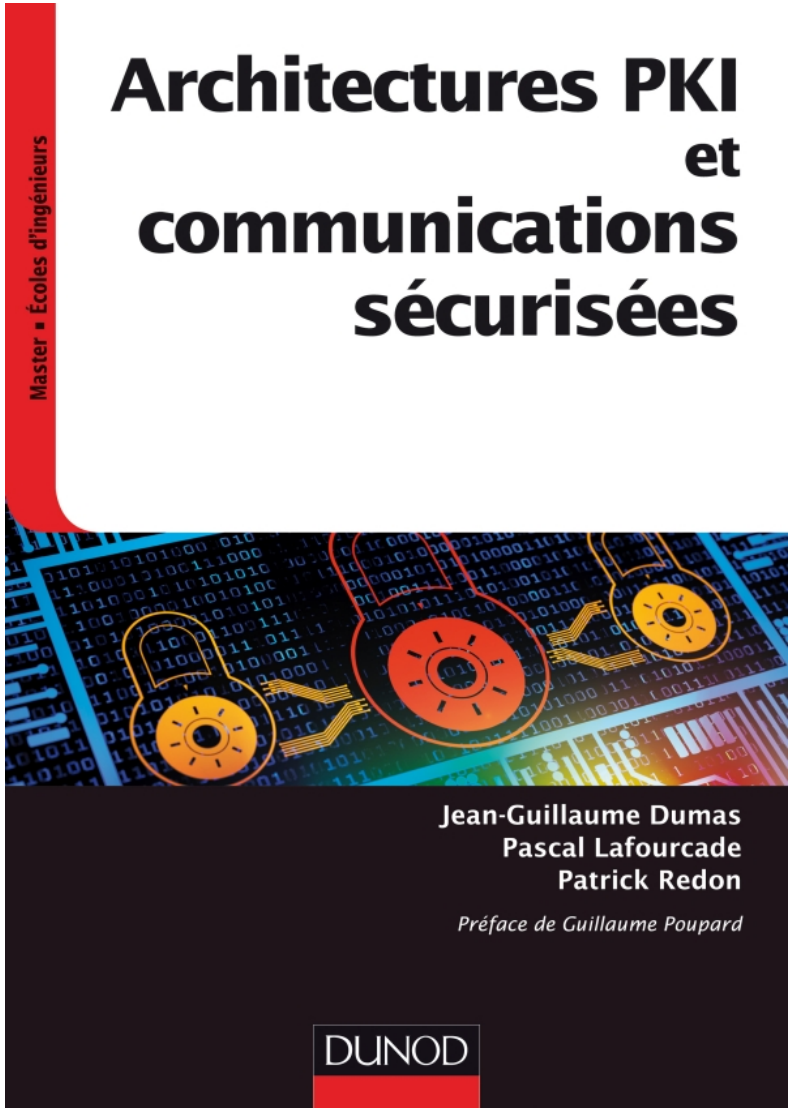
Architectures PKI et communications sécurisées

Pascal Lafourcade

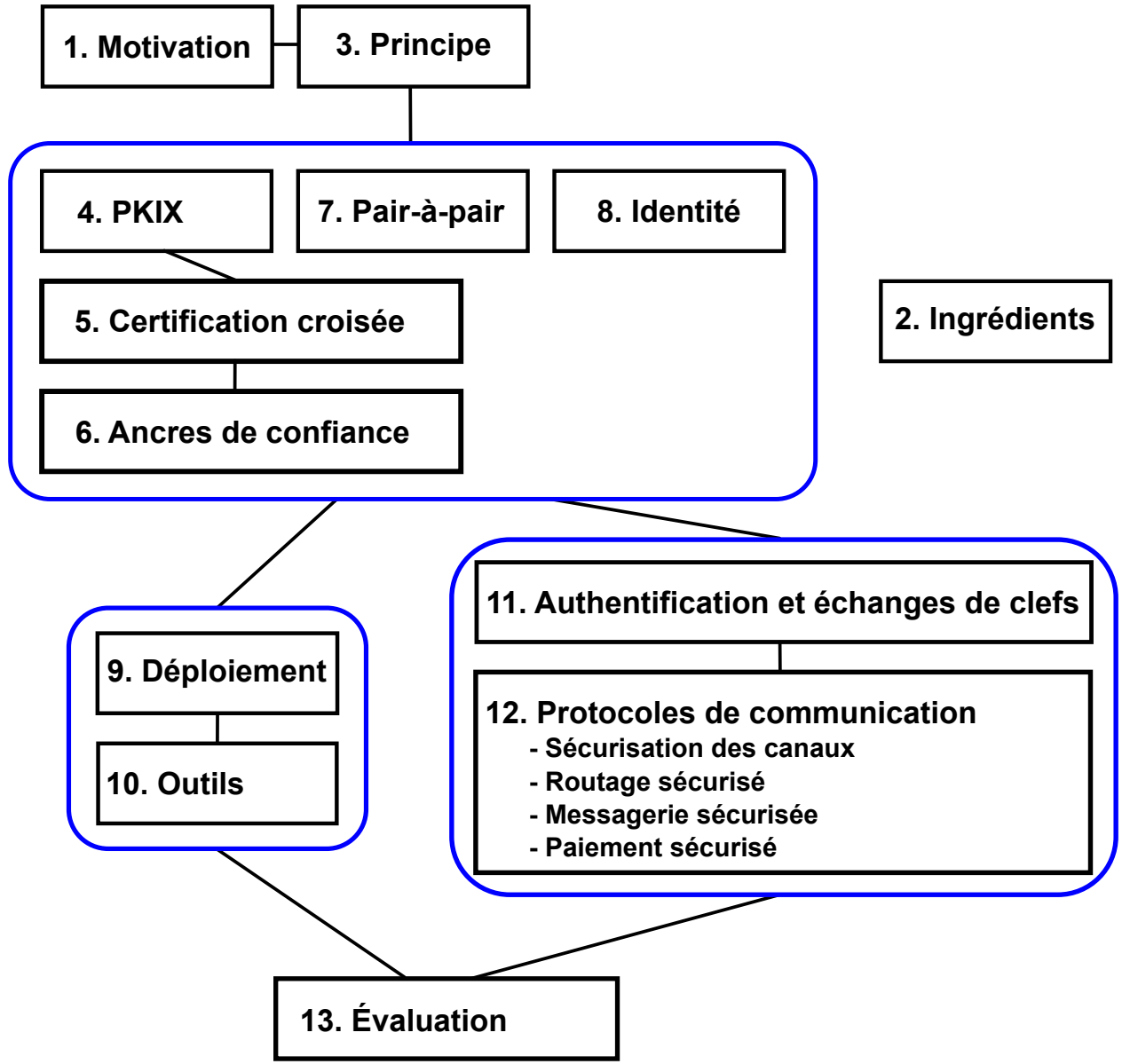
Chaire industrielle,
Confiance numérique

Octobre 2015

Juillet 2015

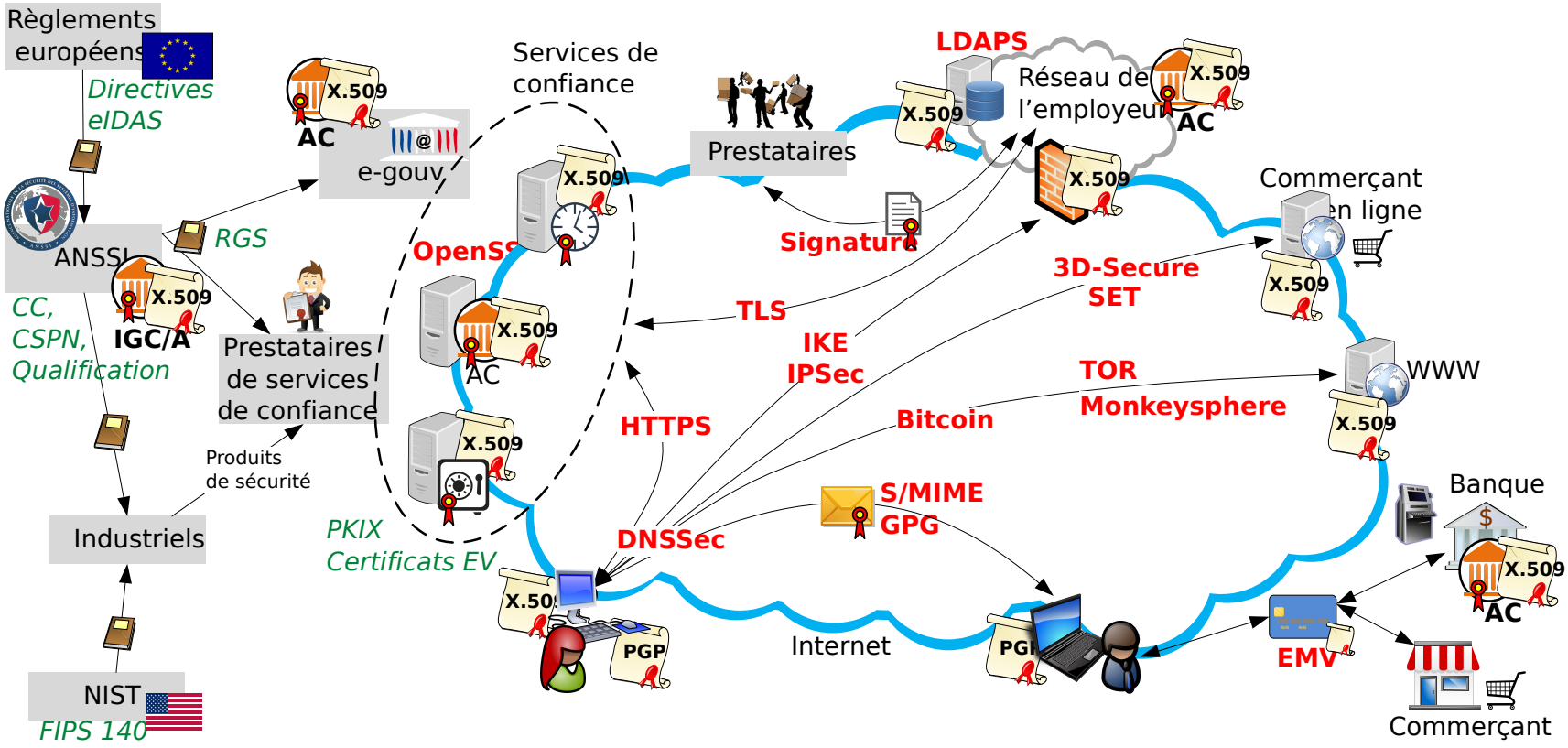


Organisation



Plus de 50 exercices corrigés

Aperçu


Règlements européens
Directives eIDAS
ANSSI
CC, CSPN, Qualification
IGC/A
RGS
AC
e-gouv
Prestataires de services de confiance
Produits de sécurité
Industriels
NIST
FIPS 140
Services de confiance
OpenSSL
AC
PKIX
Certificats EV
HTTPS
DNSSec
PGP
Prestataires
Signature
LDAPS
Réseau de l'employeur
AC
TLS
IKE
IPSec
3D-Secure
SET
Commerçant en ligne
TOR
Monkeysphere
Bitcoin
WWW
S/MIME
GPG
Internet
EMV
Banque
AC
Commerçant
X.509

Plan

Plan

Clef symétrique

Exemples

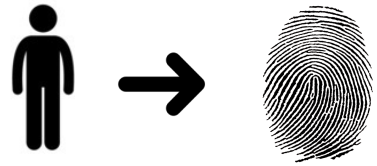
- DES
- AES

Chiffrement à clef publique

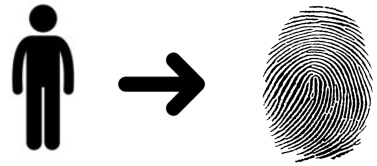
Exemples

- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Fonction de Hachage (SHA-1, SHA-3)

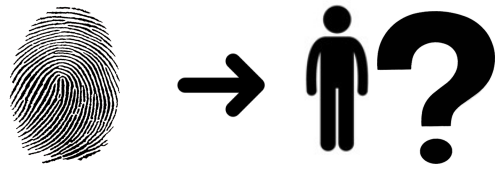


Fonction de Hachage (SHA-1, SHA-3)

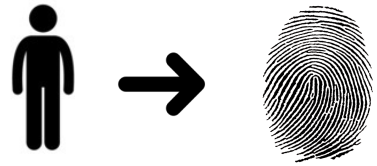


Propriétés de résitance

- Pré-image

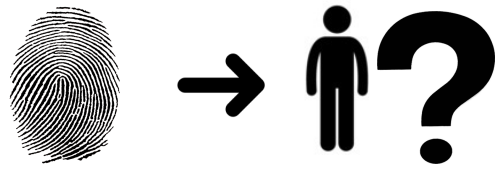


Fonction de Hachage (SHA-1, SHA-3)

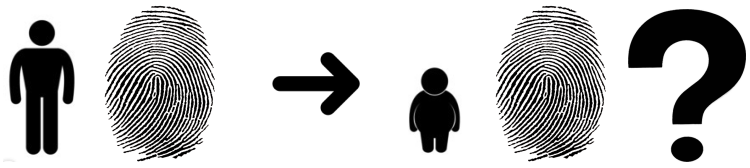


Propriétés de résitance

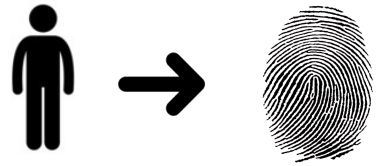
- Pré-image



- Seconde Pré-image

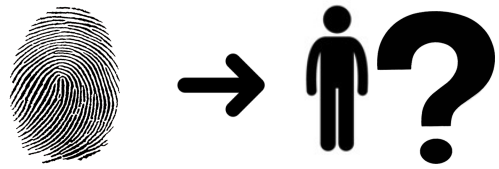


Fonction de Hachage (SHA-1, SHA-3)

