Troisième Partie

Sécurité des Réseaux

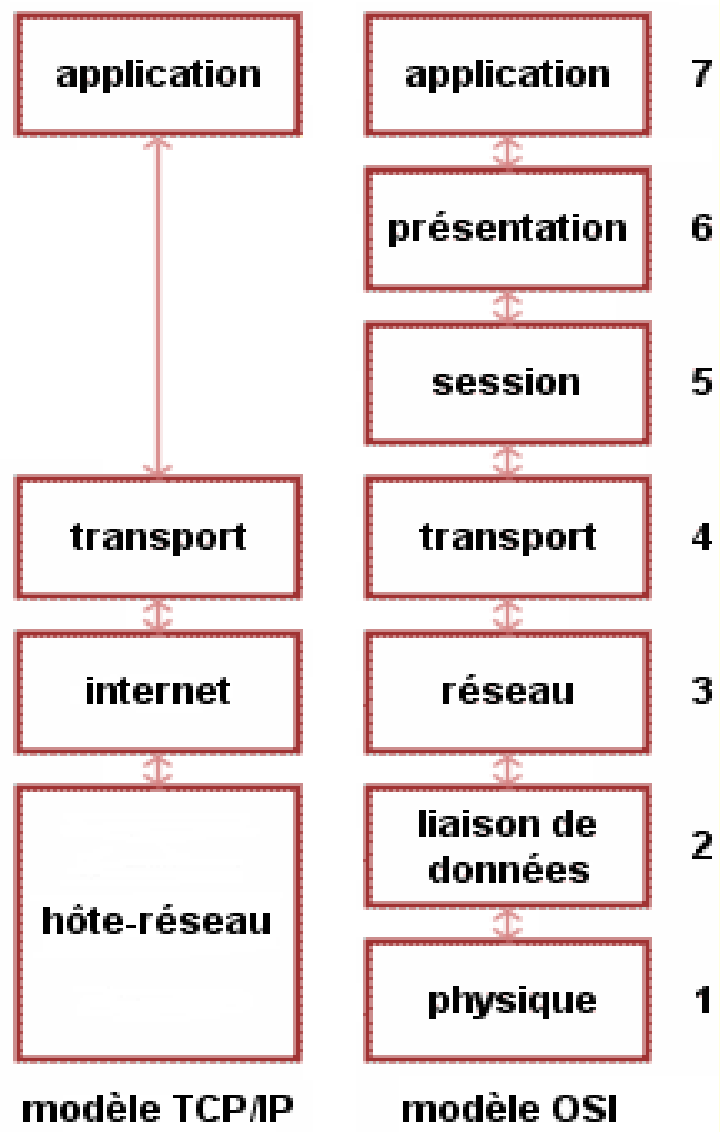
Identification / Authentification

- Un service d'authentification repose sur :
  - l'identification
    - ✓ définit les identités des utilisateurs
  - l'authentification
    - ✓ vérification des identités présumées des utilisateurs
    - ✓ authentification simple
    - ✓ authentification forte
- Plusieurs niveaux :
  - applicatif : HTTP, FTP
  - transport : SSL, SSH
  - Réseau : IPSEC
  - Transmission : PAP, CHAP

Modèle OSI (Rappel)

	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment	4. Transport	End-to-end connections and reliability (TCP)
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing (IP)
	Frame	2. Data link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

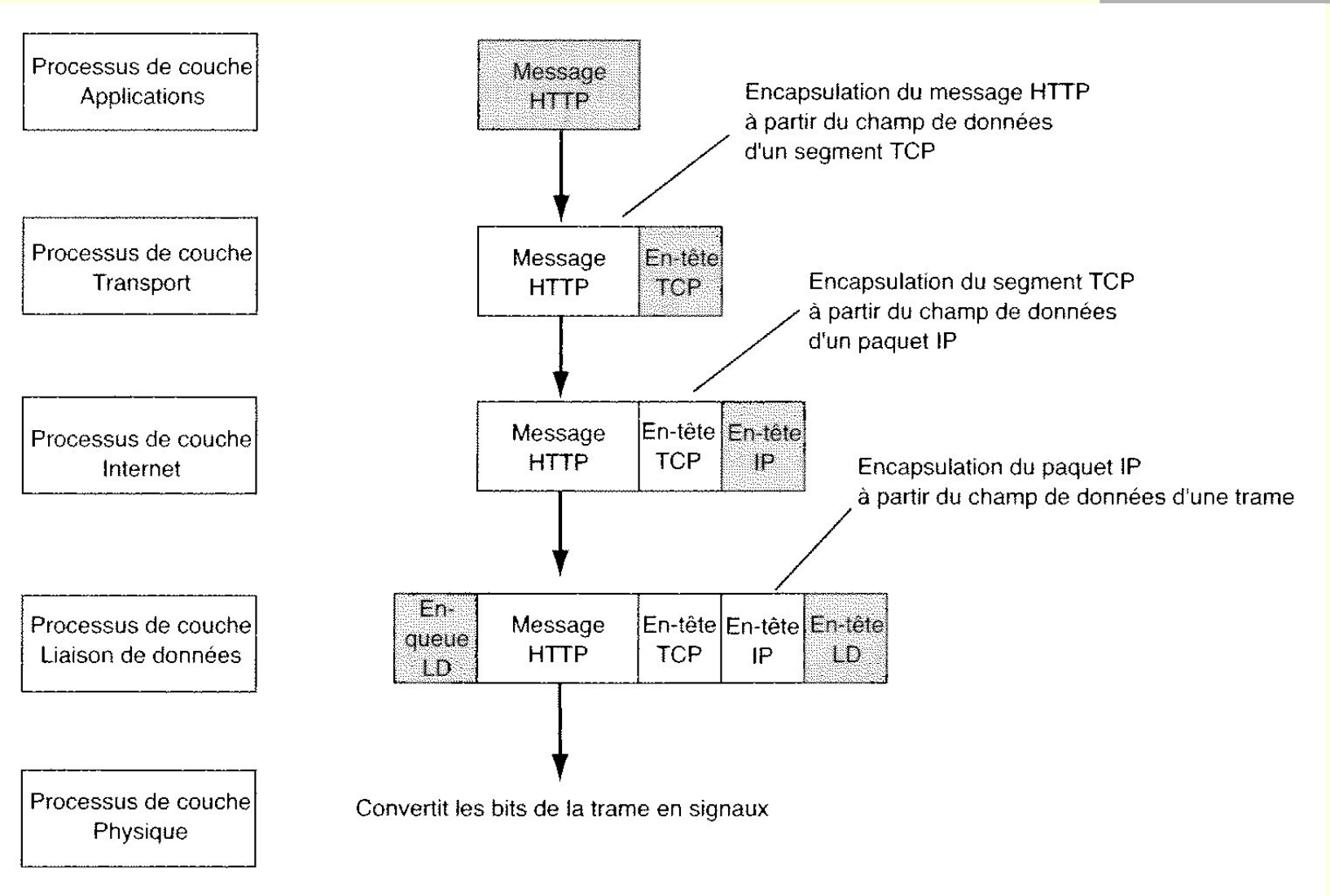
Modèle TCP/IP (Rappel)



Contrôle des accès

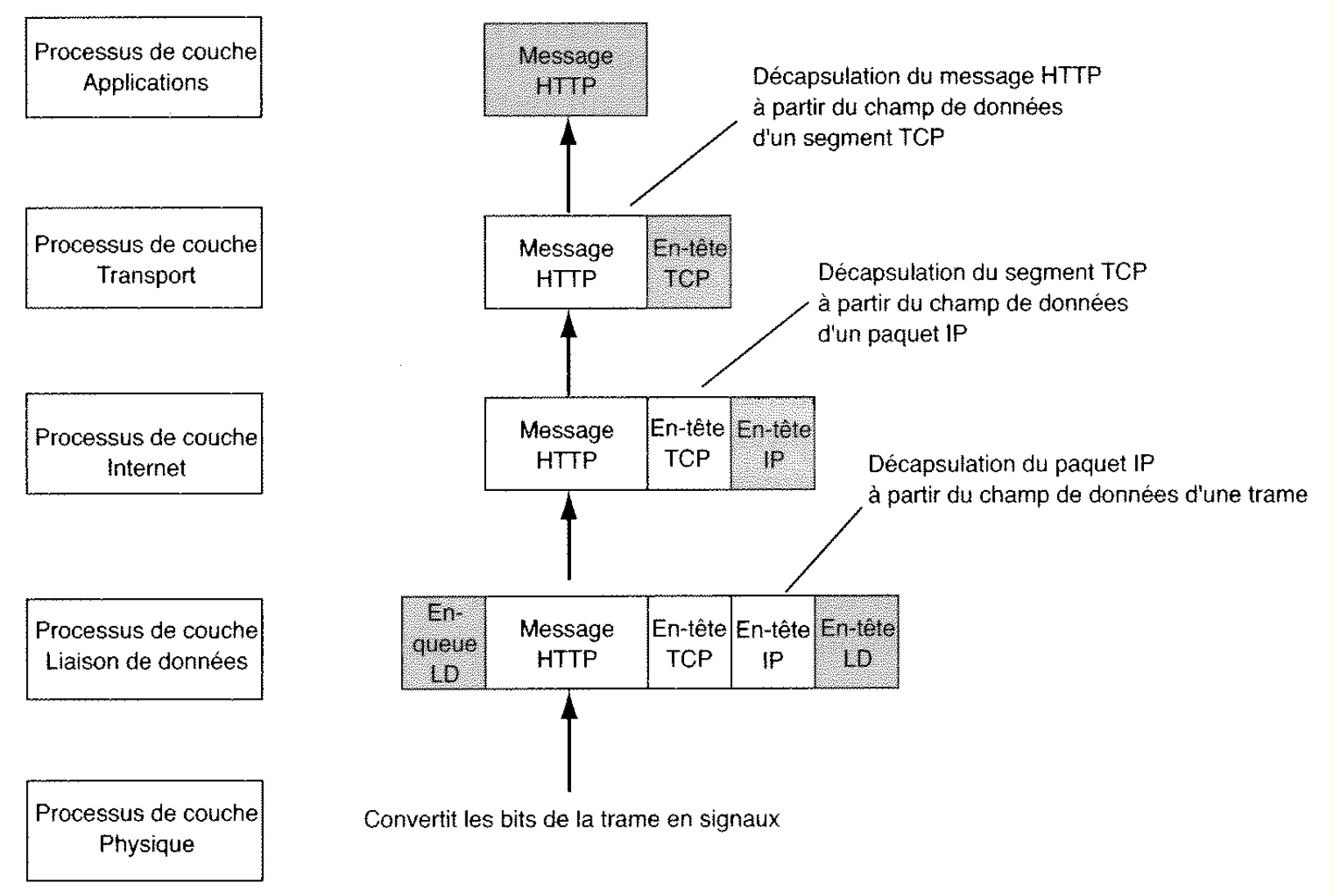
- Identification
- Authentification
- Autorisation

Modèle TCP/IP (Rappel)



D'après « Sécurité des Systèmes d'information et des Réseaux » de Raymond Panko

Modèle TCP/IP (Rappel)



D'après « Sécurité des Systèmes d'information et des Réseaux » de Raymond Panko

Authentification

- 3 types d'informations utilisables pour l'authentification :
  - quelque chose que vous **savez**
    - ✓ mots de passe
    - ✓ date de naissance
  - quelque chose que vous **avez**
    - ✓ passeport, permis de conduire
    - ✓ badge, carte à puce
  - quelque chose que vous **êtes**
    - ✓ empreintes digitales
    - ✓ scan rétinien

Authentification

- Permet de déterminer :
  - Qui peut y avoir accès
    - ✓ autorisation ou contrôle d'accès
  - Qui peut le voir
    - ✓ la confidentialité
  - Qui peut le modifier
    - ✓ l'intégrité
  - Qui l'a fait
    - ✓ traçabilité

PAP

- **P**assword **A**uthentification **P**rotocol
  - utilisé à l'origine dans le cadre de PPP (**P**oint to **P**oint **P**rotocol), utilisé généralement pour les connections par modem à un FAI (**F**ournisseur d'**A**ccès **I**nternet)
  - liaison point à point
  - basé sur HDLC
  - logon / mot de passe en clair sur le réseau
    - ✓ utilisé en pratique à travers un réseau sécurisé

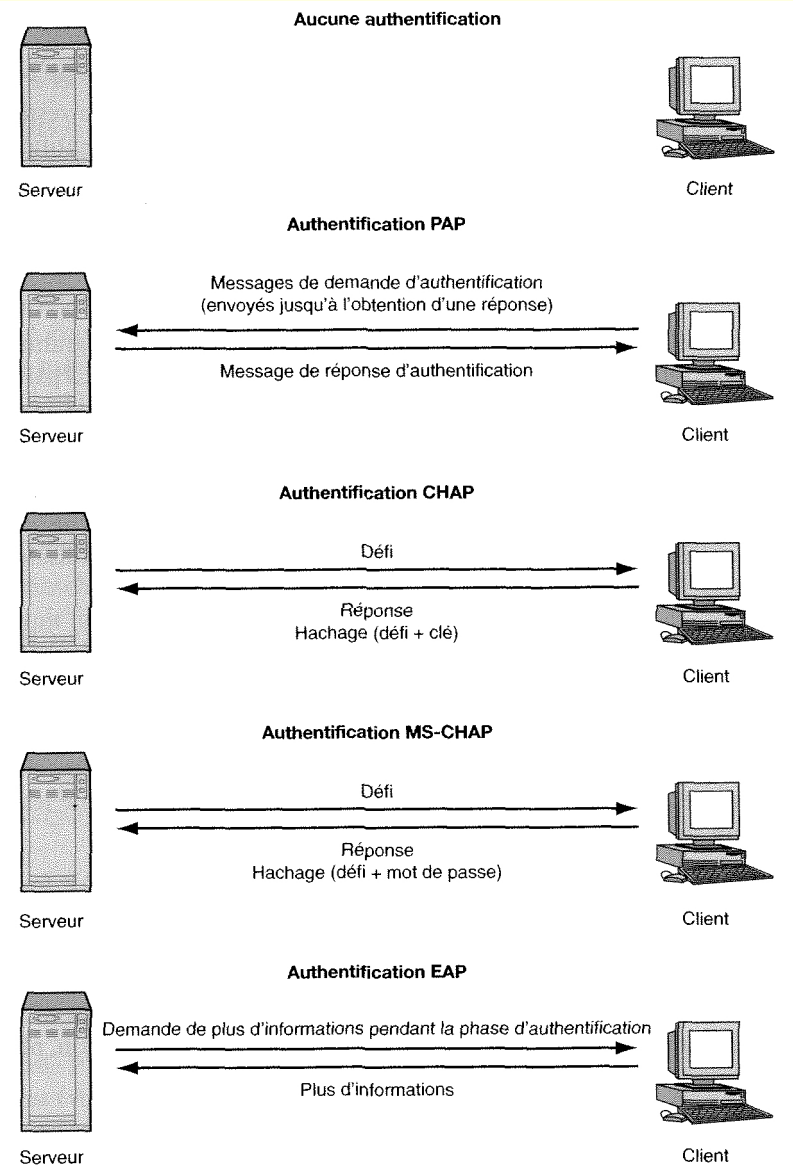
CHAP / MS-CHAP

- **C**hallenge **H**andshake **A**uthentication **P**rotocol
  - basé sur la résolution d'un défi (challenge)
  - mot de passe non transmis en clair sur le réseau
  - mots de passe stockés en clair sur le serveur
- **M**icro**S**oft **CHAP**
  - MS-CHAP version 1
    - ✓ améliore CHAP : mots de passe « hachés »
    - ✓ faiblesse dans la fonction de hachage propriétaire
  - MS-CHAP version 2 (janvier 2000)
    - ✓ authentification mutuelle

EAP

- **E**xtensible **A**uthentication **P**rotocole
  - extension du protocole PPP, permettant entre autres l'identification des utilisateurs sur le réseau
  - le plus souvent utilisé sur les réseaux sans fils (WPA)
  - Plusieurs méthode d'authentification :
    - ✓ LEAP **L**ightweight EAP (Cisco)
    - ✓ EAP-TLS obligatoirement supporté par WPA ou WPA2
    - ✓ EAP-MD5 standard ouvert, niveau de sécurité faible
    - ✓ EAP-TTLS **T**unneled **T**ransport **L**ayer **S**ecurity
    - ✓ PEAP **P**rotected EAP (Microsoft, RSA security, Cisco)
    - ✓ EAP-FAST **F**lexible **A**uthentication via **S**ecure **T**unneling
    - ✓ EAP-SIM utilisé par GSM
    - ✓ EAP-AKA **A**uthentication & **K**ey **A**grement utilisé par UMTS

