ATR - Fiche Révision





[**I - CM 1 : Enjeux futurs de sécurité**](#_i5youstzcicg) **3**

[A.Big Data](#_j5kfan4l85e) 3

[B.Cloud](#_wd1k8jod45r3) 4

[C.SDN](#_z87cevekxz42) 5

[D.IoT](#_xcvlaz2nt5yt) 6

[E.DevOps → méthode agiles #fanny](#_z0tyw0f3z8fw) 7

[**II - CM 2 : La sécurité et vous**](#_5np4buhnm0bv) **9**

[A.Attaquants](#_lopqxcoib07g) 9

[B.Traces](#_jr7y3hnr5isq) 11

[C.Espionnage](#_vvhttr1czmbc) 11

[D.Éthique](#_fivtks2npmkq) 11

[E.Habilitation](#_xb7d6bcbxg78) 12

[**III - CM 3 : La sécurité périmétrique vs BeyondCorp**](#_cczn6kvsub98) **14**

[**A.Histoire de la sécurité informatique**](#_n1yb4e8vztfd) **14**

[B.Sécurité périmétrique](#_2y45xomazife) 14

[C.BeyondCorp](#_o4cg6fikmgdz) 14

[**IV - CM 4 : La sécurité au coeur des métiers**](#_4o6wyq1brzl4) **15**

[A.L’entreprise](#_k03t6ts1comu) 15

[B.Vulnérabilité humaine](#_n9z402w1ek50) 15

[C.Sécurité des réseaux](#_nf74lypmu9l5) 15

[D.Sécurité des développements](#_6w17tqte5q5h) 15

[E.Sécurité de la communication](#_hq71wisg506) 15

[F.Sécurité de la confiance](#_h4df5qojr38x) 15

[**V - CM 5 & 6 : Cloud & Architectures**](#_199ds3mlzf8n) **15**

[A.Partie 1 : Virtualisation](#_kk11ogu5ylg0) 15

[B.Partie 2 : Cloud](#_muucyeudfdjs) 15

[**VI - CM 7 : Formation PKI d’entreprise**](#_tnzisjaeka25) **15**

[A.Introduction](#_1n9unfr7oepm) 16

[B.Rappels de cryptologie](#_gtprux579zzb) 16

[C.Certificats numériques](#_vfnschv3ah94) 16

[D.PKI / IGC](#_764e6me2u155) 16

[E.Bonnes pratiques IGC](#_tu8oziv9ep4c) 16

# I - CM 1 : Enjeux futurs de sécurité

84 % des incidents sont liés au facteur Humain

## A.Big Data

il y à octet crée par jour.

**Définition :** Le **Big Data** est un concept permettant de stocker et analyser un volume énorme de données.

**MapReduce** :

* Est un **design pattern** dans lequel sont effectués des calculs parallèles, et souvent distribués, de données potentiellement très volumineuses, typiquement supérieures en taille à 1 téraoctet.
* Permet de manipuler de grandes quantités de données en les distribuant dans un cluster de machines pour être traitées.
* **Hadoop** est un **framework** permettant d’implémenter le MapReduce.

Il y à trois nouveaux risques qui apparaissent avec le Big Data :

* a l'acquisition de données
* a la reglementation
* a la vie de la donnée

Nouvelle techno qui présentent des vulnérabilités car souvent mal comprises.

La sécurité informatique repose aujourd’hui sur deux étapes principales :

* l’entreprise se protège contre les menaces connues
* elle s’efforce d’identifier et de se protéger en temps réel contre des menaces inconnues, notamment via les technologies de “bac à sable” (sandboxing).

Big Data:

* Permet de mesurer l’impact que la menace détectée a eu ou aurait eu sur l’infra.
* Capacité d’analyser des volumes massifs et épars de données.
* Peut venir en complément des solutions de gestion des logs et du SIEM ( Security Incident Monitoring).

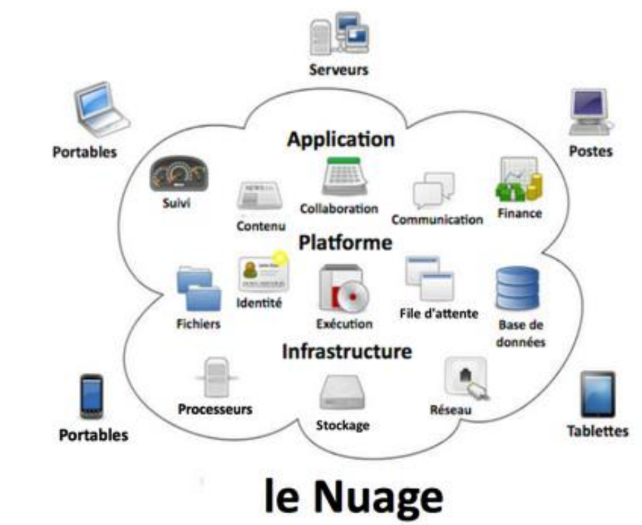
## B.Cloud

Cloud computing:

→ puissance de calcule et de stockage des serveurs via internet

→ délocalisation des infrastructure via un réseau de télécom à la demande et en libre-service, à des ressources informatiques partagées configurables.

→ consommateur se sert de puissance mise à sa disposition par un fournisseur via internet.



* **IAAS**(infrastructure as a service) → fournisseur de service ne met à disposition que le matériel virtuel. OS et applis sont installés par les clients.
* **PAAS**(platform as a service) amazon(web) → fournisseur de service met à dispo le matériel et OS virtuels. Client peut installer ses applis.
* **SAAS**(software as a service) → tout est mis à disposition clé en main, le client se connecte juste (gmail,yahoo,outlook)

**Risques du Cloud:**

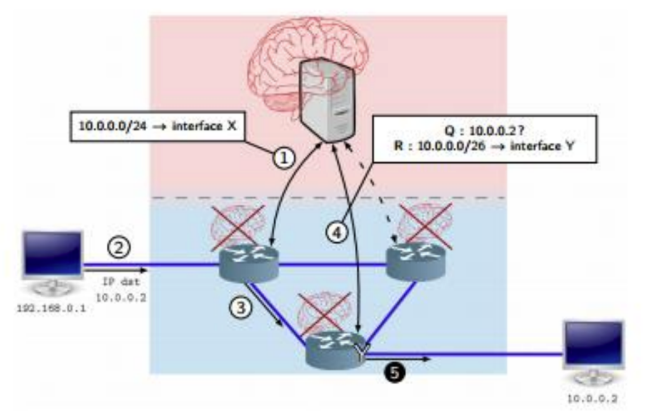
* **L’existence de brèches de sécurité** sur les couches logiques du Datacenter que celles issues d’erreurs humaines.
* **La fragilité dans la gestion des accès et des identités**, bien que certains fournisseurs renforcent les interfaces d’authentification avec d’autres moyens tels que les certificats, les smartcards, la technologie OTP et bien d’autres.
* **L’utilisation d’API non sécurisées** pour l’intégration des applications avec les services cloud.
* **L’exploit de vulnérabilités** des systèmes d’exploitation sur les serveurs du cloud et même sur les applications hébergées.
* Le piratage de compte
* Une action malveillante initiée en interne dans les effectifs du fournisseur
* Les menaces persistantes avancées
* La perte de données
* Les insuffisances dans les stratégies internes
* Utilisation frauduleuse des technologies cloud
* Le déni de service
* Les failles liées à l’hétérogénéité des technologies

