Administration système et réseau

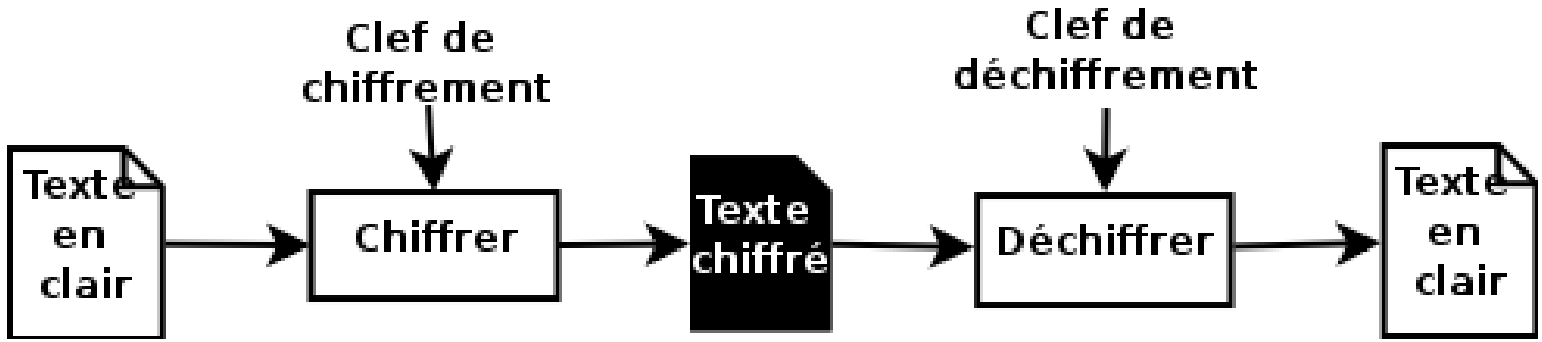
Notions de base en cryptographie appliquées à la sécurité des échanges

Nicolas Hernandez

Cours de DUT informatique – 2ème année
IUT de Nantes – Département Informatique
2006 – 20??

Cryptographie et sécurité des échanges– Sommaire

Terminologie



Définitions

Cryptographie : désigne l'ensemble des techniques de chiffrement de l'information

Cryptanalyse : techniques visant à l'obtention du message en clair ou de la clef de chiffrement sans aucune information

Cryptologie[1] = **Cryptographie** + **Cryptanalyse**

1. *crypter/décrypter/cryptage/décryptage* sont des anglicismes ; les termes français sont *chiffrer/déchiffrer/chiffrement/déchiffrement*

Services rendus par la cryptographie

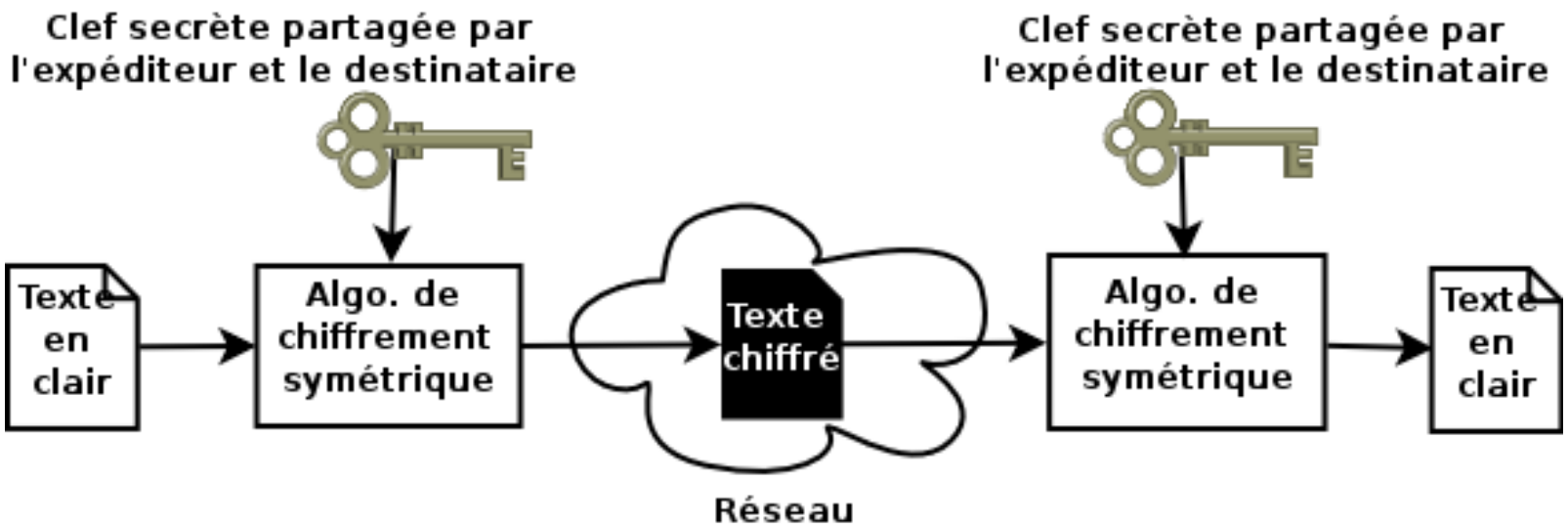
- **Confidentialité** : contenu secret par algorithmes de **chiffrement**
- **Authentification** : validation de l'expéditeur par algorithmes de **signature numérique**
- **Intégrité** : contenu non modifié vérifié par algorithmes de **hachage/empreinte**
- **Echanges de clefs** de chiffrement pour une session

