LES ARCHITECTURES PKI

Bibliographie

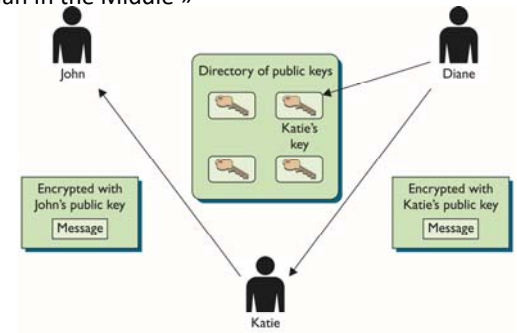
- « Principles of Computer Security: CompTIA, Security+ and Beyond », Second Edition, McGraw-Hill editor
  - La plupart des schémas utilisés dans ce support sont tirés de cet ouvrage
- « Cryptography and Network Security Principles and Practice, 5th Edition », William Stallings

Le problème de l'échange des clés publiques

- Dans une architecture publique, la prise en compte des clés publiques nécessite d'avoir confiance dans la personne qui nous la fournit
- L'obtention de la clé publique peut se faire
  - Soit par envoi en point en point (ex GPG) entre deux entités
  - Soit en passant par un annuaire centralisé comme LDAP par exemple
- Dans les deux cas, il faut s'assurer que la clé que l'on récupère provient bien de la personne concernée
  - Pas de garanties !

Le problème de l'échange des clés publiques

- Attaque « Man In the Middle »



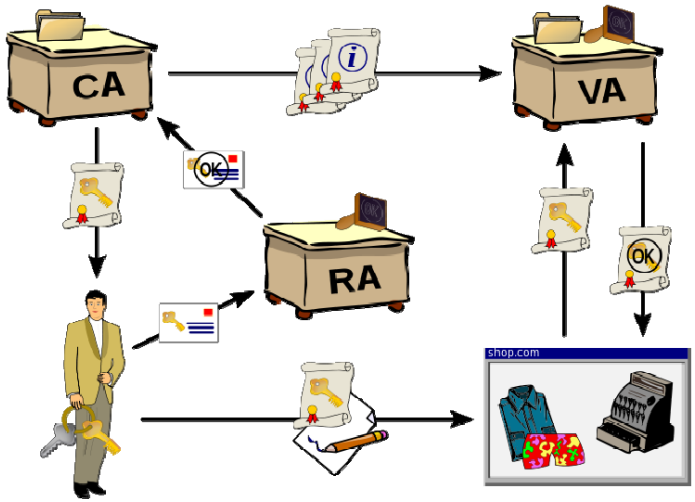
Source: « Principles of computer security », McGraw-Hill

L'infrastructure à clés publiques (PKI)

- L'objectif d'une PKI est de fournir des tiers de confiance partagés par Alice et Bob

- Une PKI va être composée de plusieurs éléments
  - Des certificats électroniques
  - Des autorités pour
    - L'enregistrement : Registration Authority ou RA
      - ★ *Va stocker et valider les clés publiques*
    - La certification: Certification Authority ou CA
      - ★ *Emet le certificat à partir d'une clé publique validée par une RA*
      - ★ *Communique le certificat aux VA*
    - La validation: Validation Authority ou VA
      - ★ *Assure la validité d'un certificat*
  - Un protocole standardisé de vérification

L'infrastructure à clés publiques (PKI)

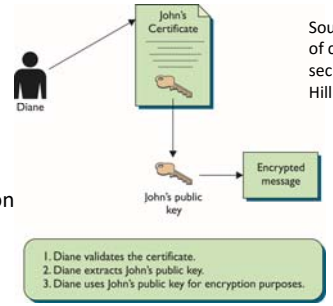


Le certificat

- Un certificat va jouer le rôle d'une carte d'identité numérique de la clé publique

- Il contient
  - L'identité de la personne
  - La clé publique de cette personne
  - Une attestation de cette association

  par un tiers de confiance



Source: « Principles of computer security », McGraw-Hill

- L'attestation est en fait la signature électronique apposée par l'autorité de certification (son sceau)
  - Il contient une empreinte du nom de l'autorité, de l'identité de propriétaire etc
  - Cette empreinte est ensuite chiffré à l'aide de la clé privée de l'autorité