**Sécurité du Cloud, les enjeux:**

* Appliquer rigoureusement une composante IAM (Identity and access management)
* Le chiffrement des données au repos
* La mise en place d’un nouveau plan de contrôle
* Sauvegarder toutes les données
* Assumer la responsabilité des instances et des applications
* Faire réaliser des audits de conformité
* Segmenter et contenir le trafic

## C.SDN

**SDN ( Software Define Network)** : Séparation du plan de contrôle du plan de données. Utilise que des commutateurs/switch SDN.



Partie rouge : Plan de contrôle, décide par ou passe les paquets.

Partie bleu: Plan de données, où circule les données de façon non intelligentes, c’est le plan de contrôle qui indique le chemin qu’elles prennent.

**Rôle SDN** : But pratique de rendre **programmables** les réseaux par le bien d’un contrôleur SDN (cerveau) centralisé.

* Avantages :
  + Centralisation du contrôle du réseau
  + Séparation du plan de contrôle et du plan de données
  + Permet le déploiement sur des plateformes de plus grande capacité que les classiques commutateurs réseau.
  + **Efficacité** : optimise les applications, infrastructures et réseaux existants
  + **Élasticité** : permet de propager rapidement des applications et services existants.
  + **Innovation** : permet de créer et fournir de nouveaux types de business models, applications et services.

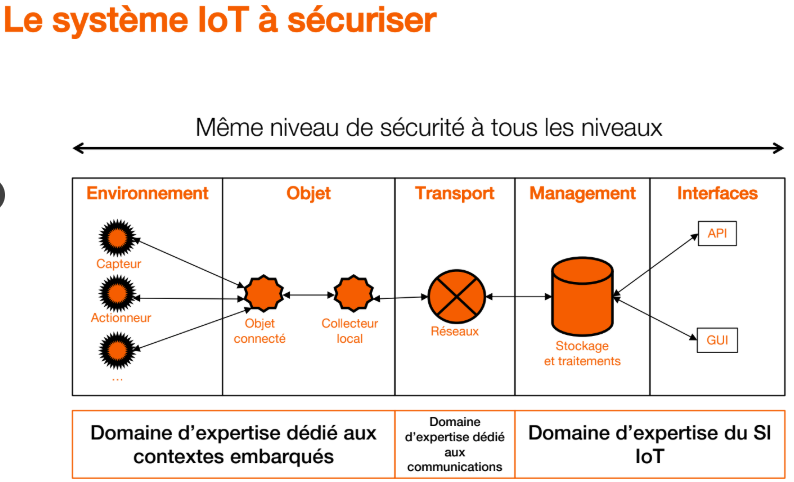
**IDC** (entreprise qui aime faire des prévision sur les trucs qui vont marcher dans le futur) prévoit une augmentation de son usage (SDN) de 90% par an.

**SDN, les enjeux:**

* Manque de système d’authentification et de chiffrement
* Failles logicielles
* Attaques DoS spécifiques
* Faiblesses dans le host spoofing
* **La gouvernance du réseau**

## D.IoT

En grande augmentation.



sécurité de l’objet en lui même, du réseau, des utilisateurs.

Secure by design

Tous ces éléments doivent être considérés pour la sécurité de l’IoT, les enjeux:

* L’objet connecté
* Le Cloud
* L’application mobile
* Les interfaces réseau
* Les logiciels
* L’utilisation de la cryptographie
* L’utilisation de l’authentification
* La sécurité physique
* Les ports USB

**→ Adopter une approche globale de la sécurité**

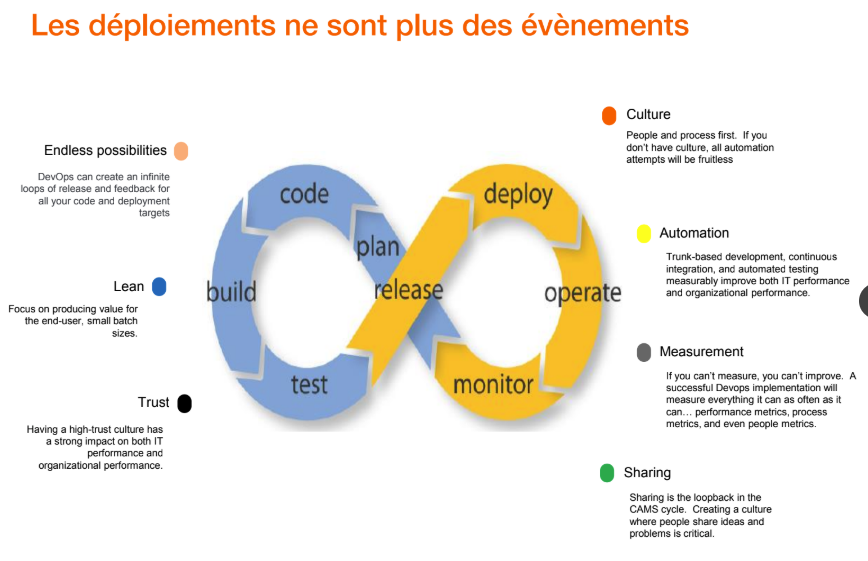
**→ Analyser les appareils**

**→ Faire un audit du réseau**

**→ compartimenter le trafic** politique de zéro confiance (car tout le monde est un crevard)

**→ Former les équipes**

## E.DevOps → méthode agiles #fanny



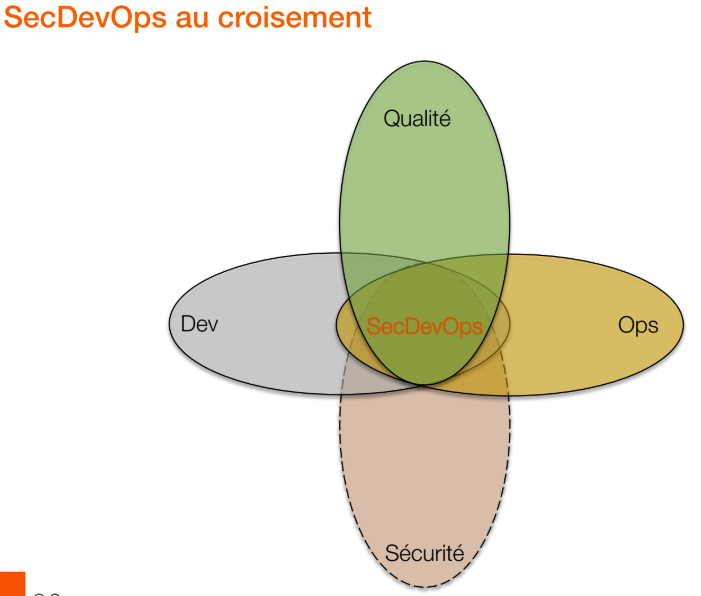
Mettre de la sécurité au plus tôt et a fur a mesure du développement.

