Sécurité des réseaux
Certificats X509 et clés PGP

A. Guermouche

Plan

Plan

Présentation

- X509 définit un cadre pour la fourniture de services d'authentification par répertoire X500.
- Le répertoire X500 sert de dépot de certificats à clés publique.
- Chaque certficat X509 contient la clé publique de l'utilisateur et est signée par la clé privée de l'authorité de certification confiance.
- X509 définit des protocoles alternatifs d'authentification basés sur l'utilisation des certificats à clé publique.
- X509 est basé sur l'utilisation de cryptographie à clé publique et de signature numérique.
  - La norme ne dicte pas l'utilisation d'un algorithme spécifique.
  - Le procédé de signature nécessite l'utilisation d'une fonction de hachage.

Certificats

Le certificats à clé publique est au coeur de la résolution X509.

- Certificats délivrés par des authorités de certifications (AC) et placés dans le répertoire par l'AC ou l'utilisateur.
- Le répertoire ne fournit qu'un emplacement facilement accessible des utilisateur pour l'obtentions des certificats.

version : Différencie les versions successives du format de certificats.
numéro de série : Valeur entière, unique pour l'AC émettrice, associée au certificat.
id. de l'algo. de signature : Type de l'algorithme utilisé pour la signature, ce champs est peu utile vu que le type de l'algorithme de signature est contenu dans la partie signature.

version
Numéro de série
id. de l'algo. de signature
Nom du créateur
Période de validité
Nom du sujet
Infos. clé publique du sujet
id. unique du créateur
id. unique du sujet
Extensions
Signature

Certificats

Le certificats à clé publique est au coeur de la résolution X509.

- Certificats délivrés par des authorités de certifications (AC) et placés dans le répertoire par l'AC ou l'utilisateur.
- Le répertoire ne fournit qu'un emplacement facilement accessible des utilisateur pour l'obtentions des certificats.

nom d'émetteur : Nom X500 de l'AC qui a créé le certificats.
période de validité : Dates de début et de fin de validité du certificats.
nom du sujet : Nom de l'utilisateur auquel le certificats se réfère.

version
Numéro de série
id. de l'algo. de signature
Nom du créateur
Période de validité
Nom du sujet
Infos. clé publique du sujet
id. unique du créateur
id. unique du sujet
Extensions
Signature

Certificats

Le certificats à clé publique est au coeur de la résolution X509.

- Certificats délivrés par des authorités de certifications (AC) et placés dans le répertoire par l'AC ou l'utilisateur.
- Le répertoire ne fournit qu'un emplacement facilement accessible des utilisateur pour l'obtentions des certificats.

info. clé publique du sujet : La clé publique du sujet ainsi que l'identifiant de l'algorithme utilisé.

id. unique de l'émetteur : Une zone facultative de bits employée pour identifier sans ambiguïté l'AC émettrice (utile si un nom X500 a été utilisé pour différentes entités).

id. unique du sujet : Une zone facultative de bits employée pour identifier sans ambiguïté le sujet.

version
Numéro de série
id. de l'algo. de signature
Nom du créateur
Période de validité
Nom du sujet
Infos. clé publique du sujet
id. unique du créateur
id. unique du sujet
Extensions
Signature

Certificats

Le certificats à clé publique est au coeur de la résolution X509.

- Certificats délivrés par des authorités de certifications (AC) et placés dans le répertoire par l'AC ou l'utilisateur.
- Le répertoire ne fournit qu'un emplacement facilement accessible des utilisateur pour l'obtentions des certificats.

extensions : Un ensemble de champs d'extension.

signature : Couvre tous les autres champs du certificat. Elle contient le code de hachage de tous les autres champs chiffré avec la clé privé de l'AC.

version
Numéro de série
id. de l'algo. de signature
Nom du créateur
Période de validité
Nom du sujet
Infos. clé publique du sujet
id. unique du créateur
id. unique du sujet
Extensions
Signature

Notations

La norme emploie la notation suivante pour définir un certificat :

$$CA << A >> = CA\{V, SN, AI, CA, TA, A, Ap\}$$

où :

$Y << X >>$ est le certificat de l'utilisateur X émis par l'autorité de certification Y.