Confidentialité par chiffrement

Algorithmes symétriques

Définition

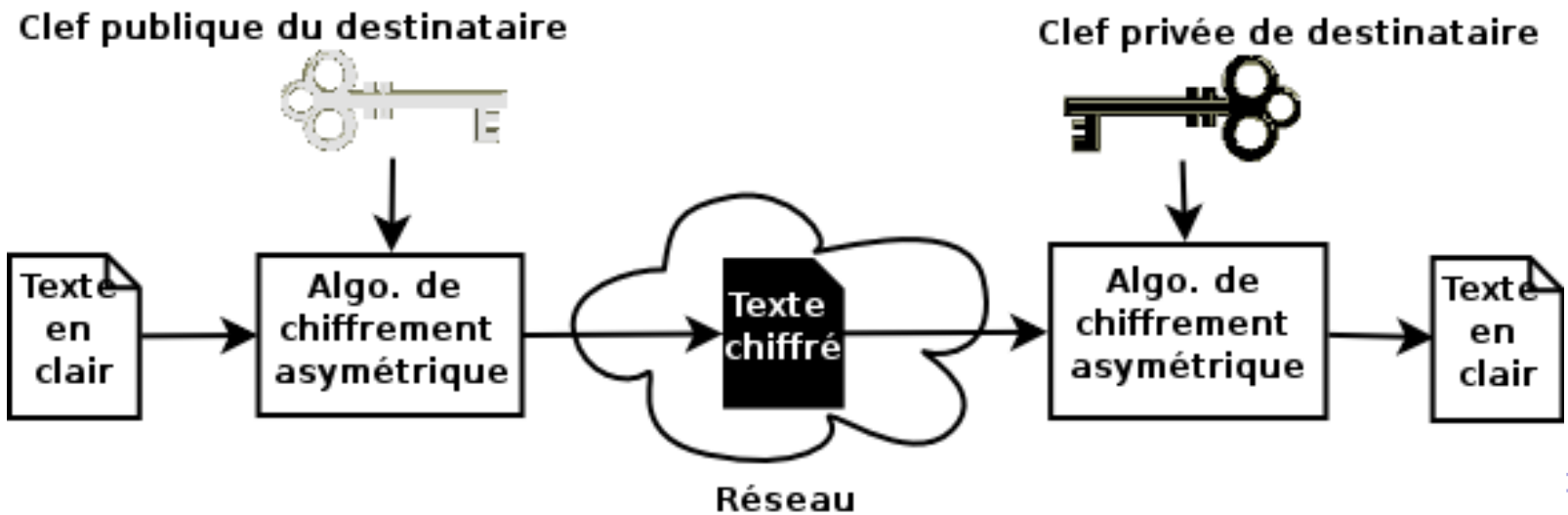
- **à clé secrète, ou symétrique** : les clefs de chiffrements et déchiffrements sont identiques
- Une même clé partagée par l'expéditeur et le destinataire
- Repose sur la non-divulgation des clés et la résistance des algorithmes aux attaques de cryptanalyse (c'est pour cela qu'on l'appelle *secrète*)



