Sécurité informatique

Sécurité Informatique

1) **Contours de la sécurité informatique**

2) Les menaces

3) Définir une politique de sécurité

4) Signature éléctronique

5) Perspectives sur la sécurité informatique

1) Contours

- Définir le champ de la sécurité informatique commencer par définir le champ de la sécurité informatique

- Par suite, on en déduira les menaces et les risques associés

- La sécurité informatique = CAID + Non Répudiation.

1) Contours

- **C**onfidentialité : les données sont consultées seulement par des personnes autorisées.
- **A**uthentification : sur un système informatique, on doit pouvoir s'assurer qu'une personne est celle qu'elle prétend être.
- **I**ntégrité : il faut que les fonctions et les données des systèmes d'informaion ne soient pas altérées, ne soient pas supprimées, sauf par des personnes autorisées.
- **D**isponibilité : les ressources doivent être accessibles au moment où elles sont nécessaires.
- **N**on-Répudiation : capacité d'un système à garantir qu'une entité a bien pris part à une action, un contrat, un transaction, sans qu'elle puisse le contester par la suite..

1) Contours

Les risques se comprennent en contraposition des principes qui définissent la sécurité.

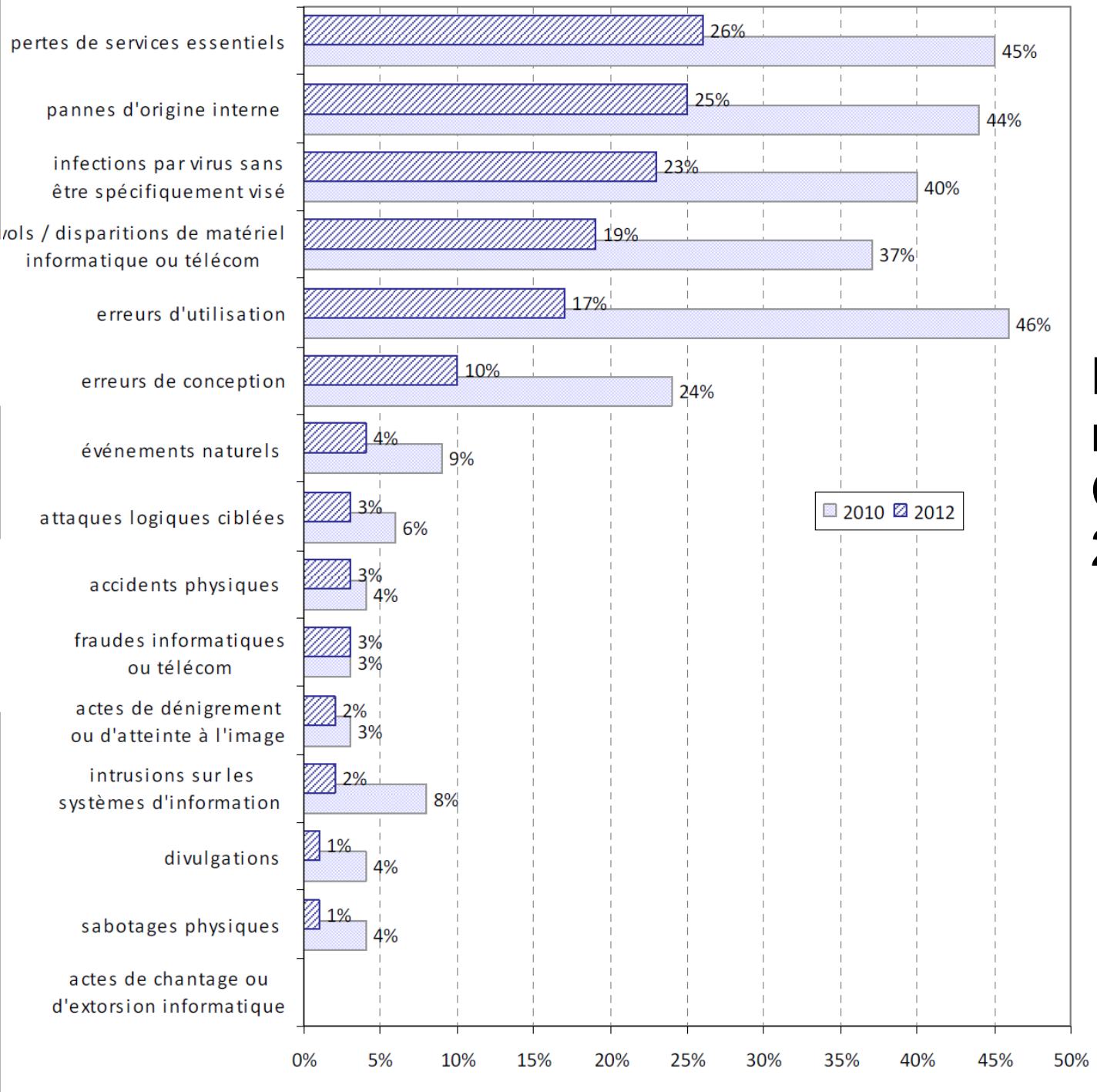
- Accès non autorisé,
- Falsification,
- Destruction partielle ou totale
- Utilisation détournée du SI
- Reconnaissance
- Rutpure dans la continuité des services informatiques
- Intrusion
- Altération ou destuction,
- Déni de service
- ...