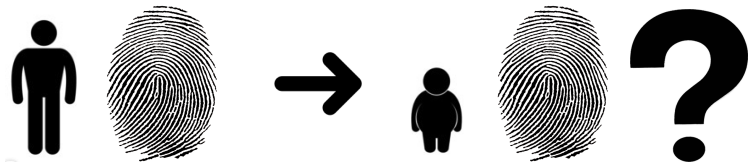


Propriétés de résitance

- Pré-image

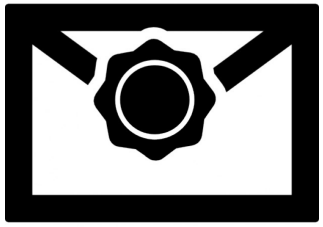


- Seconde Pré-image

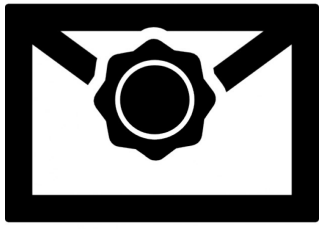


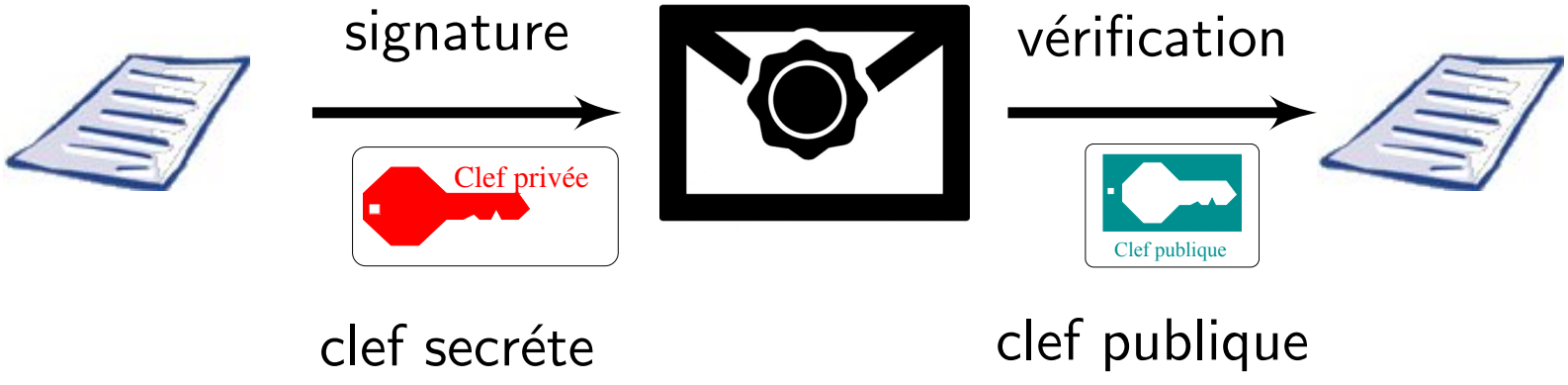
- Collision

Signature



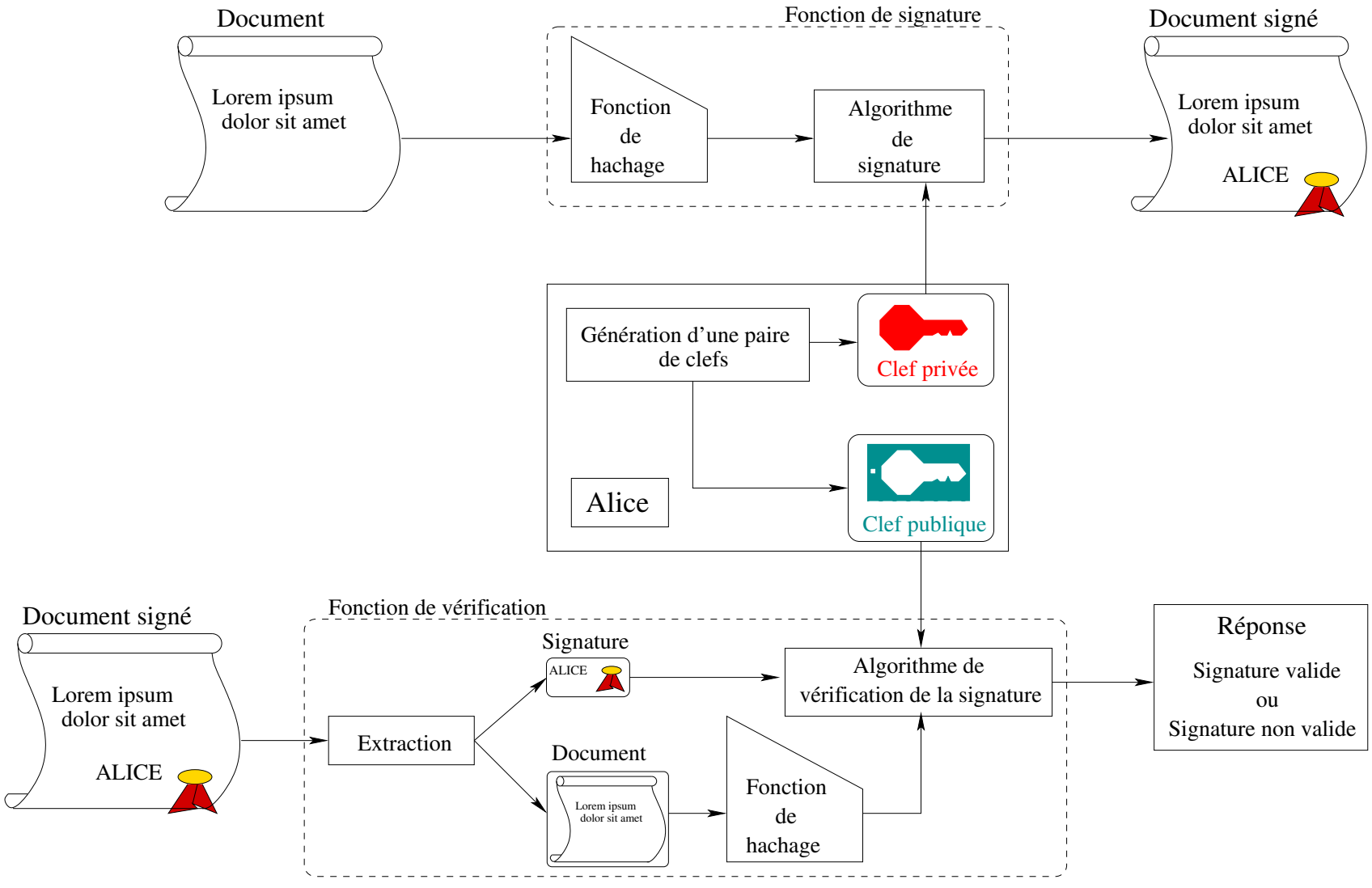
Signature





RSA: $m^d \mod n$

Signer et vérifier un document



Plan

Octobre 2014

TED
Ideas worth spreading

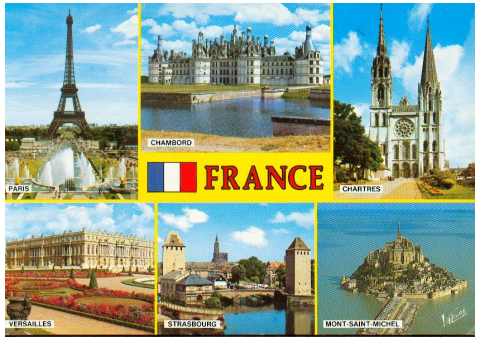
L'importance de la vie privée
Why privacy matters?

Par Glenn Greenwald

Les gens pensent ne rien avoir à cacher ...

`http://jenairienacacher.fr/`

La sécurité des emails par défaut



Première demande d'E. Snowden ...

```
amnesia@amnesia:~$ gpg -d

-----BEGIN PGP MESSAGE-----

hQIMA8xdLvrAJNGTAQ/+LbHB9i52GCPFjTICIP1RPs/WWx5/MIruNKBmB14RHe/A
KsDa/SO1KE5la8ETuDh4r4nQmtZ59TjnmIXHKyRvMo3ipQEGTPvEwNIwdI2X9Uls
KPa2oqQcWLzxrP0Zc4PzNvjXgarq/NQF1SXHtrRhiUdPij93ZFrKMxUCMOjsNOEp
Y7Ak2SY3nbiHVrOBgIZ1FaF8ljiviZSjflt/pE/81qOvQepumXOlwA1Ltcd2ME9o
5yJ1RVrnWf0SUFLh9HRCAu9wVLsgjyqVqilyqZNnUSOGDWBKqAFDPIKz+uBiF29X
vXMeV0V44ATZj7ET9DRAOAozII08LQoQIAAvgTZ3MzIB7VaZPUnU1DxcSROJ9ObR
H3oIBfH6nLRITZnlkJaNvE1M/dXDgOFGjNE500GXZo3OrvrEKL5+hnEIXyn0GBx9
fOvAbTDunJnTzY6R1nl8EvRxsdouT7B2eOLEiWUDhiciUpotJxvClZLUn/fL
SFVkhxTcHtbUsaI60TxQOA2ZhqFV8S6aX4WUbVdFic5pGubtKo0wAbeChrTc7BcS
ecwv8vPPmjC/C64iG8pdETwQ5LVTo2J+epnVKfl3oeMCdWFOFp6tSaOozcjwPleg
hhpCHgFXP2NIJ04CD4BVLeoEm9EOUj2+VaL5Qj5PdOELKp+WTNOl2IHh+fGOQ97S
6gFDn/M+LGFcOdUKpOkAGWEHfL4FBWi7Bb0Axs/bxpHZKEvnvAWIQWuG9HVTvtNc
```

... utiliser PGP

Pretty Good Privacy

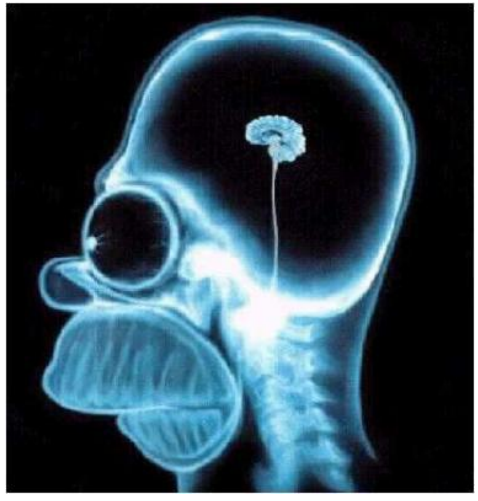
Logiciel de chiffrement, déchiffrement, signature de courriers électroniques, inventé par Phil Zimmermann en 1991.

Si la vie privée est mise hors la loi,
seuls les hors-la-loi auront une vie privée.

If privacy is outlawed, only outlaws will have privacy

Est-ce si difficile ?

1. Télécharger l'outil GPG et l'installer.
2. Générer une paire de clefs $\geq$ 4096 bits
3. Importer votre clefs
4. Télécharger les clefs de vos amis
5. Envoyer des emails chiffrés.



Plan

PKI : Public Key Infrastructure

- Utiliser des clefs publiques
- Établir une clef symétrique de session
- Confiance
- Certificats
- Authorité de certifications
- Chaîne de confiance

Comment échanger une clef secrète en toute sécurité

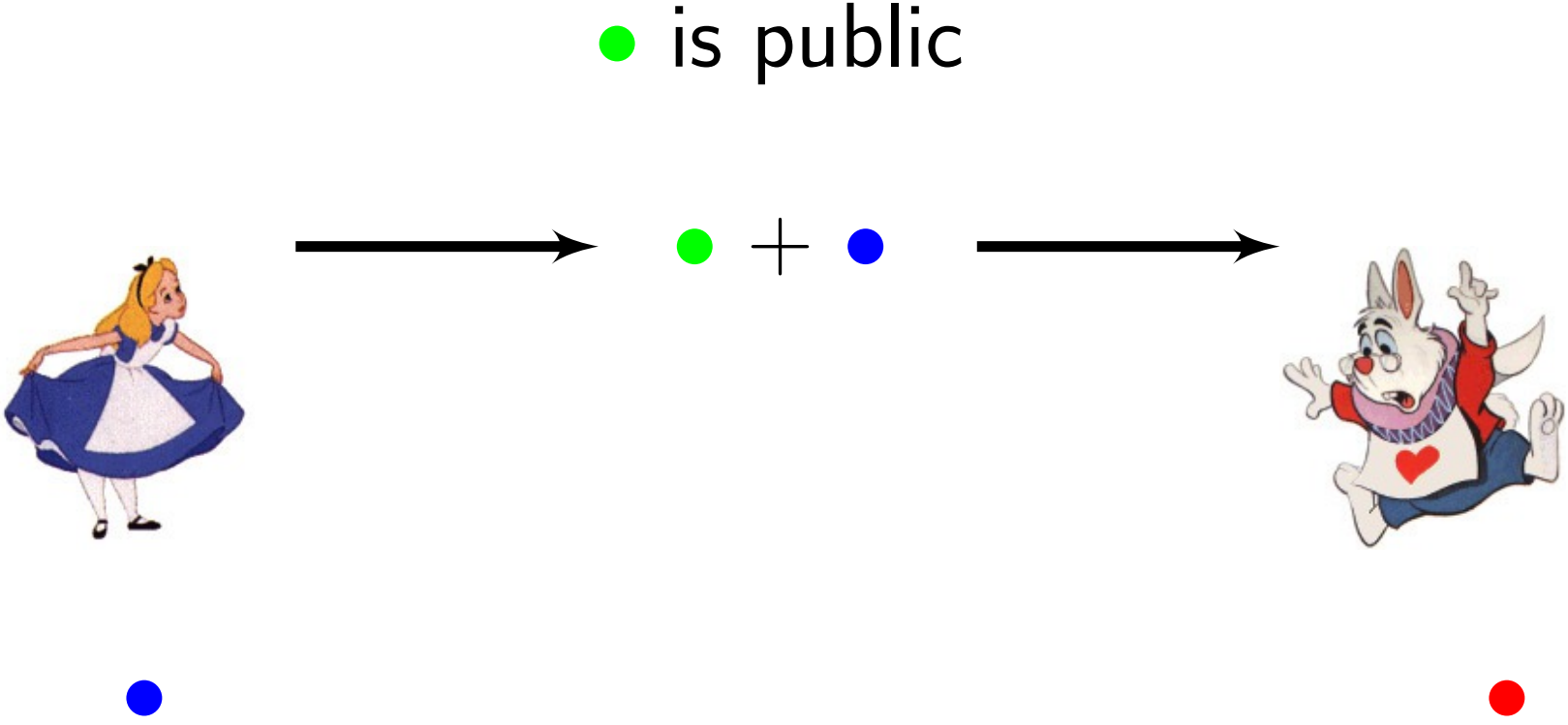
Plusieurs solutions :

