Certificats électroniques

Matthieu Herrb
Jean-Luc Archimaud, Nicole Dausque & Marie-Claude Quidoz

Février 2002

CNRS-LAAS

Plan

- ☐ Services de sécurité
- ☐ Principes de cryptographie et signature électronique
- ☐ Autorités de certification et gestion des clés
- ☐ Applications

Chapitre 1

Services de sécurité

Rappel des services de base en sécurité

Authentification vérification de l'identité
- carte d'identité, passeport

Intégrité garantie de non-modification par un tiers
- facile pour un document manuscrit

Confidentialité pas de prise de connaissance non autorisée
- coffre fort
- plis cachetés

Non-répudiation impossibilité de nier avoir émis un document
- graphologie. . .

Contrôle d'accès autorisation d'actions en fonction de l'identité
- serrures, clés

Lacunes des systèmes actuels

- Faiblesses du courrier électronique : pas d'authentification, contenu circulant en clair ;
- Multiplication des modes d'authentification et des mots de passe par application.
- Cas particulier du CNRS :
  - très réparti,
  - gros besoins de communication,
  - pas d'intranet.

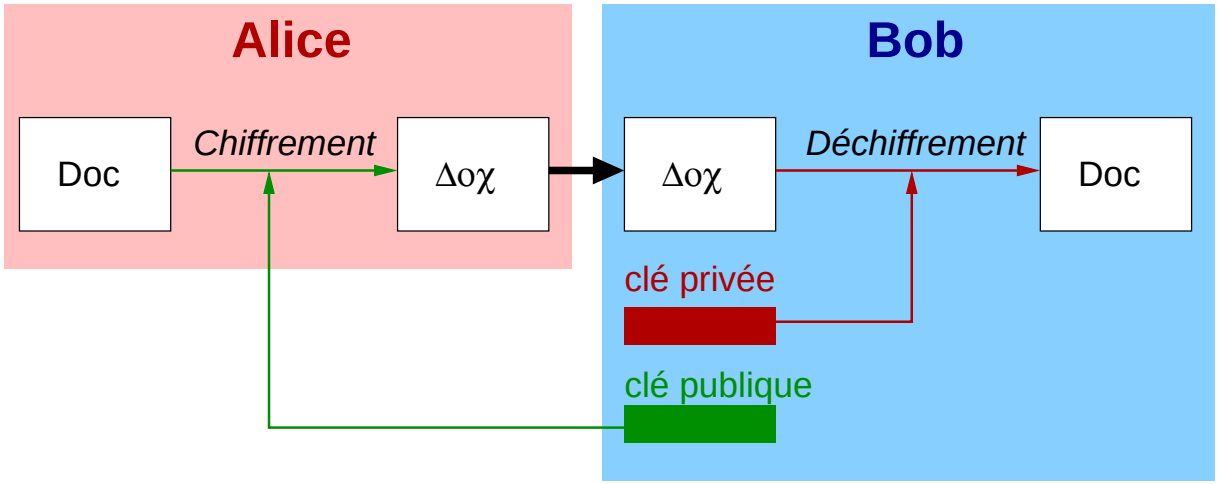
Chapitre 2

Principes de cryptographie et signature électronique

Éléments de cryptographie

Chiffrement asymétrique (RSA) : Alice et Bob possèdent chacun une clé *privée* et une clé *publique*.

Un message chiffré avec la clé publique se déchiffre avec la clé privée.