Cherche a avoir le produit le plus vite possible mais en gardant la qualité.

teste le prog pendant la conception.

Le but de DevOps est de réduire le “Time To Market”, tout en conservant:

* La qualité
* La disponibilité
* La sécurité



**SecDevOps, les avantages**

Adopter le DevOps peut permettre de plus grands changements que les méthodes qui ont vu le jour dans le passé :

* Ajouter des outils d’analyse de code dans les process de développement et permettre des corrections avant même le déploiement
* Automatiser les outils d’attaque sur des applications en pré-production et ainsi empêcher les applications d’être déployées si elles présentent des vulnérabilités
* Continuellement tester l’environnement de production pour y rechercher automatiquement des faiblesses
* Adopter la future génération d’outils de tests de sécurité pour améliorer la qualité intrinsèque des développements
* Les outils de centralisation de la configuration des systèmes et des applications permettent d’avoir une vision de la plate-forme complète en un coup d’œil.

# 

# II - CM 2 : La sécurité et vous

## A.Attaquants

ANSSI dresse six catégories d’attaquants :

* Agresseurs
* Fraudeurs
* Employés malveillants
* Militants
* Espions
* Terroristes

**Taxonomie des attaquants : agresseurs**

**hacker ou passionné**

* individu curieux, qui cherche à se faire plaisir. Pirate par jeu ou par défi, il ne nuit pas intentionnellement et possède souvent un code d'honneur et de conduite. En général il n’a pas conscience de la mesure de ses actes. L’agresseur passionné est de moins en moins expérimenté.

**cracker ou casseur**

* plus dangereux que le hacker, cherche à nuire et montrer qu'il est le plus fort. Souvent mal dans sa peau et dans son environnement, il peut causer de nombreux dégâts en cherchant à se venger d'une société - ou d'individus - qui l'a rejeté ou qu'il déteste. Il veut prouver sa supériorité et fait partie de clubs où il peut échanger des informations avec ses semblables.

**Taxonomie des attaquants : fraudeurs**

* Le fraudeur bénéficie souvent d'une **complicité**, volontaire ou non, chez ses victimes,
* Il cherche à **gagner de l'argent** par tous les moyens. Son profil est proche de celui du malfaiteur traditionnel. Parfois lié au grand banditisme organisé ou non, il peut :
  + attaquer une banque,
  + falsifier des cartes de crédit,
  + se placer sur des réseaux de transferts de fonds et, si c'est un particulier, il peut vouloir falsifier sa facture d'électricité ou de téléphone.

**Taxonomie des attaquants : employés**

**Le fraudeur interne**

* possède de bonnes compétences sur le plan technique, il est souvent informaticien et sans antécédents judiciaires. Il peut penser que ses qualités ne sont pas reconnues, qu'il n'est pas apprécié à sa juste valeur.
* Il veut se venger de son employeur et chercher à lui nuire en lui faisant perdre de l'argent. Il peut répondre à un besoin matériel personnel qui induit des conduites de dépendances (jeux, sexe...). Pour parvenir à ses fins, il possède les moyens, qu'il connaît parfaitement, et qui ont été mis à sa disposition par son entreprise.

**Taxonomie des attaquants : militants**

**Motivés par une idéologie ou la religion,**

* ils disposent de compétences techniques très variables.
* Leurs objectifs peuvent être limités à la diffusion massive de messages, comme ils peuvent s'étendre à des nuisances effectives sur les systèmes d'information des organismes en opposition avec leur idéologie.

**Taxonomie des attaquants : espions**

* Ils participent à la guerre économique. Ils travaillent pour un État ou pour un concurrent. Ils sont patients et motivés. Ils savent garder le secret de leur réussite pour ne pas éveiller les soupçons et continuer leur travail dans l'ombre. Ils agissent souvent depuis l’intérieur de l’organisme,
  + soit en ayant trouvé un moyen d’y pénétrer,
  + soit en soudoyant une personne ayant accès aux biens.
* Ils ont pour but de **voler des informations** ou de **détruire des données stratégiques** (vitales) pour l’organisme. Dans tous les cas, les espions ont un excellent niveau de maîtrise de soi, ainsi qu'une grande capacité d’adaptation aux environnements.

**Taxonomie des attaquants : terroristes**

* Souvent appelés les cyber-terroristes, moins courants, les terroristes sont aidés dans leur tâche par l'interconnexion et l'ouverture croissante des réseaux : très motivés, ils veulent faire peur et faire parler d’eux.
* Les actions se veulent spectaculaires, influentes, destructrices, meurtrières.
* Ce profil est pris de plus en plus au sérieux par les États depuis l’attentat du 11 septembre 2001. Ils considèrent qu’une cyber-attaque perpétrée par un terroriste pourrait gravement nuire aux infrastructures économiques et critiques d’un État devenu très dépendant de ses systèmes d’informations vitaux.

## B.Traces

Etre **anonyme** sur Internet est devenu un **luxe** à cause des différents **dispositifs de surveillance**.

En utilisant Internet, chacun de nous laisse des traces :

* Publication de contenus : blog, podcast, videocast, encyclopédies collaboratives (Wikipédia), plateforme de FAQ collaborative (Yahoo! Answers, Google Answers)
* Partage de contenus : photos (FlickR), vidéos (YouTube, Dailymotion, Vimeo...), musique ou liens (delicious)
* Publication d'avis sur des produits, des services, des prestations (TripAdvisor, Epinions, ...)
* Participation à des réseaux sociaux : sur un thème particulier (motos, cuisine, jeux...) entre des professionnels (LinkedIn, Viadeo, Xing...) ou sur des thèmes universels (MySpace, Facebook, Orkut...)
* Achats en ligne sur des sites comme Amazon, eBay ou Ricardo.ch avec des systèmes de paiement type Paypal
* Sites de rencontres (Meetic, celibataire.ch)
* Sites de jeux en ligne (World of Warcraft, Everquest...) ou univers virtuels (SecondLife, Playstation Home...)