- Protocole de Diffie-Hellman (Attaque Man-In-the-Middle)
- Kerberos utilise un tiers de confiance et des clefs symétriques
- Architectures à clefs publiques (PKI)

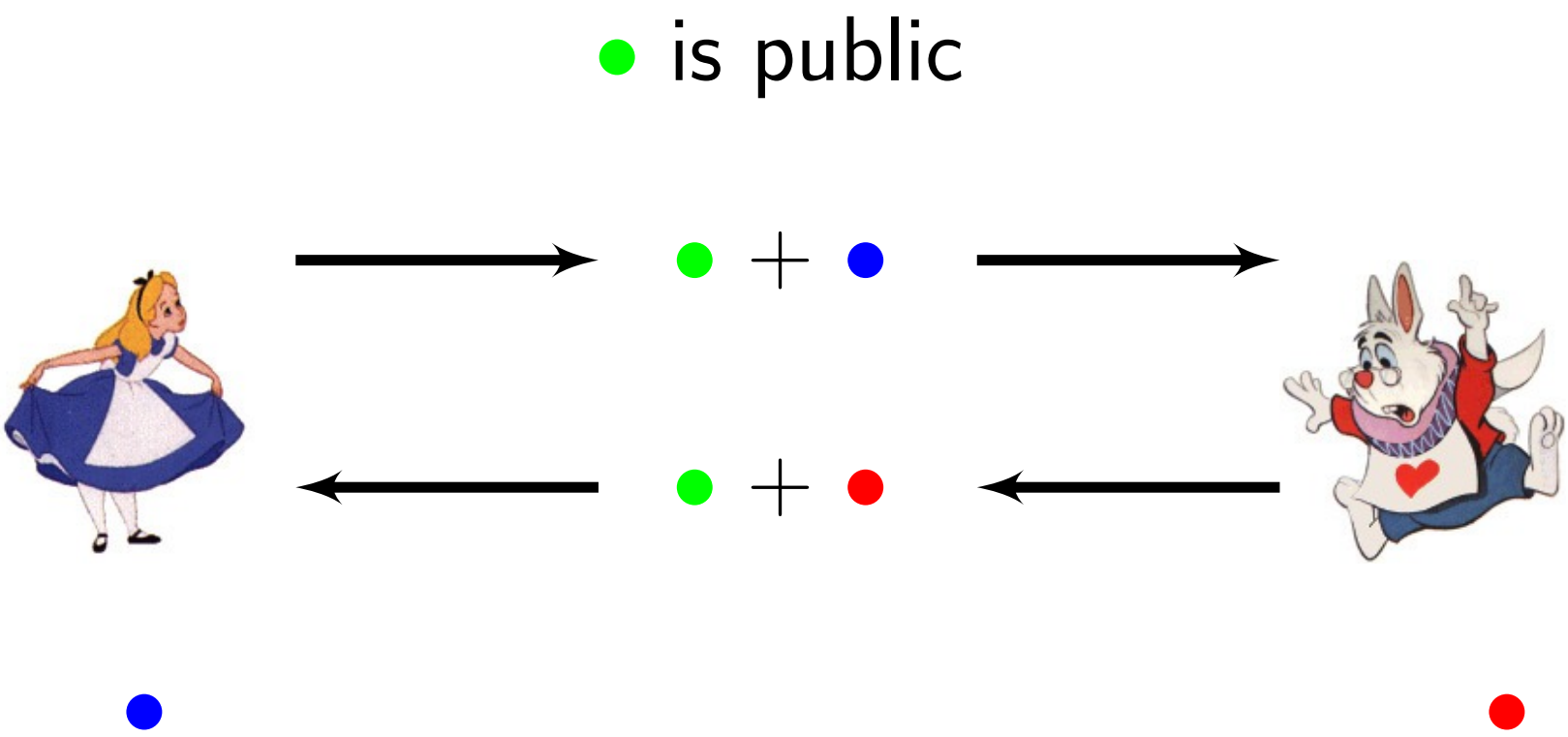
Diffie Hellman (1976)

- is public

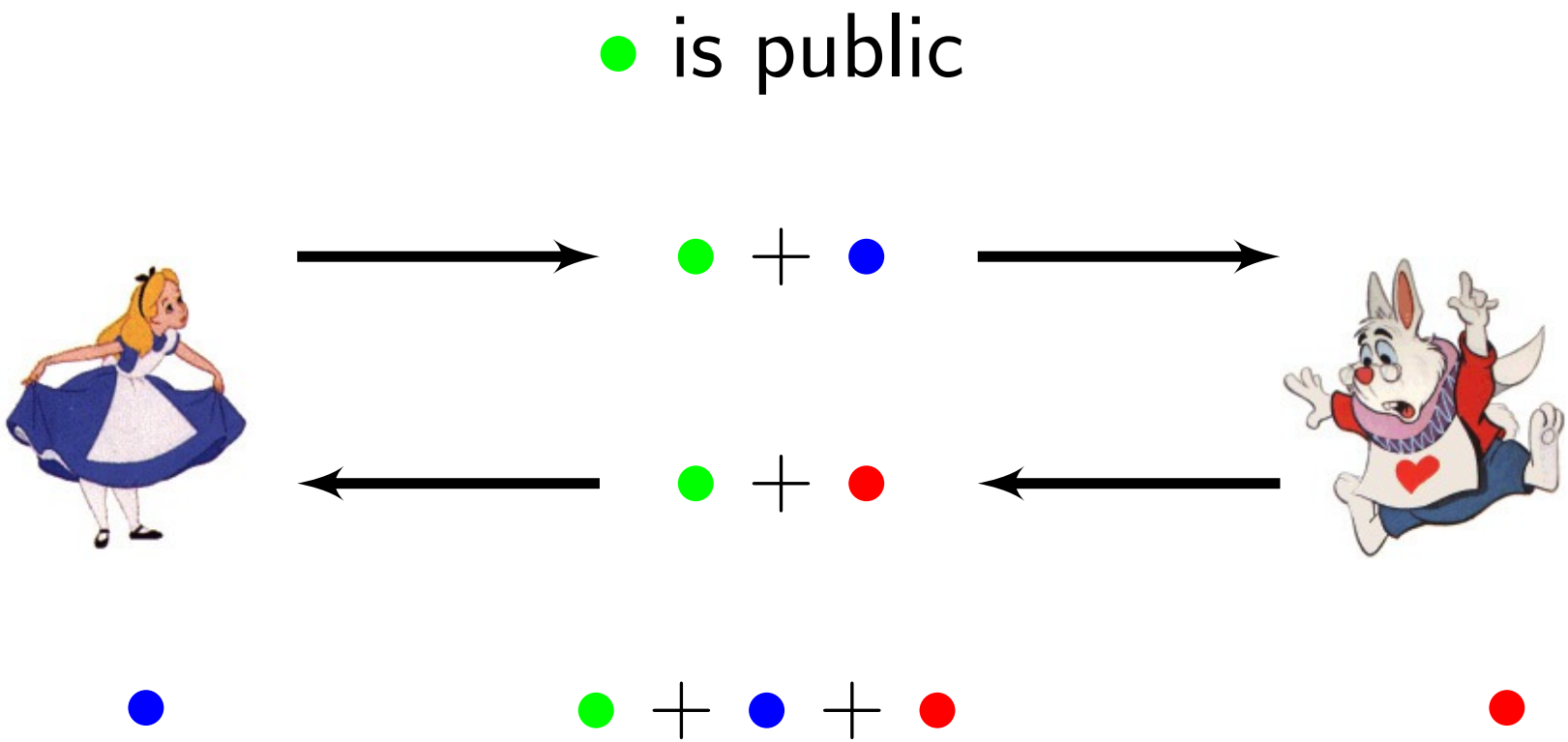
Diffie Hellman (1976)



Diffie Hellman (1976)



Diffie Hellman (1976)



Diffie Hellman (1976)

● is public

● + ●

● + ●

● + ● + ●

- $g =$ ●
- $a =$ ●
- $b =$ ●

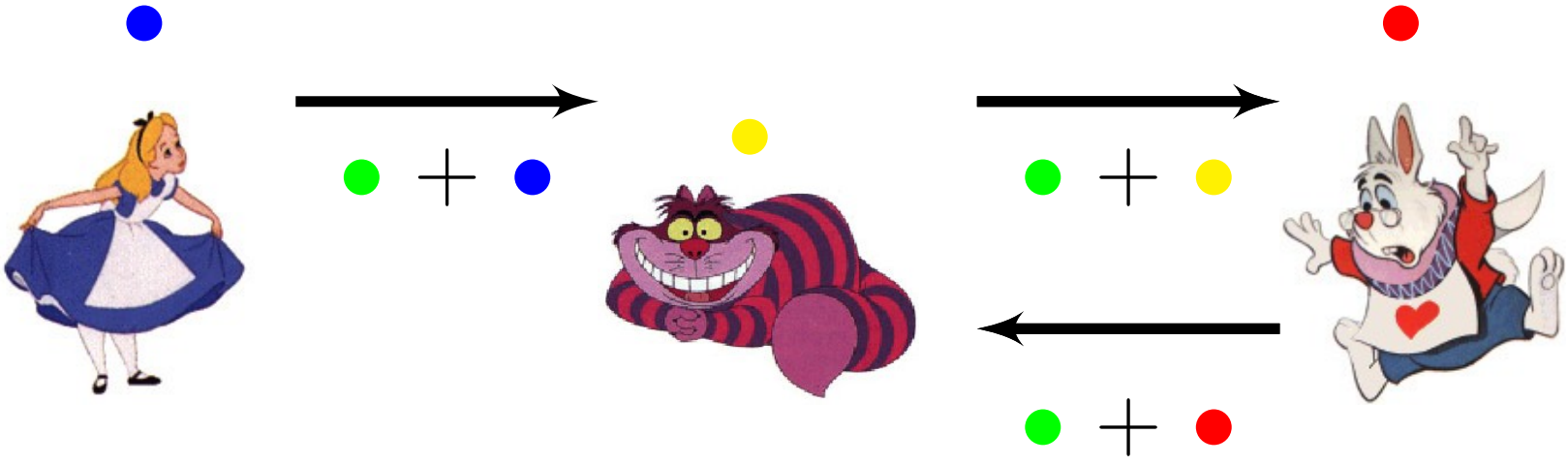
$$(g^a)^b = g^{ab} = (g^b)^a$$

Attaque “Man in the middle”

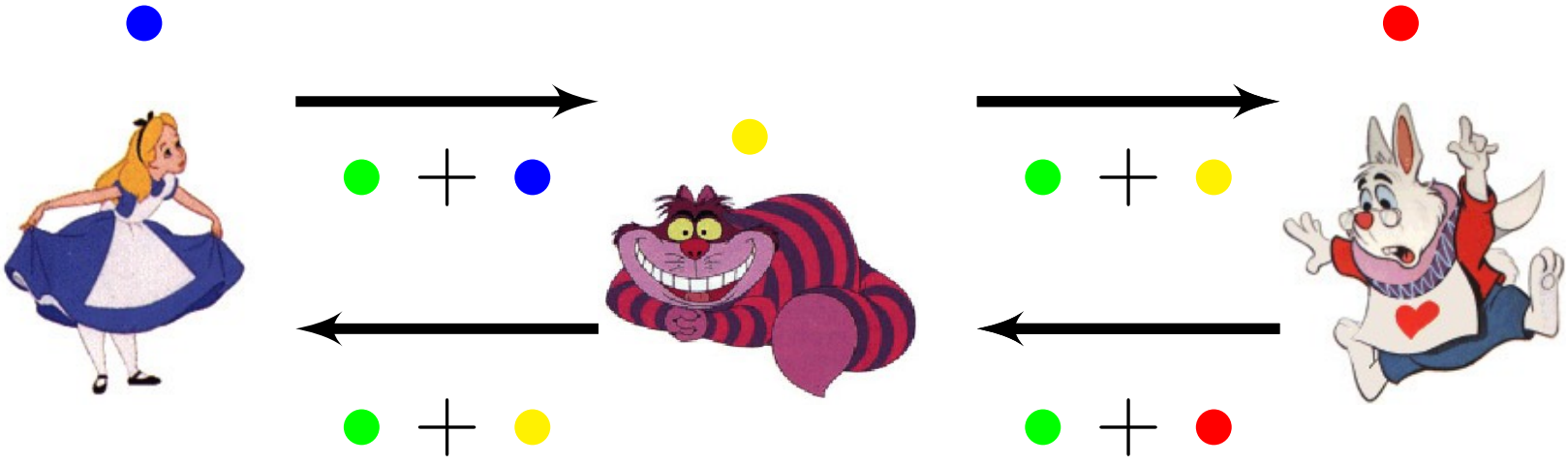
Attaque “Man in the middle”

Attaque “Man in the middle”