Algorithmes asymétriques

Définition

- **à clé privée et publique distinctes, ou asymétrique** : une clef publique pour chiffrer et une clef privée pour déchiffrer
- chaque personne possède une clé publique et une clé privée associée
- repose sur la difficulté de déduire la clé privée associée à une clé publique (temps non raisonnable)



Eléments de comparaison

- **Algorithmes asymétriques et symétriques**
  - en général dans le domaine public
- **Algorithmes symétriques**
  - grand nombre de clés (autant que de connexions)
  - problème de diffusion des clés secrètes
  - utilisé pour le chiffrement car plus rapide que les asymétriques
- **Algorithmes asymétriques**
  - temps de traitement important d'où non performant pour chiffrer les messages longs
  - utile pour chiffrer mais aussi pour "échanger des clés" et "signer" un message (voir plus loin)

Algorithmes symétriques majeurs

- Contexte : naissance d'Arpanet, besoin de solutions communes de chiffrement
- **DES** (*Data Encryption Standard*)
  - Proposition d'IBM, modifiée sur demande de NSA (réduction de taille de clef)
  - Adopté par NIST (*National Institute of Standards and Technology*) en 1977
  - Algorithme connu : opérations (décalage, permutation, ...) sur des blocs de données en fonction des 64 bits de clé secrète (56 bits utile +8 bits de parité) ; réversibles, la complexité (sécurité) réside dans la taille de la clé
- En 1998, remplacé par **Triple DES** avec clé de 3*56 bits
- Puis en 2001, par **AES** (*Advanced Encryption Standard*)
  - clé de 128, 192 ou 256 sur blocs de 128
  - instructions implémentées en dur dans processeurs modernes (chiffrement à vitesse comparable à flux du bus RAM)
- Autres algo. :
  RC2, RC4, RC5 (*Rivest Code*), diffusé par RSA Sec. Inc. clé jusqu'à 2048 bits
  IDEA (*International Data Encryption*) clé de 128 bits sur des blocs de 64 et utilisé par le protocole de messagerie PGP (*Pretty Good Privacy*)
  Blowfish développé par Schneier avec clé de longueur variable jusqu'à 448 bits

Résistance d'un algorithme symétrique et taille de clé

Principe

Plus la clé est longue, plus la proba. de la trouver est faible et donc plus grande est la sécurité

Evaluée par attaque force brute (énumération de toutes les combinaisons de clé)
Si clé a longueur de n bits, alors il existe 2^n possibilités de clés différentes. Soit une moyenne de 2^{n-1} essais pour trouver la bonne clé

Il est devenu relativement simple de "casser" des clés de 40 bits (i.e. environ 10^{12} possibilités),
on préfère chiffrer avec des clés de 128 bits (10^{38} possibilités)
Distributed.net (réseau de machines de par le monde pour du calcul distribué)

- RSA Lab's 56-bit DES-III (3e opus et non triple DES) Encryption Challenge : Distributed.net montre le 19 janvier 1999 que la vérification d'au plus 2^56 clés est possible en 22,5 heures (avec l'aide de EFF's Deep Crack custom DES cracker)
- RSA Lab's 64-bit RC5 Encryption Challenge (RC5-64) : Terminé le 14 juillet 2002 (après 1757 jours et 83% des clés testées)

Algorithmes asymétriques majeurs

Principe

Des paramètres (publiques) d'une fonction mathématique connue permettent de transformer un message clair en chiffré mais ne permettent de déduire les paramètres produisant l'opération inverse

- **RSA** (*Rivest, Shamir et Adleman*)
  - clé de longueur variable ; facile de calculer le produit de 2 grands nombres premiers ; difficile de trouver les facteurs premiers de celui-ci (problème de la décomposition en produit de facteurs premiers)
  - Utilisé dans PGP
- **Diffie-Hellman**
  - repose sur difficulté d'inverser l'exponentiation dans un corps fini (i.e. calculer un logarithme discret)
  - aujourd'hui utilisation des courbes elliptiques à la place des corps
  - utilisée dans IPSec et SSL