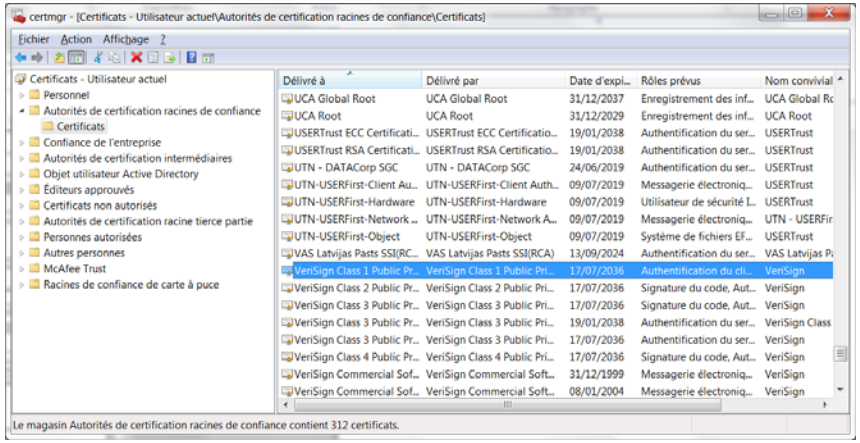
Le certificat

- La clé publique de l'autorité est ensuite largement diffusée
  - Elle peut également être signée par une autre autorité
    - On parle alors de chaine de confiance
  - La confiance est alors accordée si dans la chaîne on trouve une autorité dans laquelle on a confiance
    - VeriSign
    - GTE
    - Certinomis
    - …

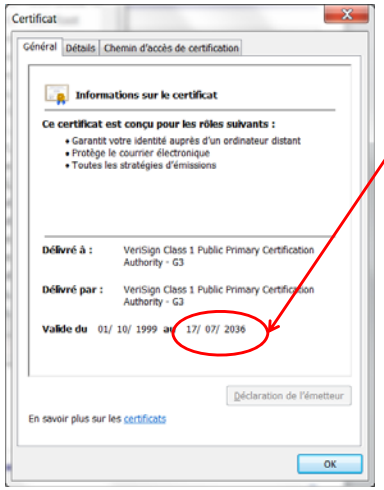
- La confiance dans la PKI repose donc sur la confiance que l'on accorde aux autorités associées
  - Par défaut les systèmes d'exploitations et les navigateurs Web disposent de clés publiques d'autorités « de confiance »

Le certificat

- Sous windows 7 (certmgr.msc)



Le certificat



- Un certificat est doté d'une date d'expiration
  - Cette date peut être très éloignée
  - Que ce passe-t-il si l'autorité disparait entre temps?
    - Ces certificats doivent pouvoir être révoqués
- L'autorité de certification doit donc
  - délivrer des certificats
  - leur donner une date de validité
  - pouvoir les révoquer
    - en particulier si sa clé est compromise

Les certificats

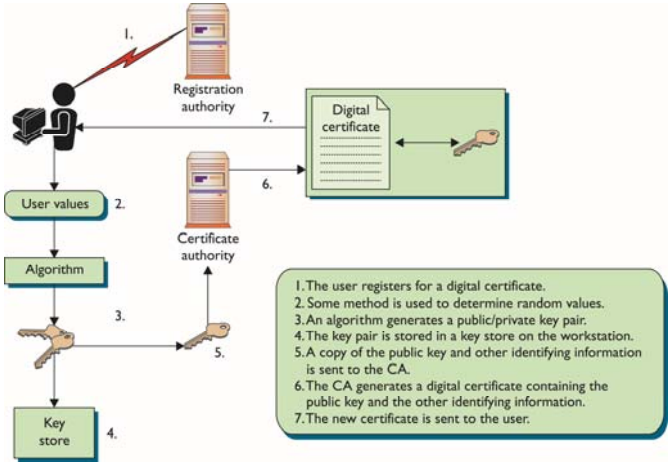
- On distingue trois classes de certificats
- Les certificats de classe 1 associent une clé publique à une adresse e-mail
  - Le demandeur reçoit un mail de confirmation
  - Pas de contrôle supplémentaire de la véracité de l'identité
  - Permet la signature et le chiffrement de courrier électronique essentiellement
  - Peuvent s'obtenir très rapidement et souvent gratuitement (Verisign et StartSSL)
  - Utilisation dans un cadre personnel
- Les certificats de classe 2 offrent les mêmes fonctionnalités que les classes 1
  - Vérification plus poussée de l'identité pouvant aller jusqu'à la présentation physique
  - Permettent de faire de la signature d'application logicielle
    - Permet de garantir l'identité de l'éditeur du logicielle
  - Utilisés dans le cadre professionnel