## C.Espionnage

* **L’espionnage industriel** : dérober des données sensibles pour être revendues sur le “marché noir”. Amène des employés à divulguer des infos.
* **L'espionnage industriel et le cloud** : Aubaine pour les cybercriminels. Données hébergées auprès de prestataires d’informatique dont le niveau de sécurité est variable. Accéder aux infos de plusieurs sociétés en exploitant “un point unique de défaillance”.
* **L’espionnage étatique** : Permet de récupérer des données et contrat sur les entreprises pour pouvoir les poursuivre en justice. **Attaque haut niveau**, met des logiciels espions sur lecteur de carte et quand elle est obsolète ont les jette et les pirates les récupèrent avec tout ce que la carte à vu passer, attaque sur le long terme. Les Etats s’espionnent entre eux. Etats attaquent les entreprises d’autres pays pour pouvoir récupérer des données.

## D.Éthique

Le rôle d’un RSSI lui impose de couvrir les trois principes clés de contrôle

des menaces de sécurité modernes :

* Prévention
* Protection
* Détection / réaction

Des questions d’éthique se posent à chacun de ces principes

**Ethique** = question pas si simple à résoudre en fonction des situations. On ne parle pas du point légal.

Ethique **Inside** = Éthique **dans** l’entreprise

Ethique **Outside** = Éthique **pour** l’entreprise

Ethical Hacking : Bon ou mauvais hacker?

**OWASP** : **Open Web Application Security Project** (**OWASP**) est une communauté en ligne travaillant sur la sécurité des applications [Web](https://fr.wikipedia.org/wiki/Web). Sa philosophie est d'être à la fois libre et ouverte à tous. **Top 10 des failles de sécurités**.

Black hat: hacker mechant

White hat: hacker gentil

Gold hat: gouvernement contre les APT

blue hat : “hacker” interne a l’entreprise pour tester celle-ci

grey hat: entre black and white.

red hat: contre attaque les black hat

<https://www.quora.com/What-types-of-hackers-are-there>

Hackers éthiques travaillent dans:

* Les télécommunications
* Finance
* Juridique
* Banques
* Electronique

## E.Habilitation

**Définition** : L’habilitation donnant accès à des informations classifiées fait partie d’un dispositif réglementaire important. Donnant accès à des informations classifiés que pour une personne pour une entreprise.

Les étapes de cette procédure sont :

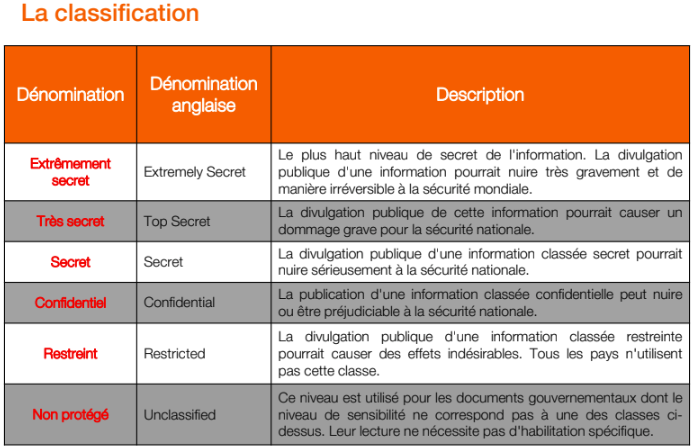
* la demande d'habilitation par la hiérarchie du service employeur ;
* l'intéressé remplit une notice individuelle de sécurité ;
* l'instruction du dossier d'habilitation par le ministère de l'Intérieur ou de la Défense.

La décision apparaît après les résultats d’enquête.

Sous réserve du « **besoin d’en connaître** » défini ci-dessus, les durées de

validation sont :

* **Très Secret - Défense** (TSD): **5 ans**
* **Secret - Défense** (SD): **7 ans**
* **Confidentiel - Défense** (CD): **10 ans**



Si des administrations nationales souhaitent partager des infos avec des gouv étrangers alors il faut se référer à la classifications de l’**OTAN**.

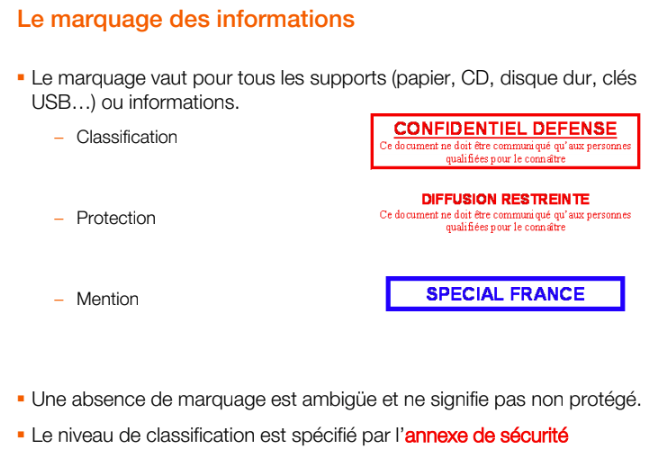
Des informations sensibles partagées par les alliés de l'**OTAN** sont

classées dans quatre niveaux de secret :

* Cosmic Top Secret (CTS),
* NATO Secret (NS),
* NATO Confidential (NC)
* ATO Restricted (NR)

Les trois principes:

* Un document doit être **marqué**
* Le personnel doit être **habilité et sensibilisé**
* Le personnel doit avoir le **besoin d’en connaître**.



**VICES** : Vénalité, Idéologie, Compromission, Ego, Sexe.

# III - CM 3 : La sécurité périmétrique vs BeyondCorp

## A.Histoire de la sécurité informatique

Provenance de l'informatique:

le génie civil

de l’industrie

Waterfall(rigide, pas d’intervention client) vs agile

Silotage vs devOps

**AWS** : Amazon Web Services

**ATAWAD** : Any Time Any Where Any Devices

Au début la cybersécurité → sécurité physique→ mnt plus ‘virtuelle’

## B.Sécurité périmétrique

Gros murs avec qq trous dans les murs pour que les gens puissent passer soit villes fortifiées dont la sécurité reposait sur des accès contrôlés concentrant les flux entrants et sortants.

**Obj** : Découper le réseau d’entreprise en **périmètres de sécurité logiques** regroupant des entités ou fonctions afin de mettre en place des **niveaux à la fois imbriqués et séparés**.

**Parefeu** = pièce maîtresse de la défense périmétrique et de la zone démilitarisée.

Il faut avoir une vue tactique et renforce les défense extérieur, sur flux entrant et sortant.

**DMZ** définit deux types de zones :

* Une plutôt ouverte aux internautes et potentiellement aux ennemis (systèmes sacrifiables) serveurs ouvert au public, DNS et SMTP.
* Une ouverte aux partenaires et potentiellement amis, données communes et privées, certificats ou serveurs d’authent.