Authentification PPP : Résumé

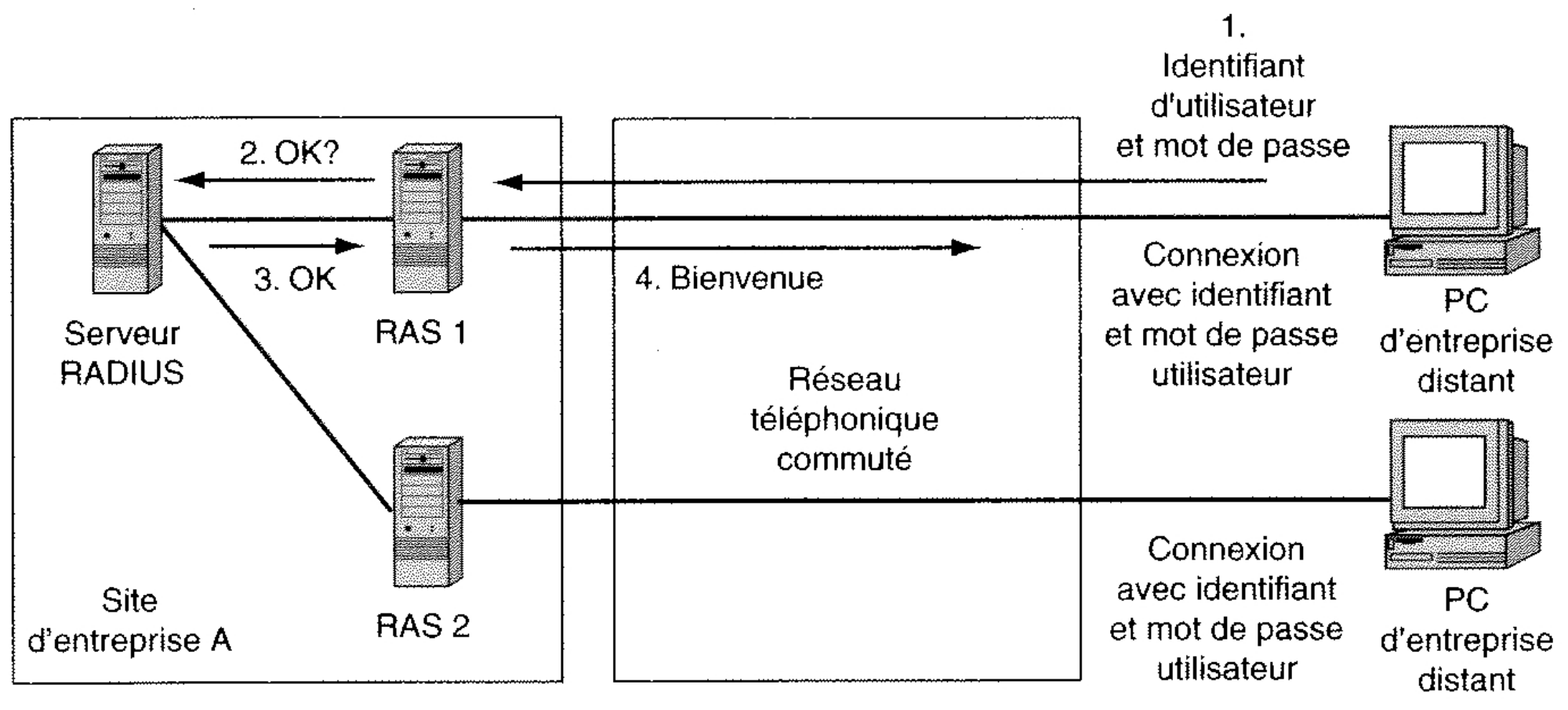


D'après « Sécurité des Systèmes d'information et des Réseaux » de Raymond Panko

Radius

- **R**emote *A*uthentication **D**ial-**I**n **U**ser **S**ervice
  - basé sur un système client-serveur
    - ✓ serveur RADIUS relié à une base d'identification
      - base de donnée
      - annuaire LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol)
    - ✓ client RADIUS : NAS (Network Access Server)
  - Utilise UDP

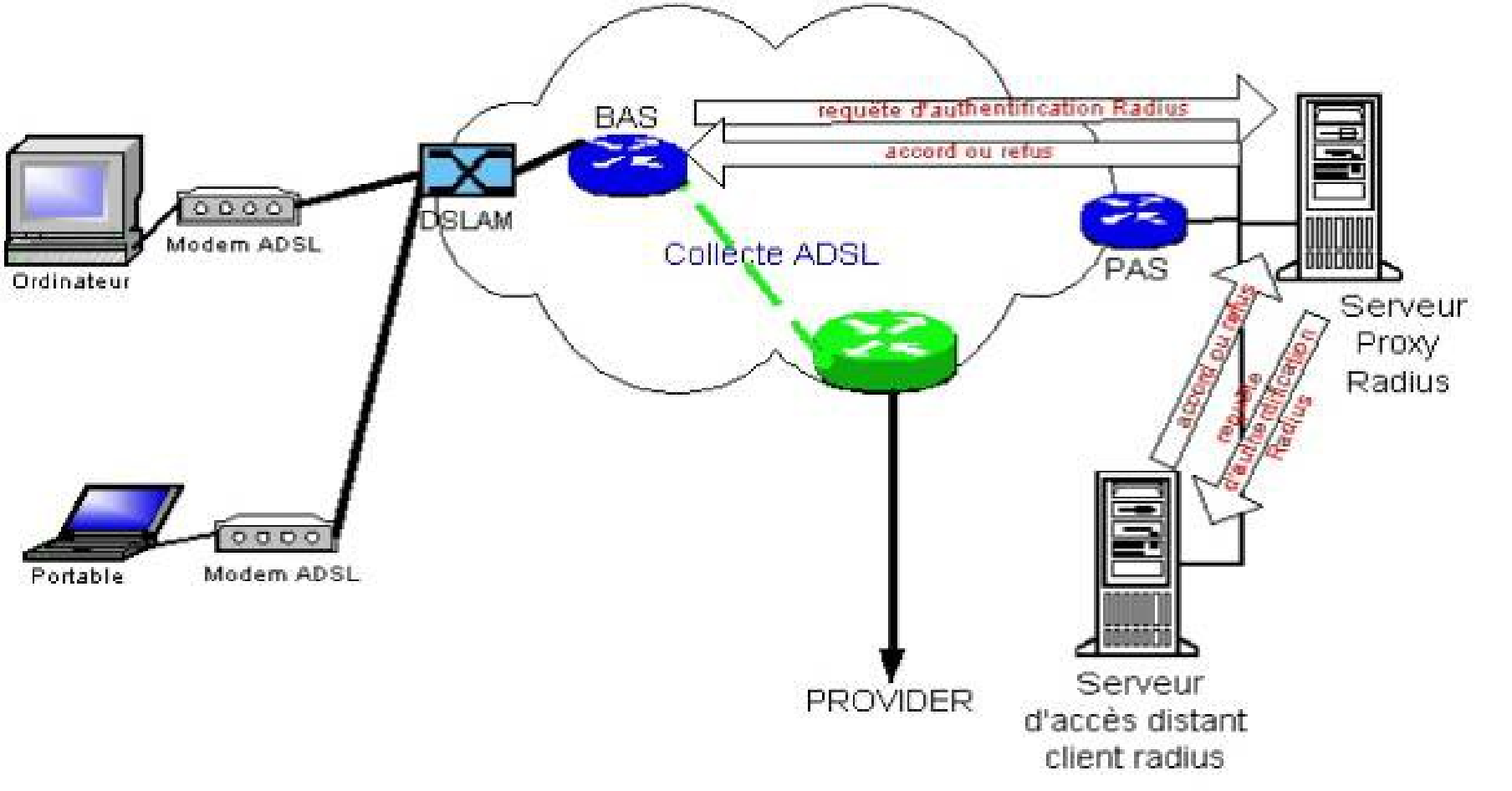
Radius : exemple



Accès à distance par ligne commutée

D'après « Sécurité des Systèmes d'information et des Réseaux » de Raymond Panko

Radius : exemple

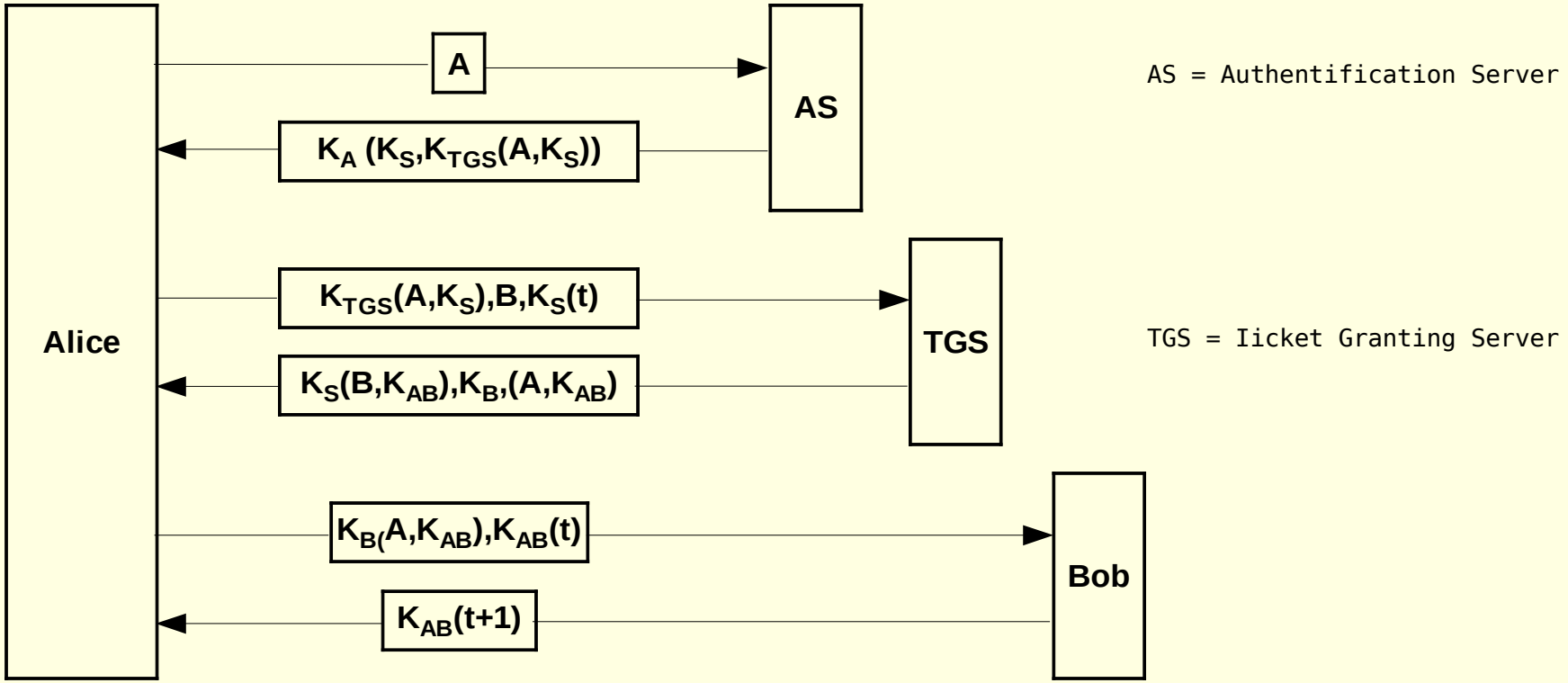


Accès à distance par connexion ADSL

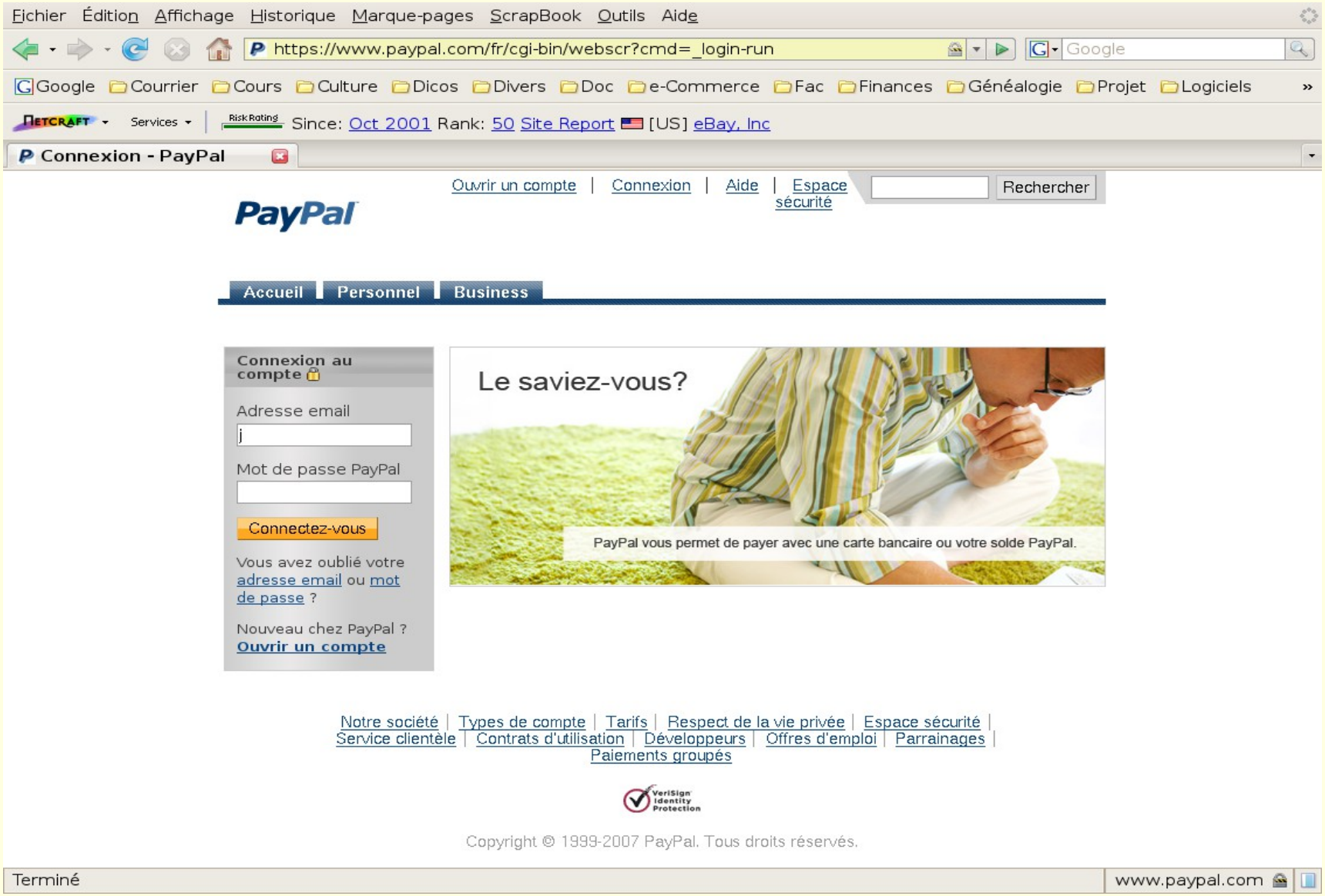
Kerberos

- Protocole d'identification réseau
- Crée par le MIT (Massachussetts Institute of Technologie)
- Utilisations
  - ✓ Mac OS X (à partir de 10.2)
  - ✓ MS Windows 2000 et suivants (authentification par défaut)
  - ✓ Apache, Samba
  - ✓ NFS, Open SSH, FileZilla, etc.

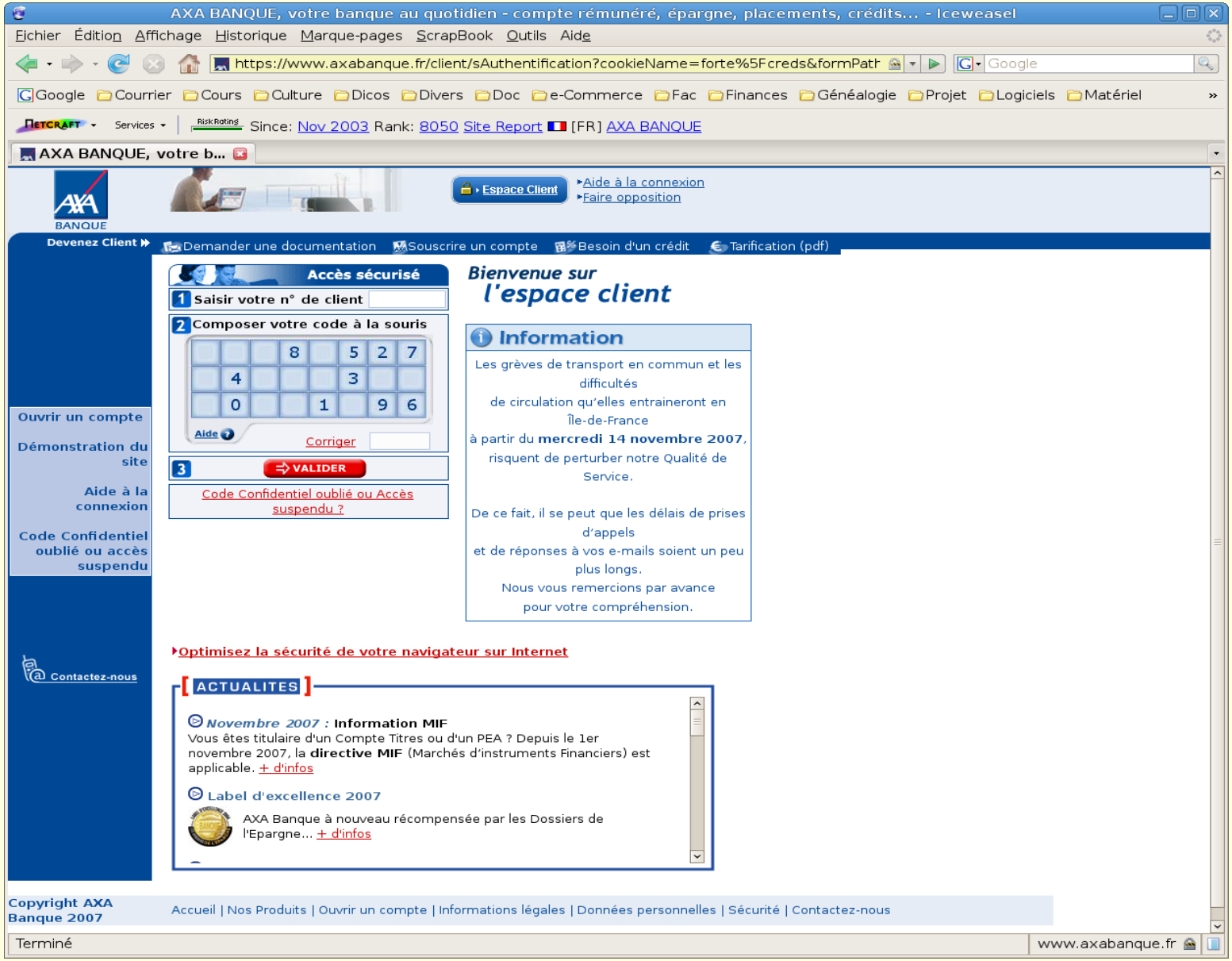
Kerberos v4 (schema)



