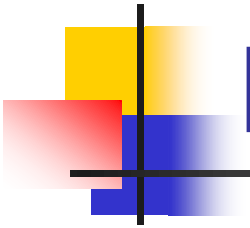
L’identité numérique

Risques, protection



Plan

- Communication sur l'Internet
- Identités
- Traces
- Protection des informations

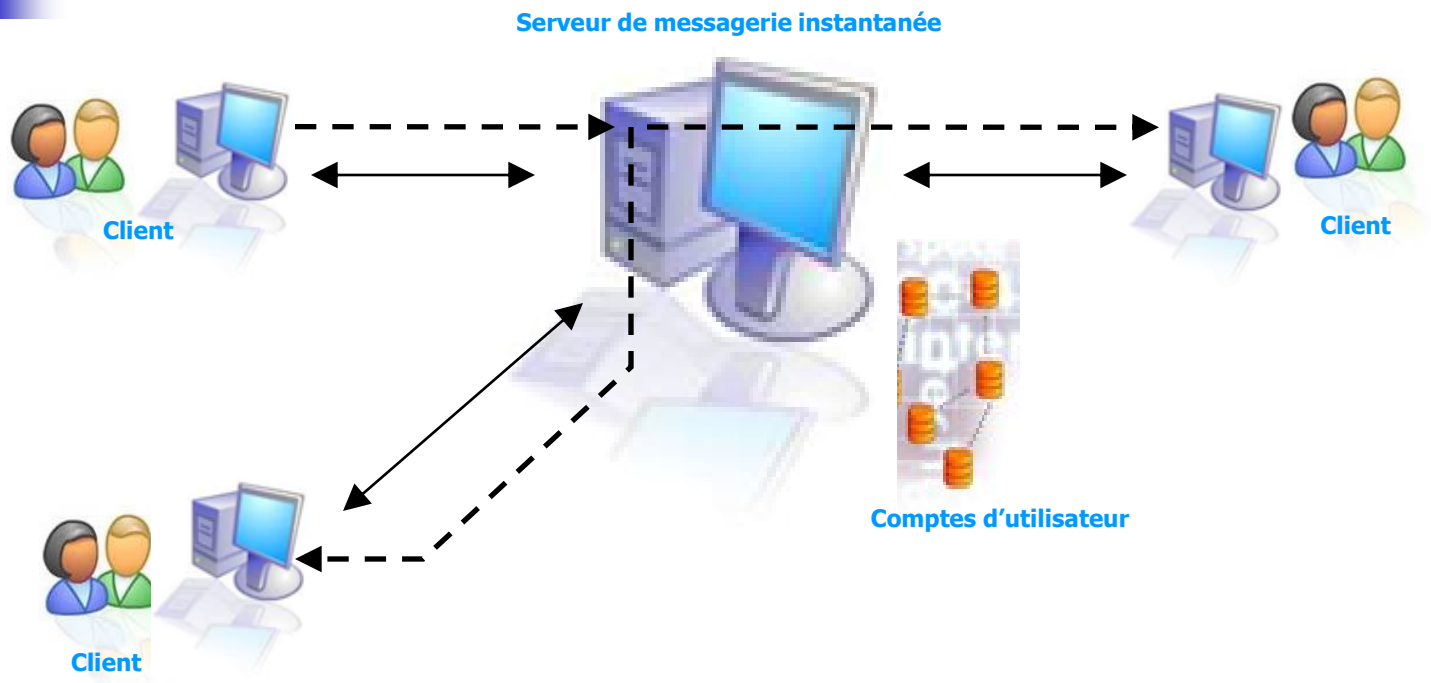
Communication numérique

- Messages
  - Chaque caractère d'un message « texte » est codé sur 1 octet, ou Byte (soit 8 bits), selon une table de correspondance (exemple : table ASCII)
  - Autres messages : le codage binaire dépend de la structure du message (ou du fichier)
- Communication
  - Les messages sont expédiés d'un ordinateur vers un autre par l'intermédiaire du réseau:
    - Notion d'adresse IP (Internet Protocol)
    - Notion de routeurs (matériel qui orientent, routent, les messages à travers les mailles du réseau Internet