La "simplicité" de RSA

Création d'une paire de clés :

- choisir deux nombres premiers (non divisible excepté par 1 et eux-même) et calculer $n = p.q$
- choisir e un entier naturel tels que p premier (et inférieur) avec $\phi(n) = (p-1)(q-1)$ et calculer d inverse de e modulo $\phi(n)$ (calculé via algorithme d'Euclide étendu)
- (e, n) est la clé publique et (d, p, q) la clé privée

Une fonction de chiffrement :

$$\text{Chiffré} = \text{Clair}^e \text{ modulo } n$$

Et une fonction de déchiffrement identique :

$$\text{Clair} = \text{Chiffré}^d \text{ modulo } n$$

avec *Clair*, message en clair et *Chiffré*, message chiffré

Authentification de l'expéditeur

Signature par clé privé

Comment Bob puisse-t-il être sûr que c'est bien Alice qui lui adresse un message ?

Principe

L'émetteur, Alice, **chiffre avec sa clé privée** *son message*

- *Alice_priv(Message_clair) = Message_chiffrée*

et l'envoie au récepteur
Pour Bob, le message reçu vient bien d'Alice, s'il peut **le déchiffrer avec la clé publique** *d'Alice*

- *Alice_pub(Alice_priv(Message_clair)) = Message_clair*

Algorithmes de signatures :
RSA, **DSA** (*Digital Signature Algo.*) développé et utilisé par le gouvernement des Etats-Unis, **GOST** (*Gosudarstvennyi Standard of Russian Federation*), ...

Contrôle de l'intégrité du message

Calcul d'une empreinte pour vérifier l'intégrité

Comment Bob puisse-t-il être sûr que personne n'a modifié le message qu'Alice lui a adressé ?

Principe

1. *L'émetteur utilise une* **fonction de hachage** *pour calculer* **empreinte (*digest*)** *du message qu'il joint à son envoi*
2. *Le récepteur recalcule l'empreinte avec la même fonction de calcul qu'il applique au message reçu*
3. *S'il constate une différence alors le message a été altéré*

- Empreinte courte, irréversible et proba. faible que 2 messages aient empreinte identique
- Principales fonctions : **MD5** (*Message Disgest #*) de 1992 défini dans RFC 1321 et conçu par Rivest fournit empreintes de 128 bits, **SHA-1** (*Secure Hash Algorithm*) de 1993 fournit empreintes de 160 bits
- Checksum des images d'ubuntu `http://releases.ubuntu.com`