Les certificats

- Les certificats de classe 3 sont les certificats de plus haut niveau
  - Vérification de toutes les informations fournies
  - Compensation financière en cas de litige
  - Les certificats de classe 3 permettent également de mettre en œuvre sa propre autorité de certification pour émettre des certificats
    - L'entité devient alors une LRA (local registration authority)
      - ★ *Si la LRA n'appartient pas à une chaine de confiance, elle émet des certificats auto-signés*
      - ★ *Utile pour certifier des éléments au sein d'une entreprise avec plusieurs sites*
- Une CA reconnue doit être plus qu'un simple logiciel
  - Il faut des moyens humains pour vérifier les informations
  - Elle doit fournir un CPS: Certification Practice Statement qui précise
    - la manière dont les informations sont vérifiées
    - les étapes suivies et les données utiles pour produire un certificat
    - La manière de révoquer un certificat

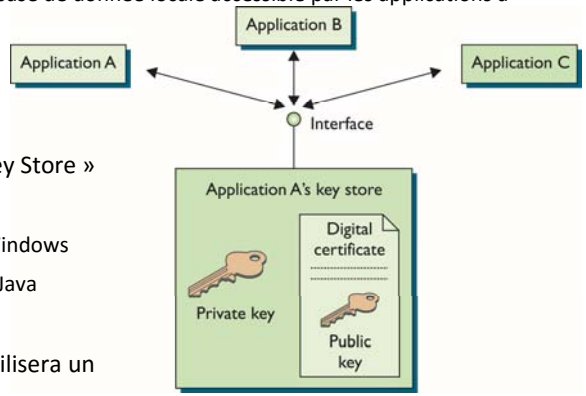
L'obtention d'un certificat

- Pour obtenir un certificat on passe par une Registration autority (RA)
  - La RA peut également être une CA mais ce n'est pas obligatoire



L'obtention d'un certificat

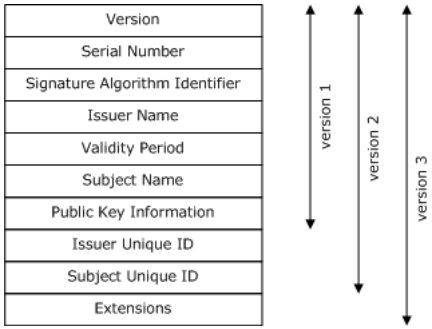
- Une fois obtenu le certificat peut être stocké localement dans un « Key store »
  - Le « key store » est une base de donnée locale accessible par les applications à travers une API dédiée



- Quelques exemple de « Key Store »
  - PKCS#11 sous Unix
  - CAPI (Crypto API) sous Windows
  - JCA (Java Crypto API) en Java
- Dans un réseau local au utilisera un annuaire LDAP

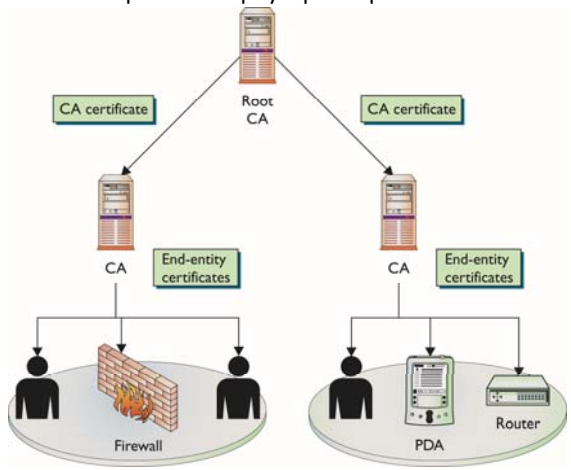
Le contenu d'un certificat

- Le format des certificats est défini par l'IETF à travers le standard X.509
  - Retenu par l'ITU-T comme standard international pour assurer l'interopérabilité des systèmes à base de certificats
- Actuellement on utilise la version 3 des certificats X.509 [RFC 5280]
  - Issuer caractérise la CA
  - Subject le propriétaire
  - Gestion des extensions
- Les noms sont représentés grâce au DN (Distinguished Name) de X.500
  - Egalement utilisé dans LDAP