Authentification (exemple 1 : PayPal)



Authentification (exemple 2 : Axa Banque)



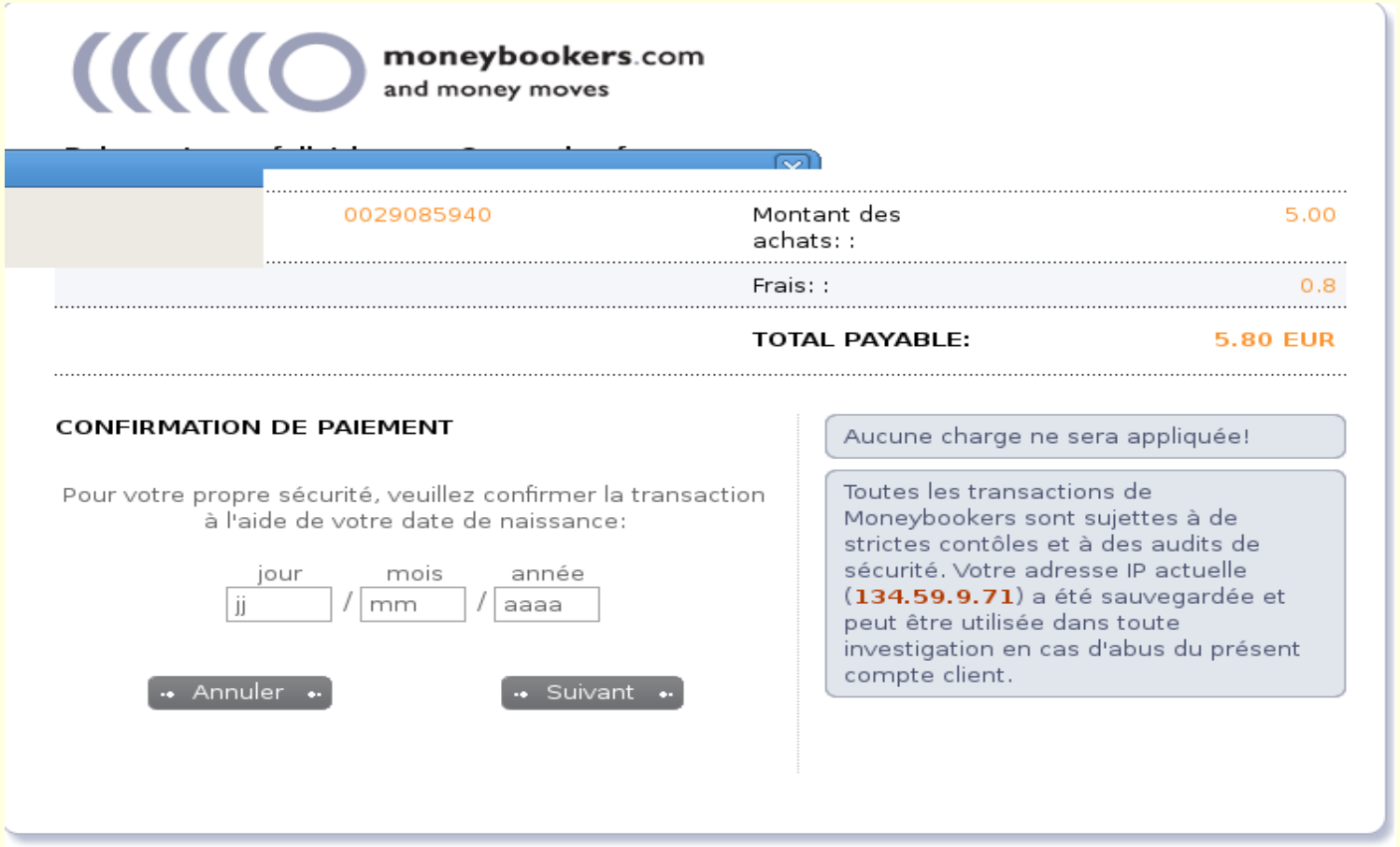
Authentification (exemple 2 : Axa Banque)

Authentification (exemple 3 : MoneyBookers)

Authentification (exemple 3 : MoneyBookers)

Authentification (exemple 3 : MoneyBookers)

- Puis, nouvel écran : Demande de la date de naissance



- et cela suffit, sinon : problème d'ergonomie

Authentification (exemple 3 : MoneyBookers)

Nous souhaitons vous informer qu'une tentative de connexion échouée a été faite sur votre compte Moneybookers. Il vous reste maintenant 6 tentative(s) de connexion avant que votre compte ne soit bloqué pour des raisons de sécurité. Nous vous rappelons les règles suivantes concernant les mots de passe Moneybookers:

- Respecter la casse (différence entre les majuscules et les minuscules)
- Etre constitué d'au moins 6 caractères
- Au moins une lettre (A-Z)
- Au moins un caractère qui ne soit pas une lettre (0-9, ., +, etc.)
- Ne peut pas être le même que votre adresse email

S'il s'agit d'une tentative de connexion non-autorisée, nous vous conseillons fortement de vous connecter immédiatement à votre compte Moneybookers sur www.moneybookers.com et de changer votre mot de passe. Nous vous recommandons de changer régulièrement votre mot de passe et de conserver le mot de passe de votre compte Moneybookers différent de tout autre mot de passe.

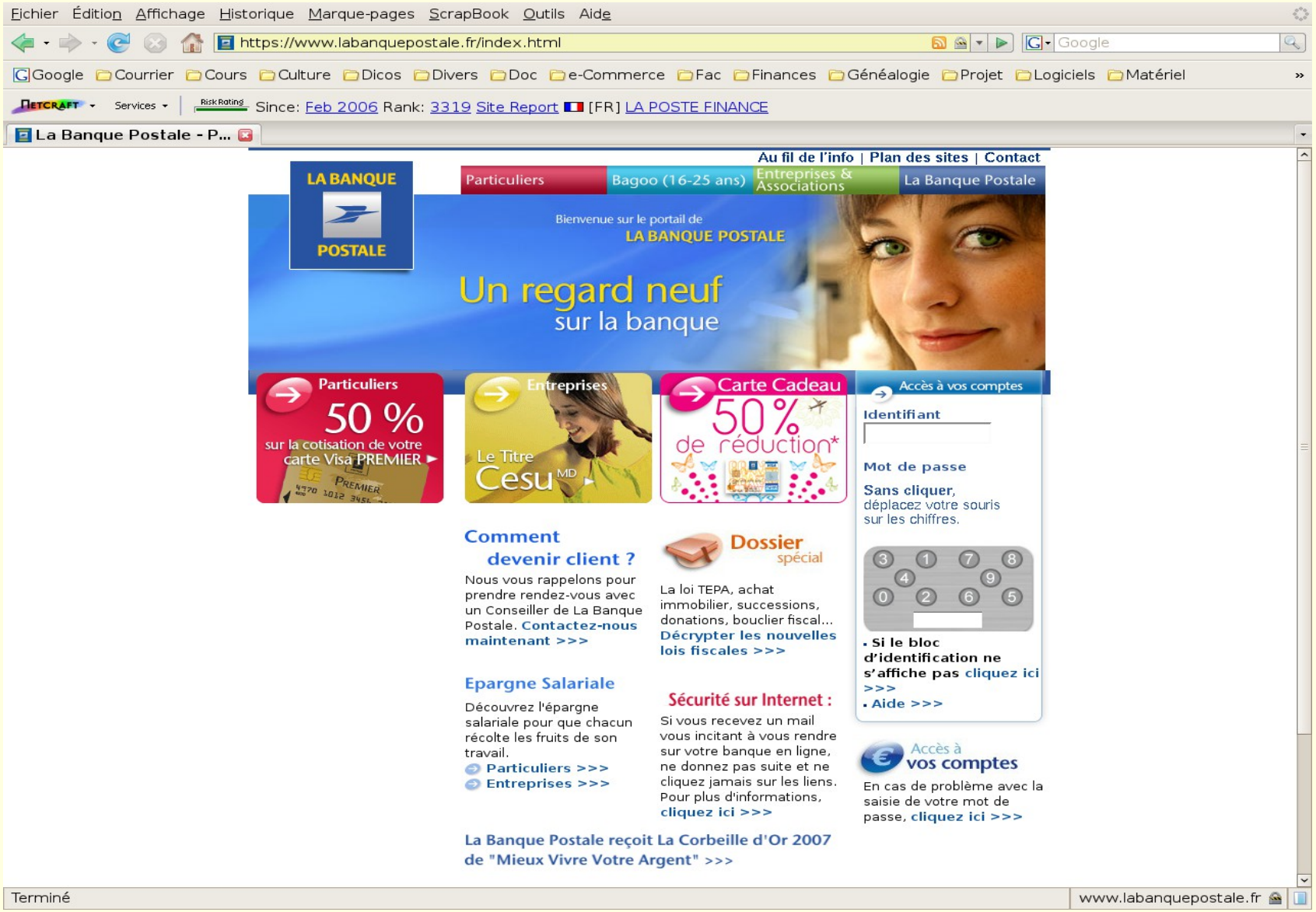
Cordialement,
L'équipe Moneybookers

****
Rappels de sécurité de Moneybookers!

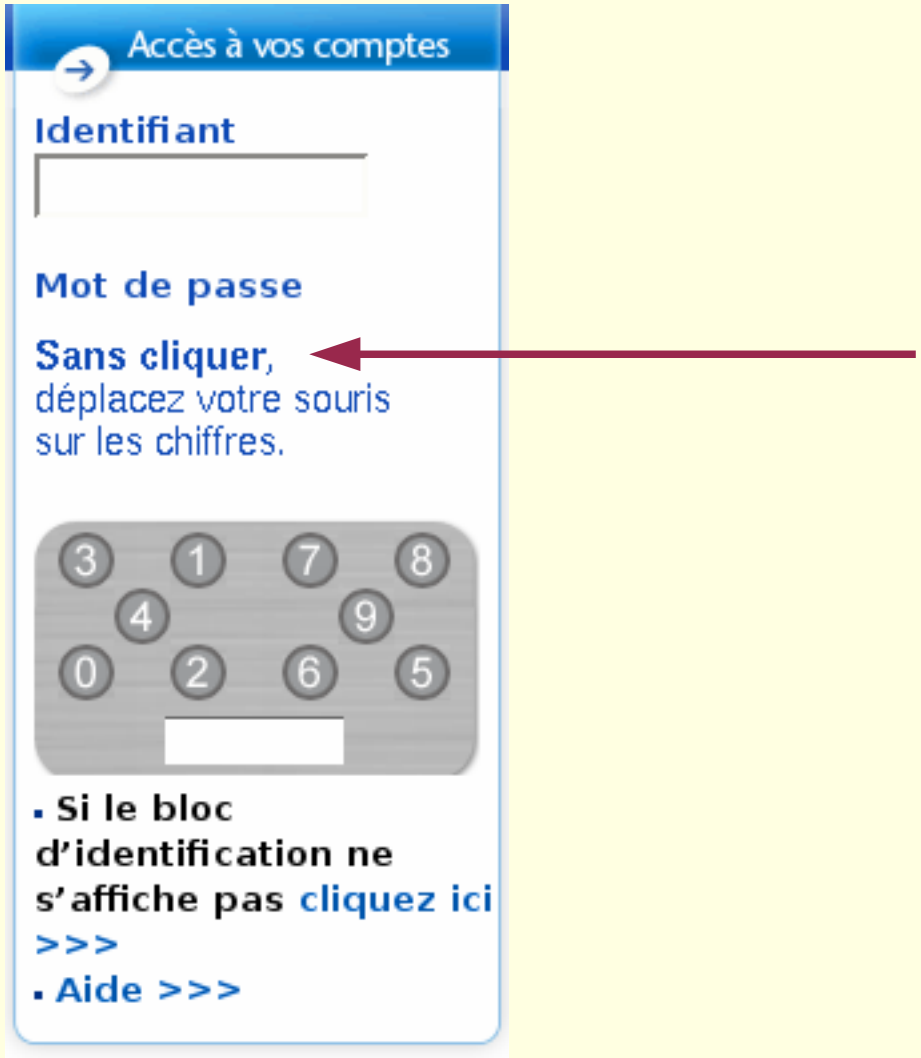
Protégez votre mot de passe
Moneybookers et ses représentants ne vous demanderont JAMAIS de révéler votre mot de passe. Il n'y a pas d'EXCEPTIONS à cette politique. Si quelqu'un vous demande votre mot de passe par téléphone ou email, ou sur un site autre que celui de moneybookers.com, déclinez la demande et signalez ceci à security@moneybookers.com.

Connectez-vous sur votre compte UNIQUEMENT en utilisant le lien de la page d'accueil de Moneybookers.
Soyez informé, que Moneybookers ainsi que ses représentants ne vous demanderons jamais dans un email d'inscrire vos détails de connection sur un formulaire ou bien de cliquer sur un lien hypertexte, afin de vous connecter directement sur votre compte!
Veuillez rapporter immédiatement tout incident de ce genre à security@moneybookers.com.

Authentification (exemple 4 : La banque postale)



Authentification (exemple 4 : La banque postale)



Mots de passe (attaques)

- Attaque par force brute
- Attaque par dictionnaire

John the ripper

- Logiciel libre de « cassage » de mot de passe par dictionnaire ou force brute.
- permet de tester la sécurité d'un mot de passe
- Fonctionne sur un grand nombre d'OS
- http://www.dawal.org/article.php3?id_article=48

John the ripper (exemple)

- Fichier /etc/shadow

root:1MNgulZf7$8AakxB2qaiQCOUSHG4EZ3.:13831:0:99999:7:::
daemon:*:13520:0:99999:7:::
bin:*:13520:0:99999:7:::
sys:*:13520:0:99999:7:::
sync:*:13520:0:99999:7:::
games:*:13520:0:99999:7:::
man:*:13520:0:99999:7:::
lp:*:13520:0:99999:7:::
mail:*:13520:0:99999:7:::
news:*:13520:0:99999:7:::
uucp:*:13520:0:99999:7:::
proxy:*:13520:0:99999:7:::
www-data:*:13520:0:99999:7:::
backup:*:13520:0:99999:7:::
list:*:13520:0:99999:7:::
irc:*:13520:0:99999:7:::
gnats:*:13520:0:99999:7:::
nobody:*:13520:0:99999:7:::
Debian-exim:!:13520:0:99999:7:::
statd:!:13520:0:99999:7:::
identd:!:13520:0:99999:7:::
messagebus:!:13520:0:99999:7:::
avahi:!:13520:0:99999:7:::
haldaemon:!:13520:0:99999:7:::
gdm:!:13520:0:99999:7:::
hplip:!:13520:0:99999:7:::
userid:1SO3Lwy0r$Q25XjnxhYpdVCXQb2gecQ0:13831:0:99999:7:::
Debian-ipw3945d:!:13521:0:99999:7:::
ntp:!:13522:0:99999:7:::
mysql:!:13523:0:99999:7:::
geneweb:!:13538:0:99999:7:::
bind:!:13552:0:99999:7:::
cupsys:!:13670:0:99999:7:::
sshd:!:13710:0:99999:7:::
festival:!:13749:0:99999:7:::
clamav:!:13798:0:99999:7:::

John the ripper (exemple)

- Session sous debian :

machineid:/home/userid# **passwd**
Entrez le nouveau mot de passe UNIX :**debian** (normalement occulté)
Retapez le nouveau mot de passe UNIX :debian (normalement occulté)
passwd : le mot de passe a été mis à jour avec succès

machineid:/home/userid# **passwd userid**
Entrez le nouveau mot de passe UNIX :**mickey** (normalement occulté)
Retapez le nouveau mot de passe UNIX :mickey (normalement occulté)
passwd : le mot de passe a été mis à jour avec succès

machineid:/home/userid# cp /etc/shadow ~userid/john_pw_to_crack

machineid:/home/userid# **john john_pw_to_crack**
Loaded 2 passwords with 2 different salts (FreeBSD MD5 [32/32])
mickey (userid)
guesses: 1 time: 0:00:00:05 16% (2) c/s: 4495 trying: EAGLE1
guesses: 1 time: 0:00:00:15 59% (2) c/s: 4538 trying: Buffy!
guesses: 1 time: 0:00:00:36 (3) c/s: 4461 trying: arte
guesses: 1 time: 0:00:03:56 (3) c/s: 4489 trying: prennya3
debian (root)
guesses: 2 time: 0:00:07:45 (3) c/s: 4470 trying: debian
machineid:/home/userid#

