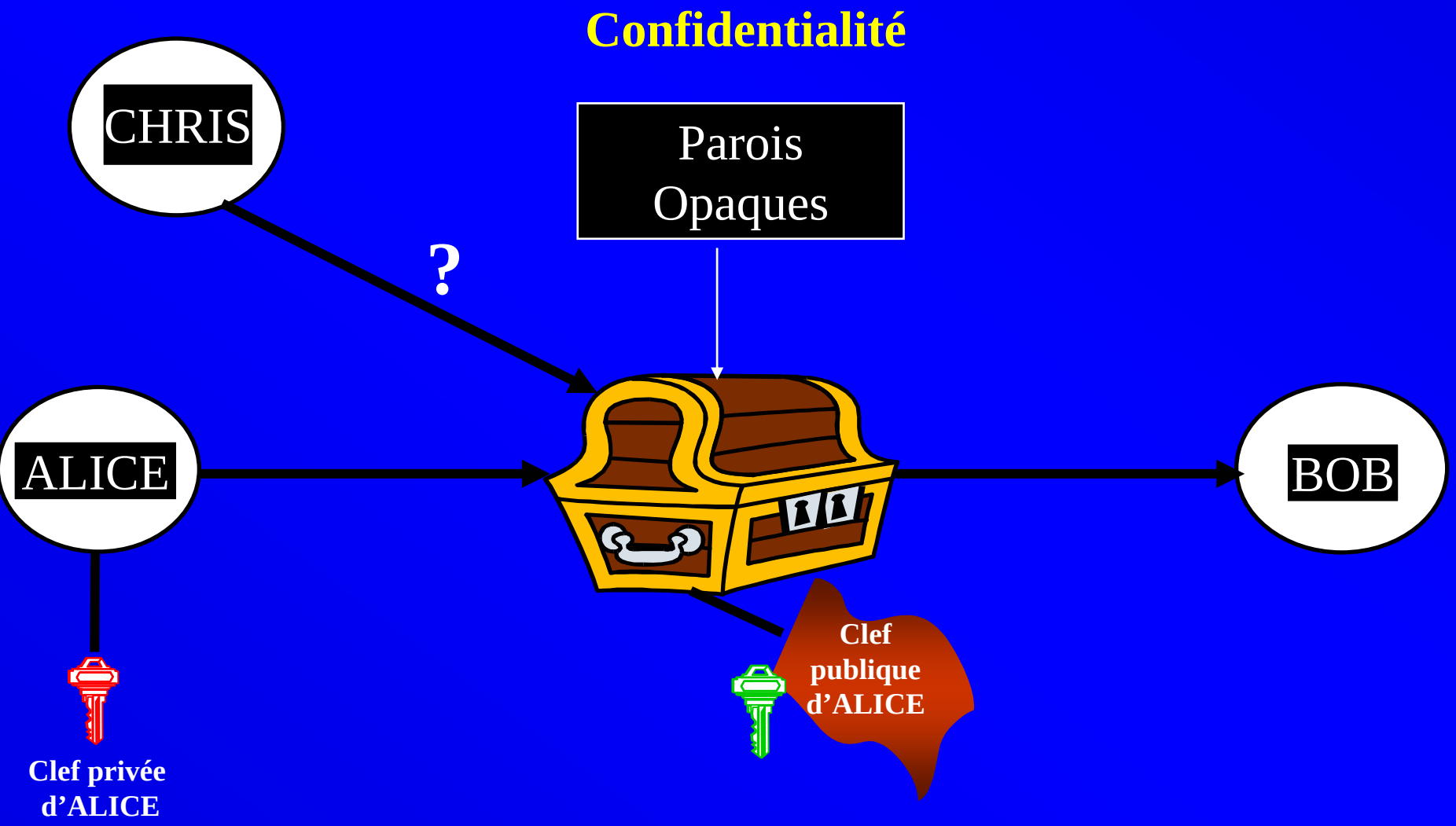
La signature digitale (3)



Signature digitale et confidentialité (1)

- Dans la signature digitale, le cryptage sert uniquement à l'authentification, au contrôle d'intégrité et à la non-répudiation , pas à la confidentialité
- On peut ajouter une étape de cryptage additionnelle pour garantir la confidentialité ; on dit alors que l'on procède à la signature et au chiffrement

Signature digitale et confidentialité (2)



Les certificats (1)
Pas de falsification !

Un certificat établit un lien entre la clef publique et l'identité du titulaire

La signature du CA garantit l'intégrité du certificat

CA = Autorité de Certification

Certificats normalisés X.509

Les certificats (2)
Les chaînes

Identité: CA Sigbel

Clef publique de CA: 4a 543...

Validité : 1/1/2001 - 31/12/2005

Certificat de CA #: 31

Emetteur: super CA Sigsup

Signature du super CA Sigsup

Identité: Alice

Clef publique: 9f 0a 3..

Validité : 1/1/2001 - 31/12/2002

Certificat #: 123465

Emetteur: CA Sigbel

Signature du CA Sigbel

Chaîne de certificats

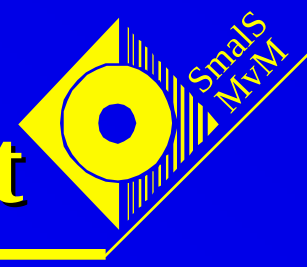
Les certificats (3)
Le certificat racine

Identité: **super** CA Sigsup
Clef publique de CA: z?67u...
Validité : 1/1/2001 - 31/12/2007
Certificat de CA #: 23
Emetteur: super CA Sigsup
Signature du super CA Sigsup

Identité: CA Sigbel
Clef publique: 4a 543...
Validité : 1/1/2001 - 31/12/2005
Certificat #: 31
Emetteur: super CA Sigsup
Signature du super CA Sigsup

Root Certificate

Les certificats (4)
Les autorités d'enregistrement



Question : **Même si le certificat d'ALICE est valide, comment BOB peut-il être sûr que la personne à laquelle le CA a attribué le certificat d'ALICE est bien ALICE et non pas CHRIS se faisant passer pour ALICE ?**