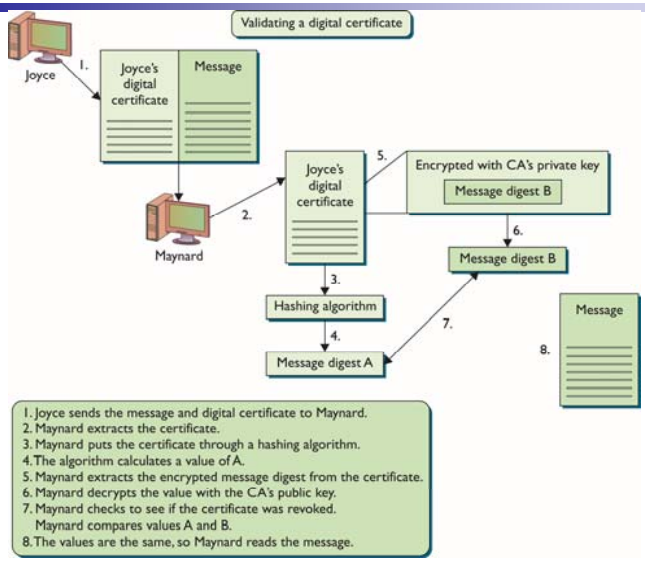


Des certificats pour tout le monde

- Les certificats ne sont pas limités à des personnes physique ils peuvent aussi identifier
  - Une CA
  - Des CA intermédiaires
  - Des matériels
  - Des utilisateurs
  - Des applications

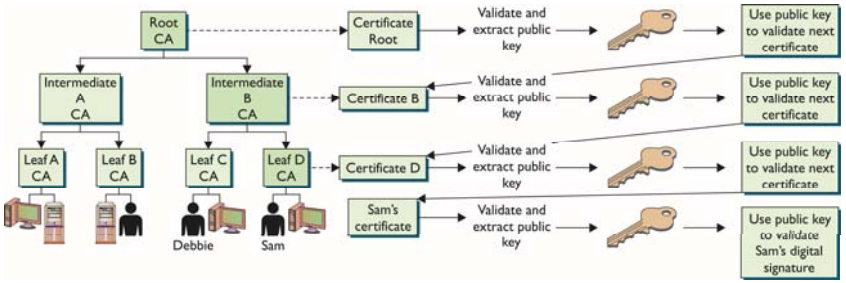


La validation d'un certificat



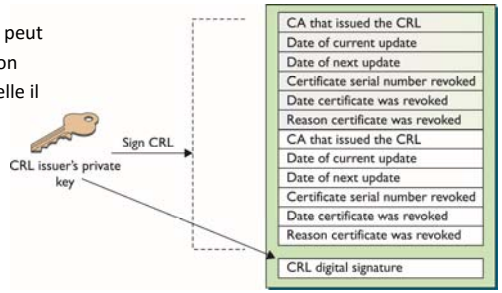
La validation d'un certificat

- La validation d'un certificat nécessite de valider la chaine de confiance
  - Exemple pour une architecture hiérarchique



La validation d'un certificat

- La vérification se passe en plusieurs étapes
  - On vérifie en premier lieu que le certificat n'a pas expiré
  - On authentifie ensuite l'empreinte avec la clé publique de la CA
  - On vérifie l'intégrité du certificat
  - Puis, on vérifie que le certificat n'a pas été révoqué en consultant la liste des révocations de certificats (CRL) de la CA
    - Pour chaque entrée de la CRL on peut connaître la cause de la révocation ainsi que la date à partir de laquelle il n'est plus valable



La validation d'un certificat

- Les CRL peuvent donc être vues comme des listes noires de certificats
  - En fonction du code, la gravité de la révocation va varier

Reason Code	Reason
0	Unspecified
1	All keys compromised; indicates compromise or suspected compromise
2	CA compromise; used only to revoke CA keys
3	Affiliation changed; indicates a change of affiliation on the certificate
4	Superseded; the certificate has been replaced by a more current one
5	Cessation; the certificate is no longer needed, but no reason exists to suspect it has been compromised
6	Certificate hold; indicates the certificate will not be issued at this point in time
7	Remove from CRL; used with delta CRL to indicate a CRL entry should be removed

Et la clé privée alors ?