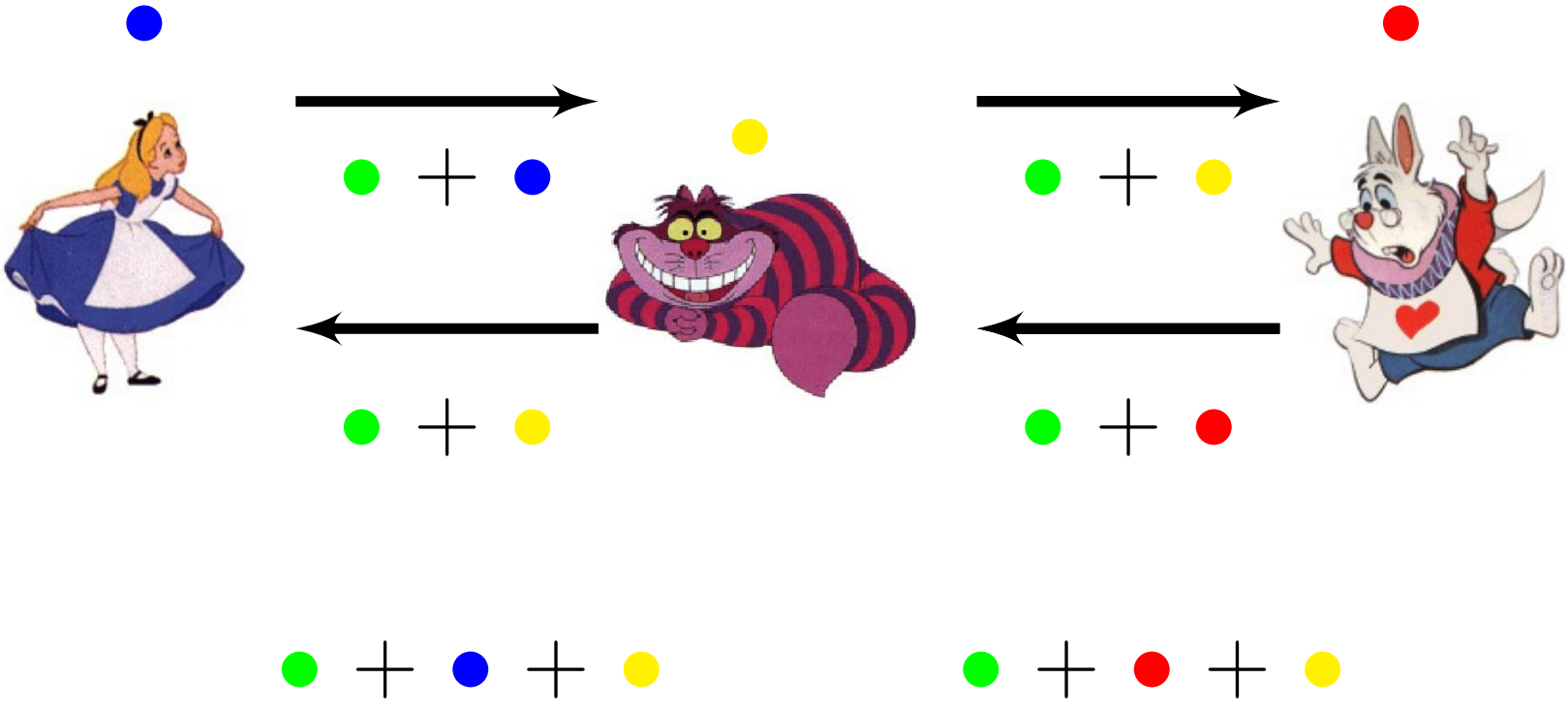
Attaque “Man in the middle”



Attaque “Man in the middle”



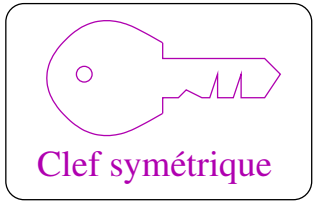
Attaque “Man in the middle”



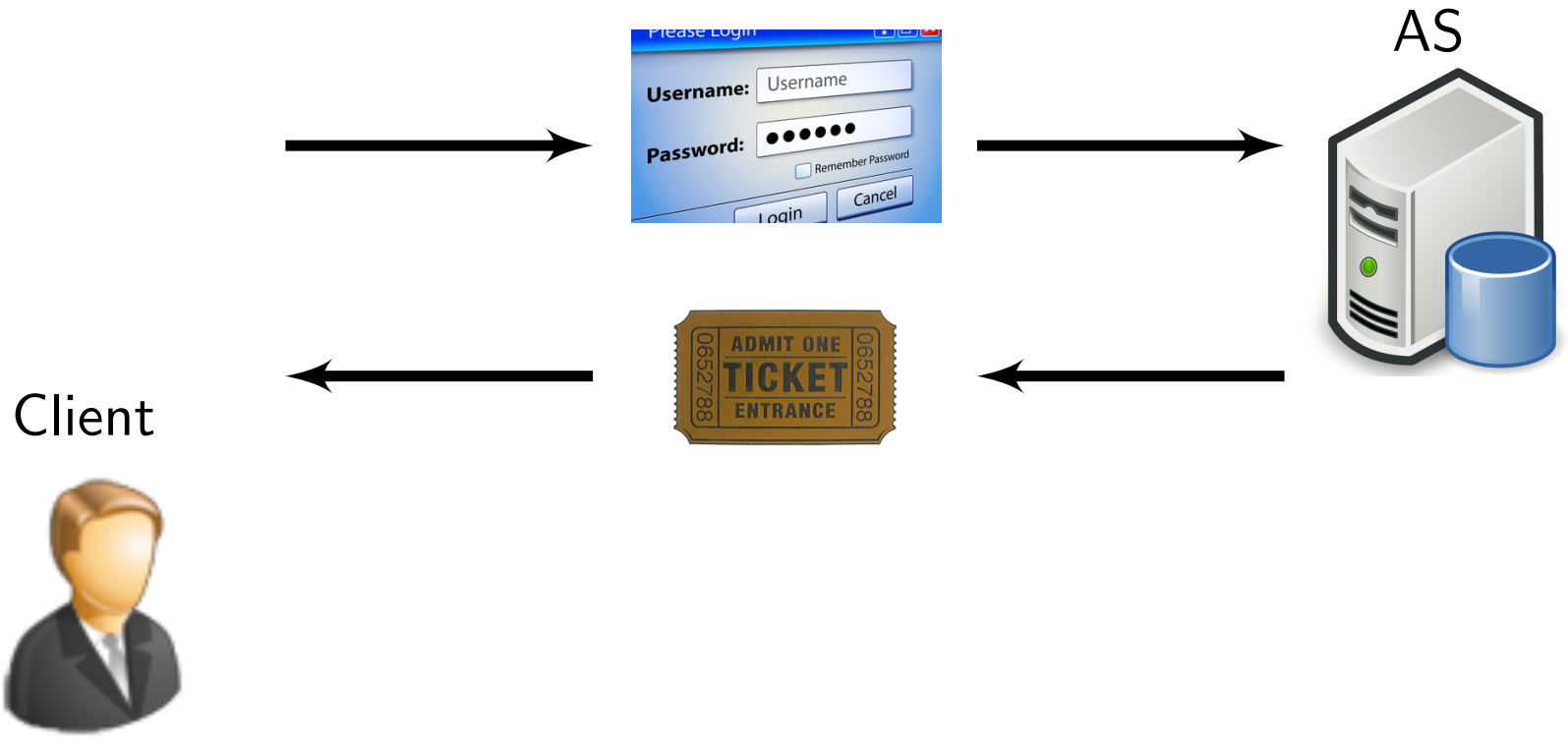
Kerberos V5

Utilise pour les communications:

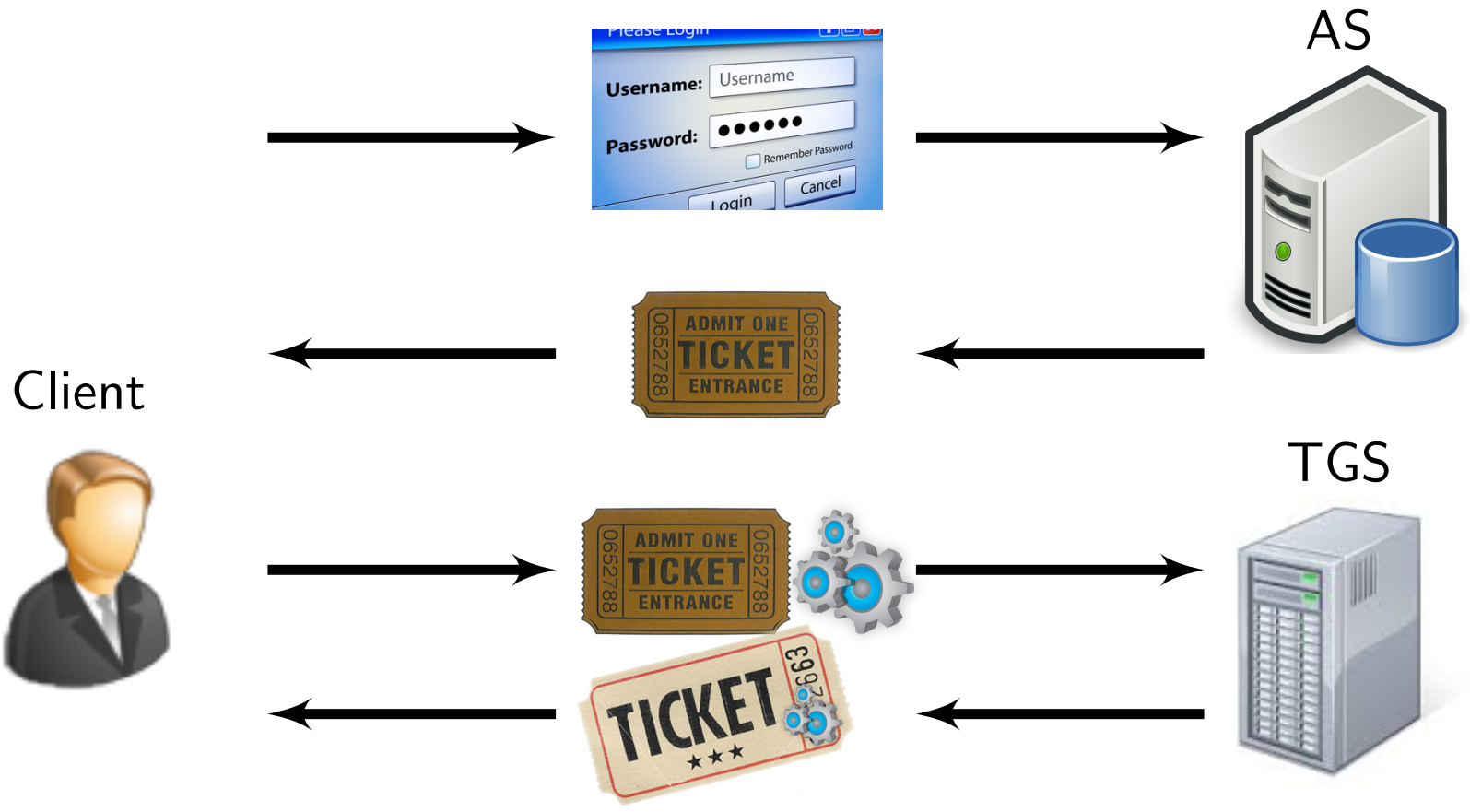
- un tiers de confiance : AS (Authentication Server)
- chiffrement symétrique (clefs privées)
- des tickets : TGS (Ticket Granting Service)
- des mots de passe