Réponse : **ALICE doit introduire sa demande de certificat via une AUTORITE D'ENREGISTREMENT (RA)**

Les certificats (5)
La protection des clefs privées

Question : **Comment BOB est-il sûr que la personne qui signe en utilisant la clef privée d'ALICE est bien ALICE et non pas quelqu'un qui lui a volé sa clef privée ?**

Réponse : **BOB doit être convaincu qu'ALICE protège correctement sa clef privée**

Les certificats (6)
La protection des clefs privées

Principe de base :

la clef privée ne devrait jamais être chargée en mémoire

- **Exemple de dispositif pour un poste individuel de signature : clef privée sur smart card, protégée par pincode (ou par biométrie…) : le processus de signature s'exécute sur la carte**
- **Dispositifs plus sophistiqués pour serveurs de signature (par exemple serveur ONSS qui signe les réponses aux déclarations)**

Les certificats (7)
Les informations de révocation

Question : Que se passe-t-il si ALICE craint que CHRIS ne lui ait volé sa clef privée ?

Réponse : Elle doit révoquer sa clef publique et donc son certificat

Question : Comment BOB peut-il savoir que le certificat d'ALICE est révoqué ?

Réponse : Le CA doit publier les informations de révocation (par exemple des CRL=Certificate Revocation Lists ou via OCSP=On-line Certificate Status Protocol)

Les certificats (8)
Question de confiance ?

LES CAs DE CONFIANCE

BOB fait-il confiance dans le CA utilisé par ALICE et dans les CA 'supérieurs' ?

Confiance basée notamment sur les CPS (Certification Practice Statement)

Comment BOB exprime-t-il sa confiance en un CA ? En insérant le certificat de CA (et ceux des CA ‘supérieurs’ jusqu’au certificat racine) dans une ‘liste de confiance’

Les certificats (9)
Question de confiance ?

- Exemple d'implémentation des listes de confiance : Microsoft IE : 'magasin de certificats' utilisé par le browser et la messagerie
- Exemples d'autorités de Certification (CA) : Certipost, Globalsign, Isabel
- Certificats d'authentification et de signature stockés sur la carte d'identité électronique

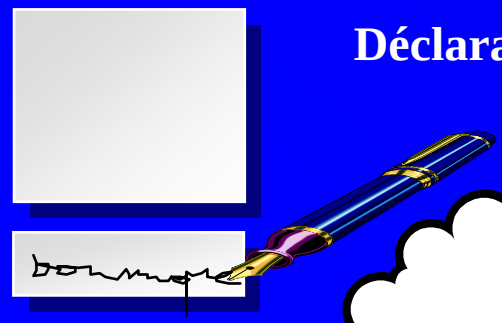
Systèmes PKI

- Un RA ou un ensemble de RAs et une chaîne de CAs constituent une infrastructure de clefs publiques (système PKI)
- Certipost, GlobalSign, Isabel ont établi des systèmes PKI
- PROBLEME : interopérabilité des systèmes PKI

Quelques risques liés à la signature digitale

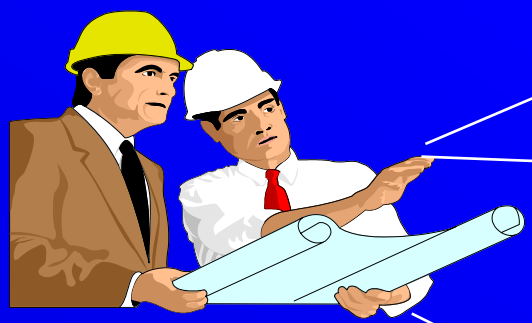
- **Calcul de la clef privée à partir de la clef publique : considéré comme ‘pratiquement impossible si on utilise des clefs suffisamment longues’ (plus longues que 512 bits)**
- **Vol de la clef privée : mesures de protection de la clef privée**
- **Le titulaire de la paire de clefs n’est pas la personne que l ’on croit : règles de bonne pratique des autorités de certification et d ’enregistrement**

Signature digitale et sécurité sociale : DIMONA



Déclaration

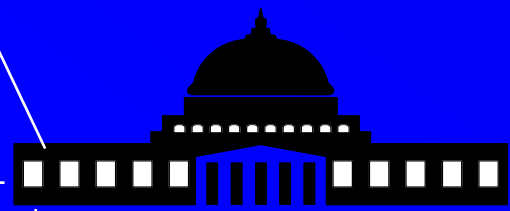
Employeur ou mandataire



FTP

Isabel

ONSS/RSZ



Internet

Exemples classiques d'applications de la sig.dig.

- La messagerie sécurisée S/MIME
- La signature de formulaires

La messagerie sécurisée (1)