Authentification forte

- Two-factor authentification
  - appartiennent à 2 des 3 catégories catégories
  - exemples :
    - ✓ carte à puce (smart card= + mot de passe)
    - ✓ usb token + mot de passe
- Multi-factor authentification

Authentification forte

- Token (authentifieur)
  - Cartes à puces
  - Token USB
- Biométrie
  - Empreintes digitales
  - Empreintes rétiniennes
- Téléphones
- One time password

One Time Password (OTP)

- PRO :
  - Beaucoup plus sécurisé que logon/password
- CON :
  - Utilisation d'un logiciel de chiffrement pour se loguer:
    - ✓ OTP generator : Winkey, OPIE , JOTP (java)
  - Utilisation d'un secret partagé
    => pas de possibilité d'assurer la non-répudiation
  - Maillon faible : mot de passe utilisateur

Protocoles sécurisés

- TLS / SSL
- SSH
- SCP / FTPs / HTTPs
- S-HTTP
- SET
- S/MIME
- PGP

SSL (1/2)

- **S**ecure **S**ocket **L**ayer :
  - système standardisé permettant d'échanger des informations de façon sécurisée entre 2 ordinateurs, en assurant :
    - ✓ Confidentialité
    - ✓ Intégrité
    - ✓ Authentification
      - du serveur
      - du client (optionnel)
  - développé par *Netscape* et *RSA Security*

SSL (2/2)

- complément à TCP/IP
- très répandu (supporté par la quasi totalité des navigateurs)
- très cryptanalysé => très robuste
- version libre : OpenSSL

TLS

- **T**ransport **L**ayer **S**ecurity
  - Nouveau nom de SSL (suite au rachat par l'IETF Internet Engineering Task Force)
  - TLS v1.0 <=> SSL v3.1
  - Très peu de différence avec SSL v3.0
  - par abus de langage on parle de SSL pour désigner indifféremment TLS ou SSL

SSL et Modèle OSI

Couche du Modèle OSI		Protocoles
7	application	HTTP, SMTP,FTP, SSH, Telnet, IRC, SNMP, SIP...
5	session	**TLS, SSL**, NetBIOS
4	transport	TCP, UDP, SCTP, RTP, DCCP
3	réseau	IPv4, Ipv6, Ipsec, ARP, IPX...
2	liaison	Ethernet, 802.11 WiFi, Token Ring, FDDI...
1	physique	

HTTPs / FTPs / SSH

- Pile de protocoles :
  - **HTTPS** : HTTP over SSL
    Hyper**T**ext **T**ransfer **P**rotocol **S**ecure
    - ✓ URL commençant par https
  - **FTPS** : FTP/SSL : FTP over SSL
    File **T**ransfer **P**rotocole **S**ecure
  - SSH : **S**ecure **SH**ell

La négociation SSL

- SSL Handshake protocol

  Au début de la communication le client et le serveur s'échangent :

  - la version SSL
  - la liste des méthodes qu'ils supportent pour :
    - ✓ le chiffrement (symétrique, asymétrique, longueur de clé, etc.)
    - ✓ la signature
    - ✓ la compression
  - des nombres aléatoires
  - les certificats

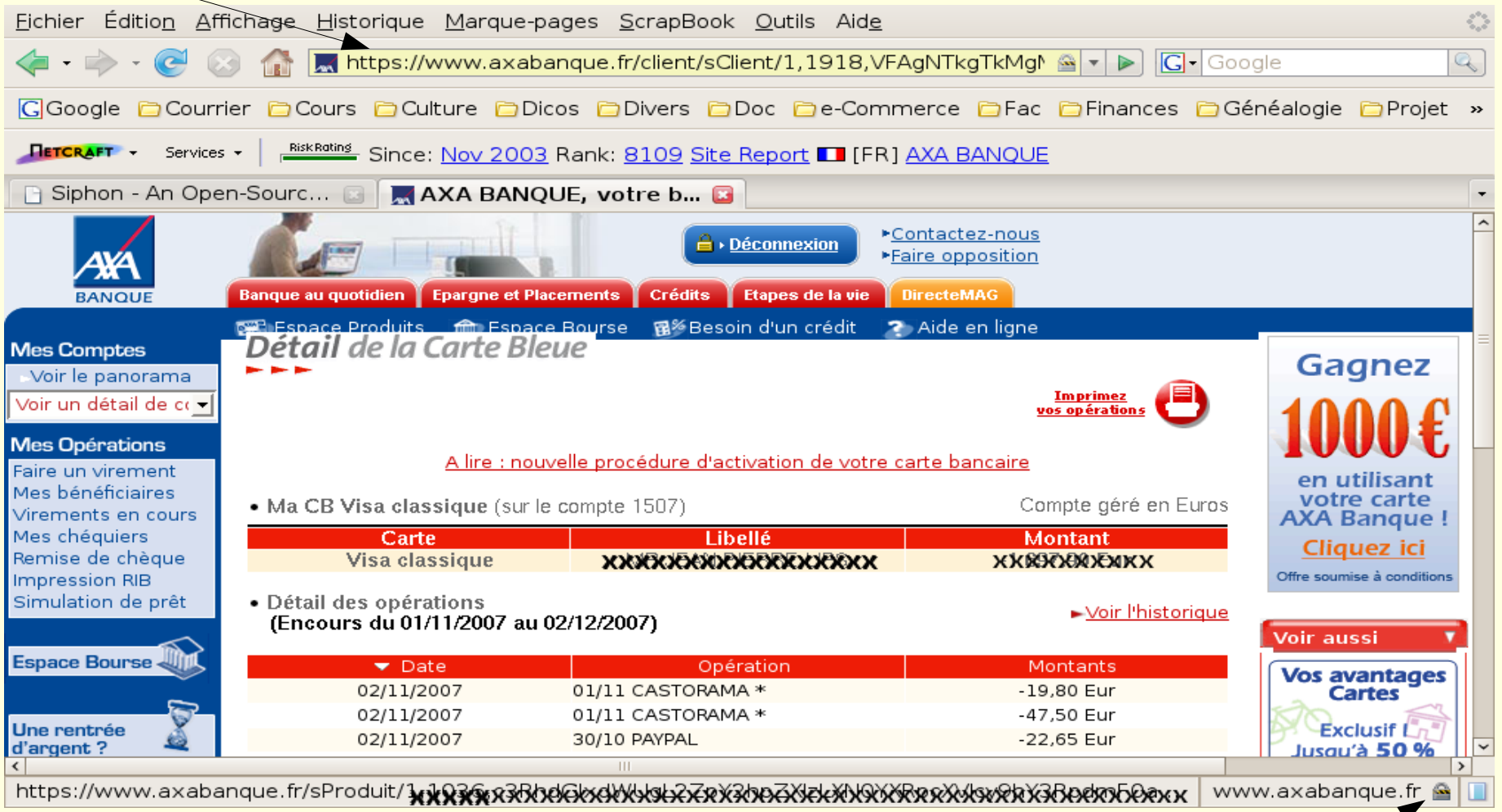
- La méthode commune la plus puissante est alors adoptée

La communication SSL

- SSL Record protocol
- Côté expéditeur, les données sont :
    1. découpées en paquets
    2. compressées
    3. signées cryptographiquement
    4. chiffrées
    5. envoyées
- Le récepteur procède:
    1. au déchiffrement
    2. à la vérification de la signature
    3. à la décompression
    4. au réassemblage

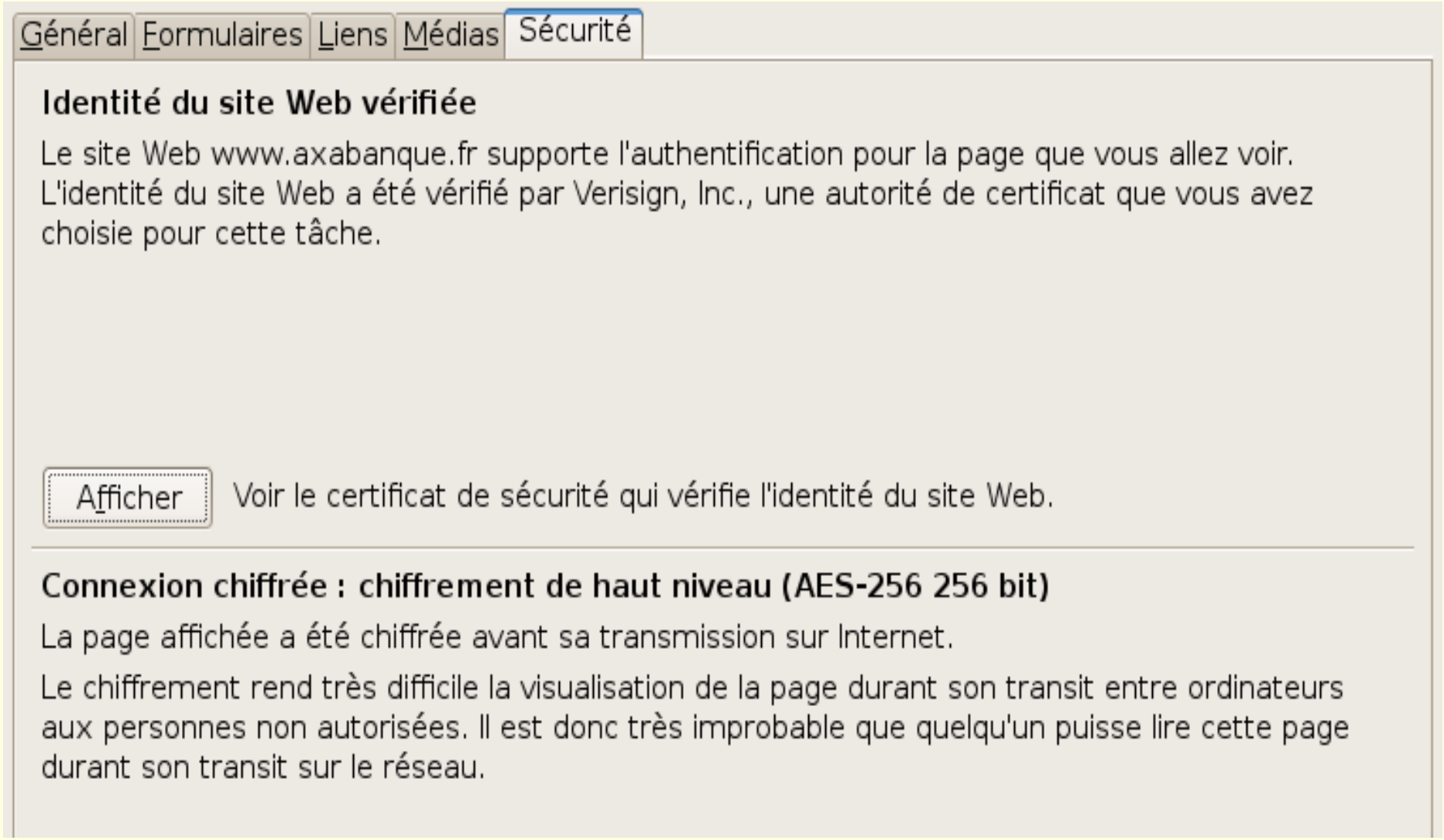
Exemple (1/4)

HTTPS



Pour voir la liste des systèmes utilisés, placer le curseur sur le cadenas

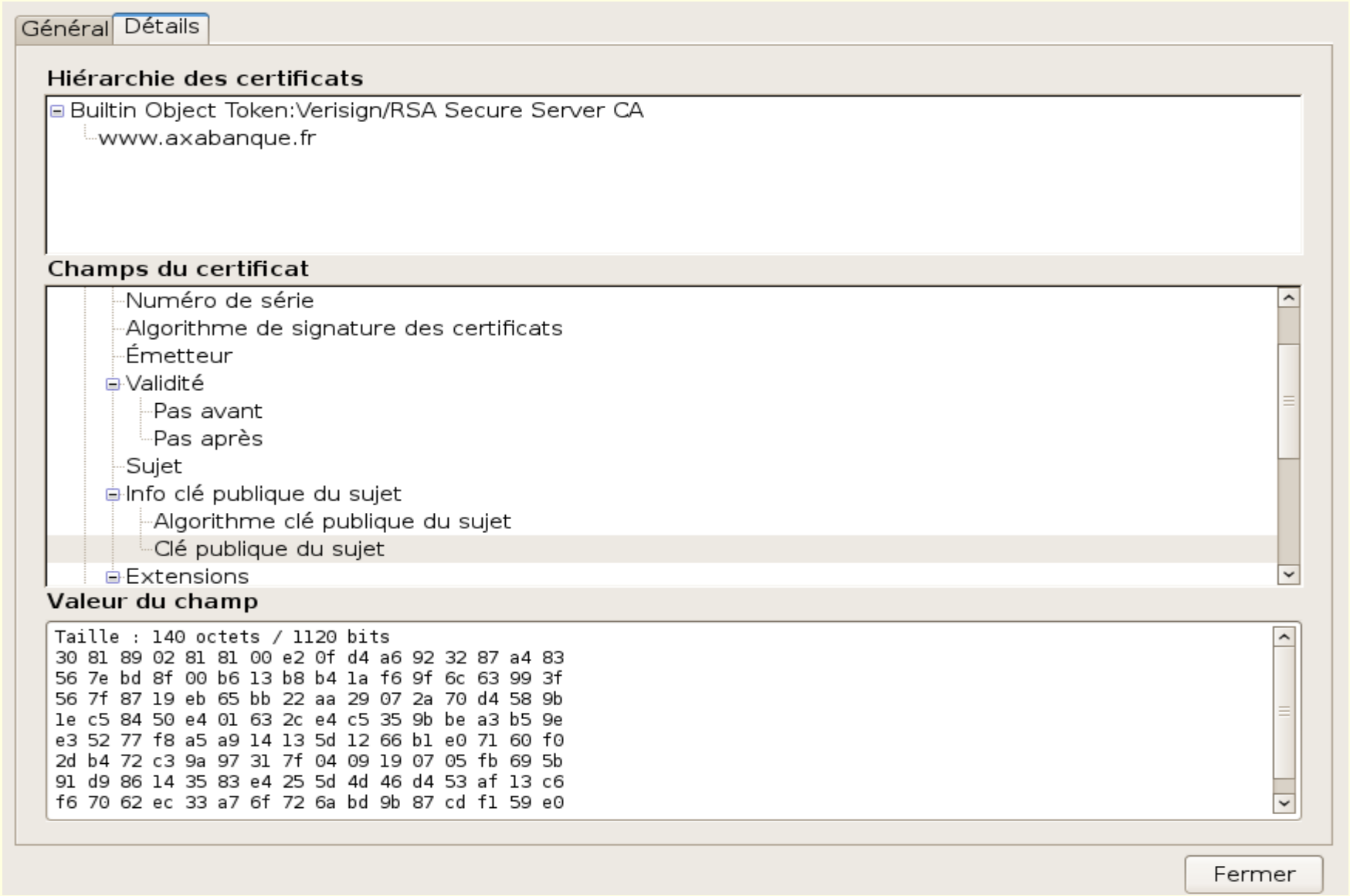
Exemple (2/4)


Général
Formulaires
Liens
Médias
Sécurité
Identité du site Web vérifiée
Le site Web www.axabanque.fr supporte l'authentification pour la page que vous allez voir. L'identité du site Web a été vérifié par Verisign, Inc., une autorité de certificat que vous avez choisie pour cette tâche.
Afficher
Voir le certificat de sécurité qui vérifie l'identité du site Web.
Connexion chiffrée : chiffrement de haut niveau (AES-256 256 bit)
La page affichée a été chiffrée avant sa transmission sur Internet.
Le chiffrement rend très difficile la visualisation de la page durant son transit entre ordinateurs aux personnes non autorisées. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

Exemple (3/4)


Général
Détails
Ce certificat a été vérifié pour les utilisations suivantes :
Certificat serveur SSL
Émis pour
Nom commun (CN) www.axabanque.fr
Organisation (O) Axa Banque
Unité d'organisation (OU) Direction technique
Numéro de série 56:A0:B4:8F:40:71:C3:9C:F9:5D:D0:15:38:40:25:99
Émis par
Nom commun (CN) <Ne fait pas partie du certificat>
Organisation (O) RSA Data Security, Inc.
Unité d'organisation (OU) Secure Server Certification Authority
Validité
Émis le 24.01.2007
Expire le 25.01.2008
Empreintes numériques
Empreinte numérique SHA1 83:63:0B:F2:E2:12:51:AA:1F:F9:71:E4:0E:C8:BA:FE:44:B8:BB:2F
Empreinte numérique MD5 42:01:D7:27:44:76:4E:D5:1D:60:AB:52:6E:73:AC:C4