1) Contours

- La sécurité informatique ne se limite pas au champ des attaques logicielles (cf l'aspect physique de la sécurité)

- Importance également du facteur humain.

Au cours de l'année précédente, votre organisme a-t-il subi des incidents de sécurité de l'information consécutifs à…



Extrait du rapport du Clusif - 2012

1) Contours

- La sécurité n’est pas un état, c’est un processus.

- "Security is a process not a product" - Shneier

1) Contours

Les risques sur la sécurité du système d'information ont pris une nouvelle ampleur avec

- le développement de la micro-informatique
- Le développement des réseaux (diffusion de virus, risques d'intrusions, sécurité des données…)
- Le développement des téléphones portables ?

Sécurité Informatique

1) Contours de la sécurité informatique

2) **Les menaces**

3) Définir une politique de sécurité

4) Signature éléctronique

5) Perspectives sur la sécurité informatique

2) Les menaces

Les menaces peuvent d'abord être physiques :

- Foudre,
- Incendie
- Vol de matériel
- Dégat des eaux,
- Destruction
- ...

2) Les menaces

- Les risques de pannes

- Celles-ci peuvent être matérielles ou logicielles.

- Risque surtout de panne des serveurs.

2) Les menaces

- Les menaces d’interception

- Les menaces de brouillage des communications

2) Les menaces

- Les attaques logicielles :
  - Intrusion
  - Exploration
  - Altération
  - Destruction
  - Saturation
  - …
- Celles-ci sont menées à l'aide de logiciels malveillants, conçus dans le but de nuire.
- Intrusion, vol de données, risque sur l'intégrité des données, ...

2) Les menaces

- Les virus. Programmes informatiques de petite taille, qui utilisent un programme hote pour se reproduire et se diffuser. Des dommages peuvent par suite être réalisé par le virus. Virus : couche 4 du modèle TCP/IP
- Les vers. Ce sont des virus, mais ils utilisent plus particulièrement la mise en réseau pour leur diffusion.
- Les macro-virus

2) Les menaces

Quelques exemples de virus célèbres :

Nom	Date	Dommage estimé	Description
MyDoom	2004	27 MM €	Ce virus se répand par email. Une fois le courriel ouvert, MyDoom se télécharge et « vole » tout le carnet d'adresse de l'ordinateur infecté. Ainsi, il est devenu le virus qui s'est le plus vite répandu au monde.
Sodig F.	2003	26 MM €	était capable de se dupliquer lui-même et se répandait par email. Quand l'email était ouvert, il déclenchait le ver qui se mettait en chasse de nouvelles adresses électroniques sur l'ordinateur infecté. Le flot de messages qu'il envoyait submergeait les boîtes mails et ralentissait tout le système informatique. De nombreuses grandes entreprises en ont été victimes, comme Air Canada par exemple.
I Love You	2000	11 MM €	Ce ver tire son nom de la pièce jointe au courriel qui le transporte : Love-letter-for-you.txt.vbs. Lorsqu'il est ouvert, un programme malveillant est déclenché. Ce virus a été conçu pour voler des mots de passe d'accès Internet et il se renvoyait lui-même à l'intégralité du carnet d'adresse de l'ordinateur infecté.
Code Red	2001	1,9 MM €	Code Red exploitait une faille dans le système d'exploitation de Windows 2000 et Windows NT ce qui lui a permis de « défigurer » et de planter certains sites web, dont le site de la maison blanche. Il choisissait au hasard 100 adresses IP à la fois en scannant le système Microsoft.
Slammer	2003	0,87 MM €	Slammer était un ver internet qui causait des dénis de service sur les serveurs Internet et qui ralentissait considérablement le trafic général. Ce ver est un petit code qui générait des adresses IP de façon aléatoire et envoyait des copies de lui-même à ces adresses. Il se répandit à une vitesse fulgurante sur Internet, doublant de volume toutes les 8,5 secondes. Parmi ses victimes, on peut compter Continental Airlines, une centrale nucléaire dans l'Ohio, une banque américaine ainsi que le système des appels d'urgence dans l'État de Washington.