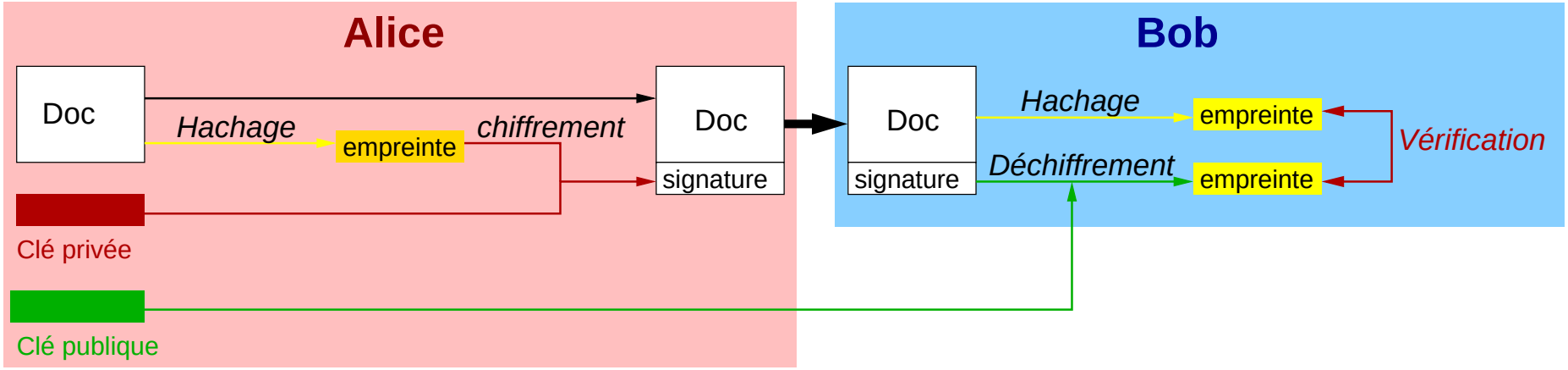


Signature numérique (1)

Utilise une fonction de hachage appliquée au document :

- Calcule une suite de bits de taille fixe : l'*empreinte*.
- Un bit du document modifié $\Rightarrow$ empreinte différente.
- MD5 (Message Digest) : empreintes de 128 bits
- SHA1 (Secure Hash Algorithm) : empreintes de 160 bits.

Signature numérique (2)



Signature :
- calcul de l'empreinte du document
- chiffrement de l'empreinte avec la clé privée de l'expéditeur

Vérification de la signature :
- déchiffrement de l'empreinte avec la clé publique de l'expéditeur,
- comparaison avec l'empreinte calculée

Sécurité d'une signature numérique

La sécurité d'une signature numérique dépend :
- de la qualité des algorithmes de chiffrement utilisés,
- de la longueur des clés de chiffrement,
- de la qualité de l'implémentation des algorithmes,
- mais surtout de **la manière dont est protégée la clé privée** de l'utilisateur

En pratique :
- protection par « passphrase » (mot de passe) $\Rightarrow$ le plus courant.
- carte à puce : la clé privée est sur une carte à puce. Insérer la carte dans un lecteur rend utilisable la clé privée.

Pas nécessaire de protéger la clé publique. Au contraire, elle doit être facilement accessible à tous.

Garantir l'authenticité de la clé publique $\rightarrow$ la signer par un tiers.

Chapitre 3

Autorités de certification et gestion des clés

Certificats : principes

☐ Comment être sûr de la clé publique d'une personne ?

$\longrightarrow$ Certificat = carte d'identité numérique.

Un certificat : un fichier émis par une autorité de certification contenant :
- Nom, prénom, adresse email + infos diverses
- Clé publique de la personne
- Date de validité
- Nom de l'autorité de l'autorité de certification
- Signature de l'autorité de certification

Vérification du certificat à l'aide de la clé publique de l'autorité de certification et de la date de validité.

$\longrightarrow$ Pour vérifier un certificat il faut et il suffit de connaître la clé publique de l'autorité émettrice.

Contenu d'un certificat (exemple : CNRS)

```
  Version: 3 (0x2)
  Serial Number: 8 (0x8)
  Issuer: C=FR, O=CNRS, CN=CNRS-Standard
  Validity
    Not Before: May 10 15:28:57 2001 GMT
    Not After : May 10 15:28:57 2002 GMT
  Subject: C=FR, O=CNRS, OU=UPR8001, CN=Matthieu Herrb/Email=matthieu.herrb@laas.fr
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
     Modulus (1024 bit):
       a8:3f:d9:27:89:ad:2c:97:39:e2:08:8d:d8:41:dd:
       [...]
  X509v3 extensions:
    [...]
    X509v3 CRL Distribution Points:
      http://igc.services.cnrs.fr/cgi-bin/loadcrl?CA=CNRS-Standard
    Netscape Renewal Url:
      https://igc.services.cnrs.fr/cgi-bin/renew?CA=CNRS-Standard
Signature Algorithm: md5WithRSAEncryption
  99:b0:16:d4:ef:e2:d2:a7:cf:bd:b5:8d:54:12:c5:91:0e:86:[...]
```

Autorité de certification

☐ Quelle autorité pour signer les certificats ?