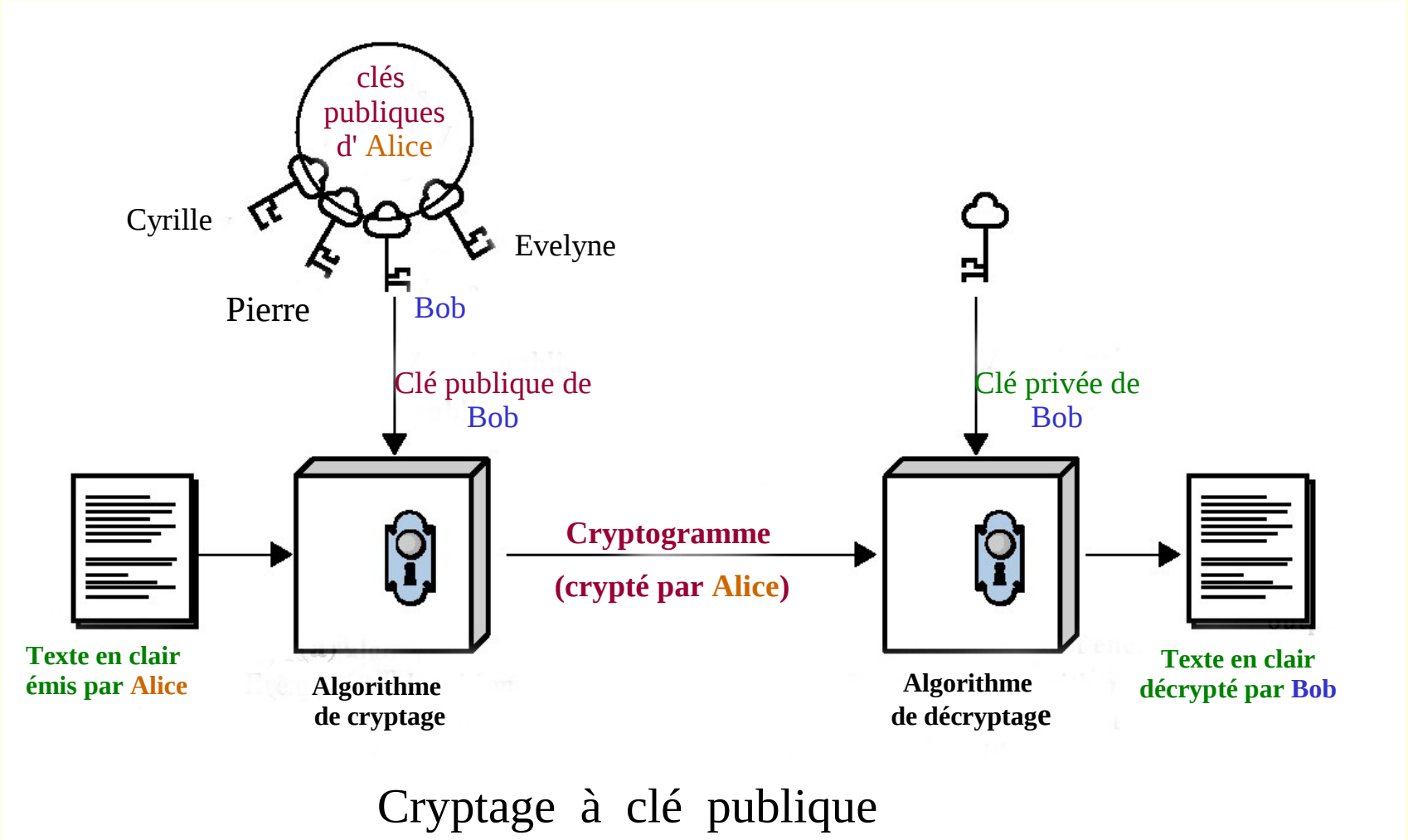
Exemple (4/4)


Général
Détails
Hiérarchie des certificats
Builtin Object Token:Verisign/RSA Secure Server CA
www.axabanque.fr
Champs du certificat
Numéro de série
Algorithme de signature des certificats
Émetteur
Validité
Pas avant
Pas après
Sujet
Info clé publique du sujet
Algorithme clé publique du sujet
Clé publique du sujet
Extensions
Valeur du champ
Taille : 140 octets / 1120 bits
30 81 89 02 81 81 00 e2 0f d4 a6 92 32 87 a4 83
56 7e bd 8f 00 b6 13 b8 b4 1a f6 9f 6c 63 99 3f
56 7f 87 19 eb 65 bb 22 aa 29 07 2a 70 d4 58 9b
1e c5 84 50 e4 01 63 2c e4 c5 35 9b be a3 b5 9e
e3 52 77 f8 a5 a9 14 13 5d 12 66 b1 e0 71 60 f0
2d b4 72 c3 9a 97 31 7f 04 09 19 07 05 fb 69 5b
91 d9 86 14 35 83 e4 25 5d 4d 46 d4 53 af 13 c6
f6 70 62 ec 33 a7 6f 72 6a bd 9b 87 cd f1 59 e0
Fermer

Techniques mises en œuvres

- SSL utilise la cryptographie :
  - Chiffrement asymétrique
    - ✓ RSA, Diffie-Hellman
    - ✓ génération de la clé principale
  - Chiffrement symétrique
    - ✓ DES, 3DES, IDEA, RC4...
    - ✓ chiffrement des données
  - Signature
    - ✓ MD5, SHA...
    - ✓ intégrité des messages

Chiffrement asymétrique



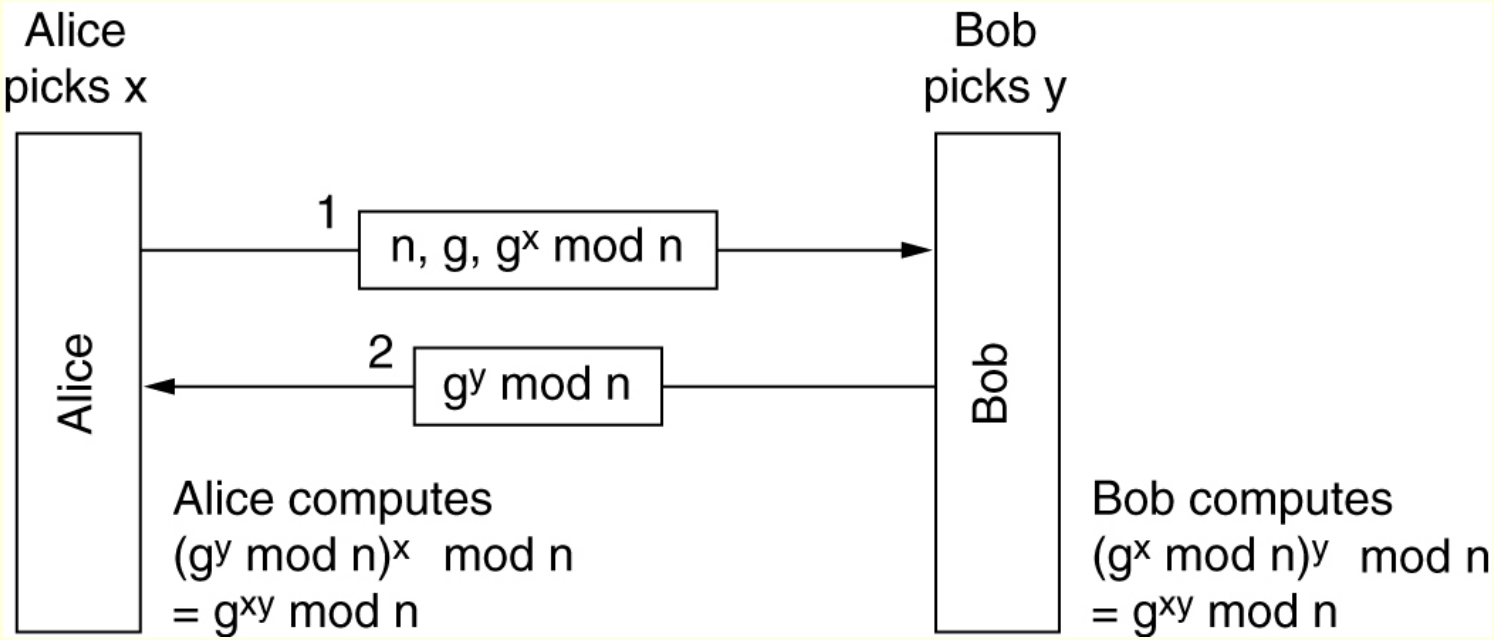
Cryptage à clé publique

Chiffrement asymétrique

- Premier algorithme en 1977 (Merckle et Hellman)
- RSA : Rivest, Shamir et Adelman
  - algorithme à clé publique mis au point en 1978
  - basé sur la difficulté à factoriser de grands entiers

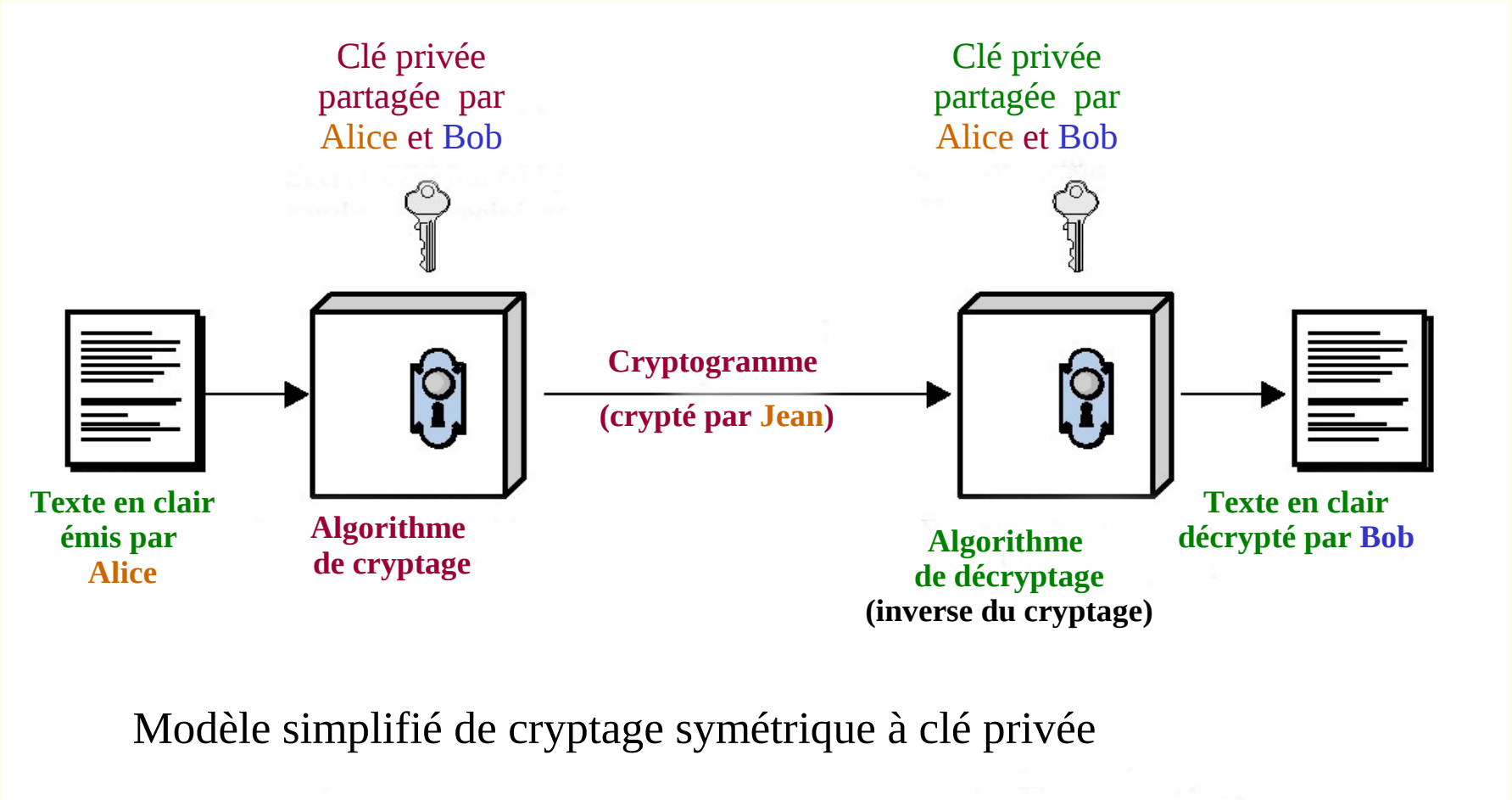
Échange de clé Diffie-Hellman

- Permet à deux interlocuteurs ne se connaissant pas de créer une clé secrète (date de 1976)



n et g = 2 grands nombres premiers avec (n-1)/2 premier et certaines conditions sur g

Chiffrement symétrique



Modèle simplifié de cryptage symétrique à clé privée

Chiffrement symétrique

- DES : **D**ata **E**ncryption **S**tandard
  - Approuvé en 1978 par le NBS (National Bureau of Standard)
  - longueur utile de la clé : 56 bits
- 3-DES (Triple DES)
  - Chaînage de 3 DES
- AES (**A**dvanced **E**ncryption **S**tandard)
  - Nouveau standard standard choisi en 2000 par le NIST (National Institute od Standard and Technology)
  - Algorithme Rijndael (Rijmen et Daemen)
  - clés : 128, 192 et 256 bits

Signature / Hachage (1/2)

- La fonction de hachage permet :
  - de créer un résumé du message de longueur fixe :
    - ✓ condensat, signature, empreinte
  - de garantir l'intégrité des données
- Elle doit avoir trois propriétés importantes :
  - Étant donné M il est facile de calculer $R_M(M)$
  - Étant donné $R_M(M)$, il est impossible de trouver M
    Fonction à sens unique (one-way function)
  - Il est extrememement difficile d' engendrer deux messages différents ayant le même résumé

Signature / Hachage (2/2)

- Calcul du résumé d'un message beaucoup plus rapide que le chiffrement
- Grand nombre de fonctions de hachage. Les plus utilisées sont :
  - ✓ MD5 (**M**essage **D**igest 5) (Ron Rivest,1992) :
    - chaque bit de sortie est affecté par chaque bit d'entrée
    - 128 bits
    - a été cassé en 2004
  - ✓ SHA (**S**ecure **H**ash **A**lgoritm) développé par la NSA (**N**ational **S**ecurity **A**gency)
    - SHA0, SHA1 (160 bits), SHA256, SHA 384, SHA512

Signature / Scellement des données

- Authentification
- Non-répudiation
  - l'expéditeur ne peut pas renier être l'auteur du message
- Principe :
  - l'expéditeur chiffre (signe) le condensé avec sa clé privé

Certificats

- Garantit que la clé publique est bien celle de l'utilisateur à qui elle est associée :
  - Permet de s'assurer de l'identité du correspondant
- Carte d'identité de la clé publique
  - délivré par une autorité de certification (PKI : **P**ublic **K**ey **I**nfrastructure) qui
    - ✓ vérifie l'authenticité du certificat
    - ✓ signe cryptographiquement les certificats des entreprises, banques, e-commerçants....
  - Verisign, Thawte...
- Normalisation : standard X.509

Certificat X.509

- Principaux champs :

Field	Meaning
Version	Which version of X.509
Serial number	This number plus the CA's name uniquely identifies the certificate
Signature algorithm	The algorithm used to sign the certificate
Issuer	X.500 name of the CA
Validity period	The starting and ending times of the validity period
Subject name	The entity whose key is being certified
Public key	The subject's public key and the ID of the algorithm using it
Issuer ID	An optional ID uniquely identifying the certificate's issuer
Subject ID	An optional ID uniquely identifying the certificate's subject
Extensions	Many extensions have been defined
Signature	The certificate's signature (signed by the CA's private key)

SSH

- **S**ecure **Sh**ell
- Version 2 (01/2006)
- Objectif : remplacer de façon sécuriser :
  - rlogin (remote login)
  - telnet
  - rsh (remote shell)

  qui font circuler en clair login/mot de passe sur le réseau

S-HTTP

- Secure HTTP
- Amélioration du protocole HTTP
- Au dessus du protocole HTTP, très lié à HTTP
- Ne pas confondre avec HTTPS (basé sur SSL)
  - S-HTTP chiffre individuellement chaque message
  - HTTPs est basé sur SSL qui chiffre l'intégralité de la communication

SET

- **S**ecure **E**lectronic **T**ransaction
  - Décrit les protocoles et algorithmes nécessaires à sécuriser les paiements sur des réseaux ouverts de type Internet
- Spécification technique écrite par Visa et MasterCard
- Objectifs :
  - ✓ Authentification des porteurs de cartes,
des commerçant
des banques des acheteurs
  - ✓ Confidentialité des paiements
  - ✓ Intégrité des données du paiement

S/MIME (1/2)

- Secure MIME
  (**S**ecure **M**ultipurpose **I**nternet **M**ail **E**xtension)
  - apporte à MIME les fonctions de sécurité suivantes
    - ✓ basées sur la signature digitale :
      - authentification
      - intégrité des messages
      - non-répudiation de l'origine
    - ✓ basées sur le chiffrement :
      - confidentialité
      - sécurité des données
  - permet de chiffrer le contenu des messages, mais pas la communication