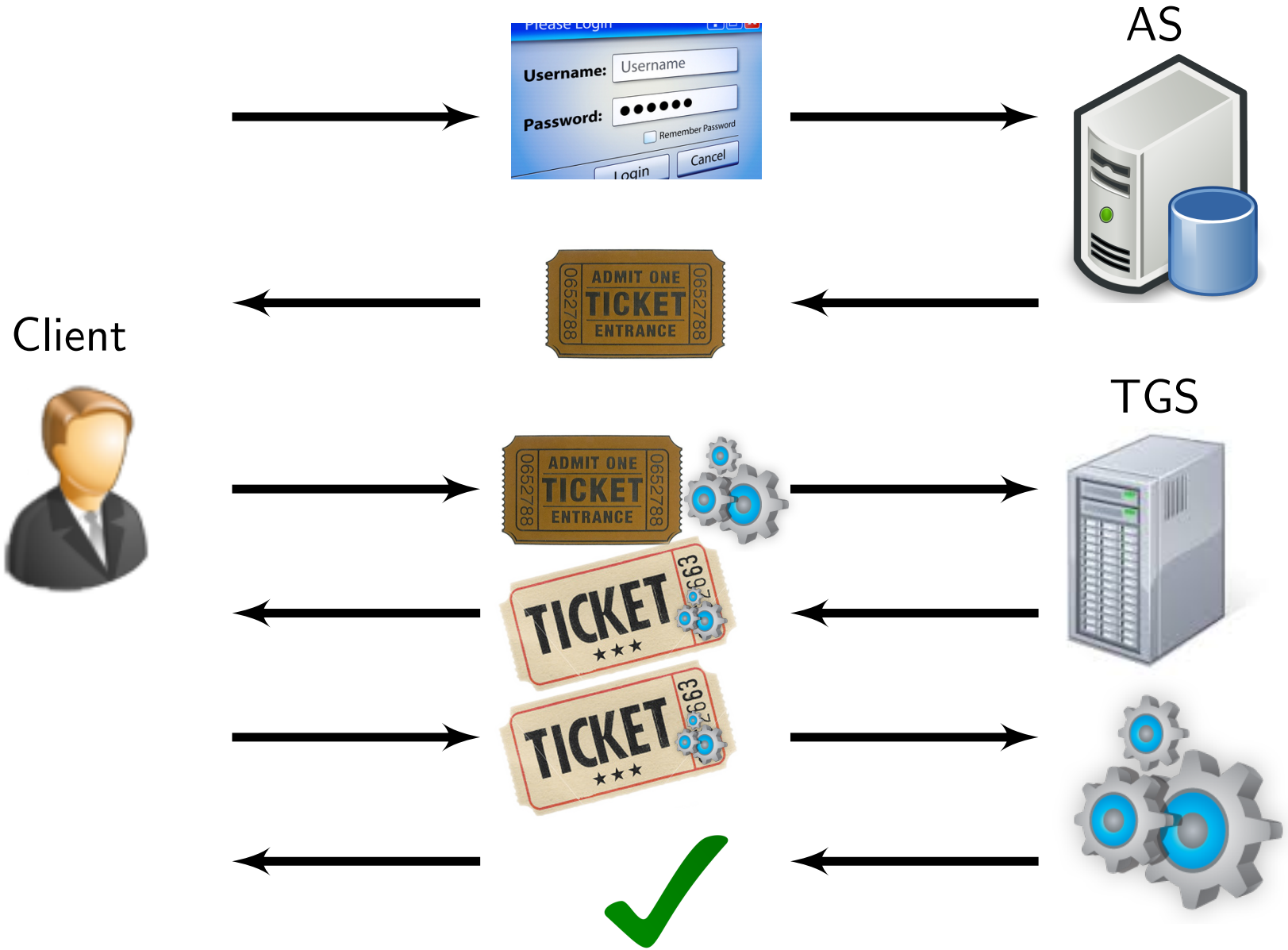
Kerberos V5: Principe en 3 phases



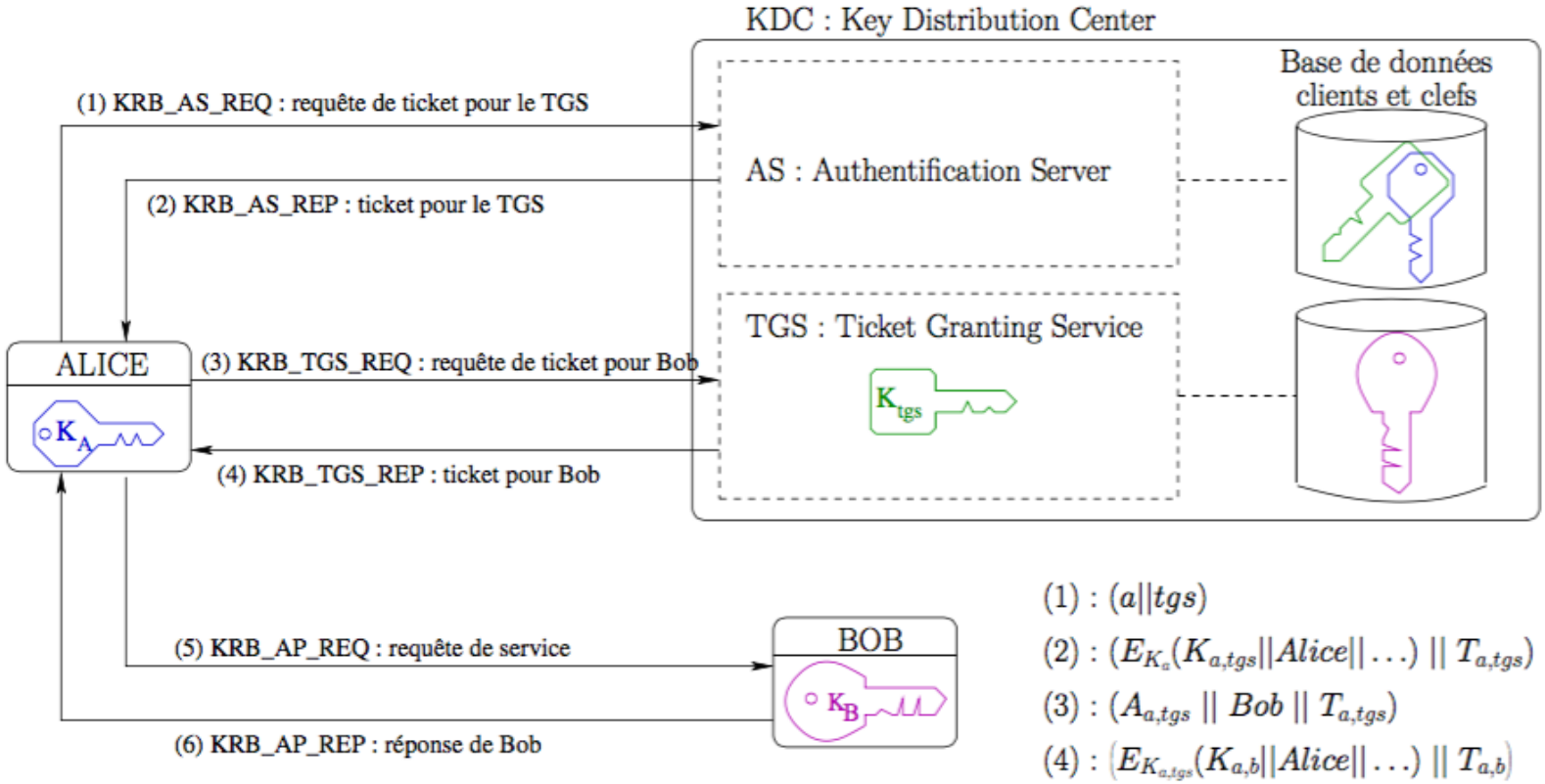
Kerberos V5: Principe en 3 phases



Kerberos V5: Principe en 3 phases



Kerberos V5



(1) : $(a||tgs)$

(2) : $(E_{K_a}(K_{a,tgs}||Alice||\ldots) \,||\, T_{a,tgs})$

(3) : $(A_{a,tgs} \,||\, Bob \,||\, T_{a,tgs})$

(4) : $\left(E_{K_{a,tgs}}(K_{a,b}||Alice||\ldots) \,||\, T_{a,b}\right)$

(5) : $(A_{a,b} \,||\, T_{a,b})$

(6) : $\left(E_{K_{a,b}}(t+1)\right)$

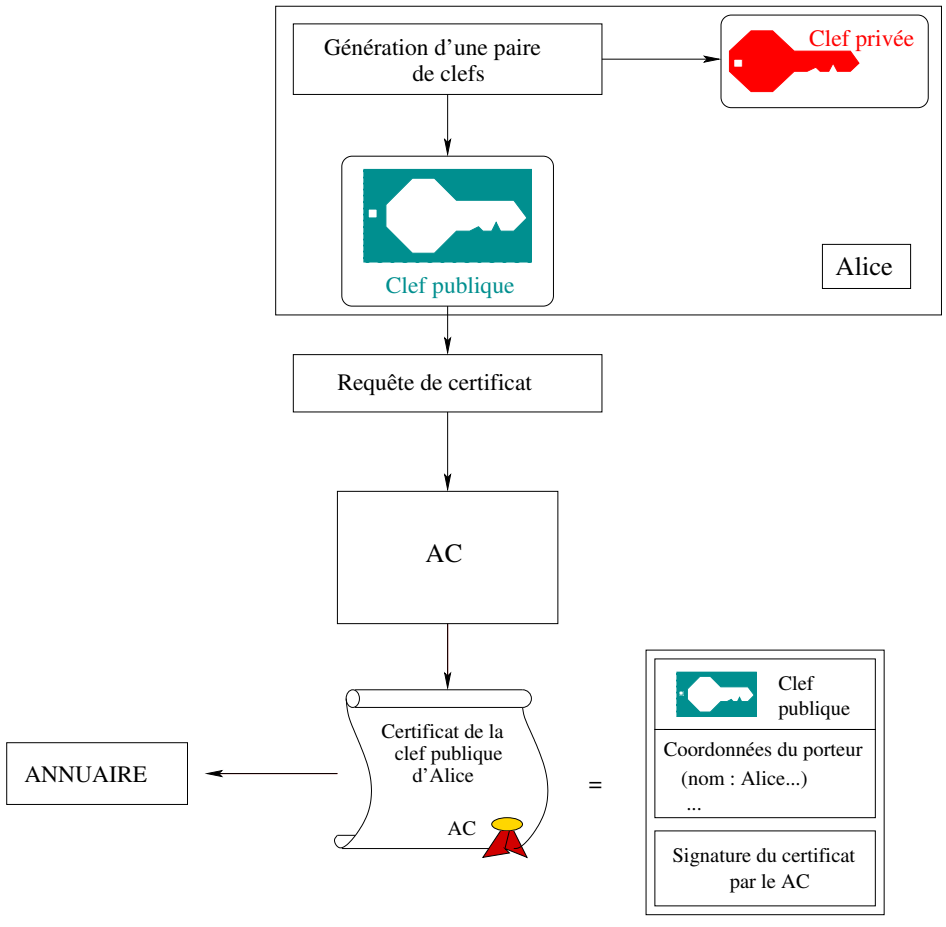
Public Key Infrastructure (PKI)

Principales fonctionalités d'une PKI

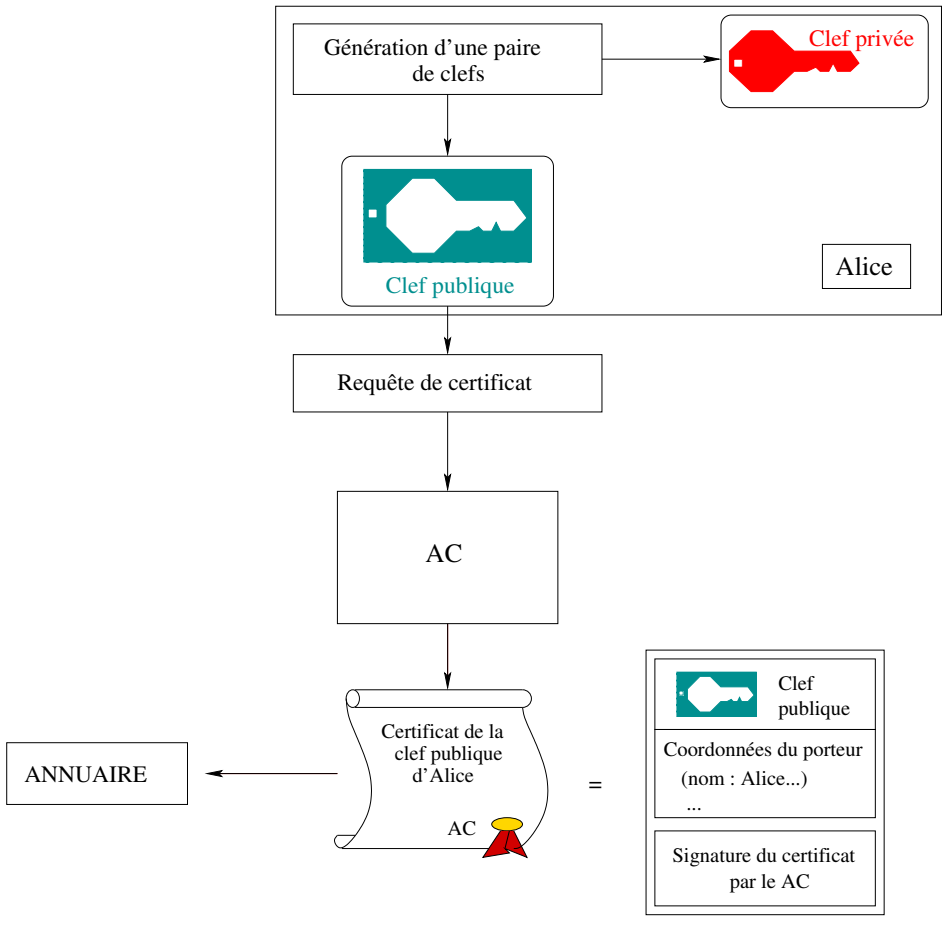
- Création d'une paire de clef
- Génération d'un certificat
- Remise du certificat au porteur
- Publication des certificats
- Vérification des certificats
- Révocation des certificats (CRL)

AC : Authorité de Certification
AE : Authorité d'Enregistrement

Public Key Infrastructure (PKI)



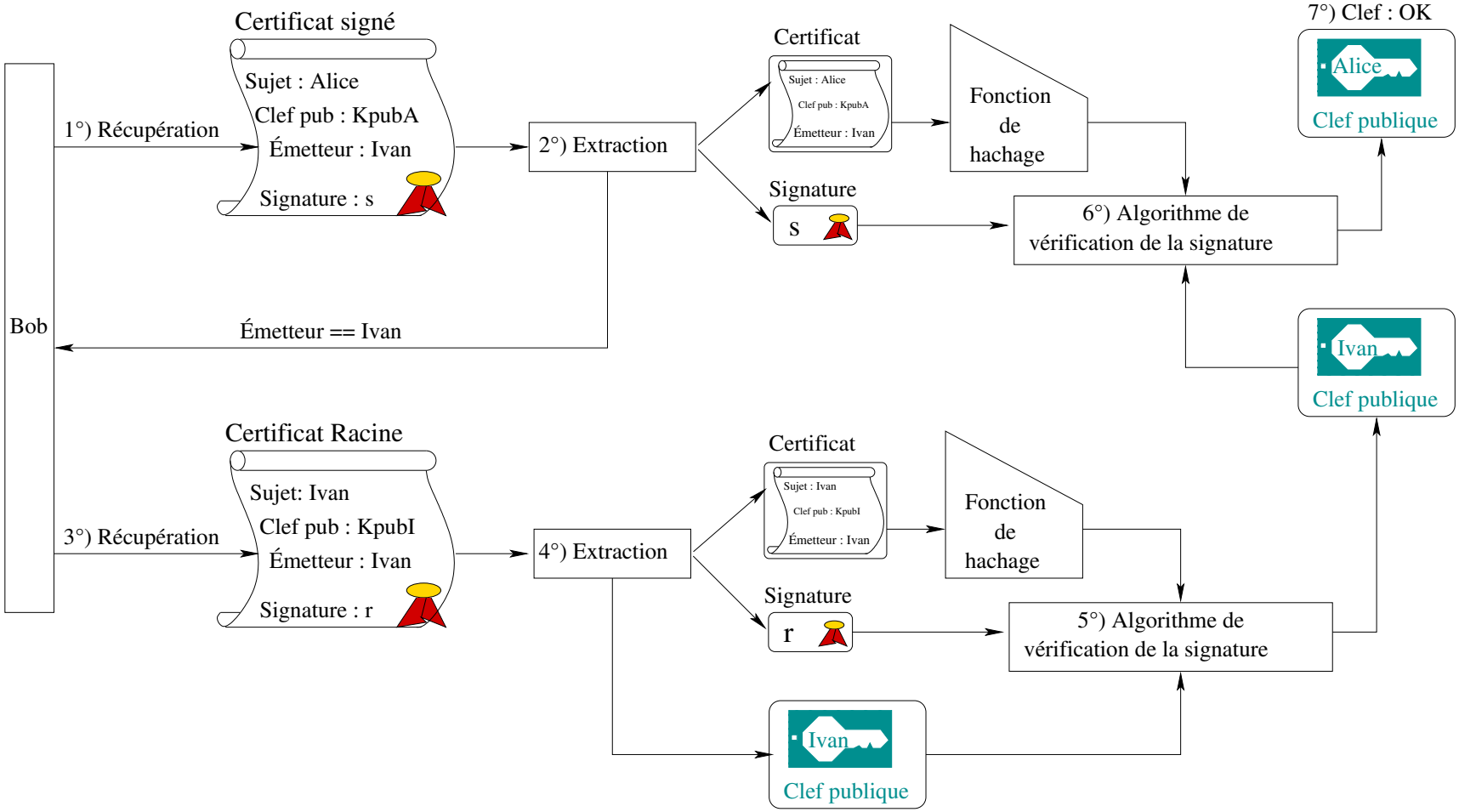
Public Key Infrastructure (PKI)