- une société commerciale *Verisign*, *CERT-Plus*, . . .
  coût : environ 25 - 30 € / personne /an.
- une autorité administrative qui propose ce service
  inexistant à ce jour en France . . .
- mettre en place soi-même ce service

C'est un choix stratégique pour une organisation

Techniquement ça peut être n'importe qui.

Infrastructure de gestion de clés

Un certificat = une carte d'identité

Mairies, préfectures, formulaires, fichiers, tampons. . .pour émettre les cartes d'identité nationales.

$\longrightarrow$ idem pour les certificats : **I**nfrastructure de **G**estion de **C**lés (IGC).
En anglais : **P**ublic **K**ey **I**nfrastructure (PKI).

Quatre éléments :
- Politique de certification,
- Autorité de certification,
- Autorité d'enregistrement,
- Service de publication.

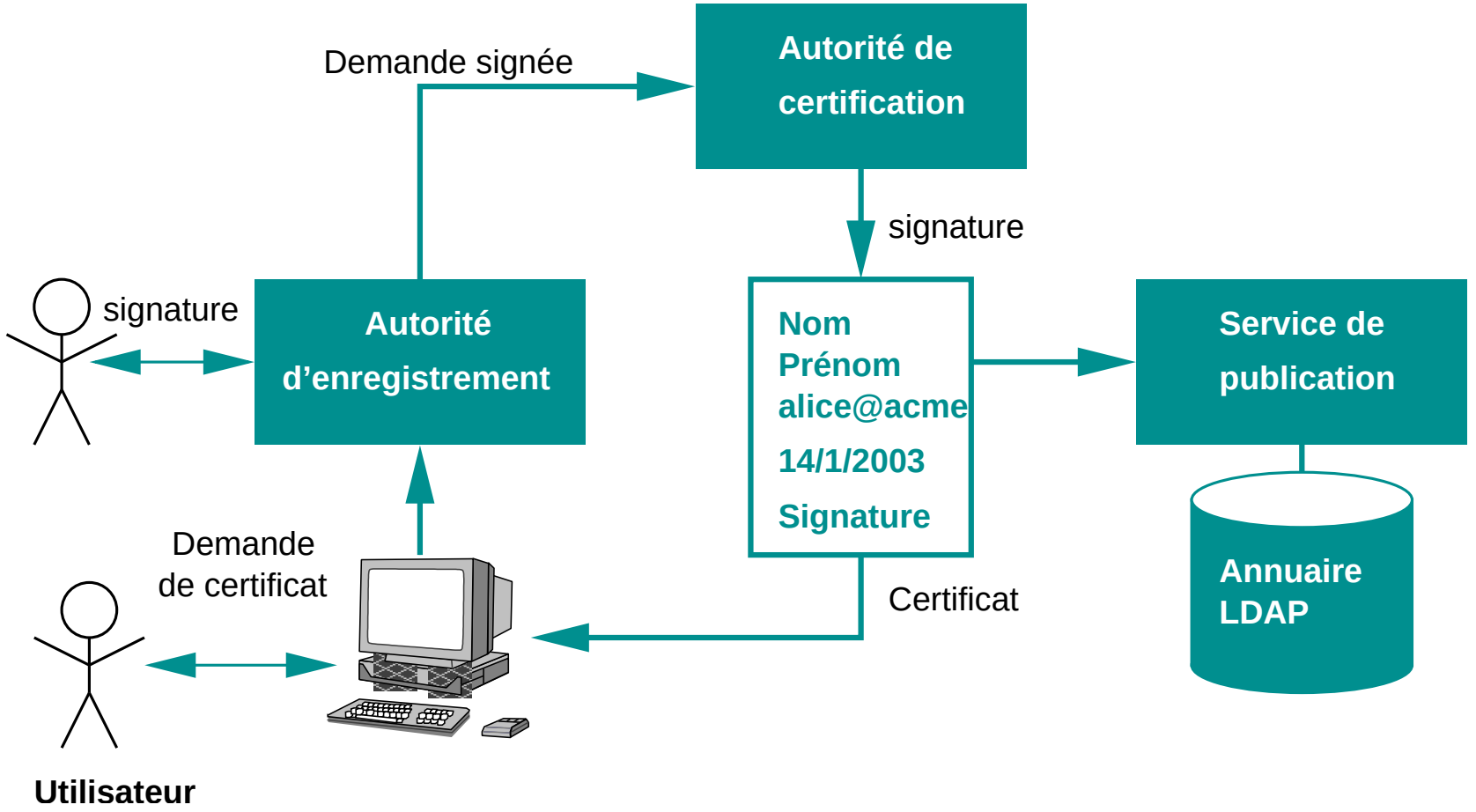
Services normalisés par l'ISO : X509, PKCS#7, PKCS#12,. . .

