Cours Authentification et Signature Numérique
Master I RSS

Mr.Ahmed KHALIFA
khalifaahmedou@yahoo.fr

Chapitre II: Gestion des Certificats

Sommaire

problématique de la distribution des clés

En cryptographie Symétrique

- Les objectifs sont :
  - Maitriser la distribution des clés (ne faire parvenir les clés qu'à leur destinataires, identifiés le mieux possible)
  - Préserver la confidentialité des clés. (Chiffrement, secret fractionné)

En cryptographie Asymétrique

- Hypothèse d'un schéma préalable (le plus répandu): la sédentarité des clés privées.
  - Les clés privées vivent et meurent là ou elles sont nées. Pas de réplication, d'externalisation ni de clonage.
  - On ne sort de ce schéma que dans le cas d'une compromission de la clé.
- Les objectifs sont :
  - Assurer une diffusion aussi large et facile que possible de la clé publique.
  - Préserver l'intégrité du lien Clé publique Propriétaire de la clé publique.

problématique de la distribution des clés

problématique de la distribution des clés

Comparaison des attaques sur les clés selon leur nature

Nature de la clé	Attaque	Atteinte	Remède
Clé privée ou secrète	Intégrité	Disponibilité	Contrôle d'accès Sauvegarde
Clé privée ou secrète	Compromission (lecture du clair)	Confidentialité Authenticité (Usages de la clé)	Chiffrement Contrôle d'accès
Clé publique	Intégrité	Disponibilité	Contrôle d'accès Sauvegarde
Clé publique	Substitution	Disponibilité	Signature ** Chiffrement Contrôle d'accès

problématique de la distribution des clés

problématique de la distribution des clés

- Pourquoi une signature
  - Utilisation de la propriété de la vérification de signature qui est aussi une vérification d'intégrité
- Signature de quoi ?
  - De la clé, de l'identifiant de sont propriétaire, établissant par là un lien entre les deux
- Signature par qui ?
  - Par un signataire qui, **en produisant une signature**, certifie que la clé appartient à son propriétaire désigné qui peut-être ce signataire ?
  - L'objet signé est un **certificat**

problématique de la distribution des clés

problématique de la distribution des clés

L'émetteur du certificat est une tierce partie de confiance

- Modèle hiérarchique
  - Sa clé publique est notoire et placée dans un certificat racine auto signé.
  - Sa clé publique est certifiée. (hiérarchie de certificats)
- Modèle réseau de confiance
  - Une clé est certifiée par plusieurs émetteurs à qui un utilisateur accorde sa confiance selon plusieurs degrés. (Modèle utilisé par PGP)
  - Une personne en certifie la clé d'une autre personne :
  - Pour une clé de chiffrement cela signifie seulement que la clé signée appartient à son détenteur.
  - Pour une clé de signature cela signifie qu'un certain degré de confiance est accordé au détenteur. Il pourra, en particulier, signer des certificats à son tour.

Fonction des certificats

Fonction des certificats

- Support de distribution des clés publiques
  - Moyen hors ligne,.remplace la consultation sécurisée d'annuaire.
  - Plutôt que de stocker, ou consulter un annuaire pour un multitude de clés, on ne stocke plus que des clés de sommets de hiérarchie de certification de ces clés.

  Il y a une économie de moyens analogue à celle obtenue par la dérivation des clés symétrique.
- Apport de confiance dans l'authenticité de la clé publique
  - Transfert de confiance sur le signataire du certificat.(Transitivité de la confiance).
  - Quelle confiance ? Est-elle de même nature pour une clé de chiffrement ou de signature. L'usager du certificat, comme son signataire peut faire la différence selon l'usage de la clé.
    - Avoir confiance que le détenteur du certificat est bien en possession de la clé portée dans le certificat,. c'est suffisant pour chiffrer vers lui.
    - La confiance est d'une nature différente pour les signatures car elle est "plus facilement" liée au contenu sémantique de la signature. (nuance traitée en réseau de confiance).

Rôle de la normalisation

Rôle de la normalisation

La normalisation joue un rôle fort dans

- La formulation et l'agencement des concepts AC, AE
- Le format des certificats X509
- Le formats des demandes et des livraisons de certificats et des CRL. PKCS 10 PKCS 7

Cette normalisation est indispensable pour assurer l'interopérabilité des mécanismes des PKI. A la base de toutes les définitions de format et toutes les codifications : ASN.1

Autorité de certification, Autorité d'enregistrement

Autorité de certification, Autorité d'enregistrement

Ces entités sont définies en particulier dans le cadre des travaux de l'IETF (Internet Le groupe de travail PKIX a notamment publié un draft qui définit le rôle et les fonctionnalités de ces entités.