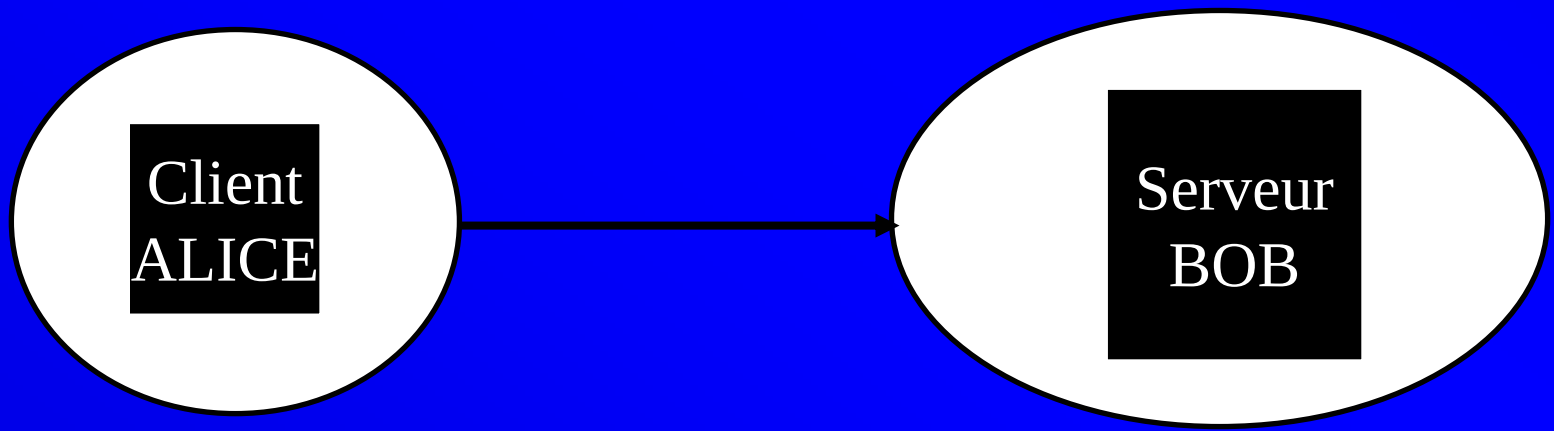
- Interopérabilité des messageries compatibles S/MIME (Microsoft Outlook, Netscape Communicator, Lotus Notes, …)
- Prudence quant au niveau de sécurité des versions actuelles des messageries 'grand public'

La messagerie sécurisée (2)

- Risque de validation incomplète par BOB du certificat de l'émetteur (ALICE) : accès optionnel aux informations de révocation
- Risque de mauvaise gestion par BOB de la liste des Autorités de Certification auxquelles il fait confiance

Authentification et autorisation

- Le client et le serveur s'identifient
- Authentification du serveur et du client
- Le serveur autorise le client à accéder à des ressources



Types d'authentification

- Pour s'authentifier auprès du serveur , le client utilise un 'secret' :
  - un mot de passe : authentification dite 'faible'
  - une clef d'un algorithme : authentification dite 'forte'

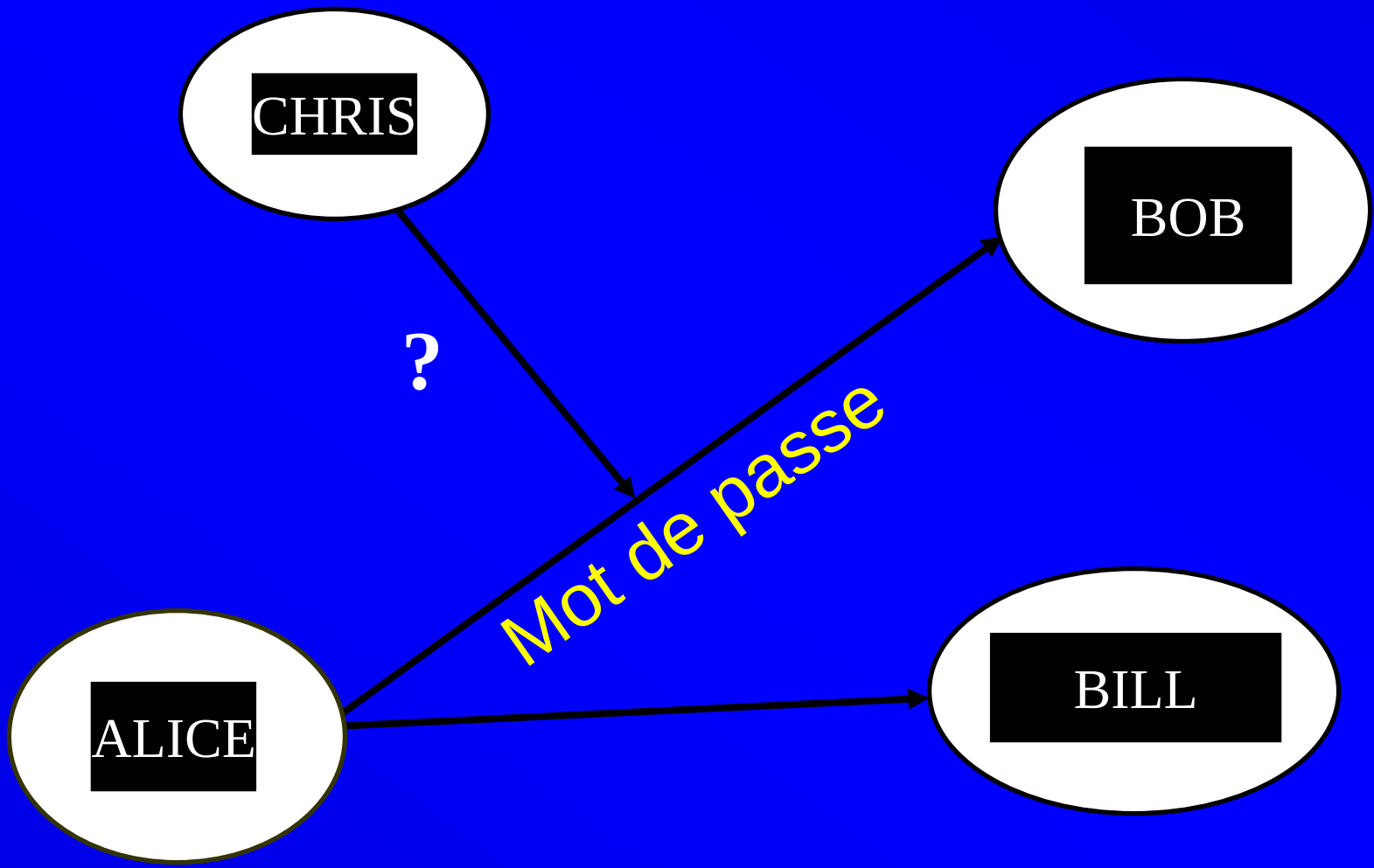
Authentification par mot de passe (1)

ALICE

ID	MOTS DE PASSE	DROITS D'ACCES
ALICE ADELE	xce?12iolrtyui ui?/$^qsd	Lecture DB1 Ecrit/Lect DB2