$Y\{I\}$ est la signature de I par Y. Elle se compose de I complété d'un code de hachage chiffré.

- L'AC signe le certificat avec sa clé privée.
- Si la clé publique correspondante est connue de l'utilisateur alors il peut vérifier la validité du certificat.

Obtention d'un certificat utilisateur

Les certificats utilisateurs produits par une AC ont les caractéristiques suivantes :

- ⋆ n'importe quel utilisateur ayant accès à la clé publique de l'AC peut vérifier la clé publique d'un autre utilisateur qui a été certifié.
- ⋆ aucune partie autre que l'AC ne peut modifier le certificat sans que cela ne soit détecté.

Si tous les utilisateurs souscrivent à la même AC alors :

- ⋆ il éxiste une confiance commune en cette AC
- ⋆ les certificats peuvent être placés dans le répertoire pour être accessibles à tous les utilisateurs
- ⋆ les utilisateurs peuvent s'échanger les certificats directement (l'utilisation la plus simple des certificats).

Obtention d'un certificat utilisateur

Les certificats utilisateurs produits par une AC ont les caractéristiques suivantes :

- ⋆ n'importe quel utilisateur ayant accès à la clé publique de l'AC peut vérifier la clé publique d'un autre utilisateur qui a été certifié.
- ⋆ aucune partie autre que l'AC ne peut modifier le certificat sans que cela ne soit détecté.

Exemple :

Si B est en possession du certificat de A, B a la certitude que :

- ⋆ les messages qu'il chiffre avec la clé publique de A seront à l'abri d'une écoute clandestine
- ⋆ et que les messages signés avec la clé privé de A sont infalsifiables.

Un cas plus complexe

Si le nombre d'utilisateurs est important, il peut être intéressant d'utiliser plus d'une AC.
Exemple : Supposons que A ait otenu son certificat de X_1 et B son certificat de X_2.
Problème : si A ne connaît pas la clé publique de X_2, le certificat de B lui est inutile.

Solution :
si les deux AC ont échangé ont échangé de manière sûre leur clé publique, alors lorsqu'il doit parler à B, A doit :

1. Obtenir à partir du répertoire, le certificat X_2 signé par X_1 et retrouver et vérifier à l'aide de la clé publique de X_1 la clé publique de X_2.
2. Utiliser le répertoire pour obtenir le certificat de B (qui est signé par X_2) et utiliser la clé publique de X_2 pour vérifier et obtenir en toute sécurité la clé publique de B.

Un cas plus complexe

Si le nombre d'utilisateurs est important, il peut être intéressant d'utiliser plus d'une AC.

Exemple : Supposons que A ait otenu son certificat de X_1 et B son certificat de X_2.

Problème : si A ne connaît pas la clé publique de X_2, le certificat de B lui est inutile.

Solution :

A dans cet exemple a utilisé une chaîne de certificats pour obtenir la clé publique de B. Cette est exprimée en notation X509 par :

$$X_1 << X_2 >> X_2 << B >>$$

Révocation de certificats

- Chaque certificats a une période de validité.
- Les certificats peuvent être retirés pour diverses raisons.
- Chaque AC maintient une liste se composant de tous les certificats révoqués mais non expirés (CRL) et la signe.
- Dès qu'un utilisateur reçoît un certificat il vérifie si le certificat a été révoqué ou non.

Plan

Pourquoi?

- Le courrier électronique est l'application réseau la plus utilisée et la plus répandue.
- Pas de sécurité dans les échanges standards de mail.
- Forte croissance de la demande de services garantissant la confidentialité et l'authenticité des messages.
- Deux modèles sont suscpeptibles d'être largement utilisés : *Pretty Good Privacy* (PGP) et S/MIME.