Modes de communication

- Communication synchrone
  - Chat (« clavardage »), messagerie instantanée
  - Tableau blanc électronique
  - Conférence en ligne, vidéo conférence
  - Téléphonie (Skype), P2P (PeerToPeer)
    - ➔ Dialogue en simultanéité
- Communication asynchrone
  - Courrier électronique
  - Liste de diffusion (abonnement à une liste)
  - Forum et blog
  - Sites web en général
    - ➔ Dialogue en temps différé

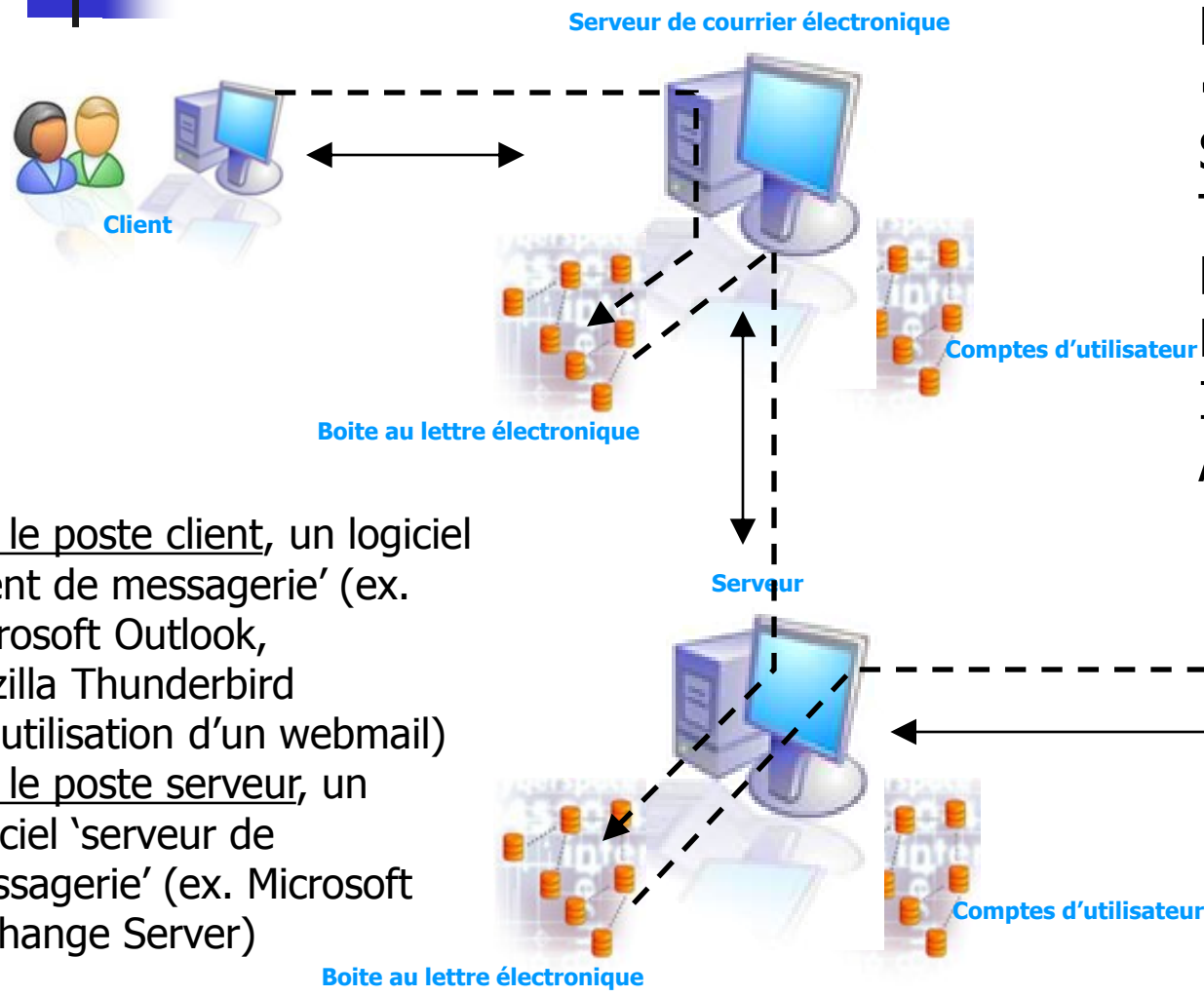
Communication synchrone



Sur le poste client, un logiciel 'client de messagerie instantanée' : ex. Windows Live Messenger
Sur le poste serveur, un logiciel 'serveur de messagerie instantanée': ex. Microsoft Live Comm.Server