BOB

Authentification par mot de passe (2)



Authentification par mot de passe (3)

- **POINTS FAIBLES :**
  - **Lors du processus d'authentification, le secret est transmis du client au serveur : risque de 'vol' du secret**
  - **Mauvais choix possibles pour le secret**
  - **Multiplication des secrets : le client dispose d'un mot de passe par serveur**

Authentification par mot de passe (4)

AMELIORATIONS :

- **Single logon : un seul mot de passe pour accéder à plusieurs serveurs**

  Exemple : Kerberos (implémenté dans Windows 2000)

- **Mot de passe 'one time'**

  Exemple : 'secure id' des inspecteurs de l'ONSS

Authentification basée sur un certificat

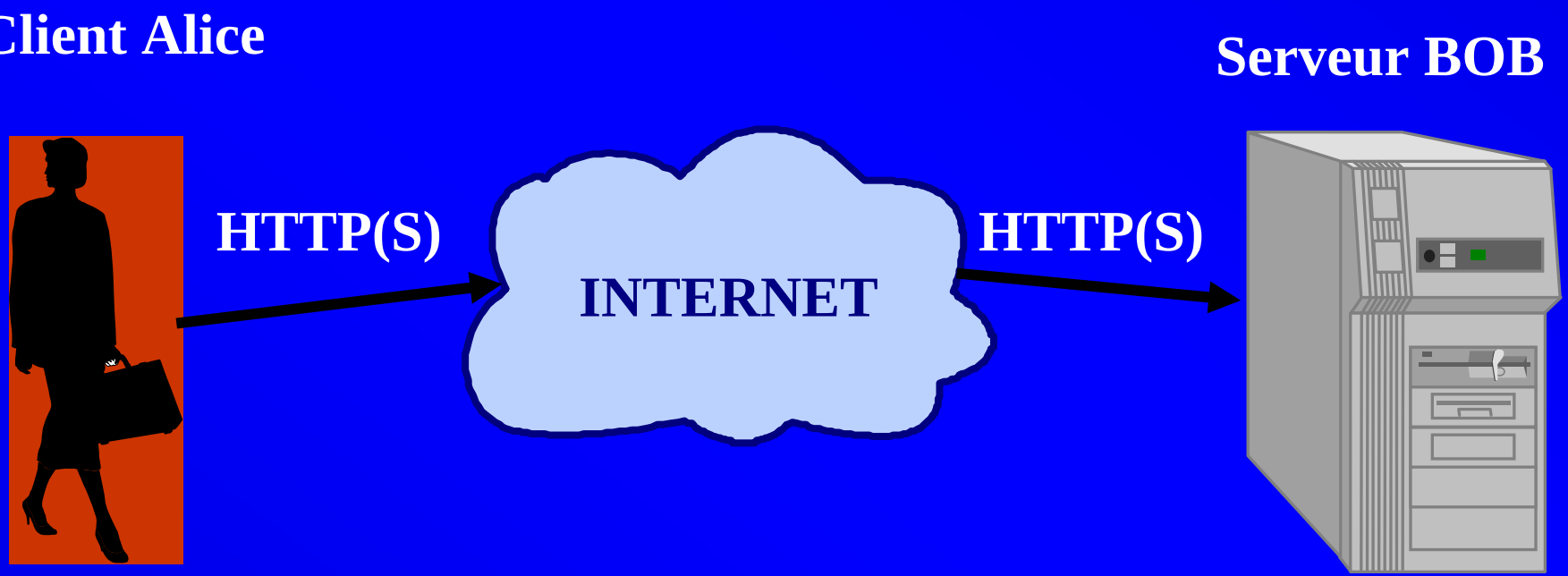
Une autre manière pour ALICE de s ’authentifier auprès du serveur BOB est d ’envoyer un message ‘ aléatoire ’ signé digitalement (accompagné de son certificat ‘ de client ’)

Il s ’agit d ’une authentification forte : le ‘secret ’d ’ALICE ne quitte pas ALICE

La même approche peut être utilisée par BOB pour être authentifié par ALICE : il faut que BOB dispose d ’un ‘ certificat de serveur ’

Ces idées sont implémentées dans le protocole SSL

Le protocole SSL (1)