- La clé privé doit rester la propriété exclusive de son propriétaire
  - Elle ne doit normalement jamais être communiquée
  - Elle ne doit pas être copiée
  - Elle doit être stockée en étant chiffrée par un algorithme symétrique
  - Le couple (clé publique, clé privée) doit avoir une durée de vie et pouvoir être révoqué
- Mais alors comment faire lorsque
  - L'utilisateur perd sa clé ?
  - Lorsqu'il est absent et que sa hiérarchie doit avoir accès à certains documents ?
  - En cas de décision de justice ordonnant la divulgation de certaines données ?

L' autorité de séquestre

- L'autorité de séquestre (Key Escrow) est une entité chargé de conserver les informations secrètes comme les bi-clés
  - Permet d'avoir accès aux échanges et/ou information d'une personne dans le cadre de son travail
- L'autorité de séquestre est un élément très important d'un PKI car il doit absolument maintenir la confidentialité des données
  - Soulève des contraintes à la fois techniques mais aussi légale
- Un moyen pour simplifier l'utilisation d'une autorité de séquestre est d'utiliser plusieurs couples de clés
  - Un couple sert pour le chiffrement des données
  - Un autre couple pour la signature

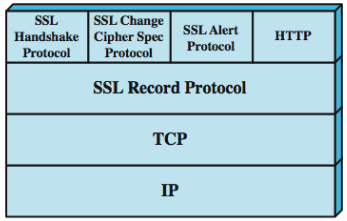
Les limites de PKI

- La révocation des certificats n'est pas optimale
  - Actuellement le système se base sur des listes noires qu'il faut sans cesse réactualiser
  - Une meilleure solution consisterait à utiliser des listes blanches
- Tout repose sur la chaine de confiance
  - Si les CA sont compromises le système flanche
  - Si trop de faux certificats sont émis la confiance va disparaître
  - L'utilisateur n'est que rarement acteur du système (les certificats sont gérés par son navigateur ou son système)
- Les CA sont toutes des entreprises privées
  - Elles se financent sur l'émission de certificat pas sur les vérification
  - Que se passe-t-il en cas de faillite ? En cas d'acquisition ?
    - Les certificats ont des durées de vie très longue que faire dans ce cas ?

SSL/TLS

Généralités

- SSL (Secure Socket Layer)
  - V3.0 sortie en 1996
  - Intégré dans les navigateurs depuis les années 90
- TLS (Transport Layer Security)
  - Version standardisé par l'IETF de SSL
  - TLS = SSL v3.1
  - Utilisé pour les communications réseaux sécurisées
    - Assure l'authentification et le chiffrement
  - Fonctionne au dessus de la couche transport



Généralités

- TLS doit être vu comme une évolution de SSL
  - SSL utilise du MD5 là où TLS utilise SHA
- Il repose sur un procédé de chiffrement à clé publique
- Il est indépendant du protocole utilisé
  - On peut mettre en œuvre TLS pour des transactions HTTP, du mail du FTP etc.
  - Pour http les urls sont de la forme: https://
- Les algorithmes supportés
  - Confidentialité: Algo symétrique (3DES, AES, IDEA, …)
  - Intégrité: HMAC: Hash Message Authentication Code
  - Authentification: X.509 et MAC

Généralités

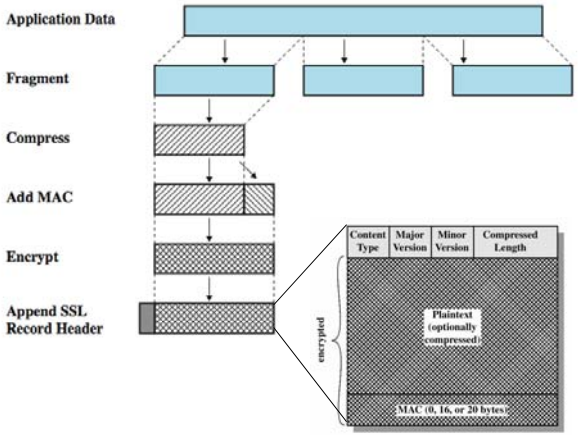
- TLS est composé de deux parties
  - Le protocole TLS Record
    - Sécurise la connexion en utilisant les méthodes de chiffrement symétriques supportées
    - Vérifie l'intégrité des données à l'aide de HMAC
  - Le protocole TLS Handshake
    - Authentifie le client et le server lors de l'initiation de la connexion
    - Négocie entre le client et le serveur l'algorithme de chiffrement et les clés de session à utiliser
    - Remonter des alertes