- Internet X.509 Public Key Infrastructure
- Certificate Management Protocols
- **Autorité d'enregistrement (RA Registration Authority)**
  - Vérifier et garantir le Lien entre une personne,une fonction, une machine et une clé.

  Les demandes de certificat sont adressées à une autorité d'enregistrement.
- **Autorité de certification**
  - Garantir l'intégrité de la clé privée de l'autorité de certification (Une autorité de certification est un bunker).
  - Publier la CRL
  - Garantir l'unicité des DN émis et des clés ?

Autorité de certification, Autorité d'enregistrement

problématique de la distribution des clés

- Relation entre AC et AE
  - Relation de confiance
  - Communication sécurisée entre les deux entités.
- Analogie
  - Un officier ministériel, assimilé à une autorité d'enregistrement, vérifie l'authenticité d'un document,
  - et demande à un employé, qui n'obéit qu'à lui, et en qui il a confiance d'apposer un cachet (tampon)sur le document

La responsabilité principale de cet employé est de préserver le "tampon" et de garantir son usage

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Public Key Infrastructure PKI Ensemble de concepts, d'entités, de relations contractuelles, de moyens informatiques,

- **Concepts**
  - Définis principalement par l'IETF Internet Engineering Task Force
  - Modèle hiérarchique AC , AE
  - Gestion des listes e révocation CRL par les AC
- **Relations contractuelles**
  - PC Politique de certification
- **Moyens informatiques**
  - AC et AE sont matérialisées par des serveurs, boîtiers cryptographiques etc

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Le rôle de l'état fait l'objet de débats.Malgré le mot public les PKI sont encore en majorité privées. Déjà présents sur le marché sont des AC :

- **Verisign, Thawte, Certplus, Certinomis.**

Il existe aussi des produits standards pour faire des CA :

- **Entrust, Baltimore, Netscape, IBM, Microsoft etc**

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Contenu d'un certificat

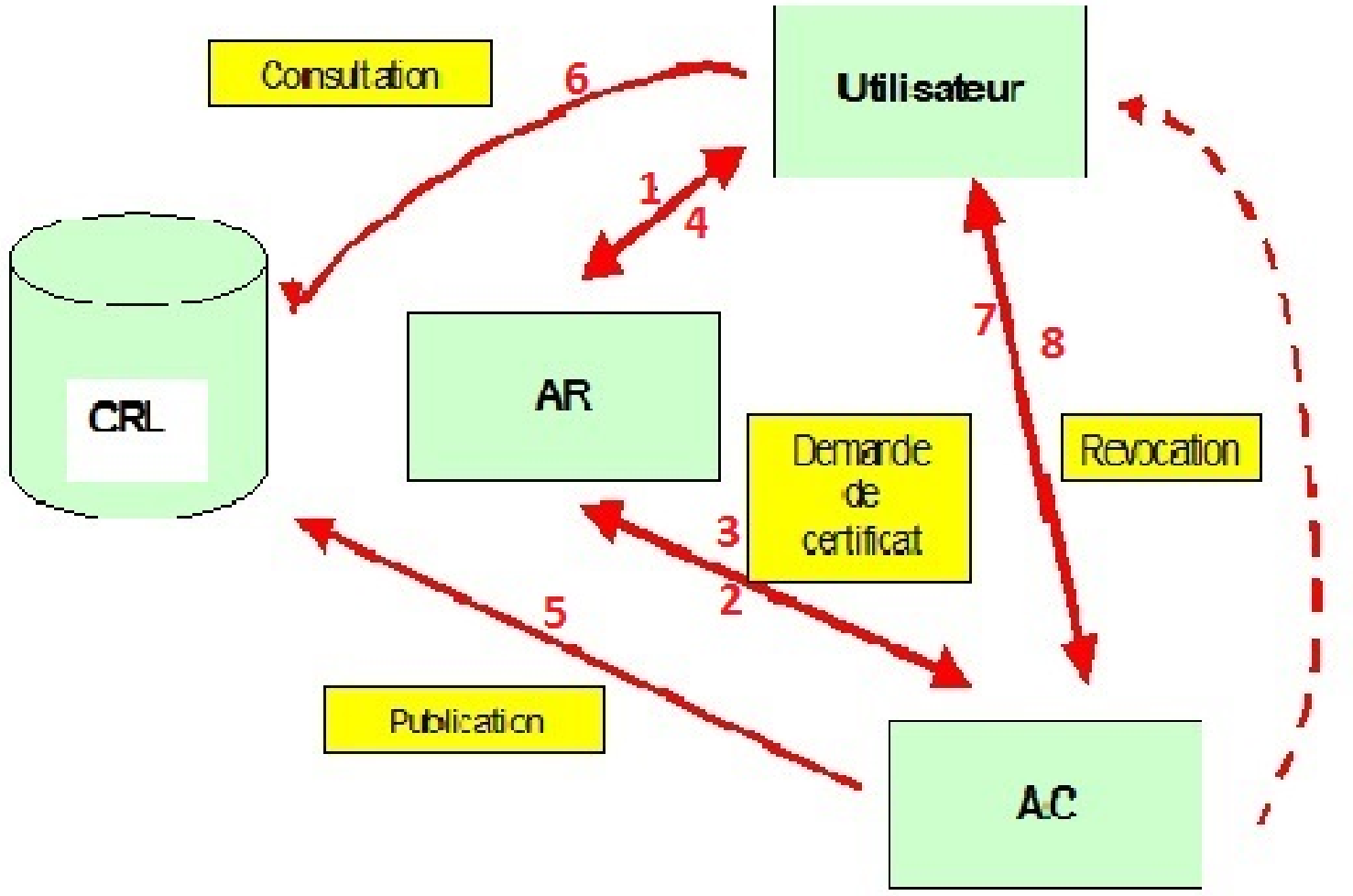
- C'est un document comprenant
  - Un identifiant de certificat
  - **Un identifiant du détenteur du certificat**
  - Un identifiant de l'émetteur du certificat
  - Une date de création
  - Une plage de validité
  - **Une clé publique**
  - D'autres informations
- Ce document est signé par une **autorité de certification** Ce qui est certifié c'est essentiellement le lien **identifiant de détenteur- clé publique**