Effectuer un **cloisonnement** entre privé et public à chaque niveau, cablage, reseau, applicatif. Sondes à déployer dans DMZ.

Un pare feu est utilisé principalement en coupure, en bordure du réseau privé d’entreprises et du réseau public. Élément essentiel de la sécurité réseau.

Tous les principaux pare-feux du marché sont stateful, gèrent le niveau 3 et 4, et apportent ainsi un premier niveau de défense périmétrique. Un pare-feu permet :

* De dissimuler la topologie du réseau et les services vulnérables.
* De différencier le trafic entrant et sortant.
* De délimiter des zones de confiance: réseau local, DMZ...
* De constituer un point d’accès distant pour l’interconnexion des réseaux d’entreprise par les connexions VPN IPSEC.

UTM est un terme pour désigner un parefeu qui possède plus de fonctionnalité de défense qu'un pare feu basic.

**UTM** : Unified Threat Management pour lutter contre les brèches du port 80.

C’est la possibilité de filtrer les paquets jusqu’au niveau 7 (applicatif) du modèle OSI. En analysant le trafic à la volée, et en le comparant à des bases de signature ou des modèles heuristiques, **UTM** permet d’accumuler sur un unique point du réseau les services suivants :

* Filtrage au niveau IP et transport
* Filtrage applicatif avec analyse du trafic HTTP, FTP, VoIP, P2P...
* **IPS (Intrusion Prevention system)** qui va détecter ou bloquer les attaques connues à partir d’une base de signature
* Antivirus et Antispam
* Filtrage des URLs

**SPOF** : Single Point Of Failure, l’indisponibilité ou la compromission du pare feu pourrait ainsi compromettre toute la sécurité du réseau.

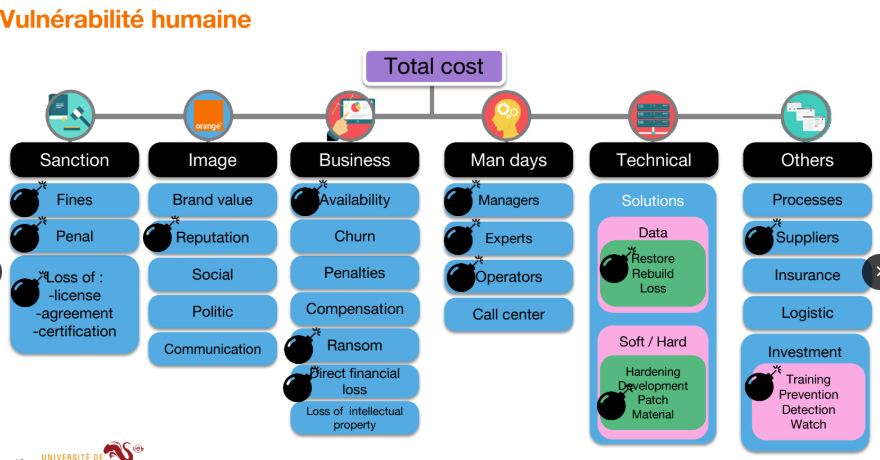
## C.BeyondCorp

1. **Identifier le terminal** : Terminal infogéré (qu’on connaît) -> Base de données d’inventaire -> ident unique pour faire certificat plus puce TPM. **PKI et BDD device** permettent d’identifier le terminal.
2. **Identifier l’utilisateur** : info sur employé, catégorisation pour savoir si on a le droit d’accéder à une ressource ou pas. Système de **SSO** permet d’authentifier des users depuis Internet. **BDD users** (info depuis qu’on est embauché jusqu'à ce qu’on parte) + **SSO**
3. **Supprimer la confiance dans le réseau** : Réseau sans privilèges comme Puppet ou Ansible. ACL (access control list) gérer de manière précise les accès au réseau. Authentification 802.1X. Serveur RADIUS (informer le switch que l’on réponde aux critères. **Serveur RADIUS** + **réseau sans privilèges**  (considéré comme Internet)
4. **Externaliser les applications et workflows** : Proxy d’accès avec accessibilité globale, load balancing, vérif contrôle accès, santé de l’application et protection anti déni de services. DNS public. CNAME pointe sur les appli via le proxy d’accès. **Proxy d’accès** (impose le chiffrement entre le client et l’application.)
5. **Contrôle d’accès basé sur l’inventaire** : Moteur de confiance d’une personne ou d’un terminal. Niveau de confiance via Gestionnaire de controle d’acces lors de son workflow de décision. Des **règles statiques et heuristiques** sont utilisés pour déterminer ces niveaux de confiance. Gestionnaire de controle d’acces est constamment alimenté par le pipeline de controle d’acces. **Moteur de confiance + Pipeline + Acces controle Engine**

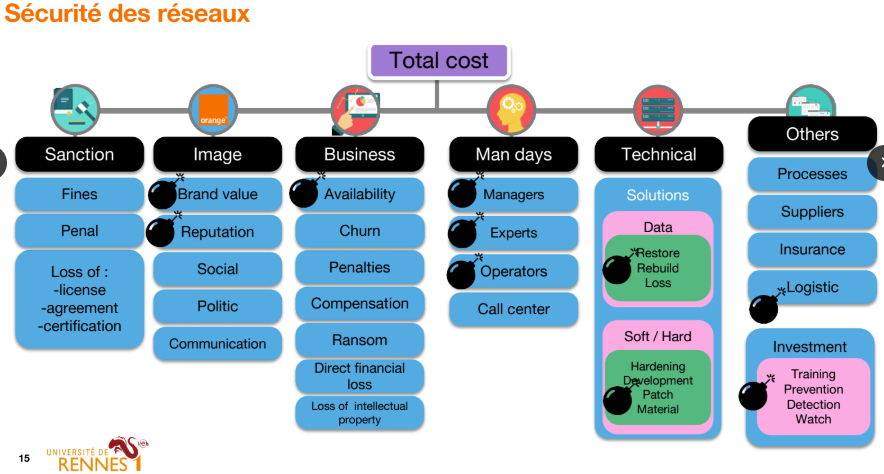
# IV - CM 4 : La sécurité au coeur des métiers