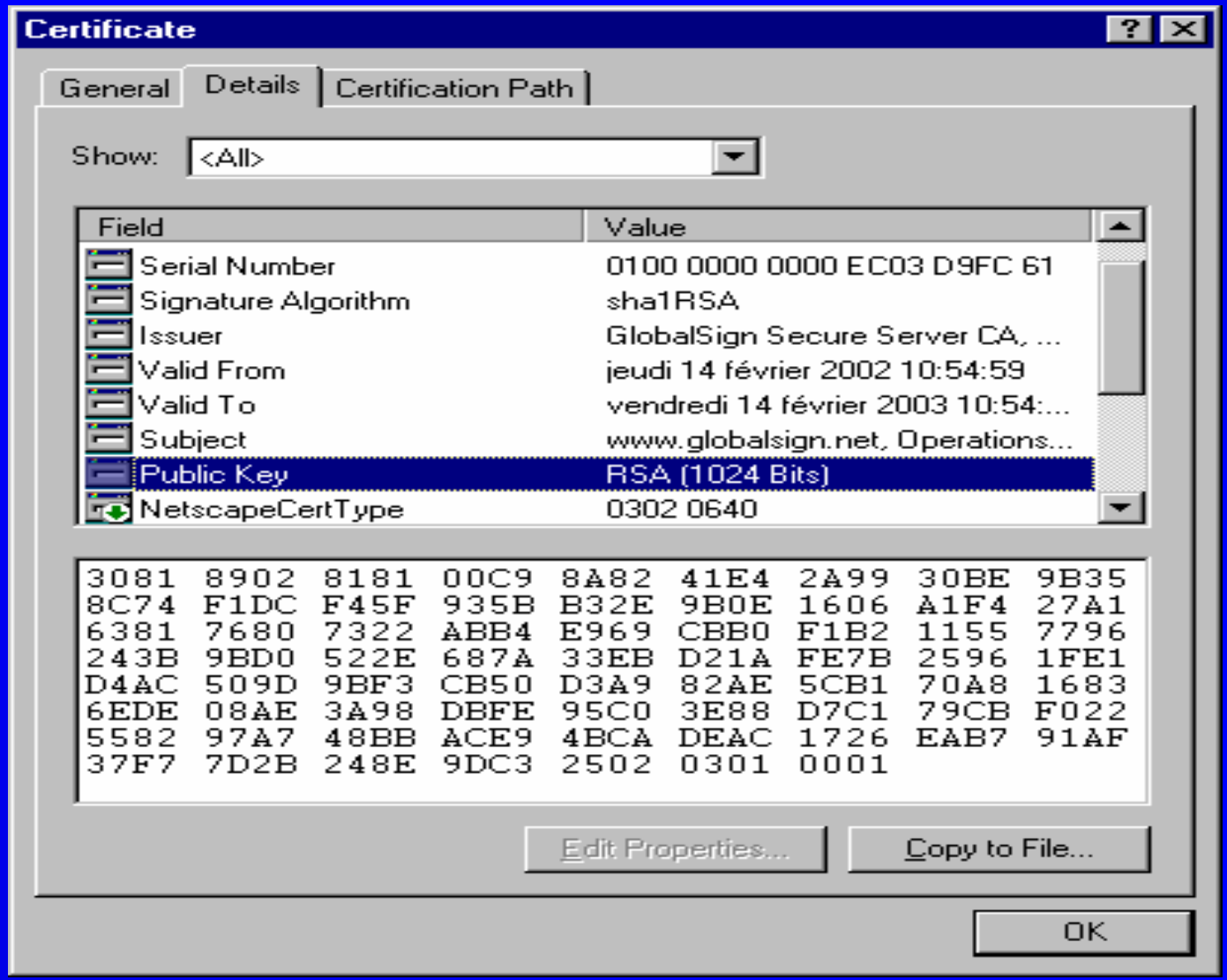
Le protocole SSL (2)

1. Authentification forte (certificat) du serveur
2. Authentification du client : plusieurs options :
   forte (certificat) ou faible (id + mot de passe) ou nulle

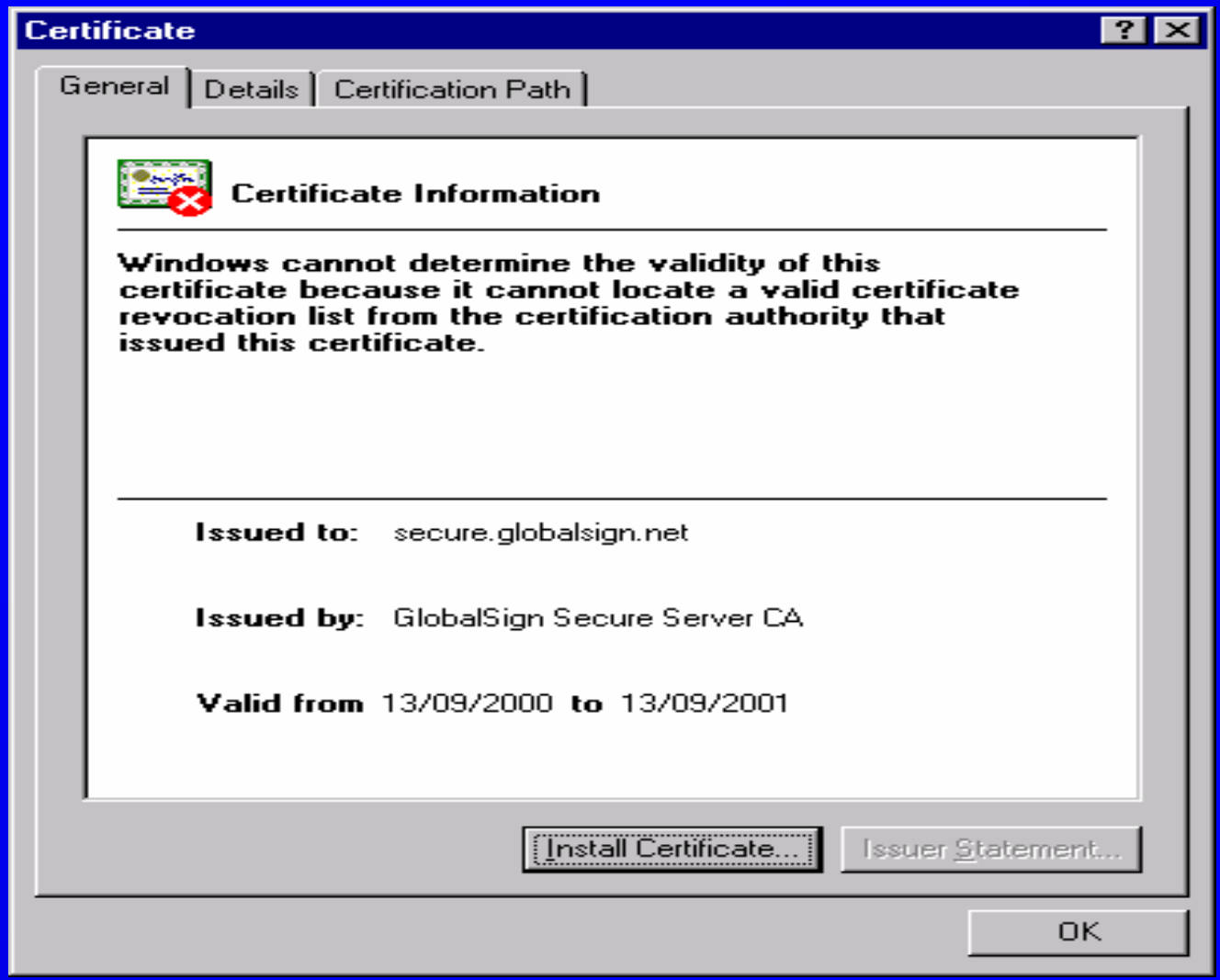
De plus :