PGP

- PGP est en grande partie le résultat des recherches de Phil Zimmermann.
- Utilisation dans les applications de courrier électronique et de stockage de fichiers.
- Succès expliqué par :
  - Sa gratuité et sa portabilité.
  - La divérsité des algorithmes de cryptages sur lesquels il est basé.
  - Un large éventail d'applications.
  - Son indépendance (n'est contrôlé par aucune autorité).
- PGP fournit cinq services : authentification, confidentialité, compression, compatibilité entre applications de courrier électronique et ségmentation.

Authentification

L'authentification se déroule en effectuant la séquence d'operations suivante :

1. L'expediteur crée un message.
2. On utilise SHA-1 pour générer le code de hachage de 160 bits du message.
3. Le code de hachage est chiffré avec RSA en utilisant la clé privée de l'expéditeur, et le résultat est ajouté au début du message.
4. Le récepteur emploie RSA avec la clé publique de l'expéditeur pour déchiffrer et récupérer le code hachage.
5. Le receveur produit un nouveau code de hachage pour le message et le compare au code de hachage déchiffré. S'il y a correspondance, le message est considéré comme authentique.

La signature est normalement attachée au message mais peut être isolée dans le cas ou un message doit être signé par plusieurs personnes (un contrat légal par exemple).

Confidentialité

La confidentialité est assurée en chiffrant les messages à transmettre ou à stocker localement comme fichiers.

- ⋆ Possibilité d'utiliser différents algorithmes de chiffrement (CAST-128, IDEA, TDEA, 3DES . . .).
- ⋆ Génération d'une clé de session pour chaque message.

Lors de l'émission d'un message :

1. L'expéditeur génère un nombre aléatoire de 128 bits à utiliser comme clé de session uniquement pour ce message.
2. Le message est chiffré en utilisant CAST-128 (ou IDEA, ou 3DES, . . .) avec la clé de séssion.
3. La clé de séssion est chiffrée avec RSA (ou DSS) en utilisant la clé publique du destinataire et est ajoutée au message.
4. Le destinataire utilise RSA avec sa clé privée pour déchiffrer et récupérer la clé de session.
5. La clé de la session est utilisée pour déchiffrer le message.

Identifiant de clé

Comment faire pour déchiffrer la clé de session si un utilisateur donné a plusieurs paires de clés ?

solution naïve. Transmettre la clé publique avec le message.

- ⋆ Gaspillage d'espace.

solution "futée". Associer à chaque clé un identifiant unique calculé à partir de l'identifiant de l'utilisateur et de la clé.

- ⋆ Les identifiants de clé doivent être attribués et enregistrés pour être permettre à l'emetteur et au récepteur d'établir la correspondance identifiant/clé.

solution retenue. Attribuer à chaque clé un identifiant qui a une forte probabilité d'être unique.

- ⋆ L'identifiant de la clé se compose de ses 64 bits les moins significatifs.

Format d'un message PGP

horodatage : Date et heure auxquelles la signature a été produite.

résumé du message : Le résumé 160 bits SHA-1 chiffré avec la clé privée de A.