2) Les menaces

Des catégories qui recoupent ou non les virus :

- Chevaux de Troie : logiciel porteur et "charge utile". Le logiciel porteur est souvent légitime, mais sa version modifiée contient un cheval de Troie. Logiciels crackés, téléchargement depuis des plateformes peu sûres
- Malware
- Backdoor : programme installé sur l'ordinateur qui ouvre des ports de communication pour installer des logiciels malveillants.
- Spyware

2) Les menaces

Les attaques par déni de servi / DOS

- Peut prendre plusieurs formes : innodation d'un réseau, perturbation de connexion entre des machines, obstruction d'accès à un service, etc.
- Attaque sur un serveur de fichier, un site Web ou un serveur de messagerie.

2) Les menaces

Exemple d’attaque DOS :

- Plusieurs chevaux de Troie déposés sur des machines diverses se connectent en même temps sur un serveur
- Envoi d’un très grand nombre de mails sur une boîte mail.

2) Les menaces

- Les défaillances humaines
- Le phishing
- Les canulars ou hoax.
- Usurpations d’identité.

Sécurité Informatique

1) Contours de la sécurité informatique

2) Les menaces

3) **Définir une politique de sécurité**

4) Signature éléctronique

5) Perspectives sur la sécurité informatique

3) Politique de sécurité

- Les protections contre les atteintes physiques
- Contre les risques "naturels" : porte, régulation de température ...
- Contre les risques de malveillance : onduleurs, caméras, porte blindée…

3) Politique de sécurité

- Les protections contre les atteintes logicielles
- Password
- DMZ
- Firewall
- Antivirus
- Proxy
- Etc...

3) Password

- Mise en place de couples Login / password.
- Identification, conservation de log de connexion
- Gestion des droits en fonction des utilisateurs
- Utilisateur root / administrateur.
- Authentification unique / serveur d’authentification

3) Authentification

- Il existe d'autres méthodes d'identification que les passwords
- Authentificaiton par carte à puce, clé USB
- Etc...

3) Configuration des postes utilisateurs

- Verouillage des postes après utilisation

- Profil nomade

3) Firewall

- Firewall
- Fonctionne au niveau des couches 2 et 3 de TCP/IP
- Une configuration possible de firewall :
  - Tout trafic entrant est interdit
  - On autorise une communication sur un port donné par adresse IP et par heure.

- Une autre configuration possible
  - Tout trafic est interdit
  - On autorise le trafic sur le port 80.

3) Firewall

Total number of firewall hits for February 10: 18

Older / Newer

Time	Chain	Iface	Proto	Source	Src Port	Destination	Dst Port
12:14:28	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
11:54:24	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
11:35:22	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
11:14:13	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
10:54:09	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
10:35:14	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
10:13:58	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
09:53:55	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
09:34:27	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
09:13:43	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
08:53:40	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
08:34:14	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
08:13:28	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
07:53:26	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
07:33:46	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
07:13:12	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
06:53:09	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317
06:33:22	DROP_INPUT	red0	UDP	111.216.133.70	16248	200.82.243.146	19317

Older / Newer

3) Firewall

Windows XP Firewall Log Viewer

File Help

Log file c:\windows\pfirewall.log Open... Refresh

View log file | Statistics

No. v	Date/Time	Action	Protocol	Source IP	Destination IP	src port	dst port	Siz
121	Mar 21, 2004 8:49:45 PM	DROP	TCP	68.174.102.251	10.251.0.46	6346	4176	40
123	Mar 21, 2004 8:49:45 PM	DROP	TCP	142.59.35.58	10.251.0.46	6346	4172	40
125	Mar 21, 2004 8:49:46 PM	DROP	TCP	62.195.173.71	10.251.0.46	6346	4159	40
126	Mar 21, 2004 8:49:47 PM	OPEN	UDP	10.251.0.46	213.112.66.28	4880	22577	-
127	Mar 21, 2004 8:49:47 PM	DROP	TCP	80.177.19.118	10.251.0.46	6346	4157	48
129	Mar 21, 2004 8:49:48 PM	OPEN	UDP	10.251.0.46	213.64.2.194	4880	3409	-
130	Mar 21, 2004 8:49:48 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
133	Mar 21, 2004 8:49:48 PM	OPEN	UDP	10.251.0.46	67.121.239.228	6346	15221	-
137	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
140	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.27	10.251.0.255	137	137	78
141	Mar 21, 2004 8:49:49 PM	DROP	UDP	10.251.0.97	10.251.0.255	137	137	78
142	Mar 21, 2004 8:49:50 PM	DROP	TCP	80.177.19.118	10.251.0.46	6346	4157	48

4069 dropped packets 31838 successful connections DROP UDP And Or Filter

3) Antivirus

- Antivirus
- Fonctionne au niveau de la couche 4 de TCP/IP
- S’utilise en complément des firerwall.
- Recherche de signature de virus. Morceau de code ou chaîne de caractères spécifique.

3) Antivirus

- Un antivirus fonctionne par scan des fichiers sur le disque

- Un antivirus scrute également le trafic entrant ainsi que les logiciels actifs.