3. Confidentialité des échanges
   (y compris id + mot de passe)
4. Intégrité des données échangées
5. Pas de garantie de non-répudiation
   Les données échangées ne sont pas signées par SSL : si nécessaire, l ’émetteur doit les signer en plus

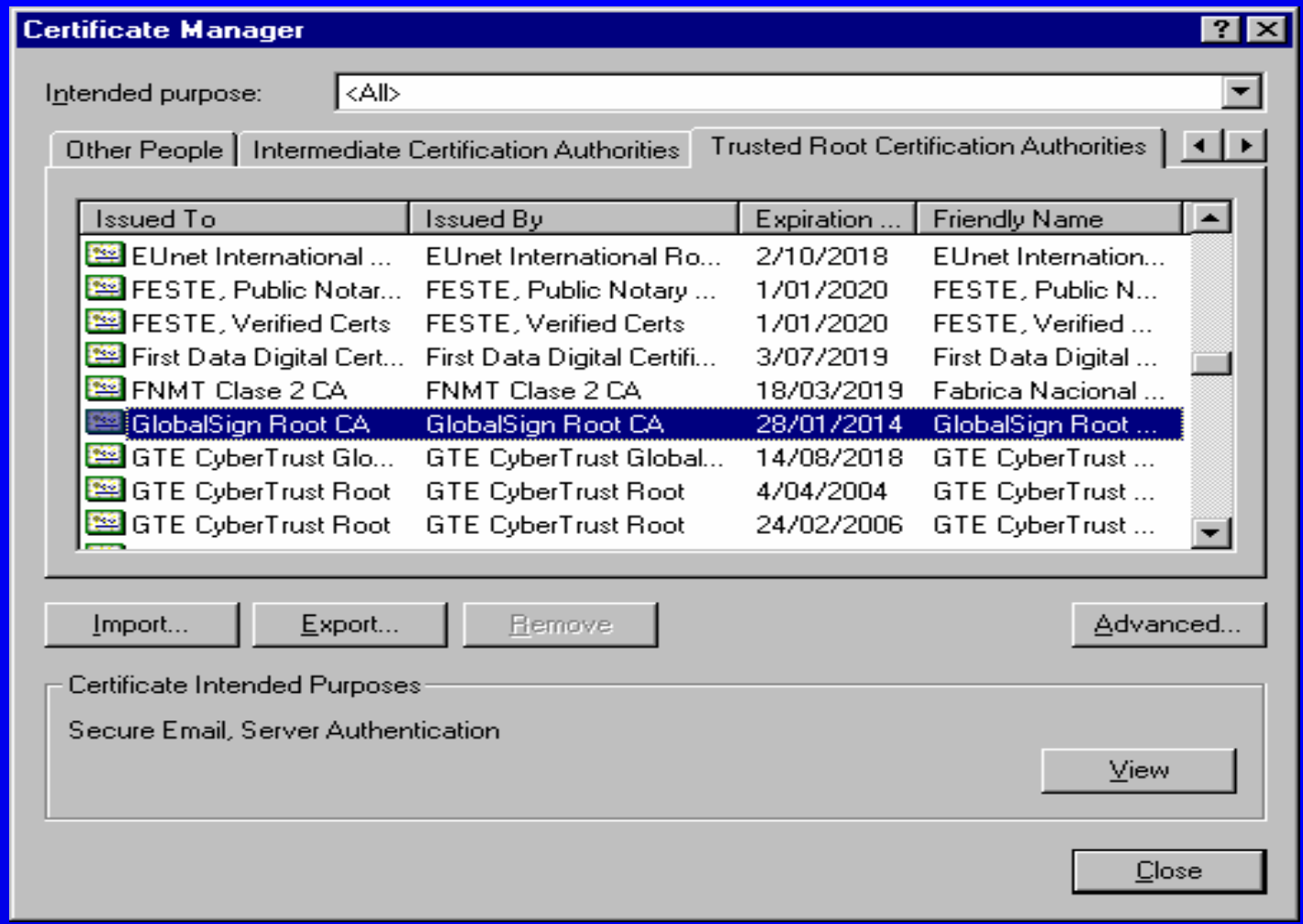
Exemple : certificat de serveur