Authentification de l'AC confiance assurée par

- Chaîne de certificats
- Certificat racine ou certificat auto-signé

Vérification

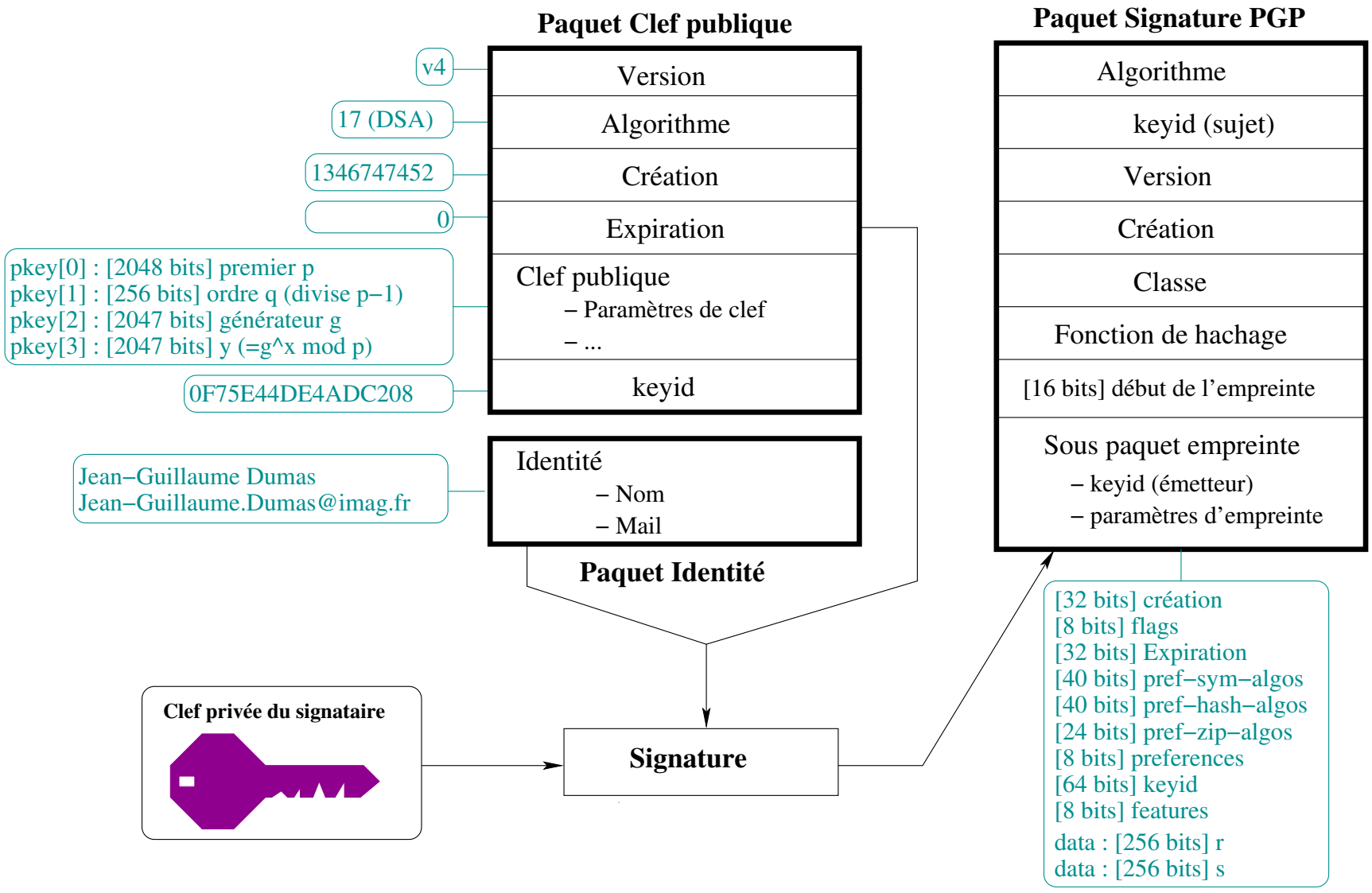


Différentes PKI

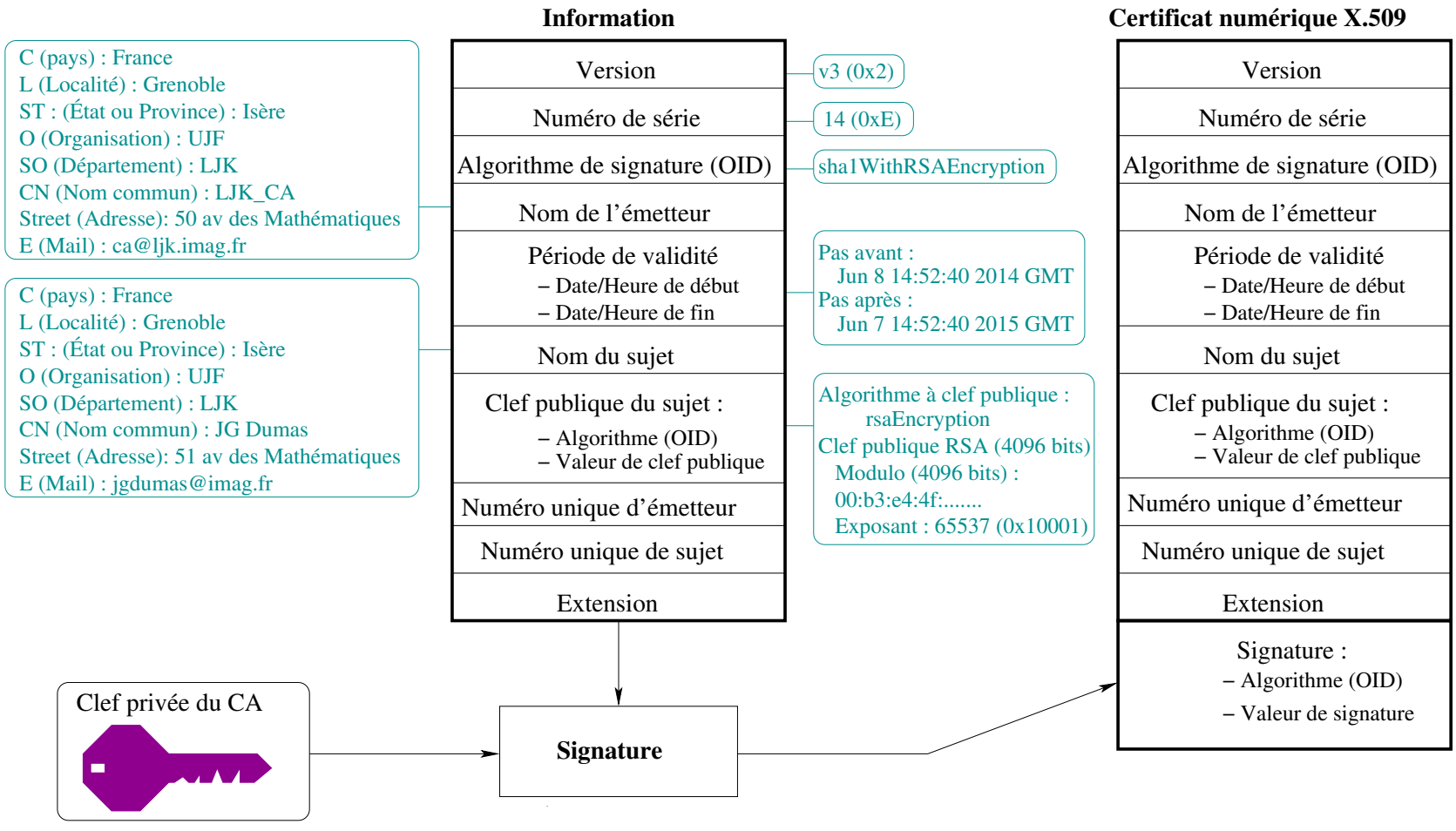
Différents modèles de confiance

- Hiérachique et ancre de confiance PKIX (PKI for X.509)
- Hiérarchique maillé et confiance distribuée
- Embarquée et magasins d'encre de confiance
- Non hiérarchique centré sur l'utilisateur (PGP)
- Autres : Simple PKI, Simple Distributed Security Infrastructure

Certificat PGP

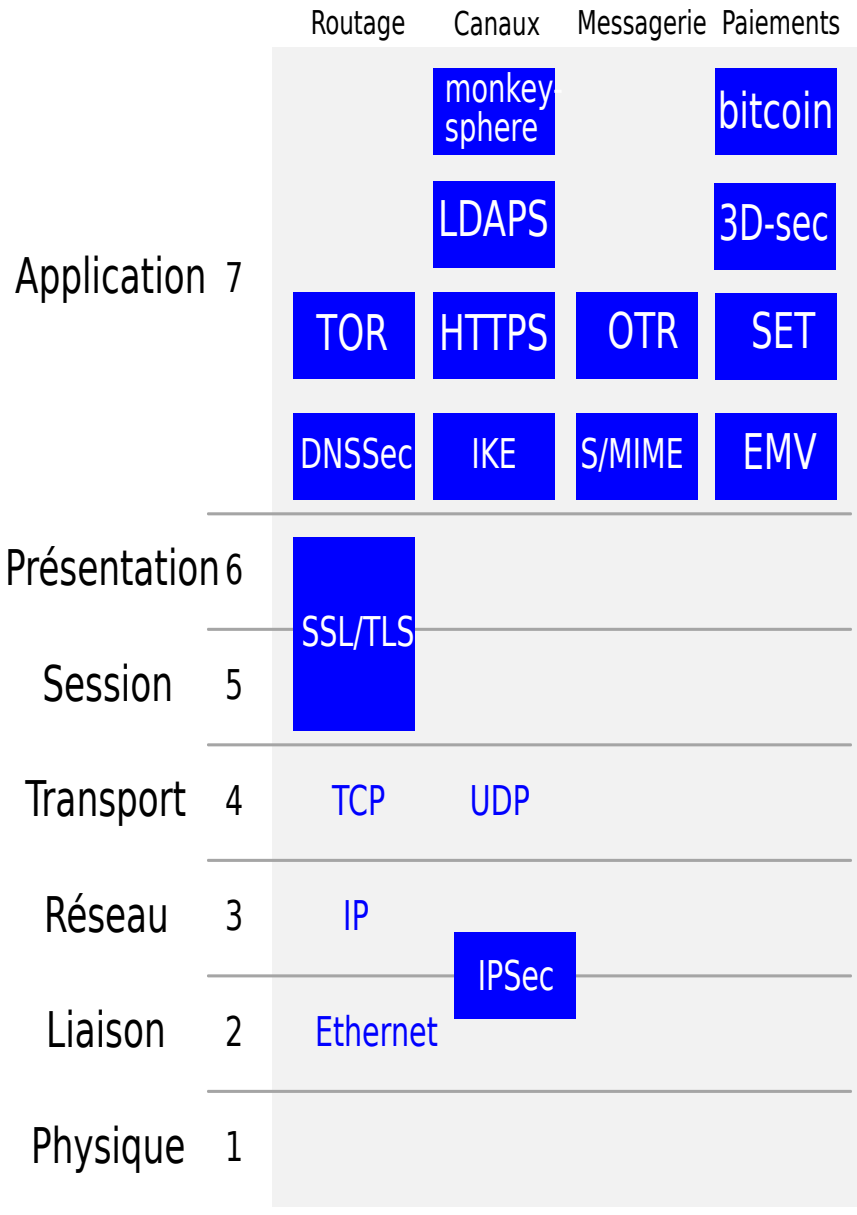


Certificat X509



Plan

Applications



Application : HTTPS

HTTP Secure utilise SSL/TLS sur le port 443 et assure

- Confidentialité
- Intégrité

Le serveur Web est authentifié par un certificat X.509.