Généralités

- La connexion SSL
  - Une connexion de niveau transport proposant un service
  - Fonctionne en point à point de manière transitoire
  - Associée à une session
- La session SSL
  - C'est une association crée entre un serveur et un client par le Handshake
  - Définit les paramètres de sécurité à utiliser et pouvant être partagés par plusieurs connexions
  - La session évite de renégocier les paramètres à chaque connexion (ex HTTP)
  - En théorie on peut avoir plusieurs session en parallèle mais ce mode n'est pas implémenté en pratique

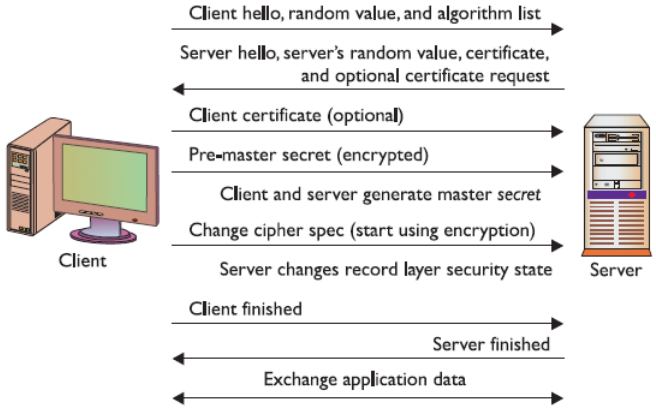
Le protocole TLS Record

- Assure la confidentialité et l'intégrité
- Manipule des fragments d'au plus 2^{14} octets
- Une compression peut également être appliquée si nécessaire



Le protocole TLS Handshake

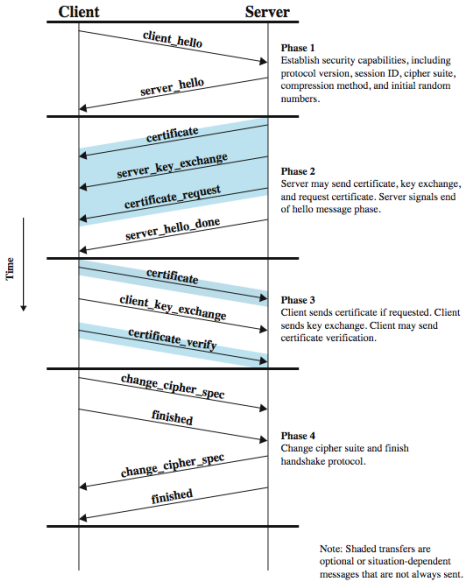
- Version simplifiée d'un Handshake TLS



Le protocole TLS Handshake

- Ce protocole est le plus complexe de TLS et permet aux deux parties de s'authentifier
- Le protocole se découpe en fait en 4 phases
  - L'Initiation de connexion
  - L'échange de certificat et de clés
  - La vérification du certificat par le client et le paramétrage de la connexion
  - La mise en place finale de la connexion sécurisée
- Ce protocole a été pensé pour résister
  - Aux attaques par abaissement de version (rollback)
  - Aux attaques par rejeu

Le protocole TLS Handshake



Quelques applications sur SSL/TLS

- SSL/TLS est très largement utilisé à l'heure actuelle et quasiment tous les principaux protocoles ont leur équivalent sécurisé
  - HTTPS (port 443 au lieu de 80)
  - SSMTP (port 465)
  - SPOP3 (port 995)
  - IMAPS
  - Telnets même si on lui préfèrera SSH
  - …

Bilan sur SSL/TLS

- Avantages
  - Protocole assez bien pensé et complet pour les échanges réseaux sécurisés
  - Supporté par quasiment tous les navigateurs modernes
  - Transparent par rapport au protocole de transport
    - Largement utilisé
  - On le retrouve dans d'autres architectures comme WAP (WTLS)

- Inconvénients
  - Les mêmes que pour les solutions basées sur des PKIs à grande échelle
    - On n'est pas averti si le certificat est répudié par exemple
  - La renégociation de session n'est pas prévue (pratique pour HTTP mais pénalisant pour FTP ou telnet par exemple)
  - La négociation sur les algorithmes de chiffrement et de signature utilisés peuvent amener à utiliser des solutions faibles