↔ Dialogues client/serveur ➔ protocole
- ***(Ouvert)*** → Jabber, IRC, SIP
- ***(Propriétaire)*** → AIM, ICQ, MSN Messenger

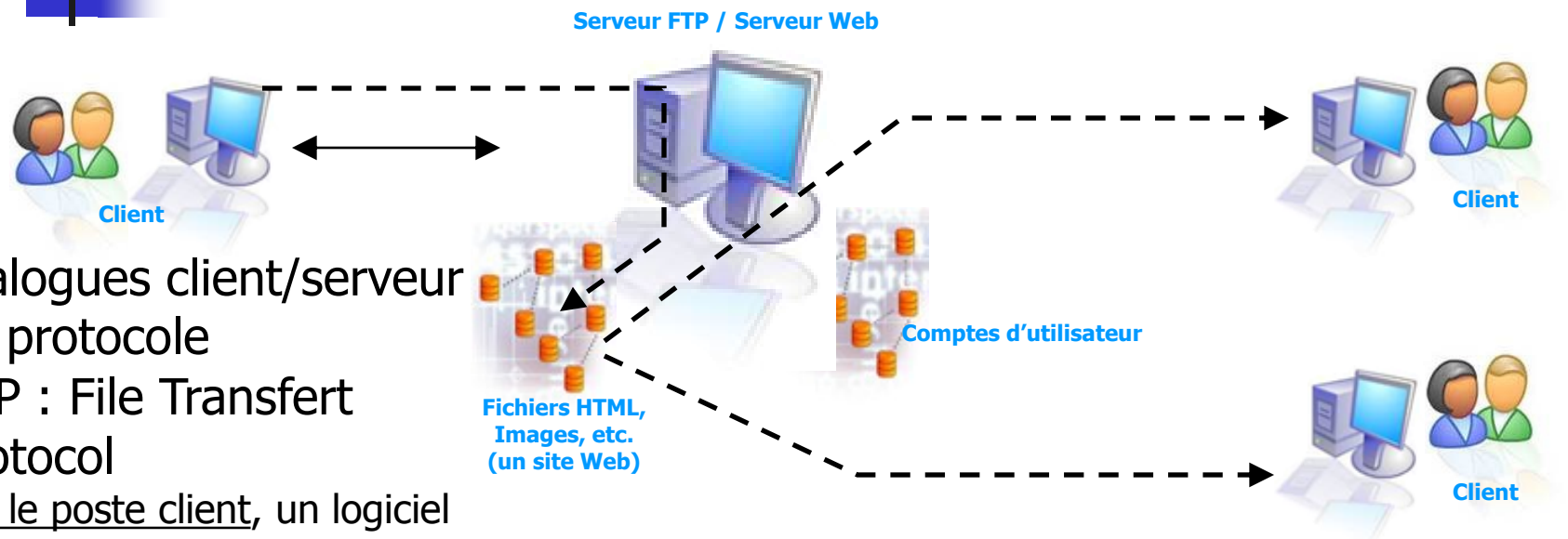
Communication asynchrone



Dialogues client/serveur
➔ protocole
SMTP : Simple Mail Transfert Protocol
POP : Post Office Protocol
IMAP : Internet Message Access Protocol

Sur le poste client, un logiciel 'client de messagerie' (ex. Microsoft Outlook, Mozilla Thunderbird
Ou utilisation d'un webmail)
Sur le poste serveur, un logiciel 'serveur de messagerie' (ex. Microsoft Exchange Server)

Communication asynchrone

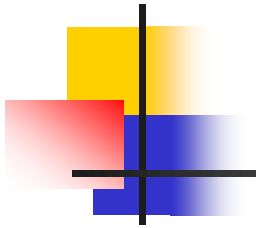


Dialogues client/serveur ➔ protocole
FTP : File Transfert Protocol

Sur le poste client, un logiciel 'client de messagerie' (ex. Microsoft Outlook, Mozilla Thunderbird Ou utilisation d'un webmail)
Sur le poste serveur, un logiciel 'serveur de messagerie' (ex. Microsoft Exchange Server)

