# CM1 PKI d’entreprise

* PKI : public key infrastructure = IGC: Infrastructure gestion de clefs en FR
* Sécurité: mesures permettant d’assurer la protection des biens, données, valeurs.
* Menace: action, événement ou entité pouvant compromettre la sécurité de ce qui est protégé.
* Confiance: sentiment de sécurité ou de sûreté qu’a une personne vis-à-vis de quelqu’un ou de quelque chose.
* Garantie: assurance ou gage de quelque chose.
* base de la confiance électronique:
  + sécurité est un vecteur de confiance
  + si sécu dans un élément d’une infra est compromise, toute la confiance envers l’infrastructure l’est.
  + si la sécu est un vecteur de confiance la réciproque n’est pas vraie, la confiance nécessite des garantie
* OBJ d’une PKI est d’établir de solides garanties électroniques afin d’établir la confiance. Permet d'instaurer un domaine de confiance entre les utilisateurs/systèmes.
  + Authentification: carte nationale d’identité
  + Confidentialité et intégrité de l’information: coffre fort
  + Non répudiation: scellés ou signatures
* Cryptologie
  + Confidentialité
  + Intégrité
  + Authentification
  + Non répudiation

# CM2 PKI d’entreprise

* Certificat X509 : Certificat le plus utilisé

# TD 1

## Exercice 1 : Questions sur les certificats

1. **Qu’est ce qu’un certificat et quelles sont les informations qu’il contient ?**C’est un fichier, elle représente la “carte d’identité” numérique.

Date de validité, organisation, pour une certaine personne, le certificat possède la clé publique (*jamais* la clé privée).

1. **Discuter des trois scénarios suivants en termes de sécurité.**
   1. **Deux certificats différents sont signés par la même clé privée.**Cas classique, tout certificats sont signé par la même clé privé de l’autorité de certification.
   2. **Deux certificats différents contiennent la même clé publique.**Non ce n’ai pas logique qu’ils contiennent la même clé publique.
   3. **Deux certificats différents ont la même signature**

Signature c’est un hash qui est chiffré avec une clé asymétrique. Deux signatures identiques signifient que le hash doit être identiques pour un contenu différent, cela se nomme, collision (donc soit la fonction de hash est “pourri” ou on trouve une collision (ultra mega pas probable)).

## Exercice 2: Questions sur S/MIME et PGP

PGP et S/MIME sont deux normes qui permettent de sécurité le courrier électronique échangé entre deux utilisateurs. Elles reposent sur des certificats différents.

1. Les certificats X509 sont utilisés par la norme S/MIME. PGP n’a pas d’autorité.
2. La différence fondamentale dans la manière de gérer les confiance avec les certificats PGP communément appelés clés PGP et les certificats X509.  
   Réseaux de confiance qui fait confiance à quelqu’un d’autre. (l’ami de mon ami)
3. **Lorsque l’on chiffre un message, même sans le signer, on a besoin d’un certificat dont on est sûr de la validité. Pourquoi ?**Si pas valide problème, car pas de garantie que la clé utilisé soit compromise.

Nous avons pas de garantie sur le clé utilisé pour chiffrer le message n’a pas était compromis

## Exercice 3 : Obtention d’un certificat

Dans le cadre d’un projet, vous avez besoin d’un certificat de confiance. Par exemple, pour assurer la confidentialité des échanges effectués sur votre site web.

1. **Quelles solutions peut-on décider de mettre en oeuvre pour obtenir un certificat ?**

Auto-signé le certificat ou créer un certificats. Demande à une autorité (un intermédiaire) pour obtenir un certificat.

Si on possède le domaine toto.com pour montrer qu’on le possède bien, on peut écrire un fichier et l’envoyer sur le site, car ça montre qu’on peut modifier le contenue de ce site.