- Mise à jour régulière de la base anti-virale.

- Vérification de l'intégrité des fichiers. Un antivirus peut stocker des infroamtions sur chacun des fichiers du système. Il lui associe des informations (taille, date et heure de modificatio, somme de contrôle etc.) Lorsque le fichier change, l'antivirus peut le voir.

- Analyse heuristique : l'antivirus simule le fonctionnement de certains programmes pour détecter leur potentielle dangerosité. Risque d'alertes sans fondement.

3) Antivirus

- Mise à jour des OS

- Quels risques pour quels OS ?

- Stratégies automatiques des pirates : de l'opportunité et de l'exploitation des failles de sécurité publiées.

3) Cryptographie

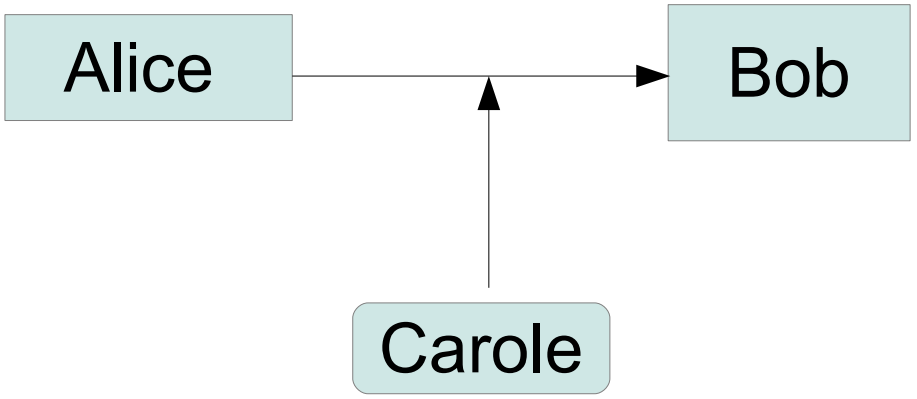
- La base de la sécurité dans la communication : cryptographie asymétrique, cryptographie symétrique.
- Un cas typique en cryptographie, Alice veut envoyer un message vers Bob

3) Cryptographie

- Cruptos - graphein
- Des méthodes de cryptographie anciennes.
- Ex : le code de César / chiffrement par décalage.
- Ex : amélioration du code de César.
- Ex : chiffrement de Vernam / Masque jetable.
- Ces méthodes sont éculées et déchiffrables désormais.
- Problème de la communication entre des machines sans "connaissance" préalable.

3) Cryptographie

- Une personne veut intercepter le message.



3) Cryptographie

- Cryptage à clé symétrique.
- Algorithme de référence : DES et Triple DES
- Alice et Bob ont une clé en commun
- Cette clé est une clé d'encryption et de décryption.

3) Cryptographie

- Limite de cette méthode ?

  - Les opérations de cryptage et décryptage sont lentes.

  - Comment échanger la clé ?

3) Cryptographie

- Cryptage à clé asymétrique
- Algorithme RSA. Rivest, Shamir, Adelman
- Alice et Bob n'ont pas de clé en commun
- Alice veut envoyer un message à Bob
- Bob crée une clé publique d'encryption et une clé privée de décryption. Il envoie la clé publique d'encryption

3) Cryptographie

- Création de clés :

Alice

Bob

Clé décr. BWX

Clé encr. XWB

- Envoi de la clé :