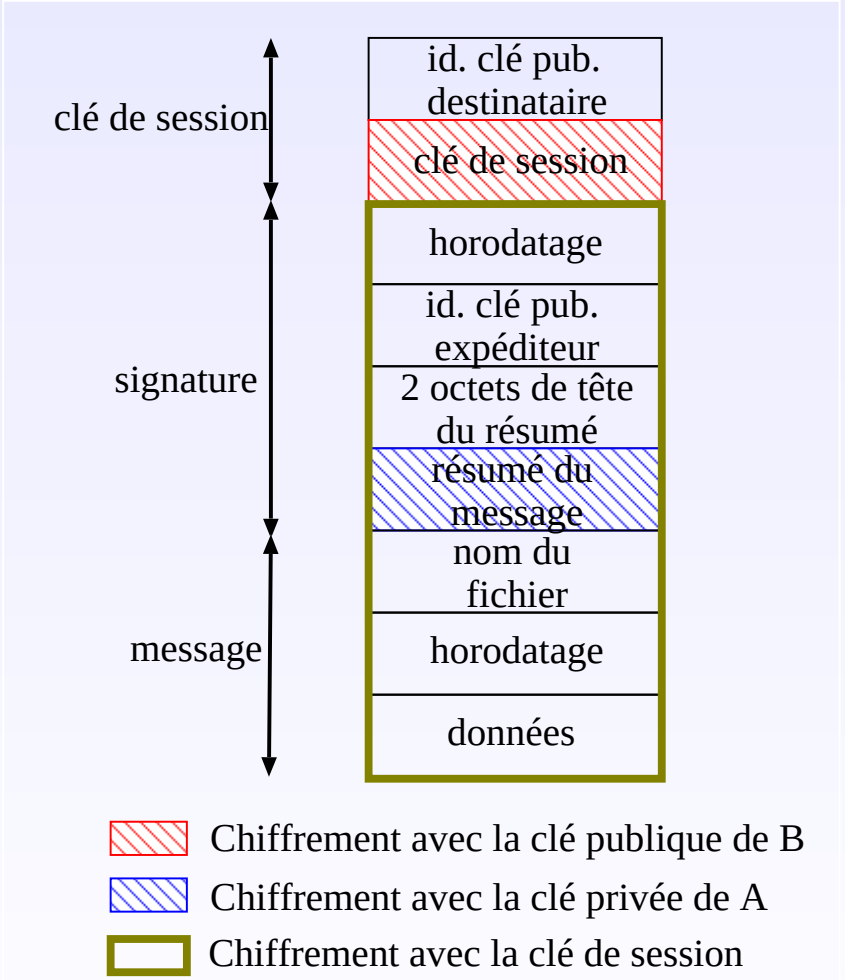

Figure: Message PGP de A à B.

Format d'un message PGP

2 octets de tête du résumé de message : Pour permettre à B de determiner si la bonne clé publique a été utilisée pour déchiffrer le résumé lors de l'authentification.

identifiant de clé publique de A : Identifie la clé publique qui doit être utilisée pour déchiffrer le message.