Les certificats dont on parle, sont tellement associés à une clé publique, que malheureusement, on entend dire et on lit le mot "certificat" pour désigner en fait un biclé ou une clé privée.

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Schéma simplifié d'une PKI



Public Key Infrastructure PKI

types de certificats selon le niveau de signature :

On distingue différents types de certificats selon le niveau de signature :

- Les certificats **auto-signés** sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés
- Les certificats **signés par un organisme de certification** sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir

Public Key Infrastructure PKI

Types d'usages des certificats

Les certificats servent principalement dans trois types de contextes

- Le certificat **client**, stocké sur le poste de travail de l'utilisateur ou embarqué dans un conteneur tel qu'une carte à puce, permet d'identifier un utilisateur et de lui associer des droits. Dans la plupart des scénarios il est transmis au serveur lors d'une connexion, qui affecte des droits en fonction de l'accréditation de l'utilisateur. Il s'agit d'une véritable carte d'identité numérique utilisant une paire de clé asymétrique d'une longueur de 512 à 1024 bits.
- Le certificat **serveur** installé sur un serveur web permet d'assurer le lien entre le service et le propriétaire du service. Dans le cas d'un site web, il permet de garantir que l'URL et en particulier le domaine de la page web appartiennent bien à telle ou telle entreprise. Par ailleurs il permet de sécuriser les transactions avec les utilisateurs grâce au protocole **SSL**.

Public Key Infrastructure PKI

Types d'usages des certificats

- Le certificat**VPN** est un type de certificat installé dans les équipement réseaux, permettant de chiffrer les flux de communication de bout en bout entre deux points (par exemple deux sites d'une entreprise). Dans ce type de scénario, les utilisateurs possèdent un certificat client, les serveurs mettent en œuvre un certificat serveur et les équipements de communication utilisent un certificat particulier (généralement un certificat **IPSec**.