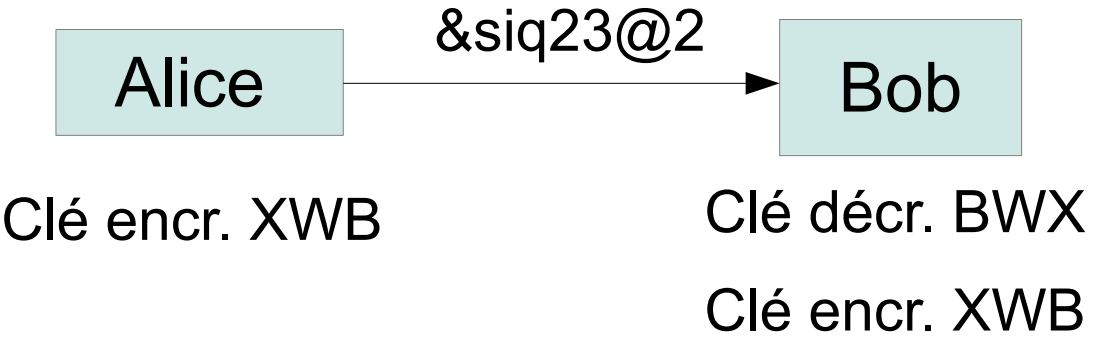
Clé encr. XWB

Clé décr. BWX

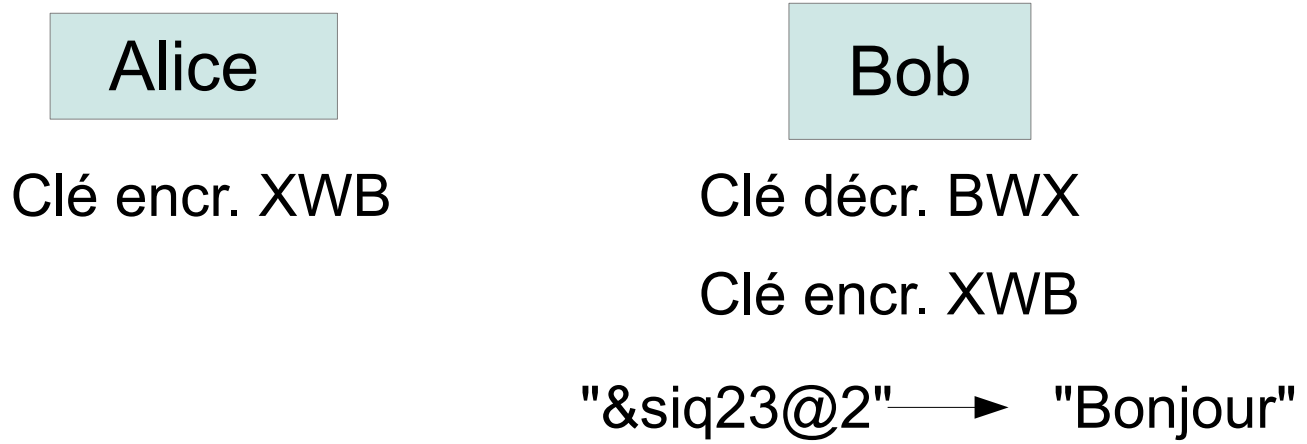
Clé encr. XWB

3) Cryptographie

- Alice envoie son message crypté à Bob



- Bob décrypte



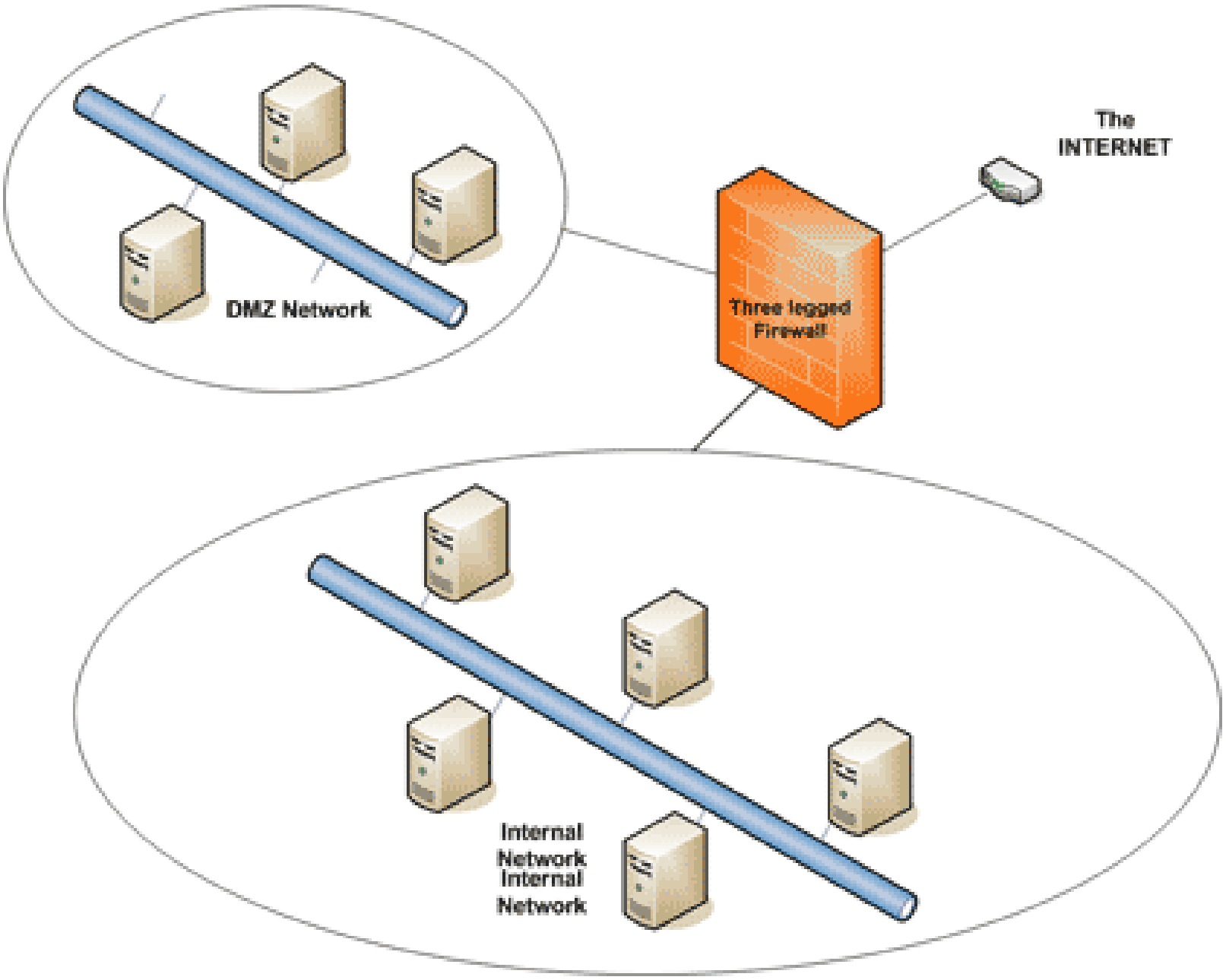
3) Cryptographie

- Ici, on ne peut pas déduire la clé privée de la clé publique.
- Les clés sont en fait des nombres premiers