Politique de certification

C'est un document qui décrit :
- les objectifs de sécurité d'une IGC,
- les moyens mis en œuvre pour atteindre ces objectifs,
- les procédures utilisées.

Base de la confiance qu'on peut placer dans un certificat émis par une IGC.

Schéma de principe d'une IGC



Autorité d'enregistrement

C'est le « guichet » auquel on s'adresse pour obtenir un certificat.

Rôle :
- vérification de l'identité de l'utilisateur,
- récupération (éventuellement génération) de la clé publique de l'utilisateur,
- transmission de la demande signée de création de certificat à l'autorité de certification.

Il peut y avoir plusieurs autorités d'enregistrement.

Autorité de certification

- Reçoit les demandes de certificat,
- vérifie la signature de la demande,
- génère le certificat,
- signe le certificat avec sa clé privée ,
- transmet le certificat à l'utilisateur.

La clé publique de l'autorité de certification peut être auto-signée ou signée par une autorité de niveau supérieur.

Les fonctions de l'autorité de certification peuvent être automatisées : l'autorité de certification est un programme.

Service de publication

Rend accessible les certificats :
– annuaire LDAP
– . . .

Publie la liste des certificats révoqués.

(Service important mais mal maîtrisé en pratique...)

Chapitre 4

Applications

Applications

- Signature et/ou chiffrement du courrier électronique (S/MIME),
- Protocole SSL/TLS :
  - Web sécurisé (HTTPS),
  - Accès distant à la messagerie (IMAPS/SMTP+STARTTLS),
- Réseaux virtuels privés : IPsec
- Niveau applicatif (remplace utilisateur/mot de passe pour l'authentification).

Messagerie sécurisée : S/MIME

Signature et/ou chiffrement des messages électroniques.

Utilise le codage MIME pour ajouter une signature ou marquer un contenu comme chiffré.

Supporté par Netscape Messenger, Microsoft Outlook, . . . ? ?

Pb : séquestre obligatoire des clés privées pour le chiffrement
(Pas possible aujourd'hui)