## A.L’entreprise

## B.Vulnérabilité humaine

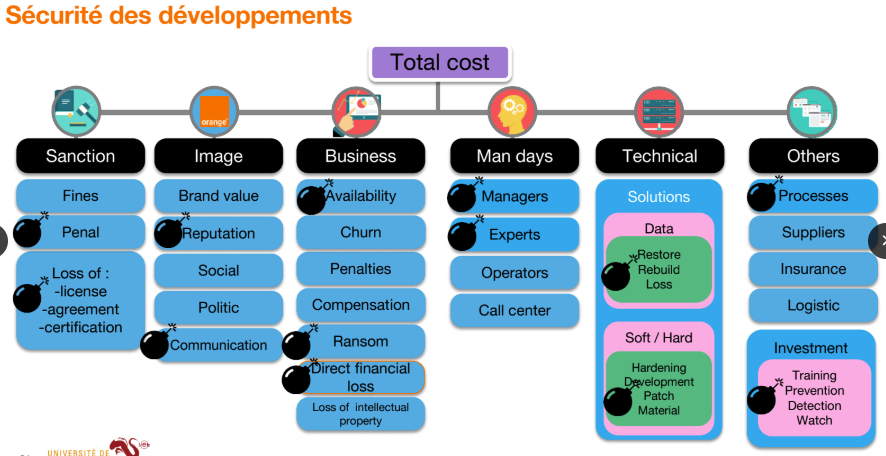


## C.Sécurité des réseaux

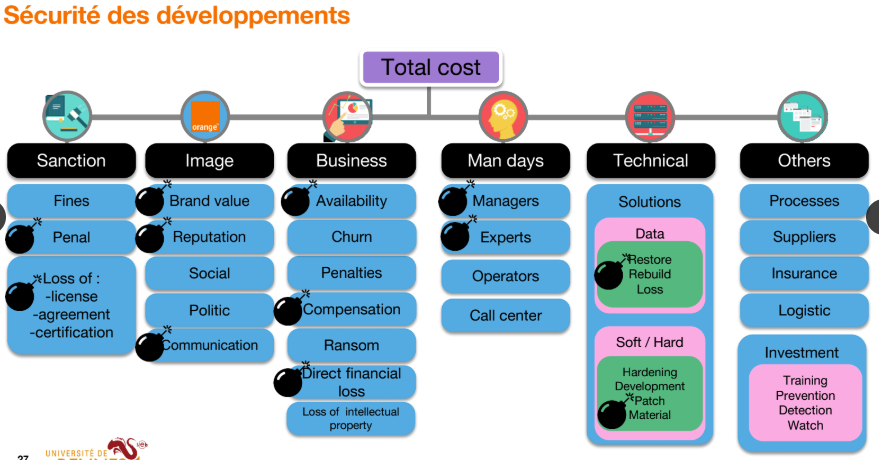


## D.Sécurité des développements

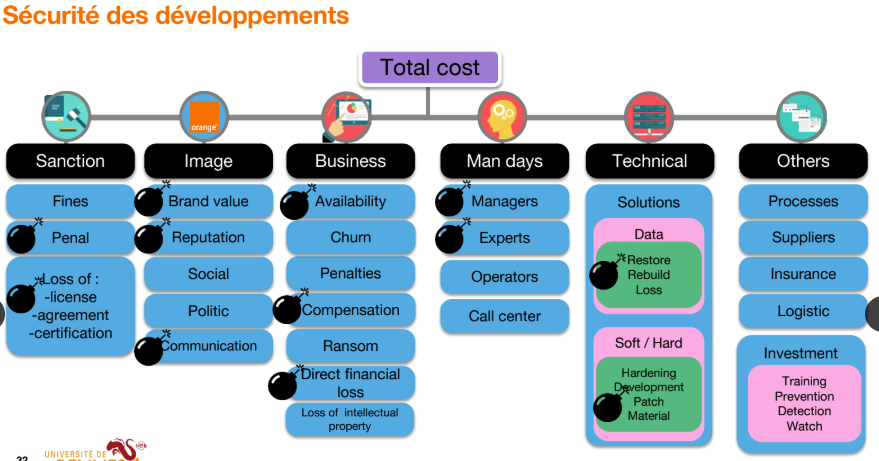
Scénario 1



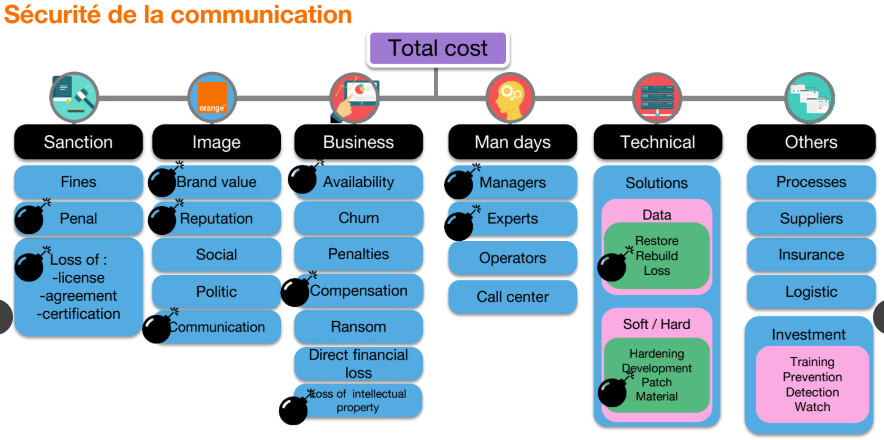
Scénario 2



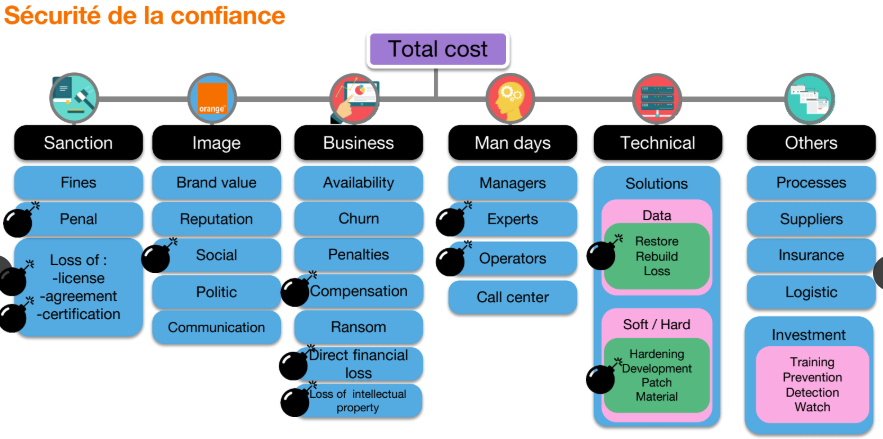
Scénario 3



## E.Sécurité de la communication

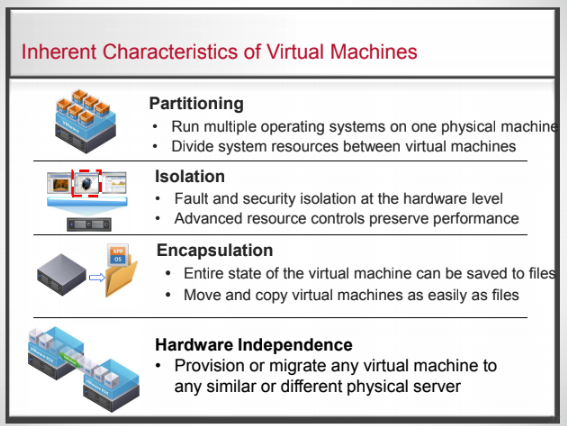


## F.Sécurité de la confiance



# V - CM 5 & 6 : Cloud & Architectures

## A.Partie 1 : Virtualisation

* **Virtualisation** : Ensemble de techniques et d’outils permettant de faire tourner plusieurs OS sur un serveur. En respectant 2 principes, cloisonnement et transparence.
  + Interets:
    - Economique
    - Facilité d’administration
    - Sécurisation
* **Hyperviseur**:
  + *Type 1* : **Hyperviseur complet**, hyperviseur bare-metal : directement sur le matériel.
  + *Type 2* : **Hosted** : Au dessus de l’OS hôte.
  + **Paravirtualiseur** : OS ne se rend pas compte qu’il est modifié. Hyperviseur au dessus du matériel avec OS modifié pour qu’il communique avec hyperviseur, donc pas vraiment de cloisonnement.
  + **Isolateur** : Conteneur, permet un certain niveau d’isolation de ressources. Au dessus du noyau OS hôte. Exemple : Docker.
* **Vmware ESX** : Hyperviseur **type 1**
  + Rajouter ou enlever du matériel à chaud
  + Quand multiplication des serveurs ESX qui peuvent apporter une couche d’abstraction complète.
  + Virtual Switch avec pleins de ports/VLAN pour utiliser les modes interne/bridge etc..
* **Datastore** : Serveur de stockage de données. Utilisé pour sauvegarder les fichiers des machines virtuelles, templates, images ISO etc…
* Options disques durs :
  + **Thick** : Taille du disque physique = taille du disque virtuel.
  + **Thin** : Taille du disque physique = utilisation du disque virtuel.
* **Snapshot** : Point de reprise en cas de crash de la VM. Ne sont pas des backups. Se garde qq heures/jours. Si 75 snapshots, la machine doit revenir au 1er snapshot pour connaître l’état initiale de la machine, donc long et perf peuvent s’effondrer.
* **VMotion** : Migration directe des machines virtuels, d’un hôte vers un autre à chaud avec des services qui tournent en continue.
* **Vmware “HA”** : Protection contre les pannes Hardware.