Echanges de clé

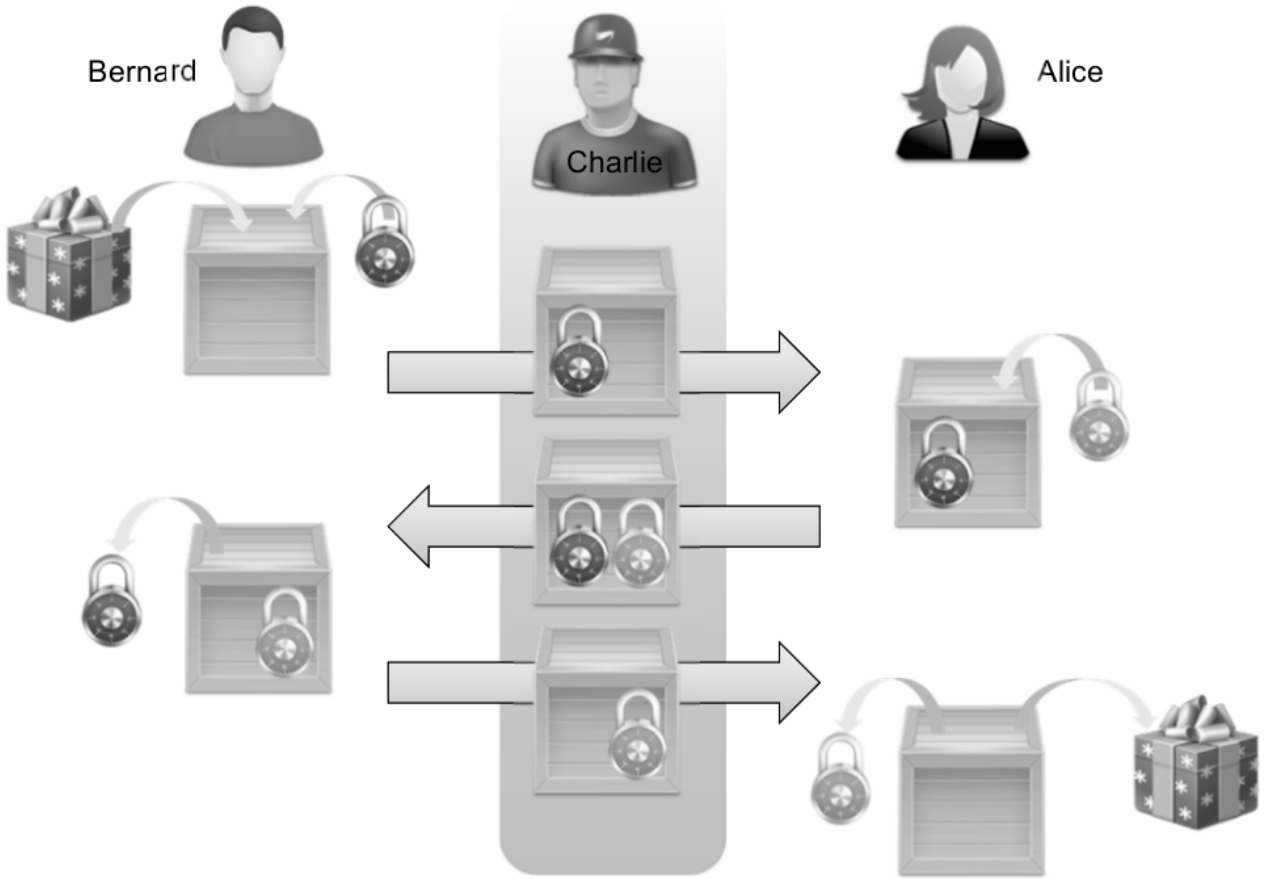
Echange de clé secrète : paradoxe

Paradoxe du chiffrement à clé secrète

Pour que deux personnes puissent communiquer secrètement, elles doivent déjà partager un secret...