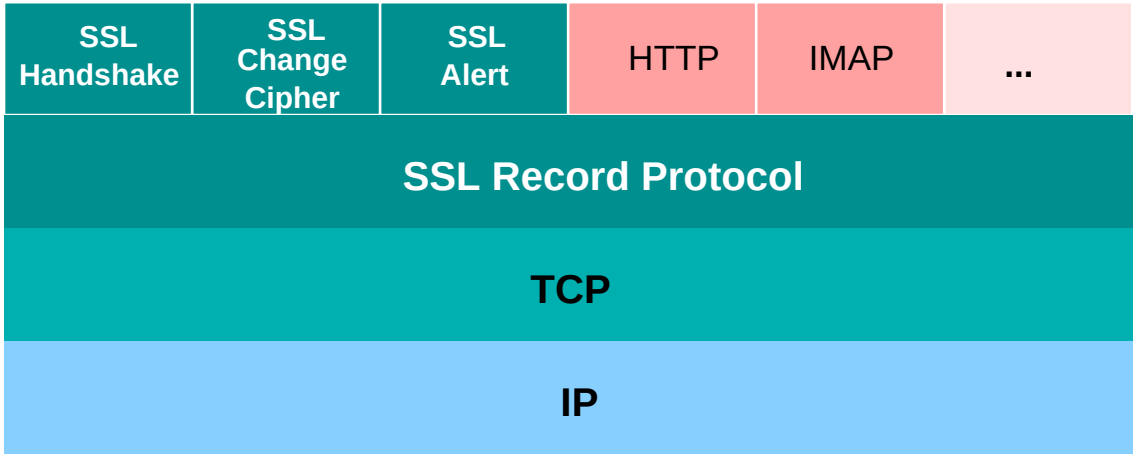
Un concurrent : PGP

Le protocole SSL/TLS

Secure **S**ockets **L**ayer

Mécanisme de transport sécurisé au dessus de TCP.

Version	**Origine**	**Supporté par...**
SSL v2.0	Netscape	Navigator 1.x/2.x, IE 3.x
SSL v3.0	Netscape	Navigator 3.x/4.x, IE 4.x
TLS v1.0	IETF Draft	Mozilla, IE 5.x



Applications de SSL (1) : HTTPS

Connexion HTTP sur un canal sécurisé par le protocole SSL.
URLs du type : `https://www.laas.fr`

Serveur identifié par un certificat.

Le navigateur vérifie le certificat du serveur.

Le serveur peut demander un certificat au client : $\rightarrow$ authentification de l'utilisateur.

Applications de SSL (2) : IMAPS/SMTP+STARTTLS

Utilisés par la messagerie
– IMAP : récupération du courrier depuis la boite à lettres
– SMTP : envoi du courrier

Même principe que HTTPS.

Connexion IMAP chiffrée : le mot de passe de messagerie ne circule pas en clair.

Identification auprès du serveur SMTP par certificat : autorisation du relayage de messages depuis l'extérieur pour utilisateurs nomades.

Applications : vue de l'utilisateur

Les principaux outils pour l'utilisateur :
son navigateur Web et son logiciel de messagerie.

Tâches pour les utilisateurs :
- Récupérer les certificats des autorités de certification
- Récupérer les listes de révocation (optionnel ?)
- Définir un mot de passe pour protéger les clés privées
- Demander un certificat
- Récupérer le certificat une fois émis
- Sauvegarde/restauration des certificats sous forme de fichiers `.p12`
- Consulter les certificats connus
- Gérer plusieurs certificats

- Envoyer un message signé
- Visualiser la signature d'un message reçu
- Se connecter à un site demandant une authentification par certificat
- Vérifier la longueur de clés utilisée par un site HTTPS.

Conclusion

Certificats : une réponse adaptée à un ensemble de besoins de sécurité.

Mais ça n'est pas une solution « magique » :

- nécessite une bonne organisation
- besoin de formation de tous les utilisateurs
- applications pas tout à fait prêtes

Chapitre 5

Références

Références

- S. Singh. Histoire des codes secrets. JC Lattes. 1999. ISBN 2-7096-2048-0.
- OSI - The Directory : Authentification Framework, Recommendation X.509, ISO/IEC 9594-8 http://www.dante.net/np/ds/osi/9594-8-X.509.A4.ps
- Internet X509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, http://www.ietf.org/rfc/rfc2459.txt
- S/MIME Version 3 Message Specification, RFC 2633, http://www.ietf.org/rfc/rfc2633.txt
- The TLS Protocol Version 1.0, RFC2246, http://www.ietf.org/rfc/rfc2246.txt
- D. Wagner and B. Schneier. Analysis of the SSL 3.0 Protocol. http://www.counterpane.com/ssl.html
- http://www.urec.cnrs.fr/securite/articles/certificats.kesako.pdf
- http://www.urec.cnrs.fr/securite/articles/IGC.pdf