Dialogues client/serveur ➔ protocole
HTTP : HyperText Transfert Protocol

Sur le poste client, un logiciel 'client HTTP' ou 'navigateur Web' (ex. Microsoft Internet Explorer, Mozilla Firefox)
Sur le poste serveur, un logiciel 'serveur HTTP' ou 'serveur Web' (ex. Microsoft Internet Information Server, Apache)

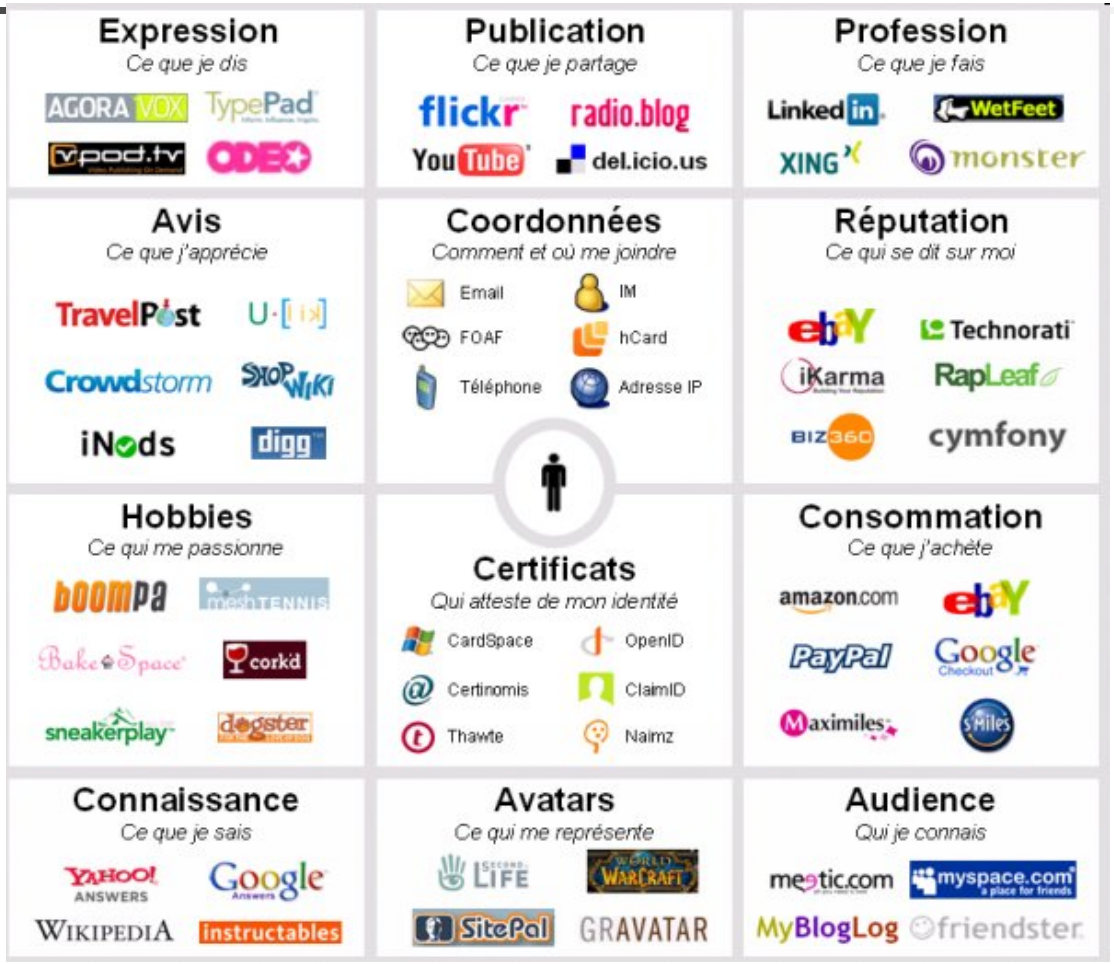


- Pour bénéficier de ces services, il est nécessaire de s’identifier...