* **VMware Distributed Resource Scheduler (DRS)** : Ordonnanceurs et rééquilibreur de charge, utilise le VMotion. Effet de bord quand trop agressif, les VMs se refilent la patate chaude.
* **Affinité et anti-affinité** : Exécution des VMs, possibilité de les regrouper sur un même ESX ou au contraire de les dispatcher sur des ESX différents.
* **VMware Fault Tolerance** : Clonage de tout sur un deuxième ESX car si ESX tombe la VM clone, prend immédiatement le pas en temps réel.  
    
  
* **SLA ( Service-Level agreement)** : Paramètre à prendre en compte concernant la disponibilité des choix d’architecture.
  + **GTD** : Garantie de Temps de disponibilité
  + **GTI** : Garantie de Temps d’intervention
  + **GTR** : Garantie de temps de rétablissement
  + **RTO** : Recovery Time Objective (retour de service)
  + **RPO** : Recovery Point Objective (données perdues)
* **Virtualisation du réseau** :
  + VLAN 802.1Q (trunk)
  + vSwitch
  + Virtual Firewall
  + vNIC
  + 10G NIC partitioning
  + VPN
* **Virtualisation de stockage** :
  + DAS: Disques en attachement direct.
  + SAN: Réseau spécialisé pour le stockage, mode bloque.
  + NAS: Périphérique de stockage en réseau, mode fichier.
* **PRA/DRS** : Plan de reprise d’activité / Disaster Recovery System
  + Réplication entre les baies de stockages
  + Réplication au niveau système
  + Réplication au niveau applicatif
* **Le point critique, le réseau** :
  + Déplacer une machine, physique ou virtuel, n’est pas vraiment compliqué.
  + Par contre, continuer à communiquer avec le reste du système, c’est pas gagné.
    - Configuration réseau de l’OS
    - Configuration réseau des applications (parfois “en dur” ou en basse)
    - Dépendances avec des services transverse d’infrastructure (DNS, NTP, SMTP, proxy..)
* **vApp** : Regroupement de plusieurs VM dans une ensemble logique. Cas d’usage : service en multi-tiers.

## B.Partie 2 : Cloud

# 

# VI - CM 7 : Formation PKI d’entreprise

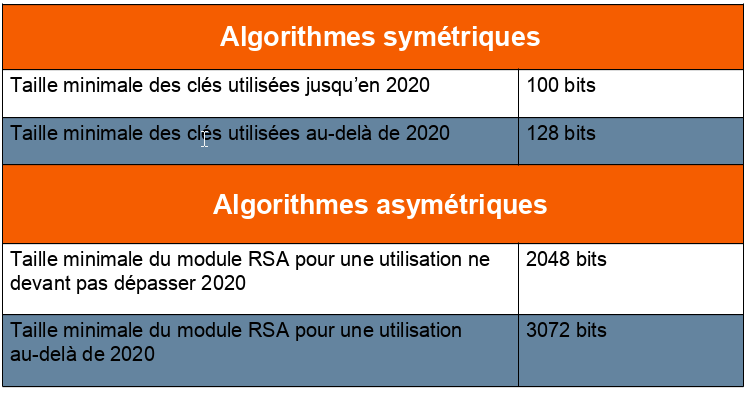
## A.Introduction

la sécurité est un vecteur de confiance, réciproque fausse.

PKI → équivalent IRL → Carte d’identité, coffre fort, signatures.

## B.Rappels de cryptologie

la crypto DOIT garantir: Confidentialité, Intégrité, Authentification et Non répudiation.

La sécurité ne repose pas sur le secret des algos mais des clés.