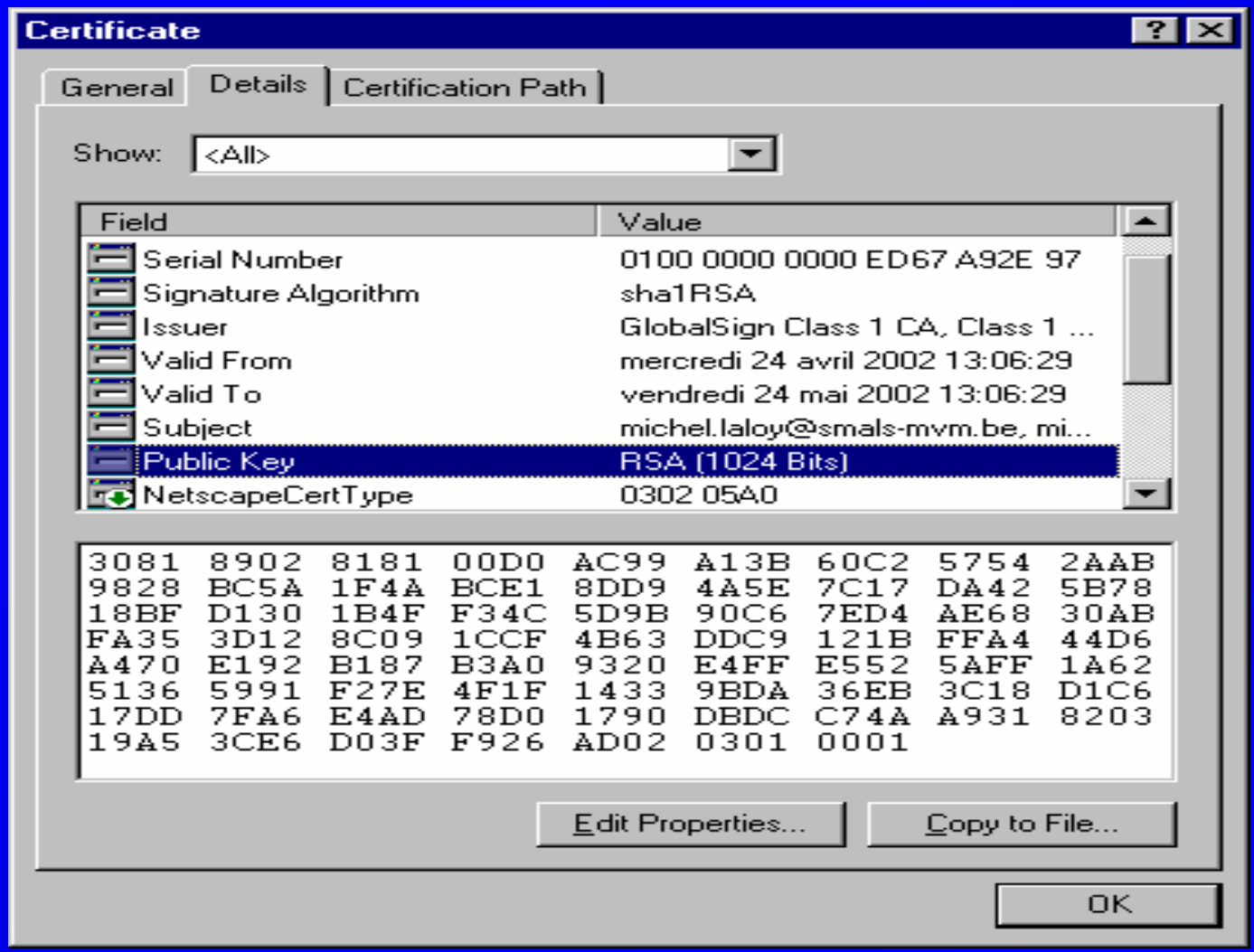
Exemple : information de révocation non disponible



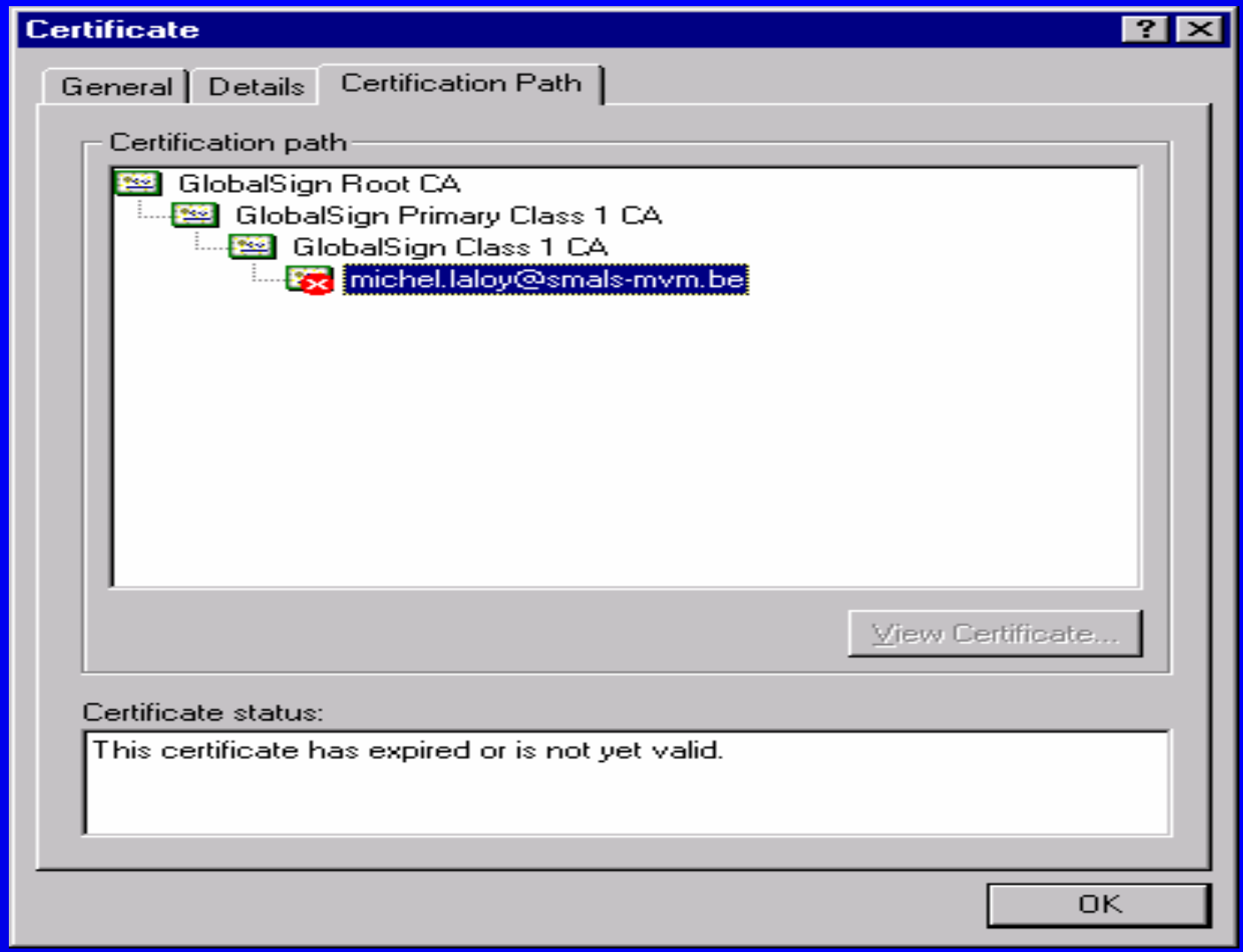
Exemple :
Liste de certificats racines



Exemple : certificat d'utilisateur



Exemple : chaîne de certification



Les projets de l'e-government

Les relations entre les citoyens/entreprises et l'administration :