S'identifier pour communiquer

- Identité électronique/numérique
  - Compte d'utilisateur pour s'identifier
    - Identifiant ou login (numéro, nom, adresse email, etc.)
    - Mot de passe
- Authentification
  - Procédure de vérification de l'identité électronique → permettre l'accès à certaines ressources, certains services
- Usurpation d'identité
  - Prendre délibérément l'identité d'une autre personne
  - **Délit pénal**

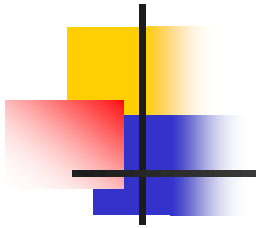
Une personne physique, des identités numériques



http://www.flickr.com/photos/fredcavazza/278973402/in/photostream/
http://www.fredcavazza.net/2006/10/22/qu-est-ce-que-l-identite-numerique/

Une personne physique, des identités numériques

http://ulik.typepad.com/leafar/2006/10/ulik_unleash_id.html



- Des identités
  - ➔une multitude de traces disséminées sur les supports de stockage ...
  - ➔des opportunités de récupération malveillante d’ informations confidentielles ...

Monde numérique, espace de liberté...surveillé !

- Chacun de nos actes virtuels laisse des traces numériques
  - Sur notre ordinateur
  - Sur les serveurs
- Pour quel usage ?
  - Repérer les habitudes de navigation de l'internaute et simplifier sa vie sur l'Internet
  - Etc. ...

Les Cookies ou témoin de connexion

- Où ?
  - Sur le poste client (votre ordinateur ou celui à partir duquel vous vous êtes connecté...)
- Sous quelle forme ?
  - Un fichier, avec l'indication du site qui l'a produit ce fichier et une date de limite de validité
- Quelles informations ?
  - Celles décidées par le concepteur du site web !

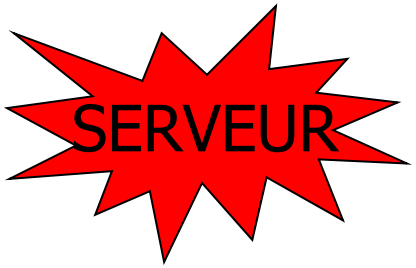
Le cache du navigateur

- Où ?
  - Sur le poste client (votre ordinateur ou celui à partir duquel vous vous êtes connecté...)
- Sous quelle forme ?
  - Des fichiers temporaires, qui seront rappelés pour une accélérer la navigation Web
- Quelles informations ?
  - Les pages consultées sur Internet : fichiers HTML, images, etc.

Le serveur Proxy ou serveur mandataire

- Où ?
  - Sur le serveur qui vous permet de vous connecter au Web
- Sous quelle forme ?
  - Des fichiers temporaires, qui seront rappelés pour une accélérer la navigation Web
- Quelles informations ?
  - Les pages consultées sur Internet : fichiers HTML, images, etc.

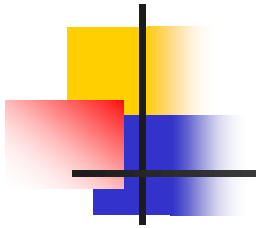
Le serveur Web (ou autres serveurs)



- Où ?
  - Sur le serveur Web que vous interrogez
  - Sur les serveurs avec lesquels vous dialoguez
- Sous quelle forme ?
  - Des données relatives à la configuration de votre ordinateur accessibles aux programmes du Web
  - Fichiers d'audit
- Quelles informations ?
  - Votre adresse IP, votre type de navigateur, le système d'exploitation de votre ordinateur, etc.
  - Les requêtes que vous effectuez...

Les réseaux

- Où ?
  - Les réseaux parcourus (des milliers de km)
  - Vos voisin sur un réseau Wifi
  - Votre voisin sur un réseaux local
- Sous quelle forme ?
  - Les messages échangés
- Quelles informations ?
  - Les adresses IP et autres informations transportées



- Protéger sa navigation sur les réseaux...mais certaines traces sont indélébiles

Protection des informations

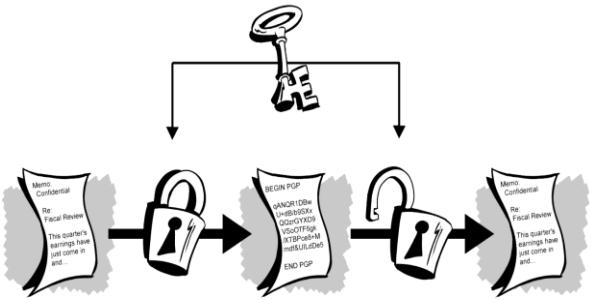
- Les informations envoyées circulent sur les réseaux à travers une multitudes de matériels avant leur arrivée à destination (routeurs, serveurs intermédiaires, etc.)
- Comment protéger les éléments de son identité numérique ?
- Comment protéger les données échangées sur le réseau Internet ?