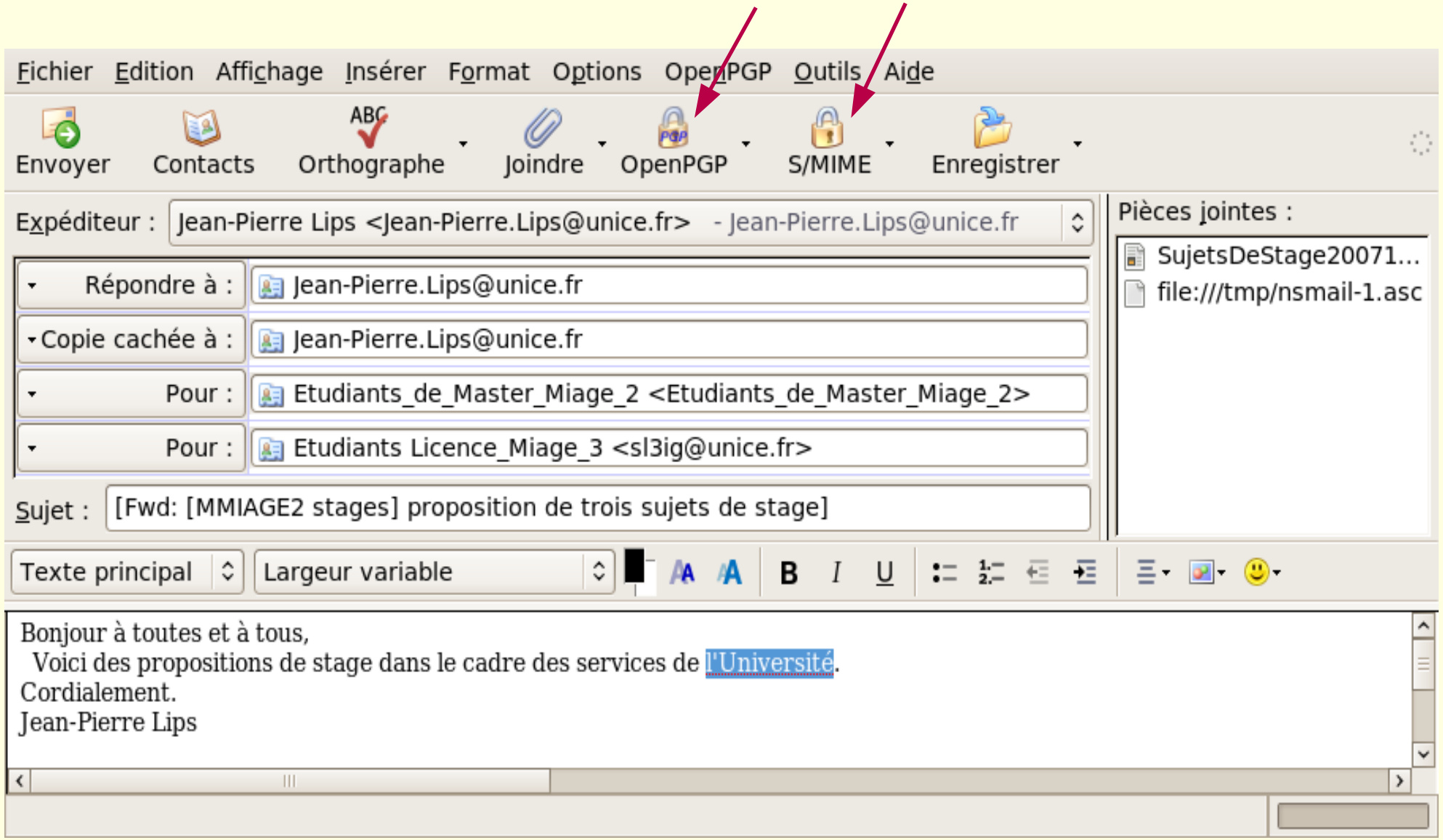
S/MIME (2/2)

- Fonctionnement
  - Principe de chiffrement à clé publique
  - Chaque partie du message chiffrée avec une clé de session
  - Clé de session chiffrée avec la clé publique du destinataire dans l'en-tête de chaque message
  - Signature du message chiffrée avec la privée de l'expéditeur

PGP

- Pretty Good Privacy
  - Signature et vérification d'intégrité de messages
    - ✓ Hachage MD5 + chiffrement RSA
  - Chiffrement des fichiers locaux
    - ✓ IDEA
  - Génération de clés publiques et privées
    - ✓ chiffrement des messages avec IDEA
    - ✓ transfert des clés IDEA avec RSA
  - Gestion des clés
  - Certification des clés

Exemple


Fichier Edition Affichage Insérer Format Options OpenPGP Outils Aide
Envoyer
Contacts
Orthographe
Joindre
OpenPGP
S/MIME
Enregistrer
Expéditeur : Jean-Pierre Lips <Jean-Pierre.Lips@unice.fr> - Jean-Pierre.Lips@unice.fr
Répondre à : Jean-Pierre.Lips@unice.fr
Copie cachée à : Jean-Pierre.Lips@unice.fr
Pour : Etudiants_de_Master_Miage_2 <Etudiants_de_Master_Miage_2>
Pour : Etudiants Licence_Miage_3 <sl3ig@unice.fr>
Sujet : [Fwd: [MMIAGE2 stages] proposition de trois sujets de stage]
Pièces jointes :
SujetsDeStage20071...
file:///tmp/nsmail-1.asc
Texte principal
Largeur variable
Bonjour à toutes et à tous,
Voici des propositions de stage dans le cadre des services de l'Université.
Cordialement.
Jean-Pierre Lips

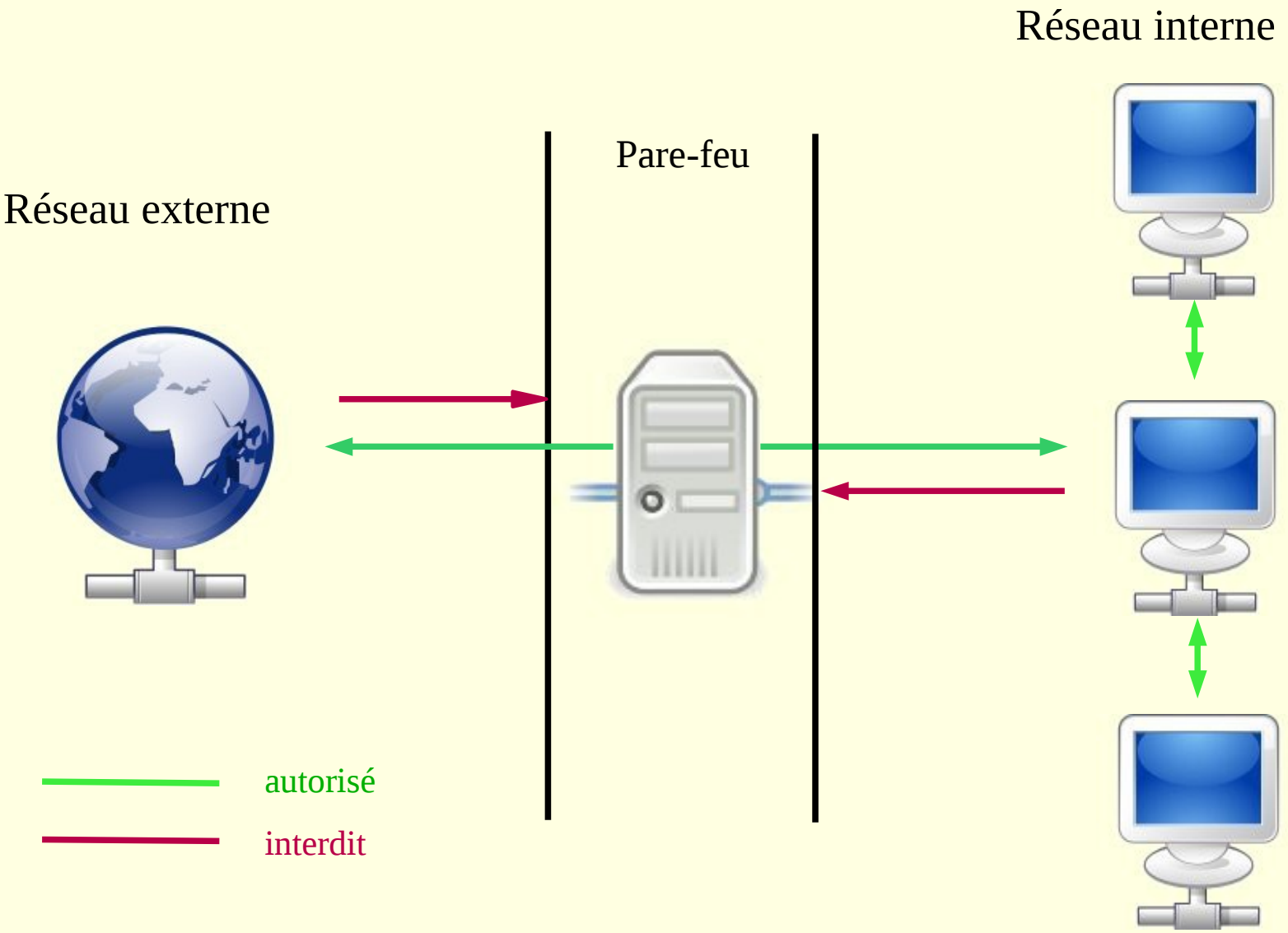
Protections Réseaux

- Pare-feu (firewall)
- Serveurs mandataires (proxy)
  - Translation d'adresses (NAT)
- Détection d'intrusions
- Réseaux privés virtuels (VPN)

Pare-feu

- Mur anti-feu (*firewall*), garde-barrière (gate-keeper)
  - Poste frontière entre réseaux comportant au minimum deux interfaces :
    - ✓ une interface pour le réseau interne à protéger
    - ✓ une interface pour le réseau externe
  - Dispositif de filtrage : passerelle filtrante
    - ✓ matériel *(appliance)* ou logiciel
    - ✓ placé à l'entrée du réseau
    - ✓ protégeant le réseau interne des intrusions externes
    - ✓ empêchant la « fuite » de données vers l'extérieur

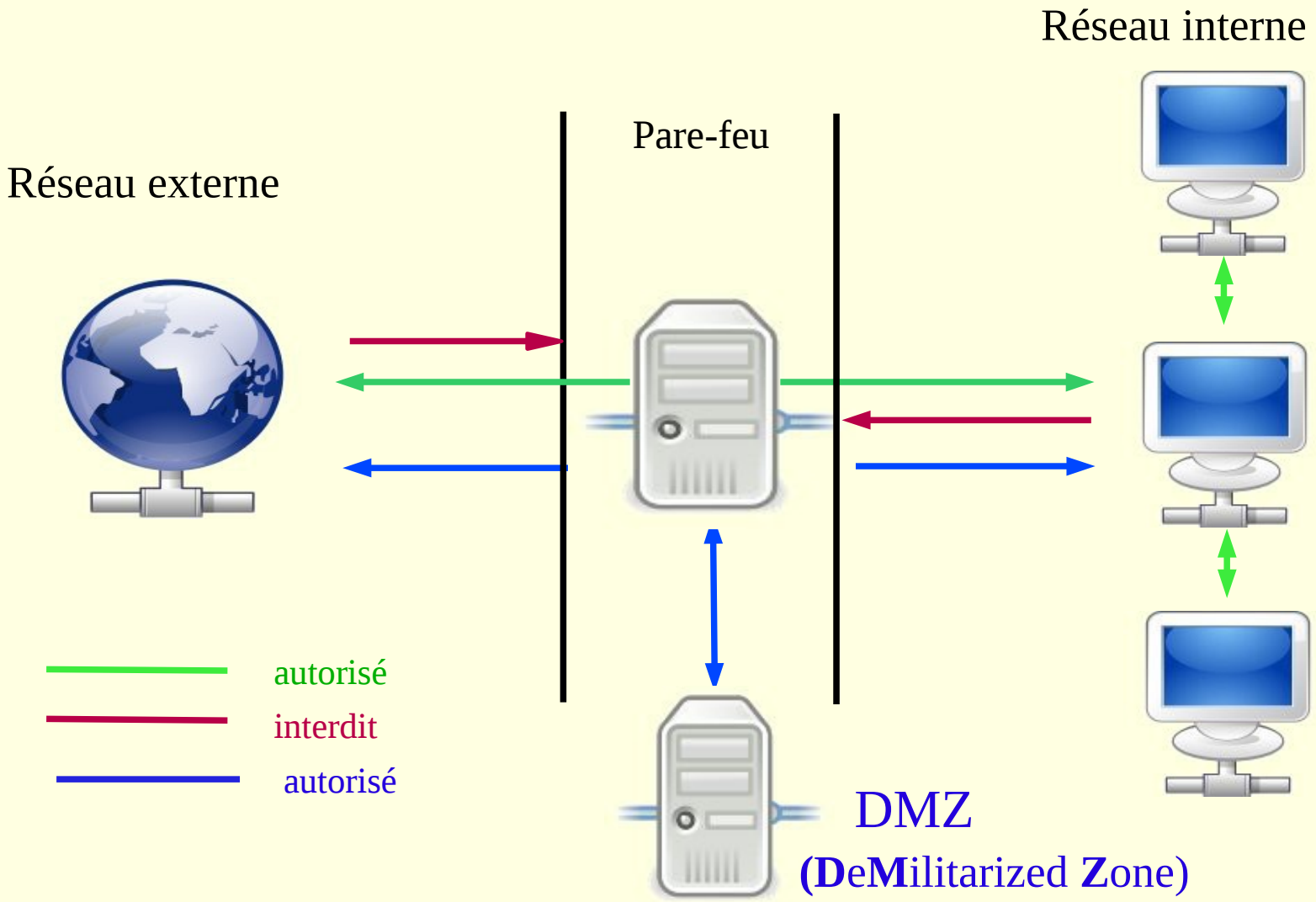
Pare-feu



DMZ

- Zone Démilitarisée *(**D**e**M**ilitarized **Z**one)*
- Réseau à part
  - accessible de l'extérieur
    - ✓ serveur Web,
    - ✓ serveur FTP,
    - ✓ serveur de messagerie, etc.
  - accessible de l'intérieur

DMZ (Zone démilitarisée)



Configuration - Règles

- Configuration du pare-feu au moyen de règles :
  - allow : autorise la connexion
  - deny : bloque la connexion
  - drop : rejette la demande de connexion sans avertir l'émetteur
- Politique de sécurité
  - Deux grandes politiques de sécurité (règles prédéfinies) :
    - ✓ autoriser les échanges explicitement autorisés
      « tout ce qui n'est pas explicitement autorisé est interdit »
      - méthode sûre mais contraignante
    - ✓ bloquer les échanges explicitement interdits
      « tout ce qui n'est pas explicitement interdit est autorisé »
      - méthode simple mais plus risquée

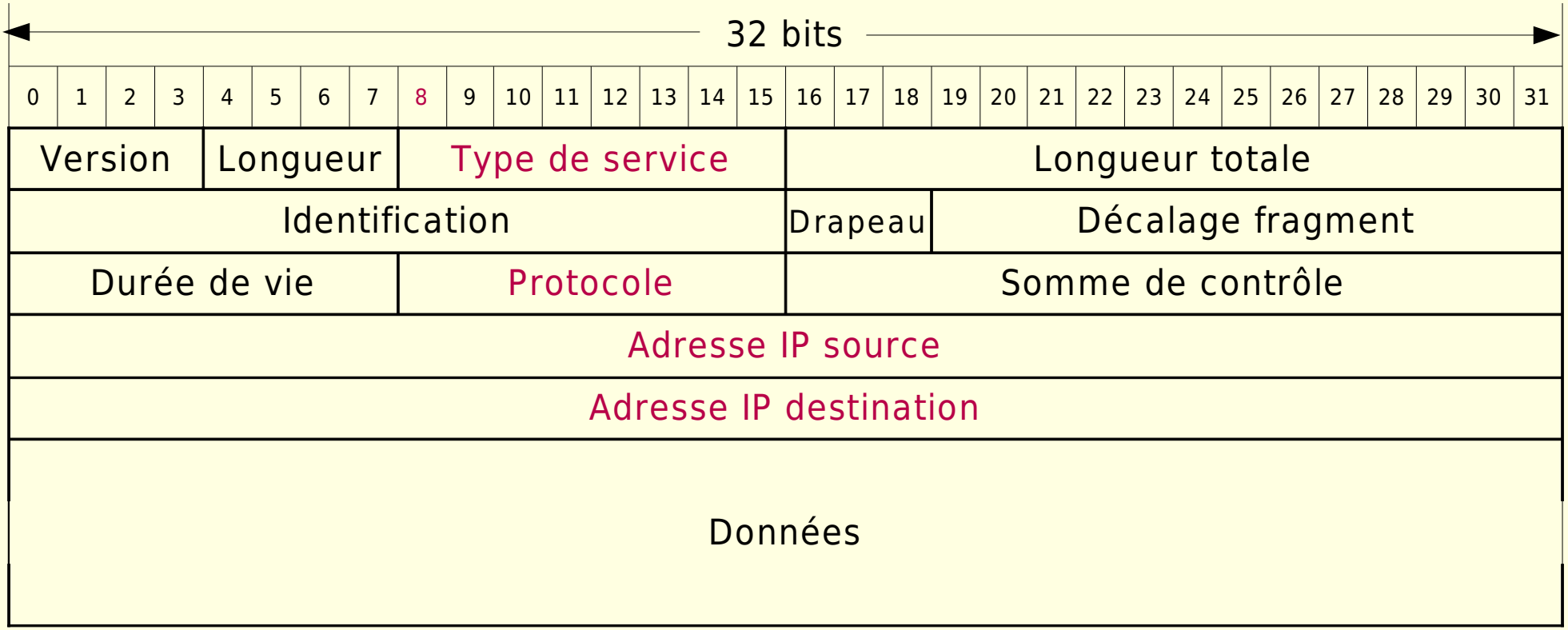
Filtrage

- Trois méthodes de filtrage :
  - filtrage simple de paquets
    - stateless packet filtering
    - ✓ filtrage statique par adresse
      - static address filtering
    - ✓ filtrage statique par protocole
      - static protocol filtering
  - filtrage dynamique
    - ✓ stateful packet filtering
  - filtrage applicatif