Echange de clé secrète : protocole de Diffie-Hellmann

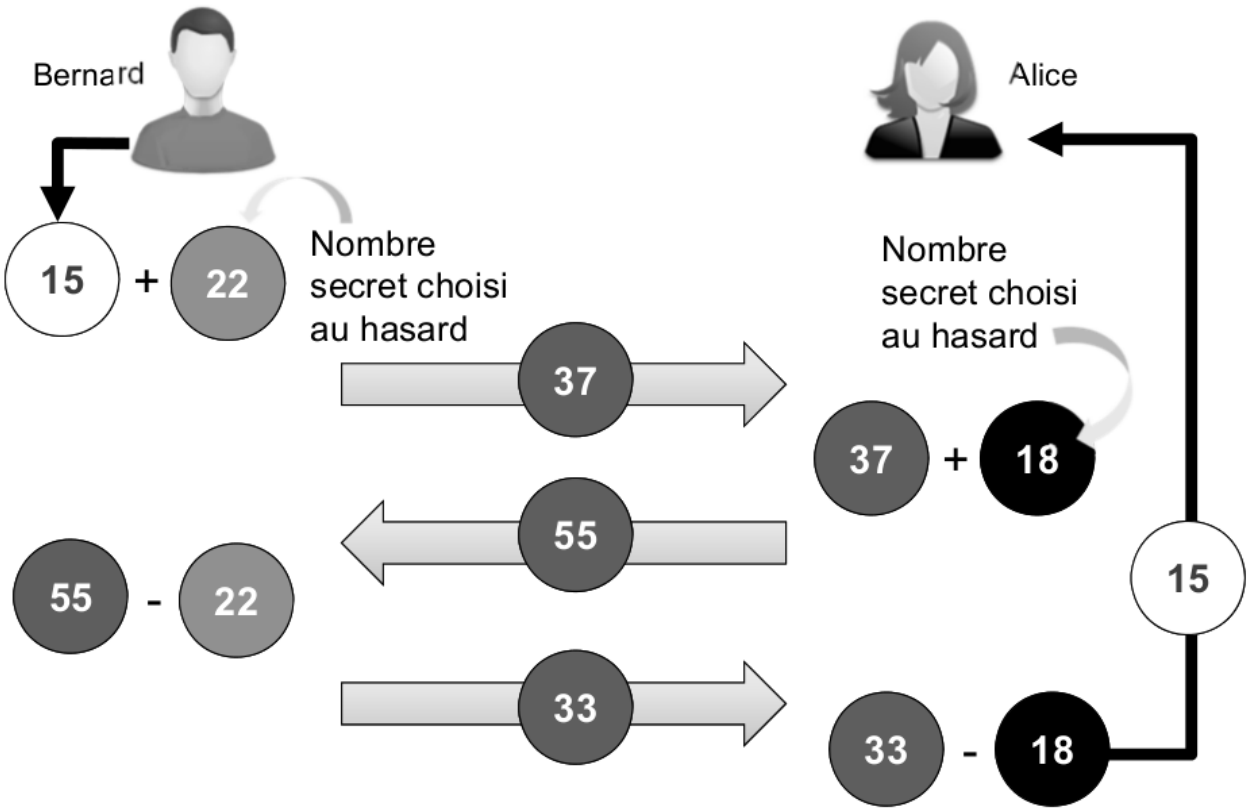
Principe



(Crédit : Christian Bulfone)

Echange de clé secrète : protocole de Diffie-Hellmann

Exemple



(Crédit : Christian Bulfone)

Echange de clé secrète : protocole de Diffie-Hellmann

Permet de construire clé secrète sans qu'elle circule sur le réseau

Repose sur le fait que

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

Alice et Bob vont donc

- s'échanger deux nombres g et p
  avec p premier et g inférieur à p et primitif [2] par rapport à p
- choisir chacun un nombre secret. Resp. a et b
- calculer la valeur $(g^a mod(p))$ pour Alice et $(g^b mod(p))$ pour Bob et se les envoyer
- calculer la clé secrète à partir de la valeur reçue. Resp. $(g^b mod(p))^a mod(p)$ pour Alice et $(g^a mod(p))^b mod(p)$ pour Bob
- In fine, Alice et Bob connaissent donc tous les deux le nombre $g^{ab} mod(p)$ dont Ève n'a pas connaissance

2. est primitif si il existe un v tel que $g^v = u \ mod p$ pour tout u allant de 1 à $p-1$

Echange de clé secrète : l'enveloppe digitale

Problème

- *Lenteur des algo. asymétiques pour les longs messages*
- *Difficulté d'échanger clés secrètes pour algo. symétrique*

Solution

L'enveloppe digitale qui combine les deux types d'algo.
Utilisation d'un algorithme de chiffrement asymétrique pour échanger une clé de chiffrement symétrique dite **clé de session**

En pratique,

1. l'un des correspondants génère une clé secrète,
2. chiffre le message avec cette clé
3. qu'il communique avec le message chiffré à l'aide de la clé publique du destinataire

Comment vérifier la clé publique du destinataire ?

Infrastructure de Gestion de Clés Publiques (IGC)

Problème

- *Risque de substitution d'identité (Man-in-the-middle)*
  Alice demande à Bob sa clé publique mais Charlie répond à sa place en fournissant la sienne
- *Impossibilité de mémoriser l'ensemble des clés publiques de tous les correspondants*

Besoin d'un tiers de confiance qui ait les fonctions suivantes :

- génération de clé privé et publique et attribution à une entité
- gestion de certificats
- diffusion de clés publiques

Solution

IGC, plus connu sous le nom anglais **PKI** (*Public Key Infrastructure*)