Application : HTTPS

HTTP Secure utilise SSL/TLS sur le port 443 et assure

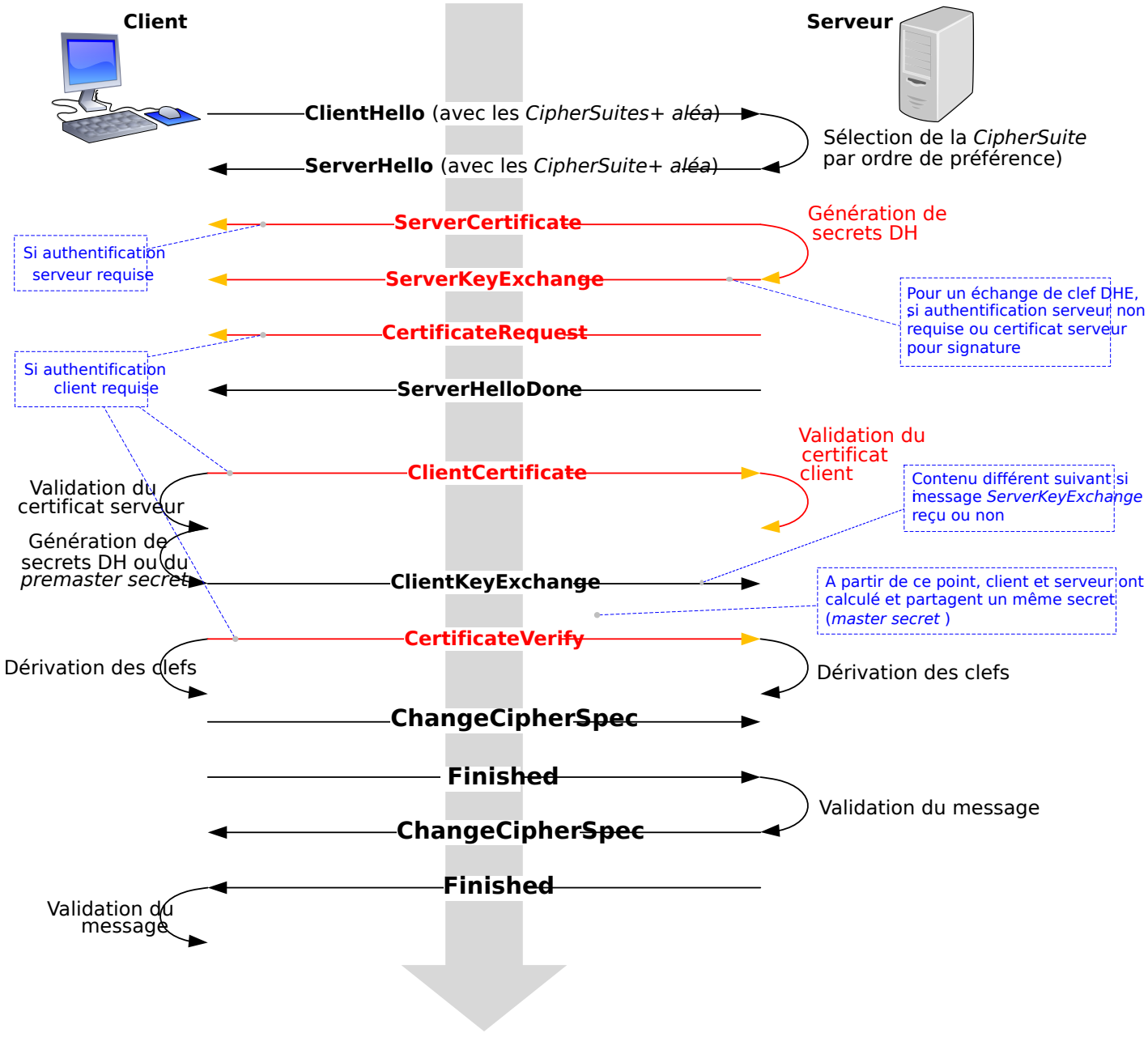
- Confidentialité
- Intégrité

Le serveur Web est authentifié par un certificat X.509.

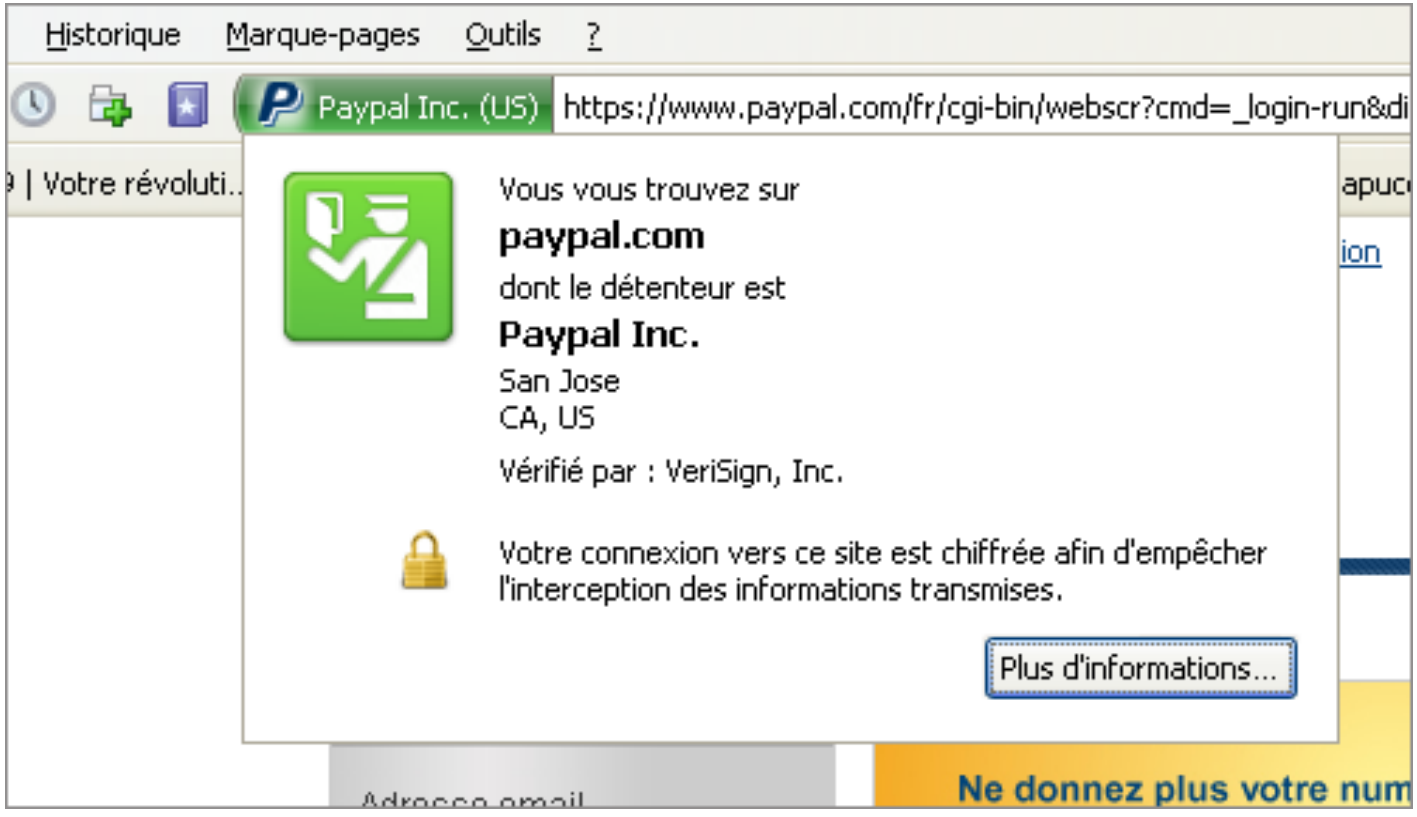
TLS = 5 protocoles

- *Handshake*, connexion sécurisée entre le client et le serveur
- *Change Cipher Spec*, nouvelle clef de session va être utilisée
- *Alert* $\Rightarrow$ Warning ou Fatal
- *Application Data*, encapsulation des données après Handshake
- *TLS Record*, encapsule puis relaye les données

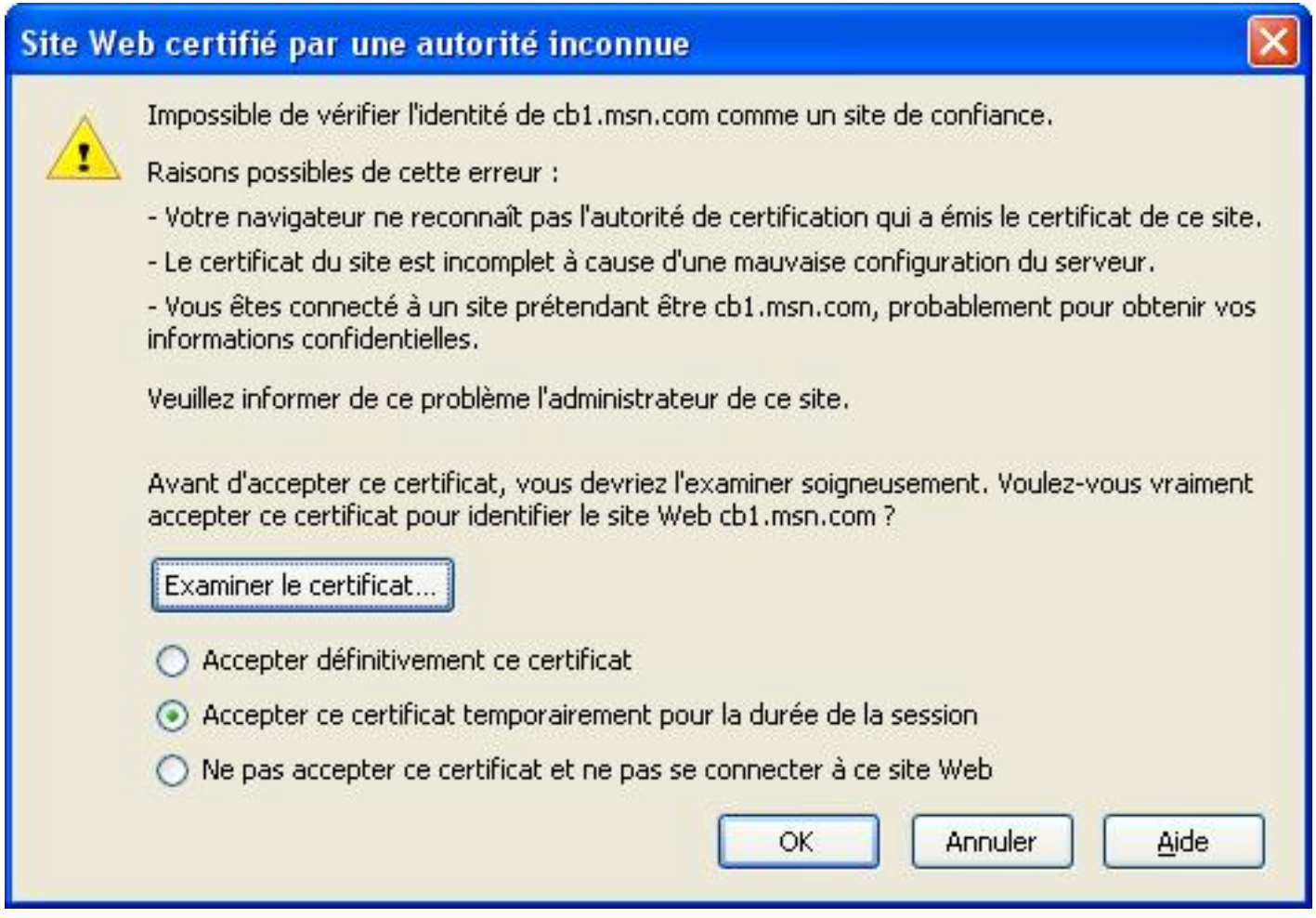
Application : TLS Handshake



Application :



Application :



AC est inconnue du magasin de certificats.

Application :

Cette connexion n'est pas certifiée

Vous avez demandé à Iceweasel de se connecter de manière sécurisée à **static.ak.facebook.com**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

Sortir d'ici !

Détails techniques

static.ak.facebook.com utilise un certificat de sécurité invalide.

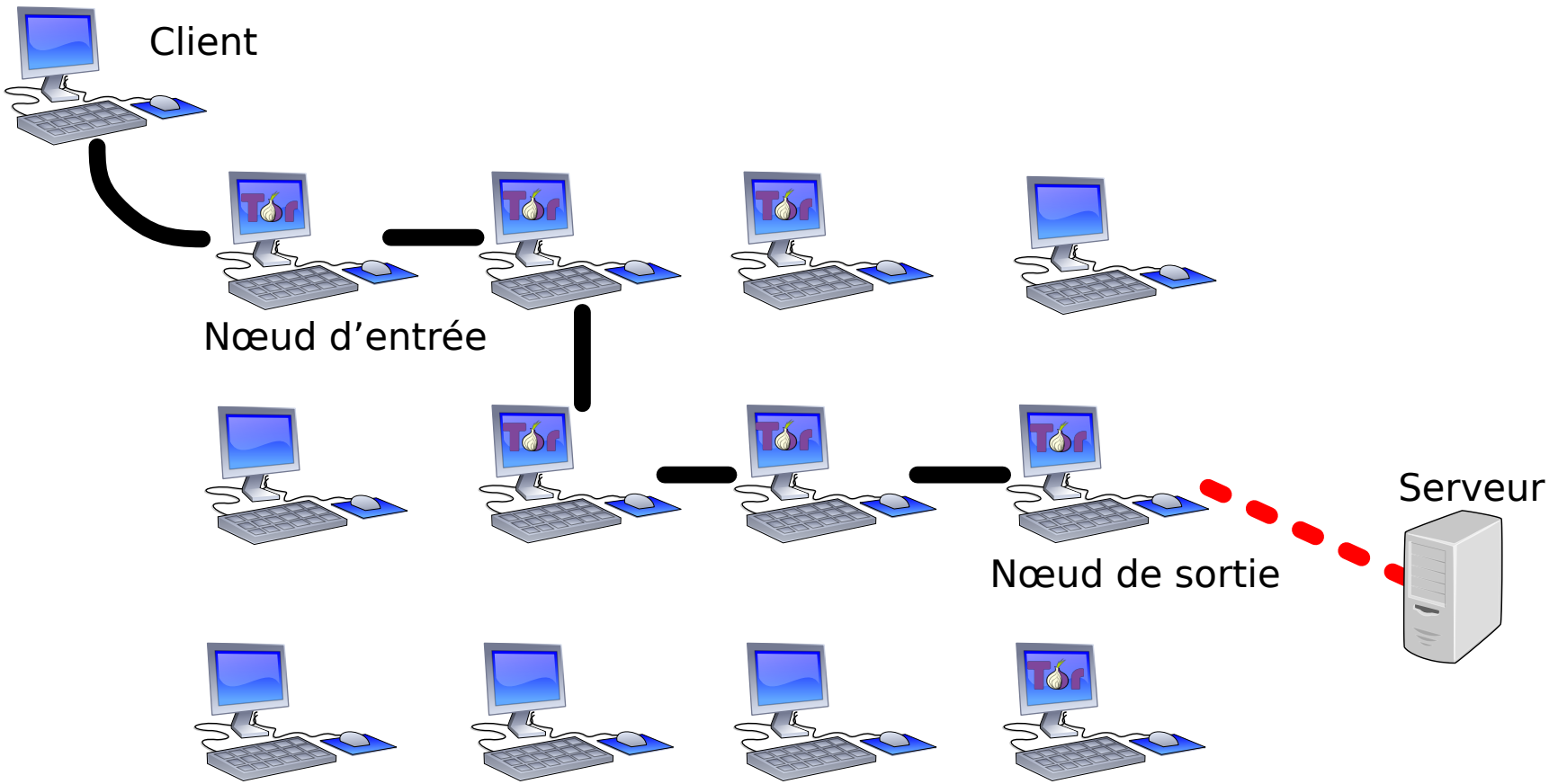
Le certificat n'est valide que pour les noms suivants :
a248.e.akamai.net , *.akamaihd.net , *.akamaihd-staging.net