Filtrage simple de paquets

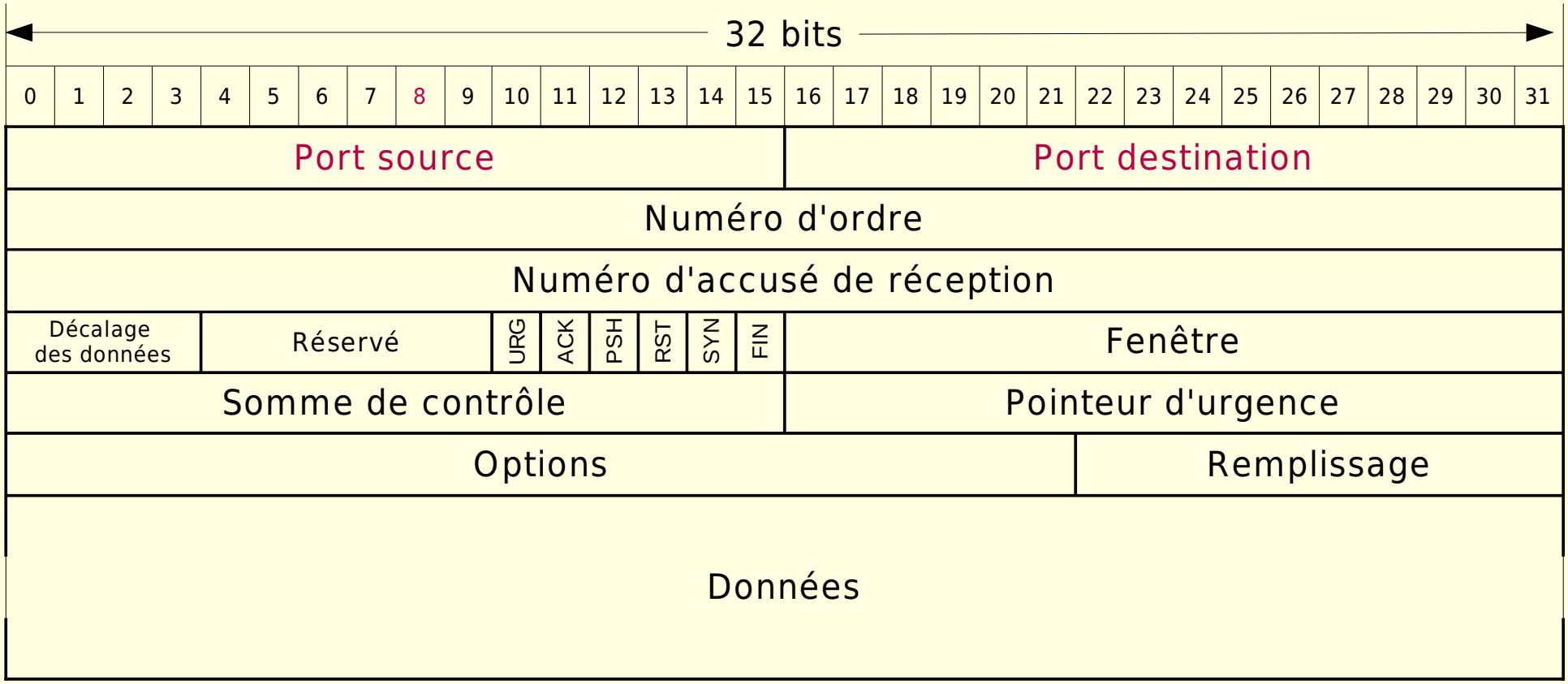
- Analyse les paquets indépendamment les uns des autres
- Niveau 3 du modèle OSI : couche réseau
- Analyse des champs suivant des datagrammes IP :
  - Adresse IP source (machine émettrice)
  - Adresse IP destination (machine réceptrice)
  - Protocole : TCP, UDP, etc.
- Analyse du champ suivant du paquet TCP :
  - Numéro de port

Datagramme IPv4



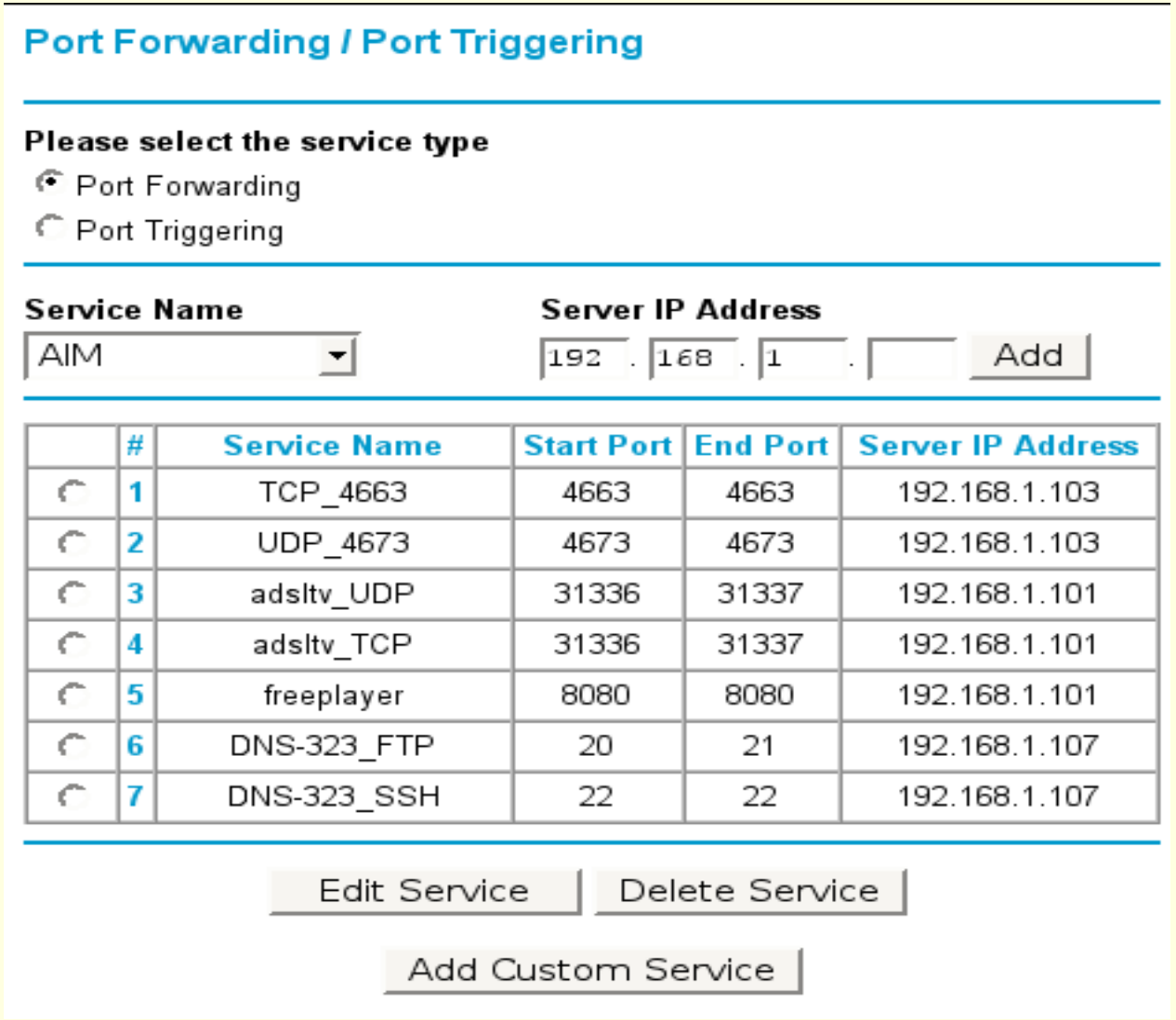
Le pare-feu analyse les champs indiqués en rouge

Segment TCP



Le pare-feu analyse les champs indiqués en rouge

Exemple



Port Forwarding / Port Triggering

Please select the service type

- (•) Port Forwarding
- ( ) Port Triggering

Service Name: AIM

Server IP Address: 192 . 168 . 1 . [ ] Add

	#	Service Name	Start Port	End Port	Server IP Address
( )	1	TCP_4663	4663	4663	192.168.1.103
( )	2	UDP_4673	4673	4673	192.168.1.103
( )	3	adsltv_UDP	31336	31337	192.168.1.101
( )	4	adsltv_TCP	31336	31337	192.168.1.101
( )	5	freeplayer	8080	8080	192.168.1.101
( )	6	DNS-323_FTP	20	21	192.168.1.107
( )	7	DNS-323_SSH	22	22	192.168.1.107

Edit Service | Delete Service

Add Custom Service

Filtrage dynamique

- De nombreux services (ex: TCP) démarre la connexion sur un port statique puis ouvre des ports dynamiquement de manière aléatoire
  - non gérable par le filtrage statique
- Stateful packet filtering (stateful inspection)
  - filtage de paquets avec état
  - suivi des différentes échanges client-le serveur
    - ✓ mémorisation des informations de session
- niveau 3 et 4 du modèle OSI

Filtrage applicatif

- Firewall applicatif :Passerelle applicative (Proxy)
  - au niveau de la couche application (couche 7 du modèle OSI)
  - suppose une bonne connaissance des applications, en particuliers de leur protocole d'échange des données
- Plusieurs approche complémentaires :
  - prise en compte des standards définis dans les RFC pour repérer les requêtes hors norme
  - mise à jour à partir de bases de signatures d'attaques connues
  - apprentissage dynamique du trafic légitime de l'utilisateur
  - utilisation de l'intelligence artificielle

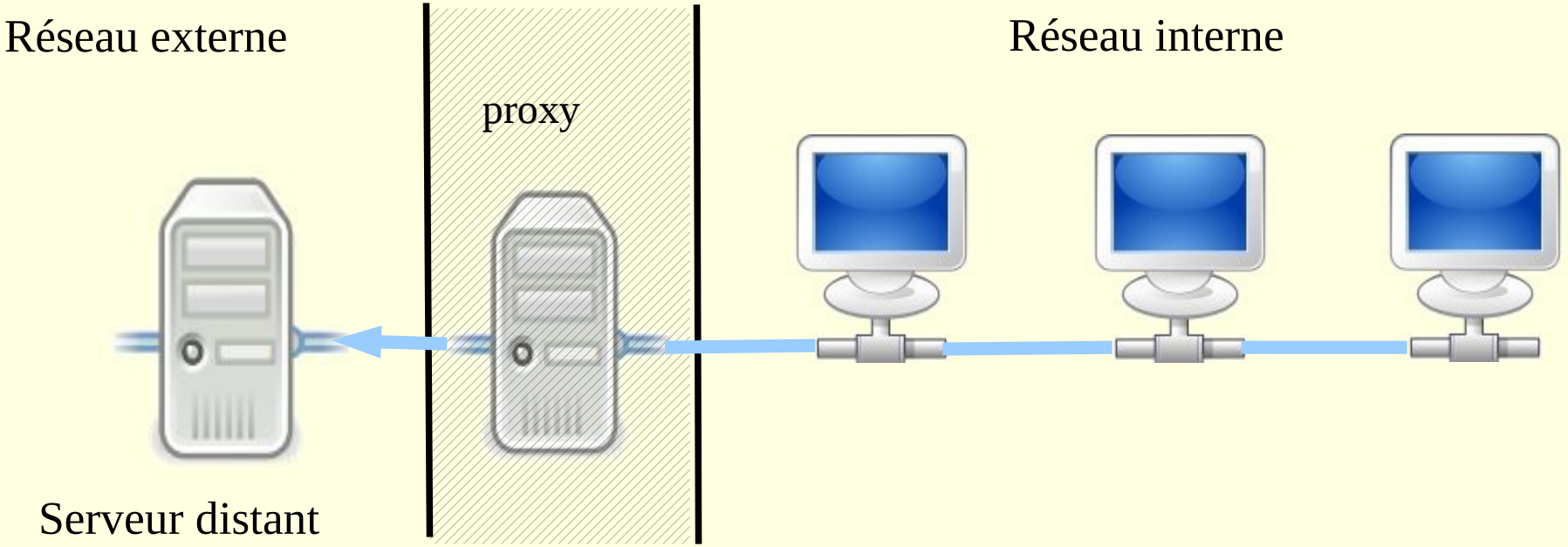
Pare-feu personnel

- Pare-feu logiciel limité à la protection de la machine sur laquelle il est installé
- Exemples:
  - netfilter : intégré au noyau Linux
    - ✓ firestarter : interface graphique sous Gnome
  - pare-feu intégré à Window XP, Vista
  - ZoneAlarm, Kerio sous Windows

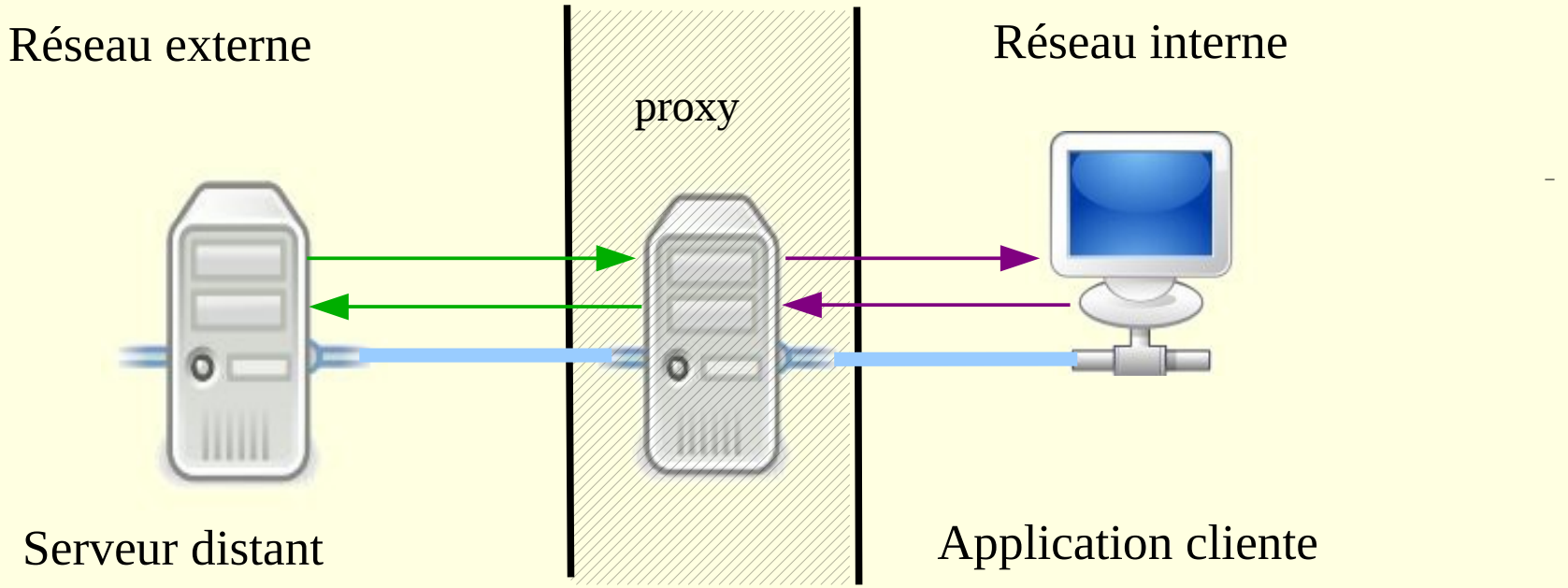
Proxy

- Serveur mandataire
  - machine intermédiaire entre les ordinateurs d'un réseau local et internet :
    - ✓ serveur mandaté par une application pour effectuer la requête sur internet à sa place
  - Autres fonctionnalités :
    - ✓ Cache
    - ✓ Filtrage
    - ✓ Authentification

Proxy



Proxy


Réseau externe
proxy
Réseau interne
Serveur distant
Application cliente

NAT

- **N**etwork **A**ddress **T**ranslation :
  - Translation d'Adresse
- 2 modes principaux :
  - Translation statique
    - ✓ une adresse externe pour une adresse interne
  - Translation dynamique
    - ✓ une adresse externe pour plusieurs adresses internes
      - permet de palier le manque d'adresse IPv4

Adressage IPv4

- Plusieurs classes d'adressage selon la taille du réseau

Classe	<net-id>	<host-id>
A	8 bits	24 bits
B	16 bits	16 bits
C	24 bits	8 bits
D	adresse de groupe de diffusion	
E	format réservé	