Certificat numérique

Définition

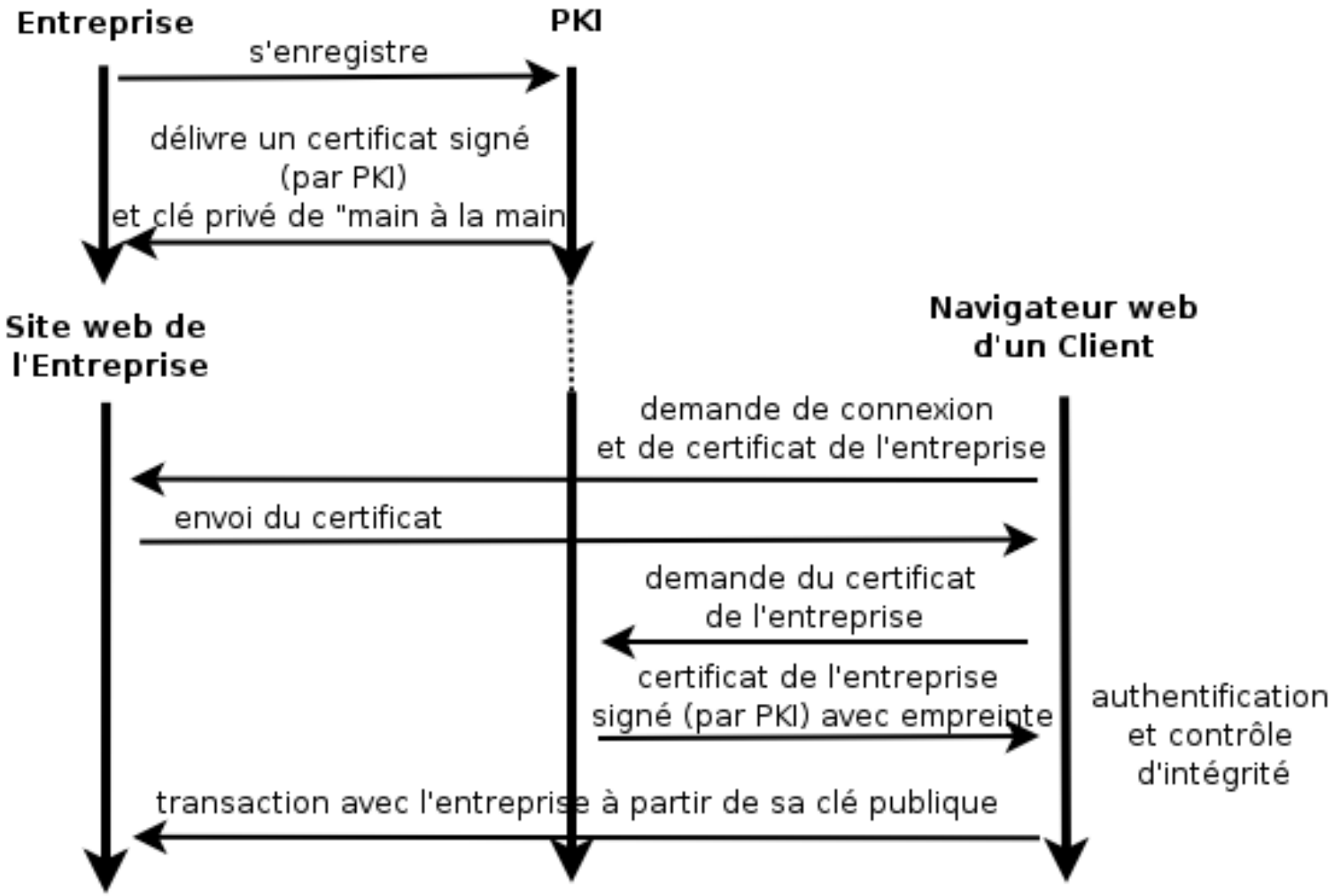
Certificat : carte d'identité numérique (clé publique) d'une entité signée et avec empreinte par un tiers de confiance

Le format le plus courant provient du standard X.509. Il contient :

- Numéro de série
- Id. de son propriétaire
- Id. de l'organisme délivreur
- Clé publique délivrée
- Période de validité
- Signature du certificat
- ...

Nos navigateurs web intègrent par défaut une liste de PKI (voir le menu préférence)

Exemple de délivrance de certificats numériques



Quizz de synthèse sur la cryptographie appliquée à la sécurité des échanges

- Quels algorithmes me permettent d'assurer la confidentialité ? L'authentification ? L'intégrité ?

Quizz de synthèse sur la cryptographie appliquée à la sécurité des échanges

- Comment puis-je signer une message à l'aide d'un algorithme asymétrique ? à l'aide d'un algorithme symétrique ?