(Code d'erreur : ssl_error_bad_cert_domain)

Je comprends les risques

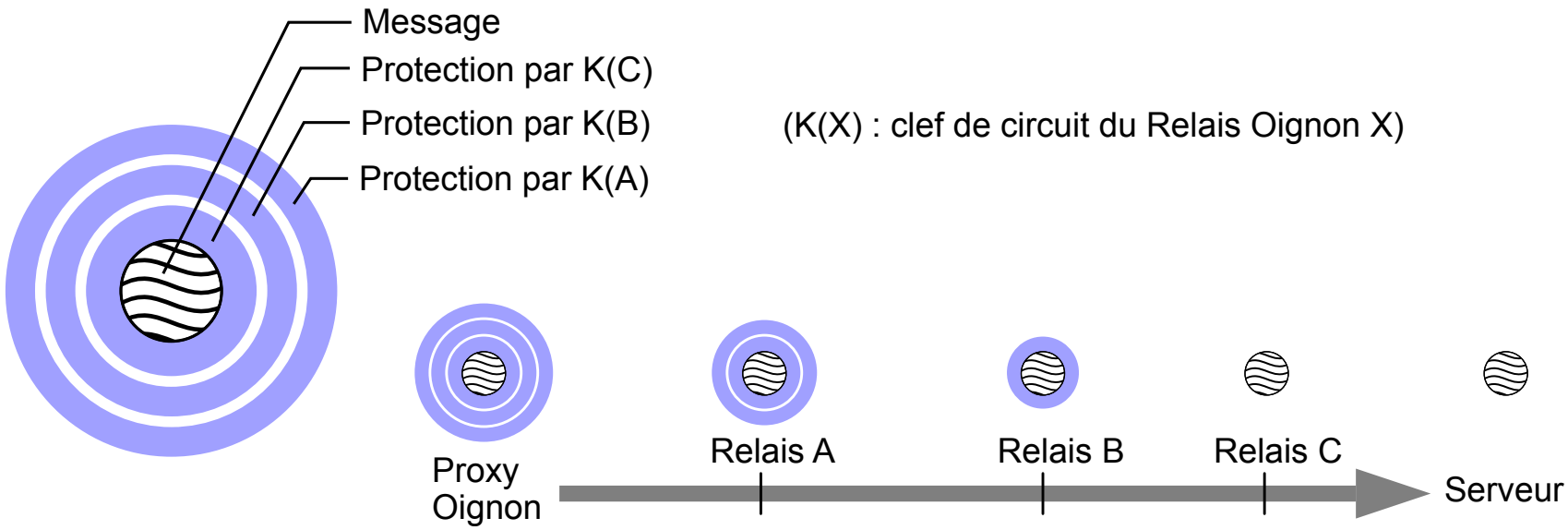
- Soit le site Web est faux
- Soit des certificats distincts sont créés pour des sites distincts
- Soit il faut ajouter une valeur dans un champ

Application : The Onion Router



https://www.torproject.org

Application : Tor



Application : Messagerie instantanée

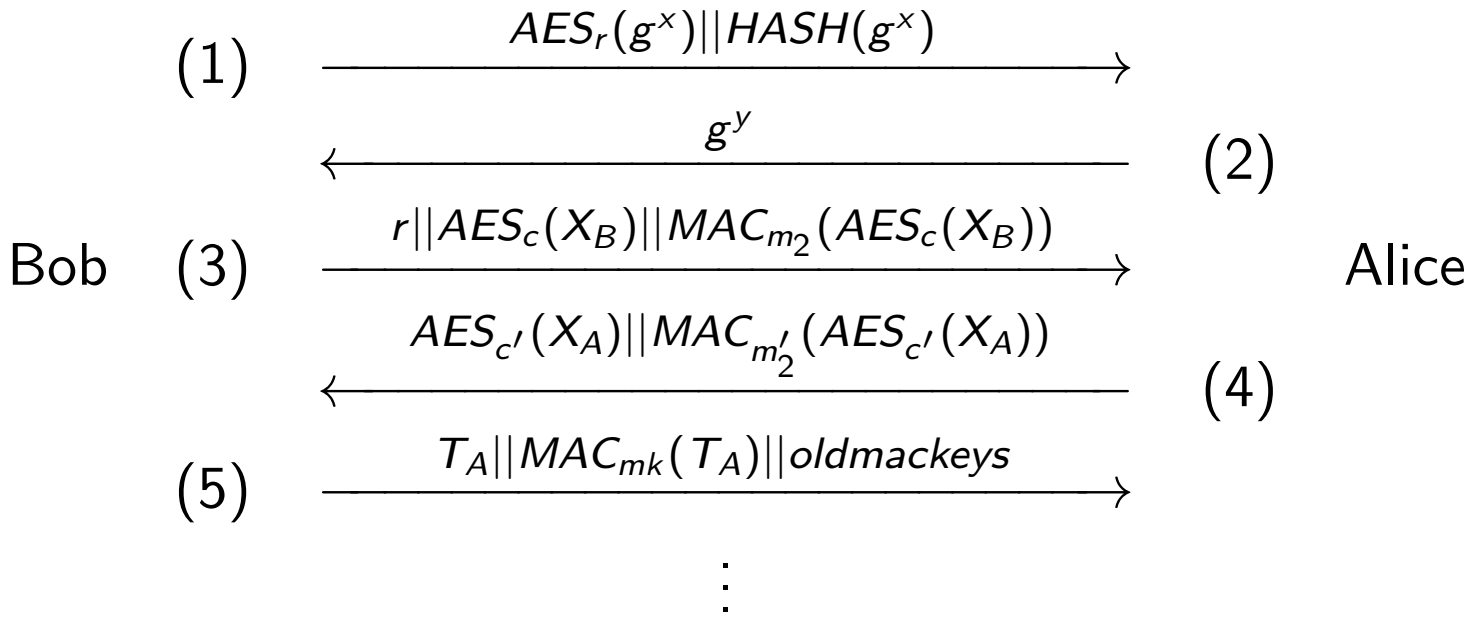
Application : Off-the-Record Messaging (OTR)

Inventé par N. Borisov, I. Goldberg et E. Brewer en 2004.

- Confidentialité : Personne ne peut lire vos messages
- Authentification : Sûr de parler à son interlocuteur
- Révocabilité (*deniability*) des conversations : personne ne doit pouvoir prouver que vous tes l'auteur des messages.
- Les messages sont authentiques et non-modifiés
- Confidentialité persistante (Perfect forward secrecy) : La perte des clefs privées ne compromet pas les conversations passées.

Utilise AES, SHA-1, Diffie-Hellman dans le protocole AKE

Application : AKE



À partir de $s := (g_y)^x$ génére par hachage :

- 2 clefs symétriques c et c'
- 4 clefs MAC m_1, m'_1, m_2 et m'_2

$X_B := Kpub_B||keyid_B||SIGB_(M_B)$
$X_A := Kpub_A||keyid_A||SIG_A(M_A)$
$M_B := MAC_{m_1}(g^x||g^y||Kpub_B||keyid_B)$;
$M_A := MAC_{m'_1}(g^y||g^x||Kpub_A||keyid_A)$;
$T_A := (keyid_A||keyid_B||next_{dh}||ctr||AES - CTR_{ek,ctr}(msg))$

Plan

Référentiel Général de Sécurité (RGS)

3 types de Prestataire de Services de COnfiance (PSCO) :

- Prestataire de Services de Certifications Electroniques (PSCE)
- Prestataire de Services d'Horodatage Electroniques (PSHE)
- Prestataire d'Audit de la SSI (PASSI)

Plusieurs services :

- Confidentialité des données
- Aunthentification des utilisateurs et serveurs
- Signature
- Cachet électronique
- Horodatage

Réglementation eIDAS

Autres aspects

Politique de Certification (PC)

- Cycle de vie d'un certificat
- Identification authentification
- Support de certificat
- Profil des certificats
- Audit et conformité
- Conditions générales d'utilisation

Deploiement d'une PKI
Évaluation de la sécurité

Plan

Pour résumer

Les PKIs sont partout : https, PGP, EMV, OTR etc ...

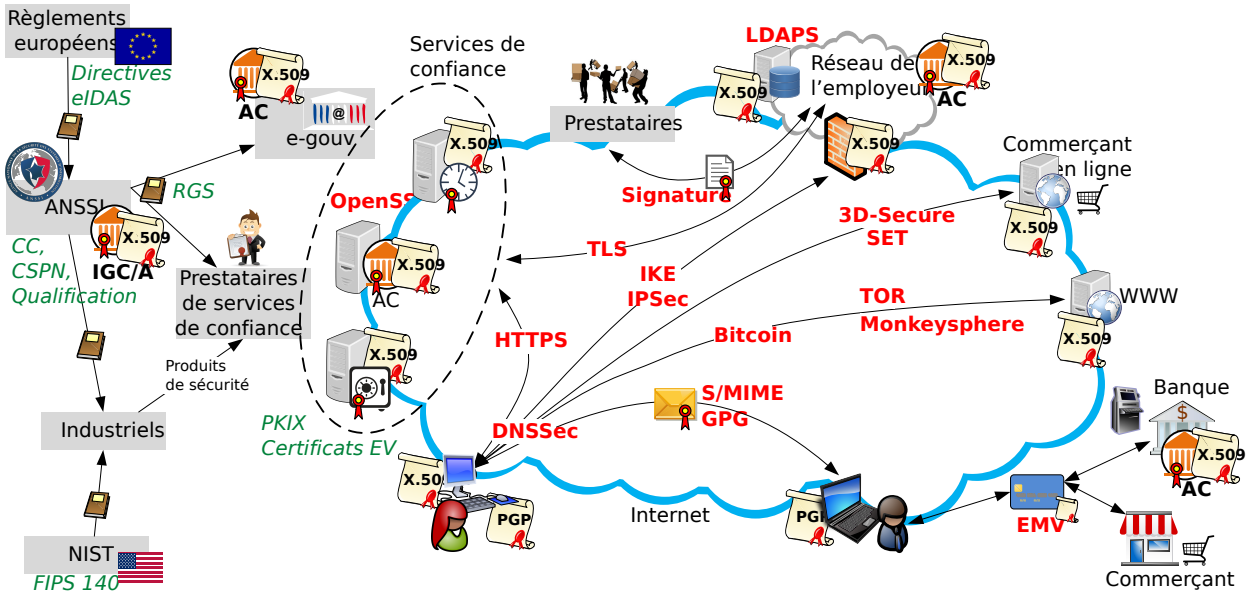
1. AVOIR une paire de clefs
2. SIGNER et CHIFFRER ses emails
3. PKI est incontournable en sécurité
4. Une PKI offre la LIBERTÉ de communiquer de manière sécurisée

Pour résumer

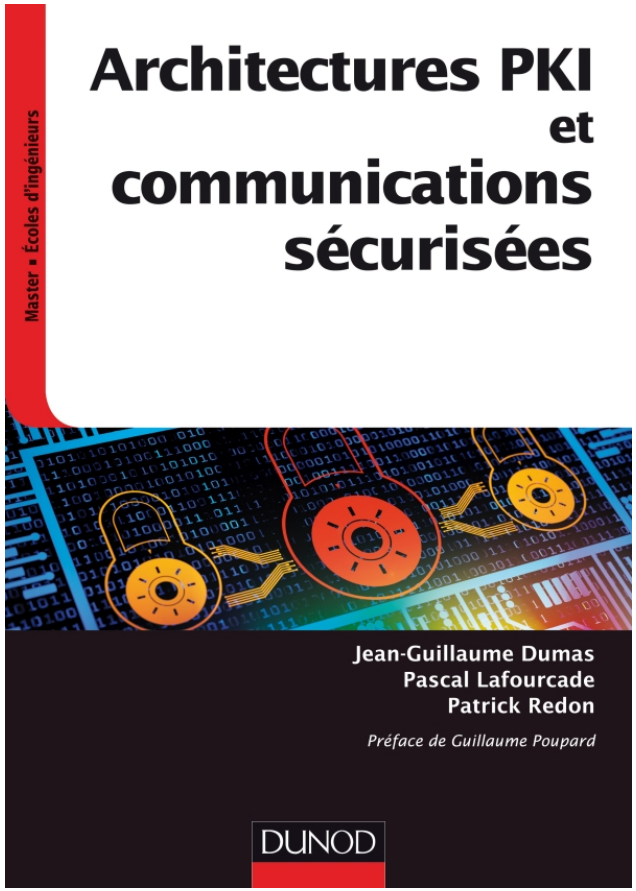
Les PKIs sont partout : https, PGP, EMV, OTR etc ...

1. AVOIR une paire de clefs
2. SIGNER et CHIFFRER ses emails
3. PKI est incontournable en sécurité
4. Une PKI offre la LIBERTÉ de communiquer de manière sécurisée

Devenez acteur de la sécurité de votre vie numérique



Merci pour votre attention



http://confiance-numerique.clermont-universite.fr/