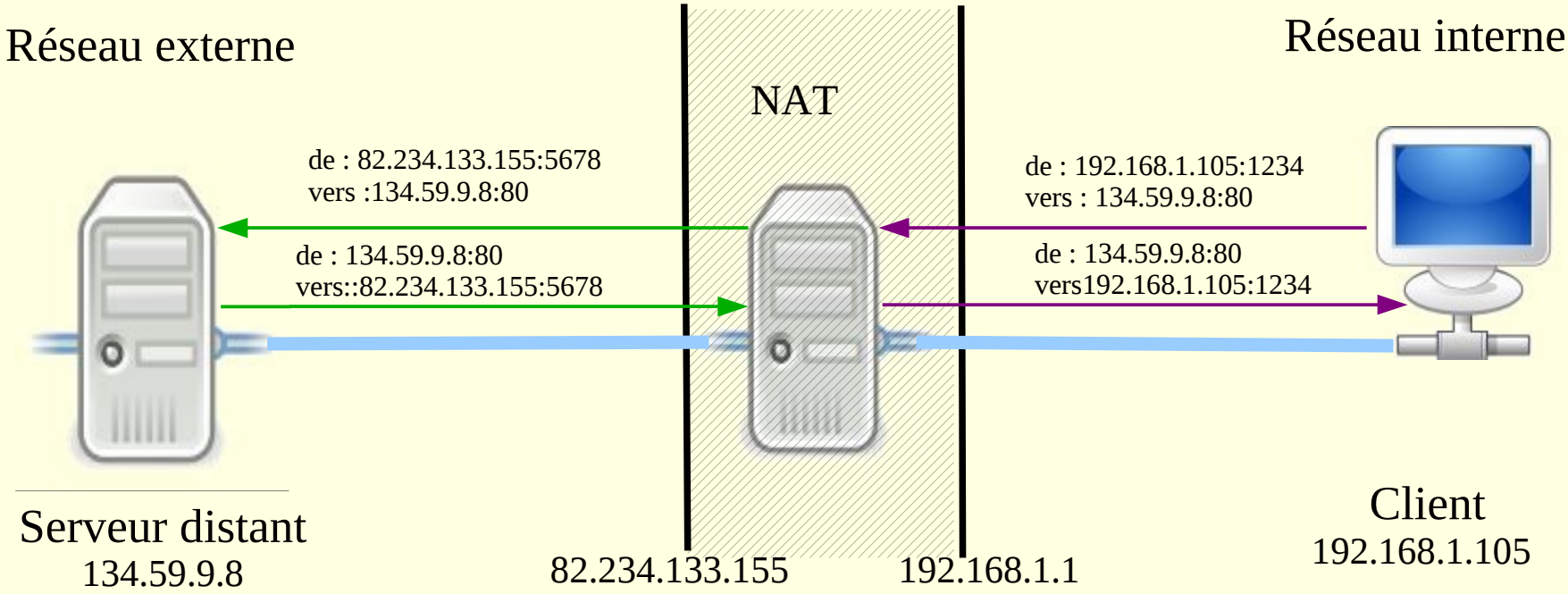
- **Masque de (sous-)réseau** (pour classes A, B, C)
  - nombre de 32 bits
  - même format et même notation qu'une adresse
  - spécifie les bits de **<net-id>** (bits à 1) et ceux de **<host-id>** (bits à 0)

Adressage privées IP

- Adresses IP publiques réservées aux réseaux privés *(Intranets)* :
  - **1** réseau de classe **A** :
    10.0.0.0
    (adresses de **10**.0.0.0 – **10**.255.255.255)
  - 1 bloc de **16** réseaux de classe **B** :
    172.16.0.0 à **172.31.**0.0
    (adresses de **172.16**.0.0 – **172.31**.255.255)
  - 1 bloc de **256** réseaux de classe **C** :
    192.168.0.0 à **192.168.255.**0
    (adresses de **192.168.0**.0 – **192.168.255**.255)

NAT

- NAT: Network Address Translation
- PAT : Port Address Tranlation



NAT : Translation d'adresse statique

- Association
  - d'une adresse IP publique (routable)
    - ✓ Ex : 82.234.133.155
  - à une adresse IP privée du réseau interne (non routable)
    - ✓ Ex : 192.168.1.105
- Modification de l'adresse dans le datagramme IP à l'émission et à la réception

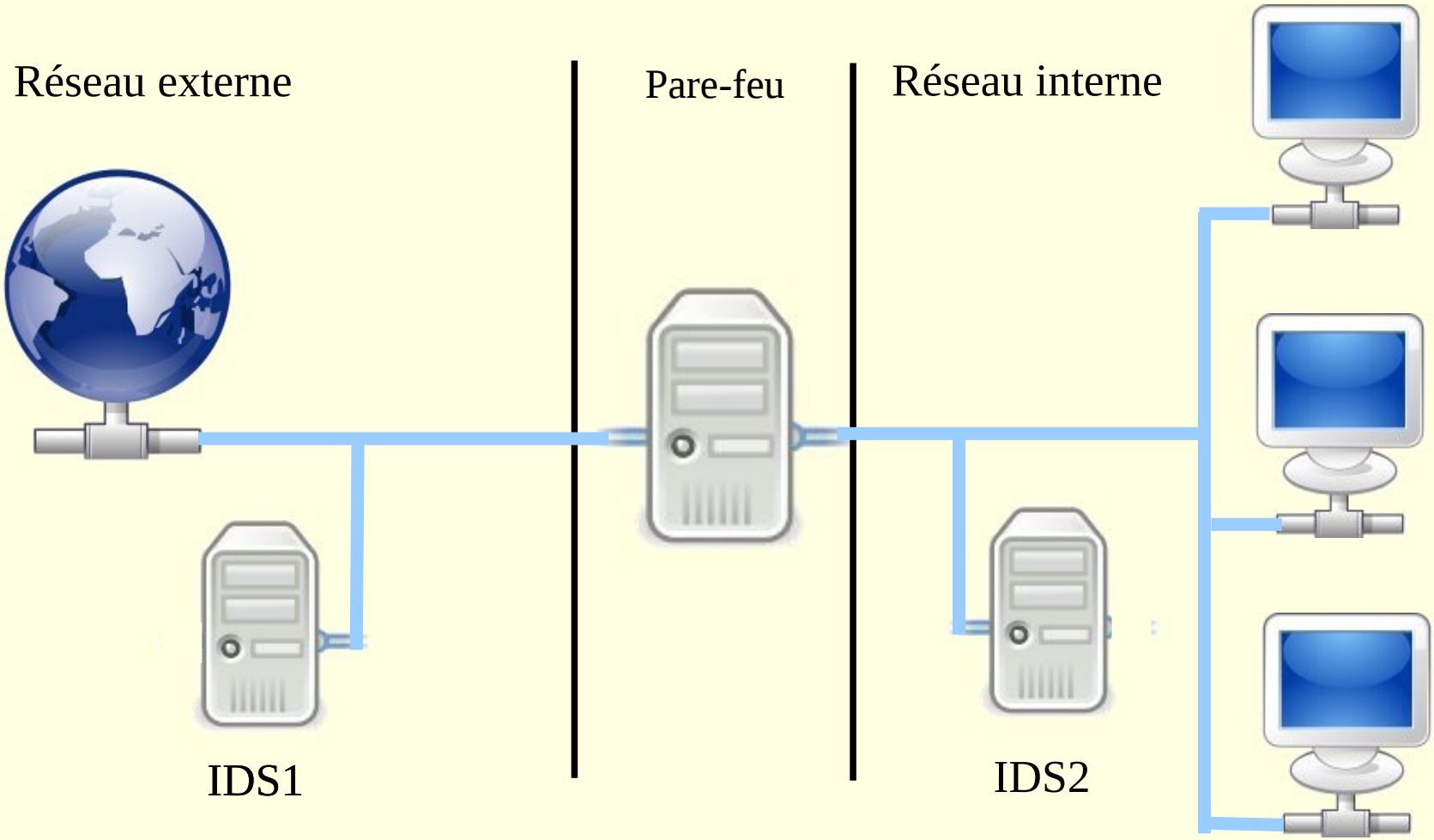
NAT : Translation d'adresse dynamique

- Permet de partager :
  - une adresse publique (routable)
  - entre plusieurs machines d'un réseau local privé
- Masquarade (IP masquerading)
  - vu de l'extérieur les machines du réseau local possèdent la même adresse IP
- PAT : **P**ort **A**ddress **T**ranslation

Detection d'intrusions

- IDS : **I**ntrusion **D**etection **S**ystem
- Deux grandes familles :
  - N-IDS : **N**etwork based **I**ntrusion **D**etection **S**ystem
    - ✓ matériel dédié
    - ✓ contrôle les paquets circulant sur un ou plusieurs liens
  - H-IDS : **H**ost based **I**ntrusion **D**etection **S**ystem
    - ✓ réside sur un hôte particulier
    - ✓ se comporte comme un démon ou un service standard
    - ✓ analyse les logs
    - ✓ analyse les paquets entrant et sortant de l'hôte

N-IDS



N-IDS

- Techniques de détection
  - vérification de la pile protocolaire
    - ✓ détection des violations de protocole
    - ✓ mise en évidence des paquets invalides
  - vérification des protocoles applicatifs
  - reconnaissance des attaques par pattern matching
    - ✓ signature
- Alertes
  - notifications : mail, logs, SNMP
  - actions : démarrage d'une application, fermeture d'une connexion, etc.

IPS

- IPS: **I**ntrusion **P**revention **S**ystem
- Positionnement en coupure sur le réseau
- Possibilité de bloquer immédiatement les intrusions
- Basé sur :
  - filtrage de paquets
  - moyen de blocages
    - ✓ coupure de connection
    - ✓ élimination de paquets suspects

VPN

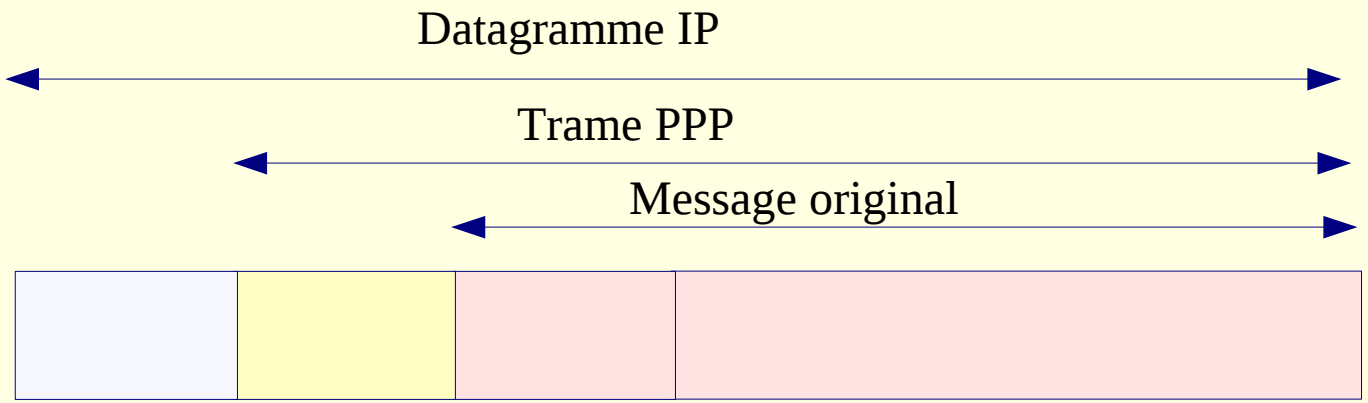
- **V**irtual **P**rivate **N**etwork
  - Réseau Privé Virtuel (RPV)
  - permet de relié à travers un réseau peu sûr (internet)
    - ✓ des réseaux privés locaux comme à travers une liaison spécialisée (ligne louée...)
      - sites distants d'une entreprise
      - sites d'une entreprise et de ses clients / fournisseurs
    - ✓ une machine particulière à un réseau privé
      - collaborateur de l'entreprise en déplacement
      - collaborateur à domicile
  - utilisation de protocoles d'encapsulation (tunneling ou « tunnelisation ») permettant de sécuriser les données entre les 2 extrémités du « tunnel »

VPN : protocoles

- PPTP : **P**oint-to-**P**oint **T**unneling **P**rotocol
- L2F : **L**ayer **T**wo **F**orwarding
- L2TP : **L**ayer **T**wo **T**unneling **P**rotocol
- IPSec

PPTP

- PPTP : **P**oint-to-**P**oint **T**unneling **P**rotocol
- Protocole de niveau 2
- Encapsulation PPP (**P**oint to **P**oint **P**rotocol) sur IP
  - machines distantes connectées point à point



L2TP

- **L**ayer **T**wo **T**unneling **P**rotocol
- Convergence entre
  - PPTP (MicroSoft, 3Com, US Robotics, etc.)
  - et L2F (Cisco, Northern Telecom, etc.)
  - standardisé : RFC 2661
- Protocole de niveau 2 basé sur PPP
- Encapsule des trames PPP encapsulant elle-mêmes d'autres protocoles (IP, NetBios, etc.)

IPSec

- Prévu pour fonctionner avec IPv6
  A été adapté pour Ipv4
- Niveau 3 (réseau) du modèle OSI
  - avantage sur SSL, TLS, SSH qui sont au niveau 4
    - ✓ pas besoin d'adapter le code des applications
- Améliore la sécurité du protocole IP :
  - garantit la confidentialité, l'intégrité et l'authentification des échanges

IPSec

- 2 modes :
  - transport mode
    - ✓ communication machine-machine
    - ✓ seule la charge utile (payload) du datagramme IP est chiffrée et/ou authentifiée
  - tunnel mode
    - ✓ communication réseau-réseau
    - ✓ le datagramme IP complet est encrypté : il doit être encapsulé dans un autre datagramme IP pour permettre le routage
- Basé sur 3 modules :
  - AH : IP **A**uthentification **H**eader
  - ESP : IP **E**ncapsulating **S**ecurity **P**ayload
  - SA : **S**ecurity **A**ssociation

IPSec

- AH Protocol (Authentification Header)
  - garantit pour les datagrammes IP :
    - ✓ intégrité des data
    - ✓ authentification (non-répudiation)
- ESP Protocol (Encapsulating Security Payload)
  - chiffrement des datagrammes
    - ✓ confidentialité des data
    - ✓ intégrité
    - ✓ authentification
- SA (Security Association)
  - Définit l'échange des clés et des paramètres de sécurité

Sécurité des Réseaux sans fil WiFi

- Configuration
- WEP *(**W**ireless **E**quivalent **P**rivacy)*
- WPA *(**W**ifi **P**rotected **A**ccess)*
- 802.1x

Configuration

- Points d'accès
  - sécurité minimale par défaut
    - ✓ administrateur
      - changer le nom et le mot de passe
    - ✓ modifier le nom du réseau : SSID (**S**ervice **S**et I**D**entifier)
    - ✓ masquer le réseau
      - désactiver la diffusion du SSID
  - Filtrage des adresses MAC
    - ✓ limite l'accès à des machines connues (mais pas à des utilisateurs)

WEP

- **W**ired **E**quivalent **P**rivacy
  - algorithme symétrique RC4
    - ✓ Clé :64 (40 utiles) ou 128 (104 utiles) bits
      - statique
      - partagée par toutes les stations
    - ✓ Chiffrement
      - Génération d'un nombre pseudo-aléatoire de la longueur de la trame à chiffrer
      - XOR avec le contenu de la trame
  - Cassable
    - ✓ très facilement par force brute (clé 64 bits)
    - ✓ relativement facilement (clé 128 bits)
  - Clé partagée par tous les postes
  - Pas d'authentification

WPA

- **W**ifi **P**rotected **A**ccess
  - version intermédiaire allégée en attendant la validation du protocole 802.11i
  - Authentification
    - ✓ serveur d'authentification (en général Radius)
    - ✓ version restreinte : WPA-PSK (Pre-shared Key)
      - clé unique partagée par les équipements
  - Cryptage
    - ✓ protocole TKIP (Temporal Key Integrity Protocol)
      - génération aléatoire de clés
      - possibilité de modifier la clé de chiffrement plusieurs fois par seconde
  - Utilisation :
    - ✓ Uniquement en mode Infrastructure

802.1x

- Standard IEEE : juin 2001
- Objectif
  - authentification des utilisateurs se connectant à un réseau (filaire ou sans fil)
  - serveur d'authentification (généralement Radius)
    - ✓ autres utilisations : log, facturation, etc.
  - protocole EAP (**E**xtensible **A**uthentification **P**rotocol)
    - ✓ transporte les données d'identification des utilisateurs
  - contrôleur d'accès
    - ✓ intermédiaire entre l'utilisateur et le serveur d'authentification
    - ✓ Point d'accès du réseau sans fil

802.11i (WPA2)

- Ratifié le 24 juin 2004
  - Basé sur 802.1x
- Utilisation :
  - Infrastructure et ad hoc
- 2 modes :
  - WPA Entreprise
    - ✓ serveur d'authentification (en général Radius)
  - WPA Personal
    - ✓ pas de serveur d'authentification
    - ✓ Clé partagée
      - PSK: Pre-Shared Key (générée à partir d'une passphrase)

802.11i (WPA2)

-
  - TKIP : **T**emporal **K**ey **I**ntegrity **P**rotocol
  - Supporte aussi AES (Advanced Encryption Standard) plus sûr

Outils (1/2)

- nslookup / dig
  - permet de connaître l'adresse IP d'un domaine et réciproquement.
- ping
  - permet de savoir si une machine est active (requête ICMP : echo vers la machine distante)
- traceroute / tracert
  - indique le chemin par un epaquet IP suivi pour aller d'une machien à une autre
- Wireshark (anciennement ethereal)
  - analyser de protocole (packet sniffer)

Outils (2/3)

- nmap : scanner de ports
  - détecte les ports ouverts, identifie les services et le système d'exploitation d'un système distant.
- Kismet
  - détecteur passif de réseaux sans fil
- nessus www.nessus.org
  - teste les faiblesses d'une machine vis à vis de la sécurité
- netcat
  - permet d'ouvrir des connexions réseaux (UDP ou TCP)

Outils (3/3)

- finger
  - permet d'obtenir des informations sur les utilisateurs d'un système
- crack / john
  - décrypteur de mots de passe
- chkrootkit / rkhunter
  - détecteur de rootkit
- firestarter / kerio / zonealarm
  - pare-feu

Plan général

- Introduction
- Principes de Bases de la Sécurité de l'Information
- Cryptographie
- Sécurité des Réseaux
- Sécurité des Applications
- Politique de sécurité
- Conclusion