Protection des informations

- Informations et identité
  - Crypter/chiffrer les informations transmises sur les réseaux
  - Certificat numérique
  - Signature numérique
  - Biométrie (Iris, morpholo

Cryptographie

- Science qui étudie les moyens de chiffrer/déchiffrer les messages
- Chiffrer un message
  - Modifier le contenu d'un message grâce à une clef, afin qu'il soit incompréhensible, sauf à celui qui possède la clef



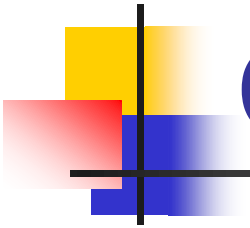
ftp://ftp.pgpi.org/pub/pgp/6.5/docs/french/IntroToCrypto.pdf

Cryptographie

- Exemple : le chiffre de César
- Méthode : décaler les lettres de l'alphabet d'un certain nombre de lettres vers la droite ou vers la gauche
- Clef : le nombre de lettres et le sens
- Exemple : clef = 3, vers la droite

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

le texte en clair « SECRET » est crypté en « VHFUHW »

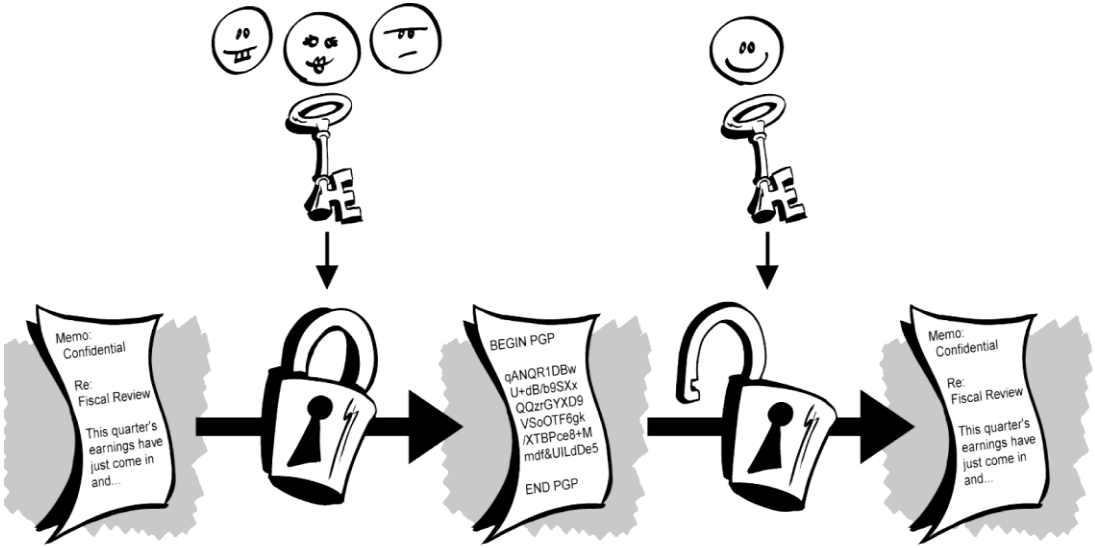


Cryptographie

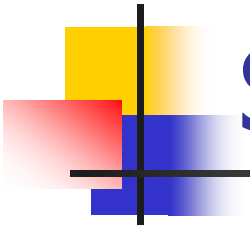
- Problème de distribution des clefs dans le système de cryptographie symétrique (même clef pour chiffrer et déchiffrer)

Cryptographie

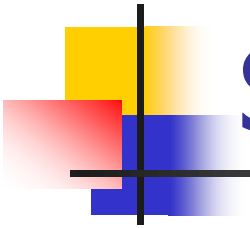
- Cryptographie à clef publique (procédé asymétrique)
  - Clé publique pour crypter
  - Clé privée (secrète) pour décrypter



Signature numérique



- MD5 : Message Digest
- Calcul d'un chiffre à partir du contenu d'un fichier
- Après téléchargement d'un fichier, on peut récupérer le fichier MD5, recalculer le chiffre à partir du fichier télécharger pour vérifier qu'aucune altération n'a été faite (introduction