Public Key Infrastructure PKI

Public Key Infrastructure PKI

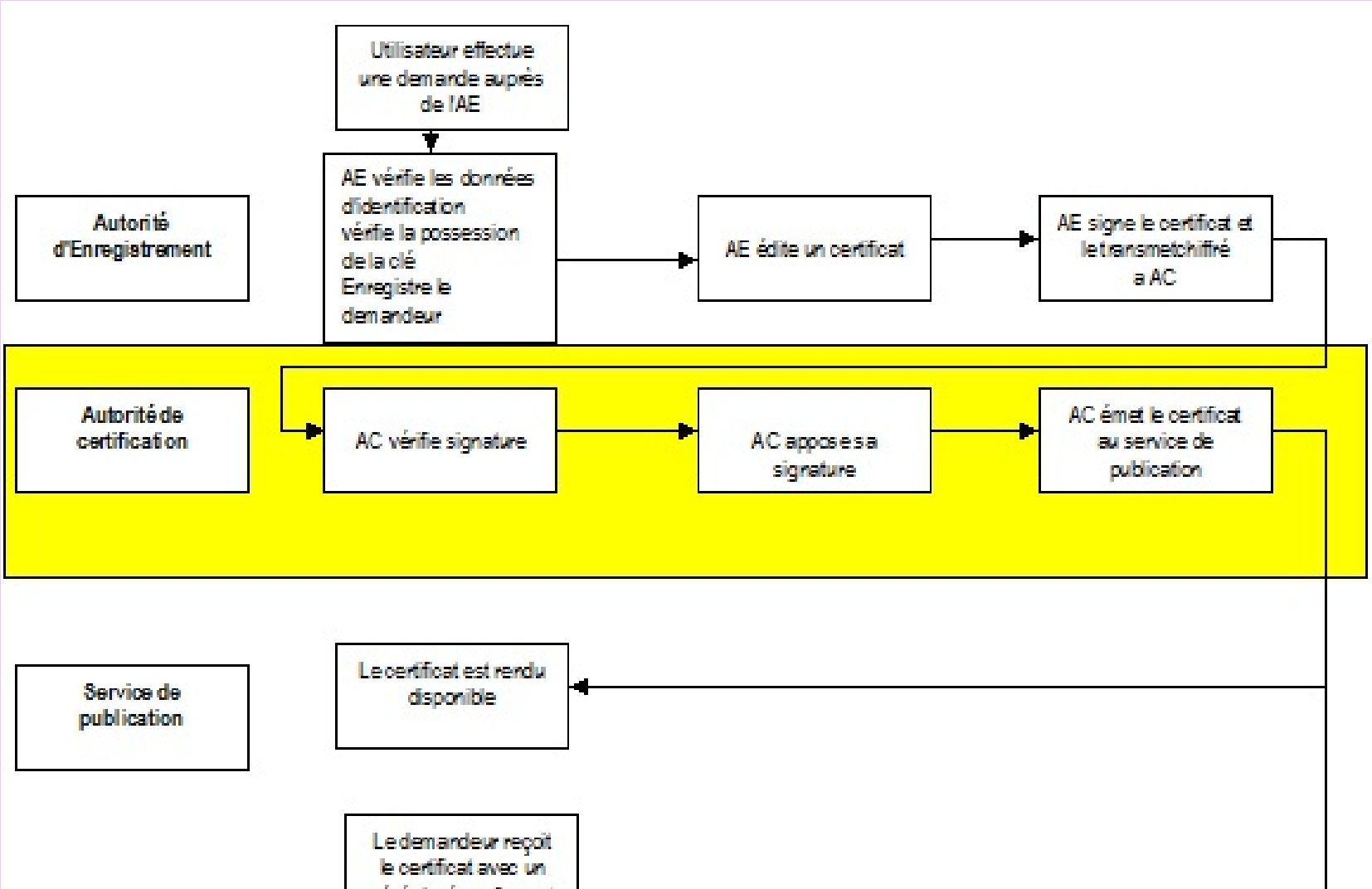
Exemple de schéma de demande de certificat de clé publique.

- Alice génère une clé privée
- Alice envoie une demande de certificat à l'AE ID et clé publique signé par sa clé privée pour
  - assurer l'intégrité de la demande qui contient la clé privée.
  - mais aussi prouver qu'elle est en possession de cette clé.
- AE vérifie l'identité d'Alice ainsi que l'exactitude des renseignements fournis dans le certificat
- AE transmet la demande à AC.
- CA vérifie signature (importance du protocole) édite et signe le certificat
- Alice vérifie le certificat reçu (signature et conformité) avant de le publier ou de donner son accord à la publication

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Schéma général d'obtention d'un certificat



Public Key Infrastructure PKI

Public Key Infrastructure PKI

Sécurité des clés

- Confidentialité de la clé privée
  - Bonne solution : dispositif cryptographique (boîtiers, cartes à microcircuits).
  - Contrôle d'accès, chiffrement.
  - Protection physique des postes de travail.
  - Technique de l'Arche Perdue
- Intégrité des clés publiques des certificats racine
  - Mêmes solutions que pour les clés privées.

Dans la pratique le niveau de protection des clés publiques est beaucoup plus faible que celui des clés privées.

Public Key Infrastructure PKI

Sécurité des clés

Scénario d'obtention d'une clé certifiée

La confusion est fréquente entre :

- Posséder une clé privée
- Avoir fait certifié sa clé publique.

La confusion vient du fait que les deux opérations sont enchaînées. L'opération se fait alors à partir d'un butineur en relation avec un serveur d'autorité de certification.