La carte d'identité électronique

La carte d'identité électronique (1)

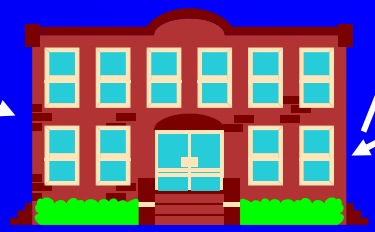
- A chaque citoyen sont allouées deux paires de clefs : une des clefs privées sert à la signature, l'autre à l'authentification.
- La CIE contient les certificats d'identité et les clefs
- Les communes jouent le rôle d'autorités locales d'enregistrement (LRAs)
- Le Registre National sert d'intermédiaire entre les communes et le CA

La carte d'identité électronique (2)

- Implémentation technique : smart card, munie d'un module cryptographique, et protégée par un pincode

Demande et livraison de la CIE

Citoyen



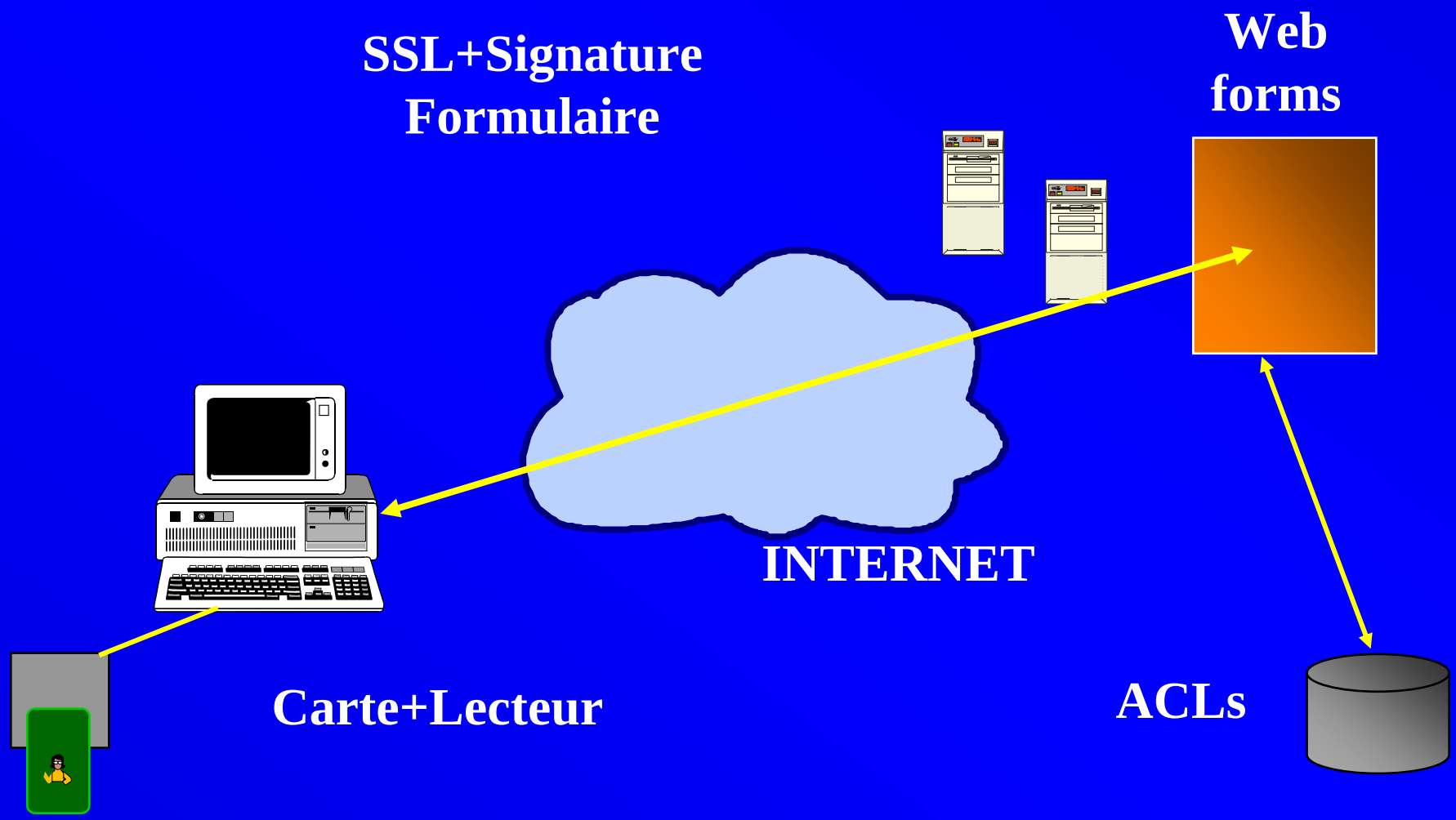
Commune
(LRA)

RN
Registre National

Initialisation
Personalisation
Carte

CA

Exemple d'utilisation de la CIE



Conclusions

- La signature digitale va s'imposer pour les relations sécurisées entre les grandes et moyennes entreprises (ou leurs mandataires) et l'Administration Publique
- En ce qui concerne les citoyens (et les petites entreprises) : le 'problème' est la démarche d 'obtention d 'un certificat digital. Sera résolu par la disponibilité de la carte d'identité électronique

Annexe : l ’algorithme RSA

Un des principaux algorithmes de cryptographie asymétrique utilisé pour la signature digitale est l ’algorithme RSA

La sécurité de cet algorithme est basé sur le fait suivant : si p et q sont de grands nombres premiers et que N est leur produit (N = p x q), alors, si on connaît seulement N, il est pratiquement impossible de trouver p et q