- Une méthode cassée ?
- Limite de cette méthode ?

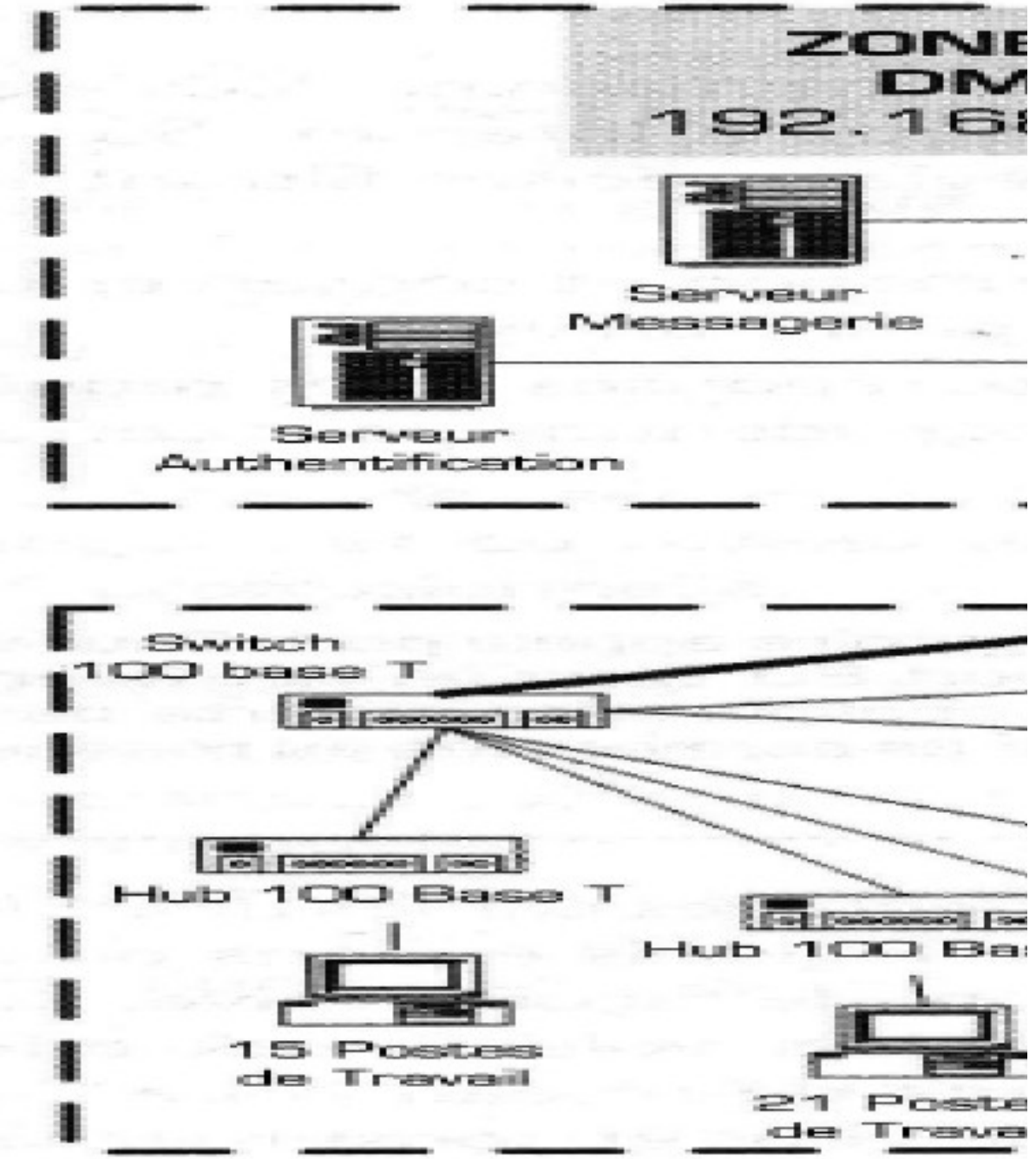
3) DMZ

- Une politique de sécurité plus complexe : DMZ.
- Dans une entreprise qui comporte des serveurs, on ne peut pas imposer les mêmes règles de connexion à toutes les machines
- Cf les machines qui doivent supporter des connexions entrantes.