1. **Quelles sont les différentes possibilités d'émettre une requête de certificat ?** <https://www.google.fr>

## Exercice 4 : Problème Diginotar

Le 10 juillet 2011, un certificat TLS pour les noms de domaine “google.com” de Google, a été délivré par DigiNotar (autorité de confiance dans tous les navigateurs). Or ces sites pour lesquels le certificat a été émis n’appartiennent pas à Google.

1. **Dans quel but ce certificat a été émis/utilisé par le “faussaire”?**phishing, men in the middle, tout pour ce faire passé de manière fiable par google.
2. **Quelle entité de la pKI a fait une erreur** ?  
   AE, autorité d'enregistrement elle a mis un certificat alors qu'elle avait pas toute les information.
3. **Quelles sont les conséquences pour DIginotar ?**

elle n’existe plus, ton business est la confiance , si tu la perds ton business meurt.

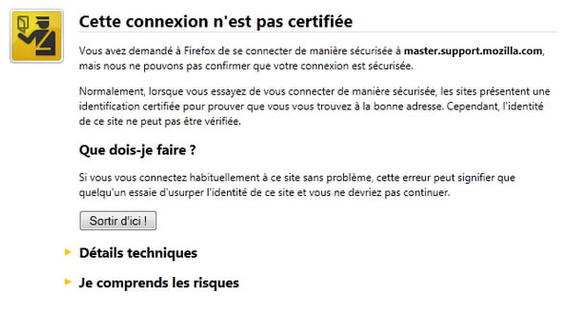
## Exercice 5 : Questions sur l'authentification

1. **Qu’est ce que l’authentification forte et qu’est ce qui la distingue de l’authentification faible ?**Authentification au moins double, multiple facteur.
2. **Quels sont les différents facteurs qui peuvent entre las l’authentification forte ?**qu'on possède (telephone) , quon sait (mdp, code pin), ou je suis (localisation), ce que je sais faire (un truc unique, genre la roue sur un doigt), qu’on est (biométrie).
3. **Les certificats X509 peuvent-ils être utilisés pour s’authentifier de manière forte ?**

Une paire de clef c’est quelque chose qu’on a. Tout seul non car qu’un facteur, peut facilement le devenir un avec support physique.

## Exercice 6 : Questions sur TLS

Lors d’une connexion TLS sur un site Web, le navigateur affiche une alerte comme ci-dessous. Qu’est ce qui peut en être la cause ?



Certificat expiré, l’autorité de certification n’est pas reconnu. Quand le certificat est révoqué (mais on le voit plus car ce n’est plus le truc par défaut lorsque c’est révoqué).

## Exercice 7 : Questions sur TLS

1. **Lors d’une connexion TLS mutuelle, quelles clé cryptographiques sont mises en oeuvre ?**

Il y a un échange de clé, différent types de clé. Puisque que c'est mutuelle deux paire de clé symétrique avec leur certificat associé.

1. **A quelles fins sont utilisées les clés asymétriques du serveur et du client TLS ?**On prends une symétrique pour partager un secret , la clé symétrique . La clé symétrique c’est rapide. La clé symétrique sont généré par la clé asymétrique.
2. **Quelles sont les différences entre SSH, TLS, SSL et IPSec ?**SSh ->  
   TLS -> Couche 5 Session  
   SSL -> Obsolète, idem que TLS, succession du protocole TLS  
   IPSec -> Tunel, couche 4 transport, sert à faire du transport au niveau IP.

## Exercice 8 : Projet PKI

Une société multinationale (composée de plusieurs filiales issues de fusions/rachats à travers le monde) désire de mettre en place une PKI groupe afin de fournir divers services de sécurité au sein de son SI:

-Messagerie sécurisé (chiffrement et signature)

-Authentification TLS

-Authentification session PC

-VPN

-NAC 802.1x (PC et smartphones)

-Sécurisation du WiFi

-Sécurisation des serveurs (TLS)

-Chiffrement des disque durs

-Signature de documents

Cette société désire que la définition de la PKI soit pérenne (au moins 30 ans) et puisse facilement s’adapter aux achats/ revente de filiales.  
  