Public Key Infrastructure PKI

Classe de certificat

Classe de certificat

- De la classe du certificat dépend
  - la procédure de l'autorité d'enregistrement.
  - la longueur de la clé privée de l'autorité de certification.
  - la qualité de la protection de la clé privée de l'autorité de certification.
  - Le montant des compensations en cas de compromission de la clé de la CA.
- Le prix du certificat dépend, lui aussi, de la classe du certificat

Public Key Infrastructure PKI

Problèmes et éléments de réflexion

Problèmes et éléments de réflexion

- Acceptation de la demande
  - Motif du refus
  - Refus non communiqué.
  - Détection de clé déjà certifiée.
  - Pré-opposition. (par qui ?).
- Acceptation du certificat
  - Acceptation ou refus du titulaire demandeur
  - Preuve d'acceptation, preuve de refus.

Public Key Infrastructure PKI

Problèmes et éléments de réflexion

Problèmes et éléments de réflexion

- Renouvellement de la clé du titulaire
  - Exploitation du biclé certifié pour certifier le nouveau.
  - Trace de cette filiation dans le certificat ?
- Publication
  - Obligation pour l'AC de publier. Où ? Dans quel délai ? (preuve de réussite, d'échec, tentative, retry)
- Doublons
  - Détection de clé déjà vue. Engagement (durée). à titre indicatif.
  - Avertissement à porteur A (contenu) à demandeur B (contenu) ou refus.
- Preuve de possession POP
  - POP en ligne, signature de la demande, livraison chiffrée (publication par le titulaire après acceptation).

Public Key Infrastructure PKI

Problèmes et éléments de réflexion

Problèmes et éléments de réflexion

- Clé privée CA
  - Perte
    - Protection contre vol
    - Protection contre perte.
    - Perte sûre.(preuve de non vol)
  - Sauvegarde,
    - Par fractionnement.
    - Génération, importation exportation.
  - Durée de vie
    - Droit ou conditions de cessation d'activité (délai , préavis , autorisation préalable, par qui ?).
    - Relation avec les durées de vies des certificats produits.
    - Fin d'activité programmée avec destruction des clés, sans révocation du parc

Public Key Infrastructure PKI

Problèmes et éléments de réflexion

Problèmes et éléments de réflexion

- Révocation
  - Responsabilité de déclaration Responsabilité de la CA, en cas de compromission de sa clé responsabilité du titulaire, , en cas de compromission de sa clé
  - Initiative
  - Authentification de la demande.
  - Délais
  - Durée.
  - Preuve de révocation (pour le demandeur)
  - Preuve de consultation (pour l'utilisateur)
  - Extension X509 de désignation du réseau de révocation.
  - Journalisation archivage de la procédure de révocation qui, quand, pourquoi, pièces jointes identique à délivrance de certificat.

Public Key Infrastructure PKI

Problèmes et éléments de réflexion

Problèmes et éléments de réflexion

- Annulation de révocation ou fin suspension ?
  - Par demandeur ?
  - Autre ?
  - Avertissement
  - Preuve d'annulation.
- Journalisation /Archivage des traitements de l'AC
  - De tous les évènements ?
  - Droit d'accès aux journaux ?

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Structure des certificats X509 V3

Les certificats X509 sont supportés par les standards importants :

- SSL, S/MIME et d'autres
- v3 autorise une plus grande souplesse dans l'attribution des noms.
- X509 fait partie d'un ensemble de normes X50x dédiées ?aux annuaires.
- contenu
  1) numéro de version (version),
  2) numéro de série (serialNumber),
  3) algorithme de signature utilisé pour produire de certificat (algorithm),
  4) nom de l'autorité de certification (issuer),
  5) date de début de validité du certificat (notBefore / UTCTime),

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Structure des certificats X509 V3

contenu

6) date de fin de validité du certificat (notAfter / UTCTime),
7) nom du porteur du certificat (subject),
8) algorithme utilisant la clé publique contenue dans le certificat (algorithm),
9) valeur binaire de la clé publique (subjectPublicKey),
10) extensions V3,
11) algorithme de signature utilisé pour produire de certificat (algorithm),

Public Key Infrastructure PKI

Public Key Infrastructure PKI

Structure des certificats X509 V3

contenu

- Extensions :
  12) AuthorityKeyIdentifier : uniquement le champ KeyIdentifier. Extension de type non critique,
  13) SubjectKeyIdentifier : uniquement le champ KeyIdentifier. Extension de type non critique,
  14) SubjectAltName : uniquement le champ GeneralName. Extension de type non critique,
  15) BasicConstraints :Extension de type critique,
  16) KeyUsage:Extension de type critique,
  17) CRLDistributionPoints : uniquement les champs directoryname et uniformRessourceIdentifier. Extension de type non critique,