3) DMZ


DMZ Network
The
INTERNET
Three legged
Firewall
Internal
Network
Internal
Network

3) DMZ


ZONE
DM
192.16
Serveur
Messagerie
Serveur
Authentification
Switch
100 base T
Hub 100 Base T
15 Postes
de Travail
Hub 100 Ba
21 Poste
de Trava

3) DMZ

- Exemple de politique dans une entreprise équipée d'une DMZ :
  - Trafic du réseau externe vers le réseau interne **interdit** ;
  - Trafic du réseau interne vers la DMZ **autorisé** ;
  - Trafic du réseau interne vers le réseau externe **autorisé** ;
  - Trafic de la DMZ vers le réseau interne **interdit** ;
  - Trafic de la DMZ vers le réseau externe **refusé.**

3) VPN

- VPN : Virtual Private Network
- Repose sur IPSec ou sur SSL
- SSL : supporté par les navigateurs.
- IPSec : non supporté par les navigateurs

3) VPN

- VPN : Virtual Private Network
- Repose sur IPSec ou sur SSL
- SSL : supporté par les navigateurs.
- IPSec : non supporté par les navigateurs => téléchargement d’un client lourd.

3) VPN

- SSL / Secure Socket Layer
- Version SSL 3.0 en 1996. Ce protocole comporte une faille. Cf faille POODLE publiée.

- Passage à TLS
- La plupart des navigateurs Web gèrent TLS 1.0

3) Politique de sauvegarde

- Différents types de sauvegarde :
  - Complète
  - Différentielle. 2 sauvegardes suffisent pour tout récupérer.
  - Incrémentale. Toutes les sauvegardes depuis la dernière sauvegarde complète sont nécessaires.
  - Journalisation. Chaque modification est immédiatement sauvegardée.

- Horizon de la sauvegarde

3) Politique de sauvegarde

- Sauvegarde sur supports amovibles

- Sauvegarde sur serveurs distants.

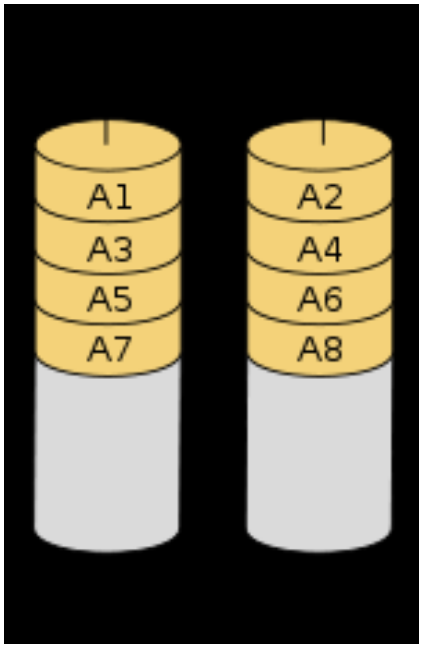
3) Politique de sauvegarde

- Technologie RAID
- Redundant Array of Independent Disk
- Stockage de données sur plusieurs disques durs

- Amélioration de la performance
  - Temps de sauvegarde
  - Taille de la sauvegarde
  - Temps de récupération du système
  - Tolérance aux pannes matérielles

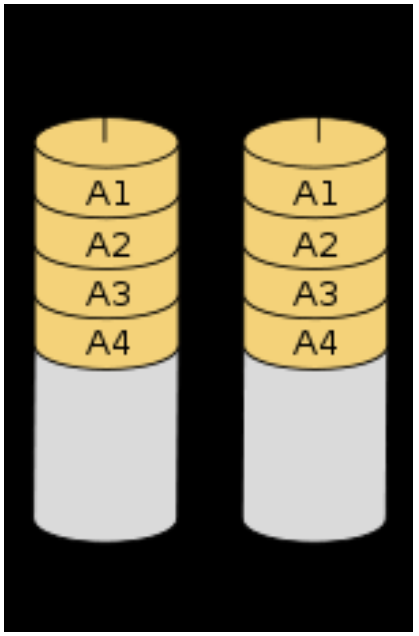
3) Politique de sauvegarde

- RAID 0
- Système de répartition qui diminue le temps d'enregistrement (ou de récupération) des données en faisant travailler deux disques durs en parallèle