## C.Certificats numériques

Pour savoir que les clé vienne bien de la personne voulu → certificat

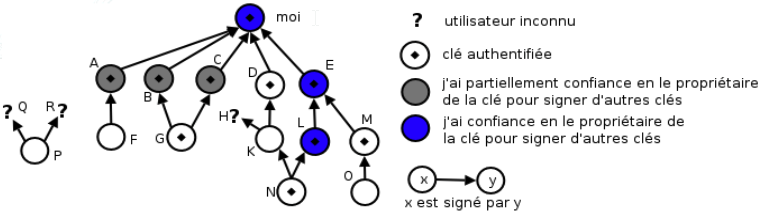
### 

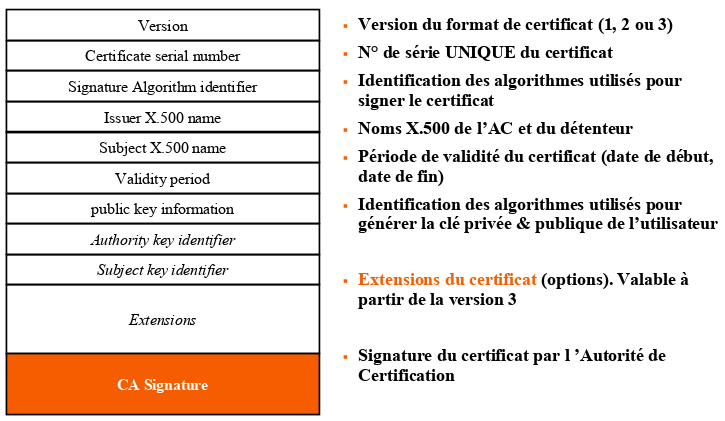
certificat → carte d’identité

Un certificat contient: clé publique, numéro de série (unique dans une AC), des infos d’identification, durée de validité, signature et info sur son usage.

Différent format de certificat X509 et CVC (une autorité de certification), PGP (certifié par plusieurs personne).

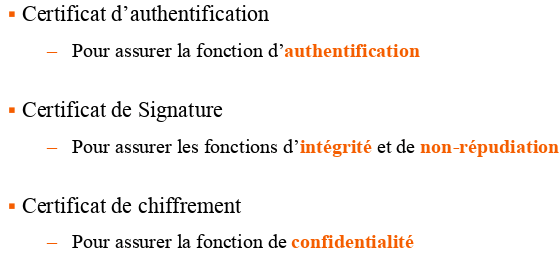
PGP:

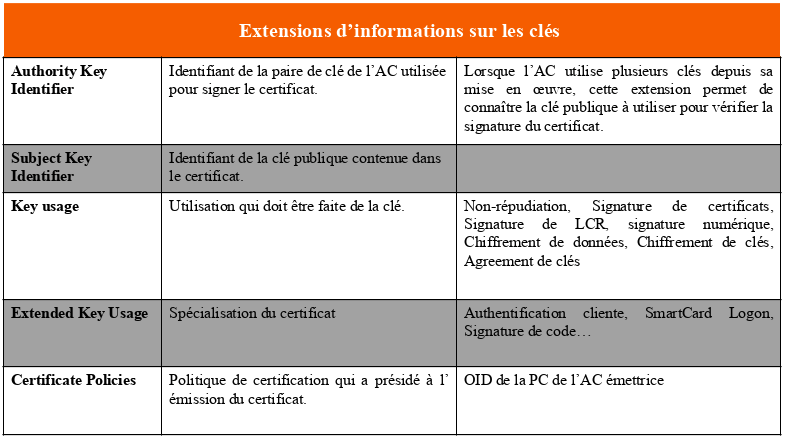


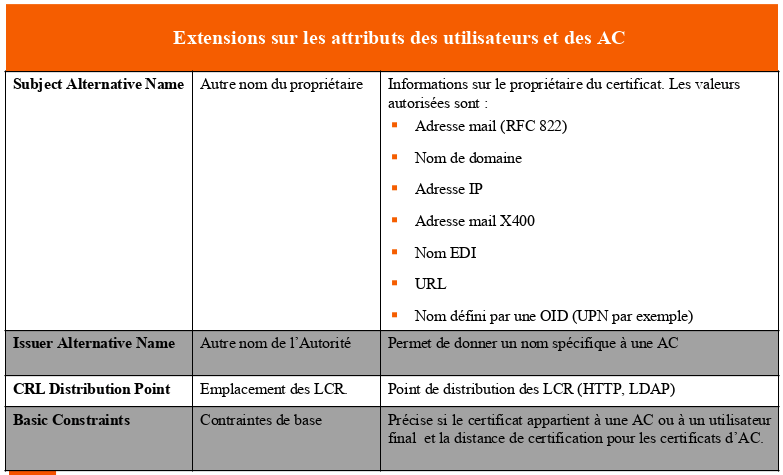


Appl des certificats X509:

SSL/TLS et IPSec et S/MIME







On peut stocker les clé privée dans : disque dur, carte à puce, token sur port usb, HSM (Hardware security Module)

## D.PKI / IGC

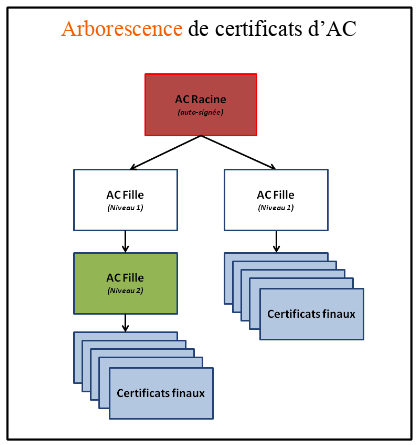
Certificat délivré par IGC (Infrastructure de Gestion de Clés)

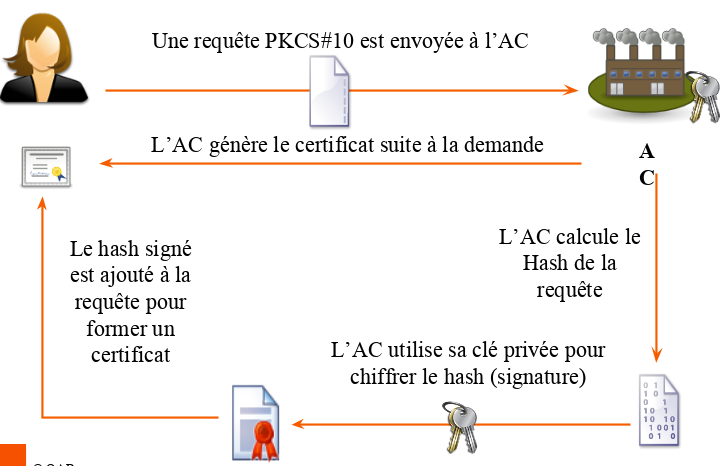
IGC est composé de plusieurs entité qui ont tous un rôle défini pour le cycle de vie

IGC est le point de rassemblement de la cryptographie et des procédures.

IGC est décomposé sous forme d’Autorités.

AC est une composant de IGC qui signe les certifcat LCR.





Rôle d’une IGC:

Garantir la confiance

Contrôler les demandes(légitimité de celle-ci)

Identifier les acteurs

Gere les certificats & les bi-clés

IGC est composé de AC et AE (autorité d’enregistrement) , A

## E.Bonnes pratiques IGC