Signature numérique

- Vérifier l'identité de l'expéditeur
- Vérifier l'authenticité du message
- Garantissent la non-répudiation (l'expéditeur ne peut pas dire qu'il n'a pas envoyé le message)
- Même utilité qu'une signature

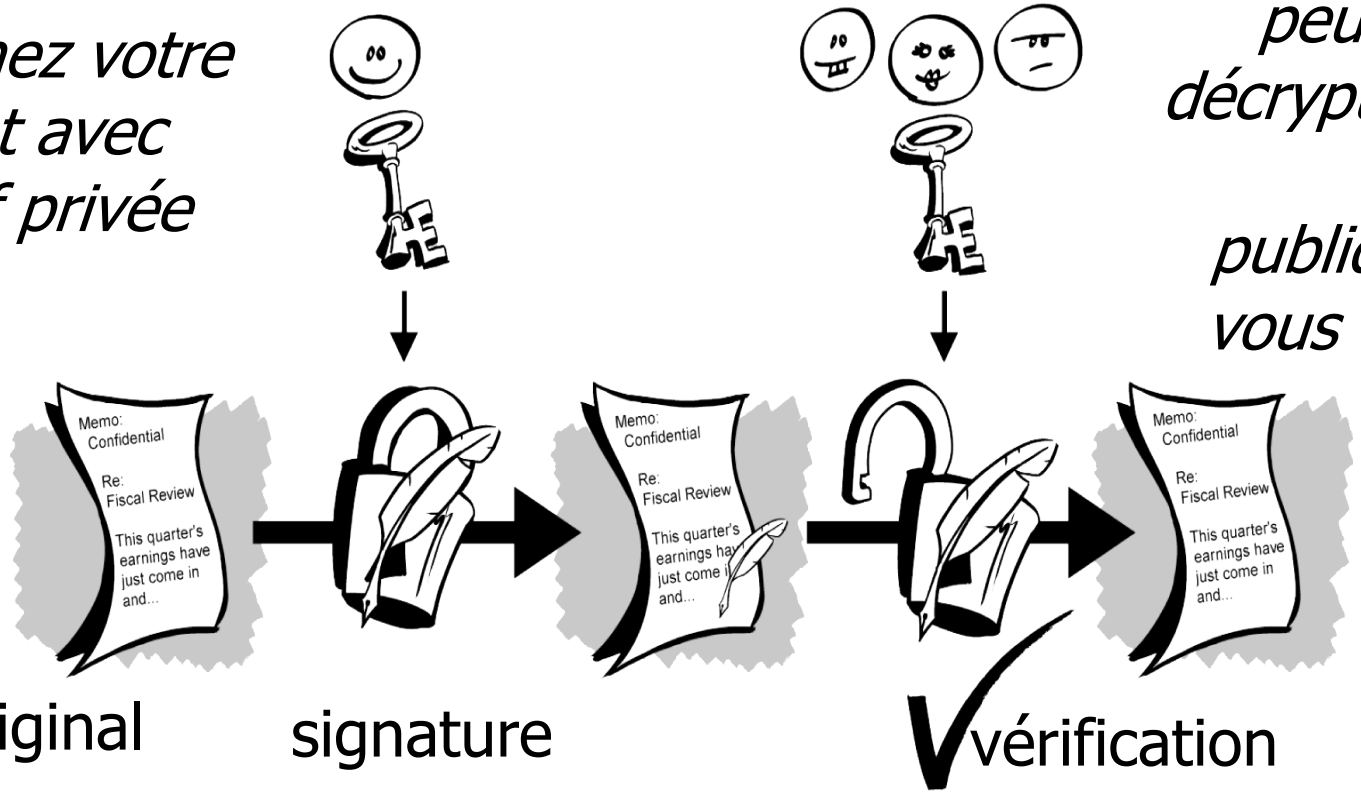
Signature numérique

Clef privée

Clef publique

Vous signez votre document avec votre clef privée

Si les infos peuvent être décryptées avec votre clef publique, c'est vous qui l'avez signé