De plus le parc des serveurs (serveurs, routeurs, etc) est hétérogène avec du matériel récent et du matériel très ancien.

Définir la hiérarchie d’AC ([autorité de certification](https://fr.wikipedia.org/wiki/Autorit%C3%A9_de_certification)) (avec les profils de certificats associés) correspondant à cette demande et répondant aux exigences mentionnées.



# TD 2 - Formation PKI d’entreprise

## Exercice 1 : Questions sur la signature

1. **Qu’est qu’une signature numérique et quelles sont les étapes d’une signature numérique ?**

Il s’agit d’un hash et d’un chiffrement avec la clé privée qui sera déchiffré avec la clé publique.

1. **Par quel moyen peut être assurée la non-répudiation ?**  
   non répudiation : on ne peut pas dire que c’est pas nous qui avons signé le document.  
   Avec un certificat et assurer la sûreté de la clé.
2. **La signature numérique à valeur probante (légale) nécessite, en France, la présence d’une autorité d’horodatage et d’une autorité de dépôt. Dans quels buts ?**  
     
   C’est une garantie supplémentaire qui va garder une trace formelle des signatures effectuées lors de la signature d’un contrat bancaire par exemple. L’autorité d’horodatage est quant à elle présente pour garantir que le contrat a bien été signé au temps X et permet aussi lors de la vérification du contrat que celui a bien été signé au temps donné. De plus, un mécanisme de CSP est ajouté pour déterminer que le certificat n’était pas révoqué lors de la signature de ce contrat.

## Exercice 2 : Questions sur les PKI

1. **A quel problème répond une PKI?**  
   C’est un tiers de confiance qui transmet les clés, les identités aux acteurs.

Attribution fiable a une identité pour une paire de clé.

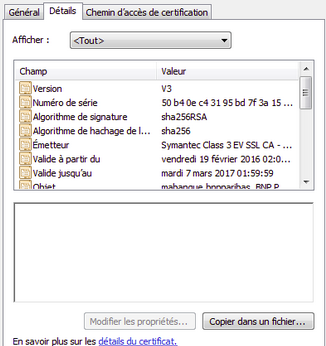
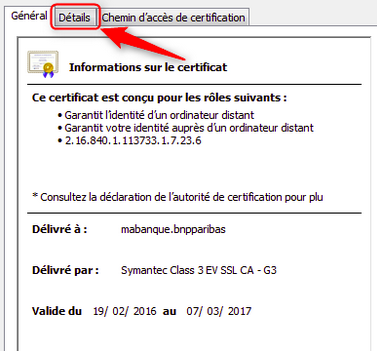
1. **Quelles sont les PKO (Public Key Operation) qui peuvent nécessiter la mise en oeuvre d’une PKI (infrastructure de confiance) ?**  
   Délivrer des certificats à des personnes.
2. **Quelles sont les préconisations à respecter pour qu’un projet de mise en oeuvre de PKI soit un succès ?**

Prévoir pour une longue durée (30 ans ?), être un organisme de confiance,

1. **Quelles sont les limites d’une PKI ?**

Les PKI sont des Infrastructures plutôt lourde et sont figées dans le temps.

## Exercice 3 : Le certificat



Dans un certificat, on y trouve une date de validité, les algorithmes de signature, de hachage, la taille de la clé, l’objet du certificat. Très important, on y voit l’autorité qui a délivré le certificat. On y voit aussi les informations relatives sur ce à quoi le certificat peut servir.

## Exercice 4 : Architecture PKI



Sujet de l’exercice

Séparer les différentes entités par des VLANs notamment les zones à risques.

Un switch semble peu, il faudrait peut-être y ajouter un pare-feu entre les accès des utilisateurs et les VLANs des zones à risques.

Mettre en place des IDS.

Doublé les matériaux pour prévenir des pannes (HA).

**CRL→ vérification des certificats, toujours up dans un infra PKI.**