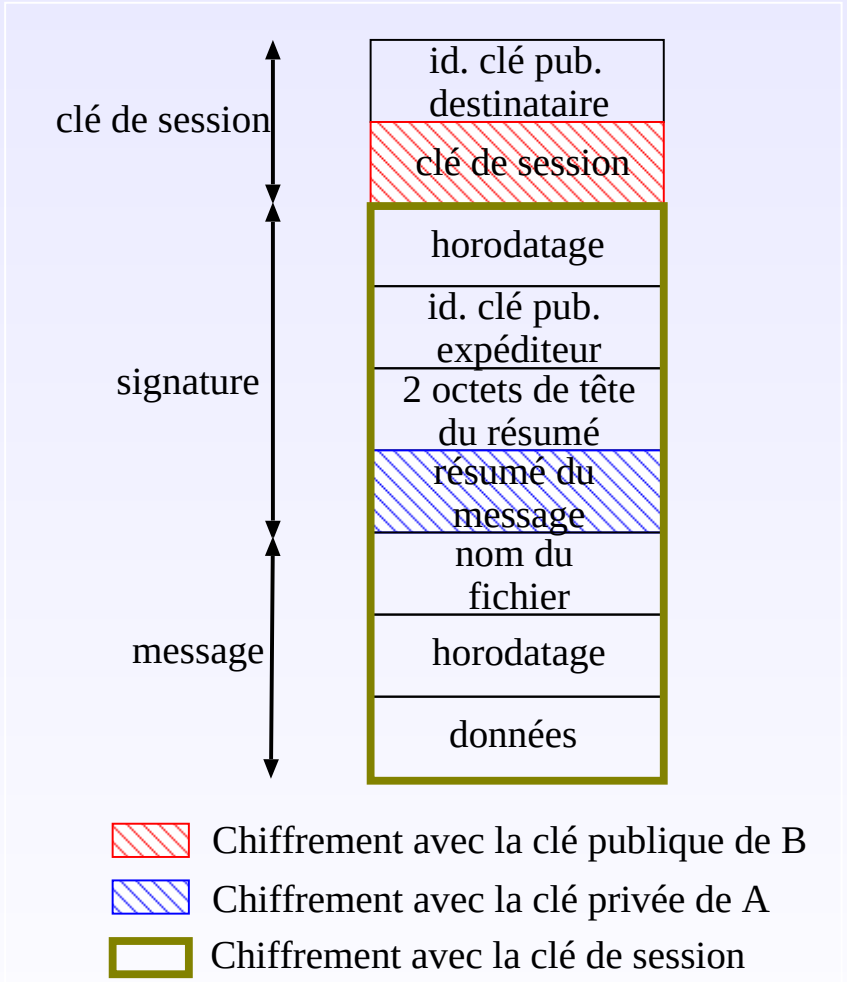

Figure: Message PGP de A à B.

Anneaux de clés

- Les paires de clés publiques/clés privées doivent être organisées et stockées efficacement sur chacun des noeuds.
- PGP utilise deux structures (*anneaux*) de données sur chaque noeud :
  - Une structure pour stocker les paires clés publiques/clés privées du noeud.
  - Une structure pour stocker les clés publiques d'autres utilisateurs connus pas ce noeud.

Anneaux de clés

Les anneaux peuvent être vus comme des tables.

L'anneau de clés privées :

- Contient pour chaque clé : un horodatage (date de création), un identifiant de la clé, une clé publique, une clé privée chiffrée, et un identifiant utilisateur.
- La clé privée est chiffrée en utilisant CAST-128, IDEA ou TDEA.
  - L'utilisateur choisit une *passphrase* à utiliser pour chiffrer les clés privées.
  - Quand le système génère une nouvelle clé privée, il demande à l'utilisateur sa *passphrase* et génère à partir de la phrase un code de hachage SHA-1 de 160 bits et la détruit.
  - La clé privée est chiffrée avec le code de hachage. Le code de hachage est ensuite détruit.

L'anneau de clés publiques :

- Contient pour chaque clé : un horodatage, un identifiant de la clé, la clé publique, et un identifiant utilisateur.

L'utilisation de la confiance (1/2)

Est ce que les clés contenues dans l'anneau de clés publiques sont authentiques?

- Utilisation d'intermédiaire de confiance pour récupérer la clé publique de l'utilisateur distant.
- Obtenir la clé publique à partir d'une authorité de certification.
- Chaque entrée de l'anneau de clés publiques est vue comme un certificat ayant un champ de confiance. Plus le niveau de confiance est élevé plus fort sera le lien entre l'identifiant utilisateur et la clé.
- Le certificat peut être signé par zéro ou plusieurs signatures. À chaque signature est associé un degré de confiance.
- Le champ de légitimité de la clé est dérivé de l'ensemble des champs de confiance de signature de l'entrée.

L'utilisation de la confiance (2/2)

- Lorsque A insère une nouvelle clé publique dans son anneau :
  - Si A est le propriétaire, la clé a un indice de confiance absolu.
  - Sinon, PGP demande à A d'évaluer le degré de confiance qui sera accordé au propriétaire de la clé.
- Quand la nouvelle clé publique est saisie, une ou plusieurs signatures peuvent lui être attachées. Quand une signature est insérée dans l'entrée, PGP vérifie si l'utilisateur est connu (à partir de l'anneau de confiance). Si c'est le cas, il lui affecte le degré de confiance de l'utilisateur.
- La valeur de légitimité de la clé est calculée sur la base des champs de confiance de signature présents dans cette entrée.