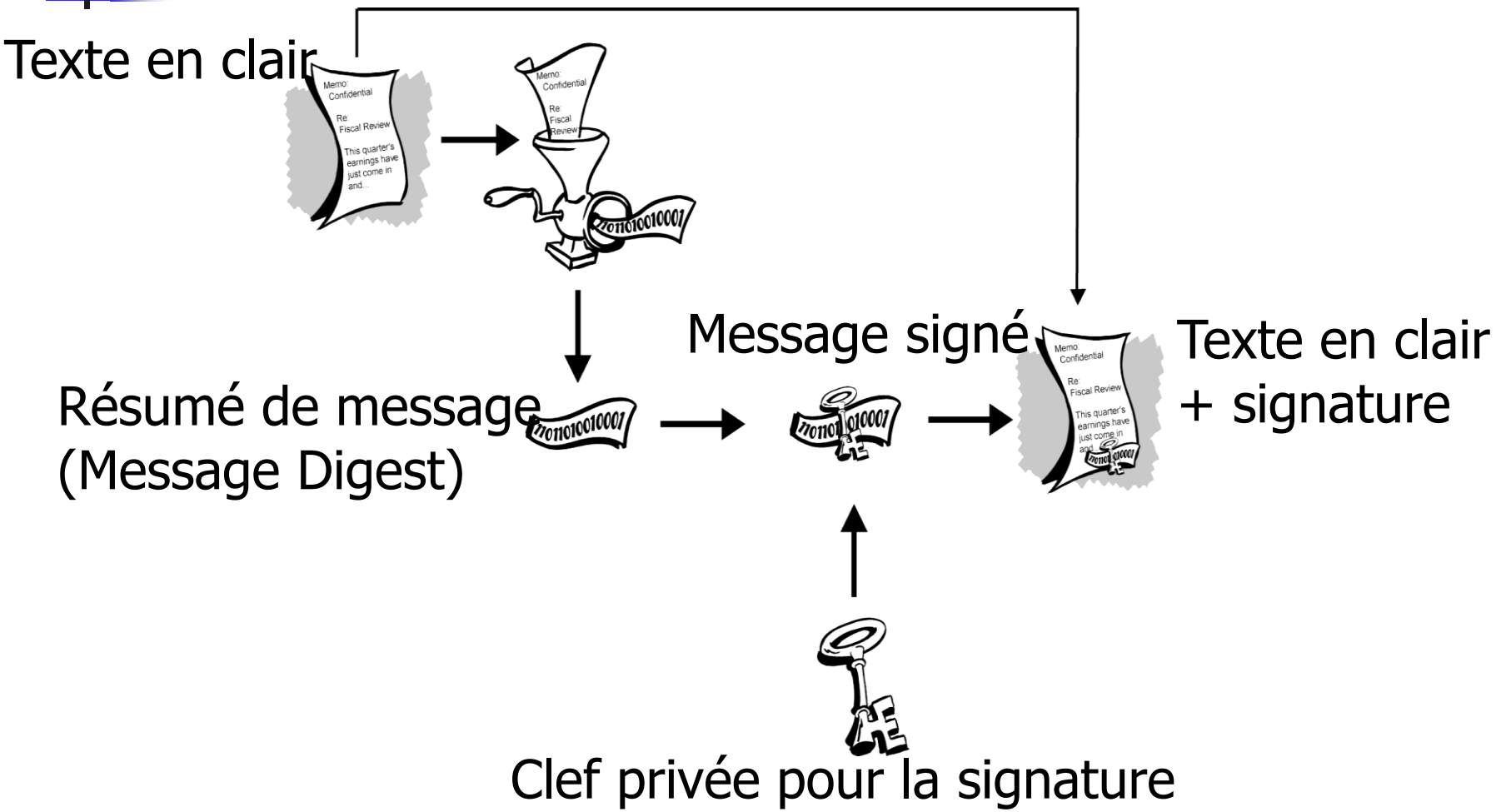


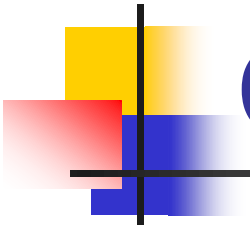
Texte original

signature

vérification

Signature numérique





Certificat numérique

- Document numérique garanti par une autorité de certification
  - Identité de l'utilisateur (nom, Identifiant, etc.)
  - Clé publique
  - signature
  - Date d'expiration du certificat
- Garantissent qu'une clef publique appartient bien à son détenteur présumé
  - Les infos d'identification sont liées à la clef publique