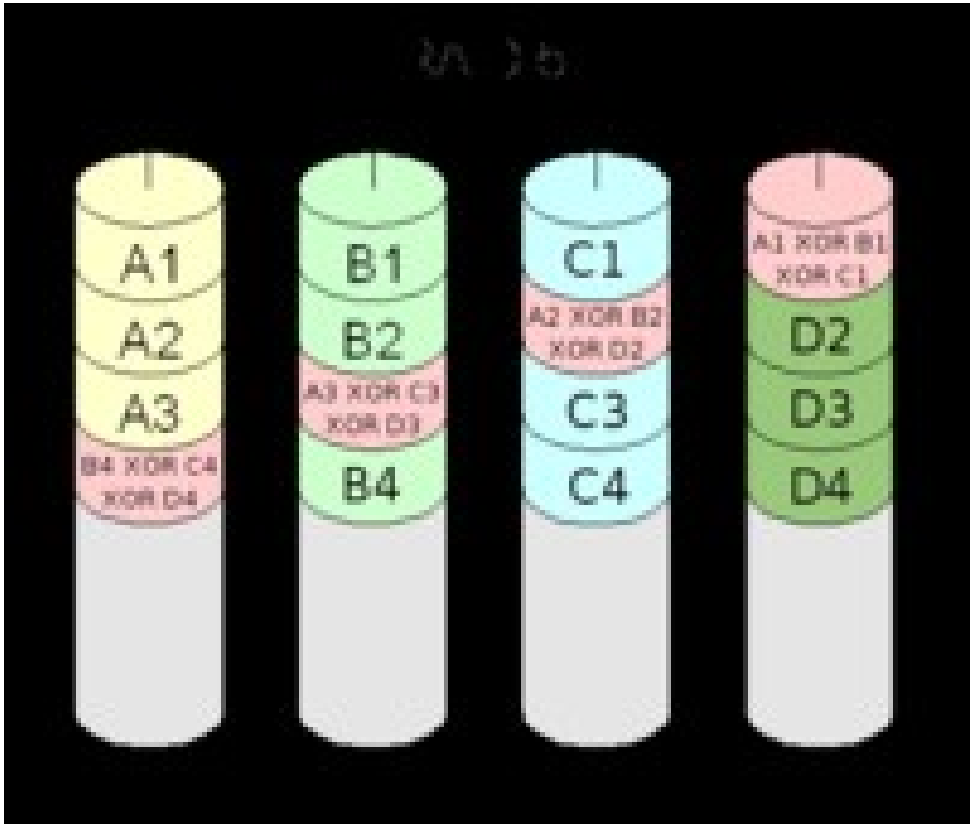
3) Politique de sauvegarde

- RAID 1
- Mirroring



3) Politique de sauvegarde

- RAID 5
- Système qui optimise le temps de stockage et est tolérant par rapport aux pannes



3) Plan de reprise d'activité (1)

- Document qui permet à une entreprise de prévoir les démarches à entreprendre pour reconstruire et remettre en route un SI en cas de sinistre.
- Objectif de réduire l'impact des dommages d'une atteinte au système d'information
- Le PRA recence différentes mesures (cf précédentes)

3) Plan de reprise d’activité (2)

- Prévoir un système relais et la transition vers ce système
- Produire un écrit explicitant la démarche
- Procéder à des essais.

3) Plan de reprise d'activité (3)

- Existe aussi le PCA : Plan de Continuité de l'activité.

- Importance => normalisation ISO : "Sécurité sociétale – Etat de préparation et systèmes de gestion de la continuité".

- L'accent est mis sur les processus critiques des organisations.

3) Plan de reprise d'activité (3)

- L'élboration d'un PCA :
  1) Nommination d'un chef de projet indépendant de la DSI
  2) Audit des activités critiques de l'entreprise
  3) Réalisation d'un document de synthèse proposant une classification des activités par niveaux d'exigence.
  4) L'élaboration d'un cahier des charges précisant les éléments nécessaire au plan de reprise.
  5) Le choix d'un prestataire.
  6) Formalisation du plan de continuité.
  7) Phase de test et maintenance.

3) Sensibilisation et formation des utilisateurs

- Introduction d’une charte informatique
- Formation des utilisateurs.

3) Proxy

- Proxy : interface entre les utilisateurs et Internet

- Le Proxy peut être configuré en fonction de règles de sécurité.

3) Redondance

- Cela rejoint pour partie le RAID
- Au delà : redondance des serveurs.

Sécurité Informatique

1) Contours de la sécurité informatique

2) Les menaces

3) Définir une politique de sécurité

4) **Signature éléctronique**

5) Perspectives sur la sécurité informatique

4) Signature éléctronique

- On cherche un système qui apporte deux garanties :
  - La source de l'information
  - L'intégrité du message transmis.

- Retour à la cryptographie

4) Signature éléctronique

- Notion de haché du message : condensé du message : si le message change, le hasché change.

- On veut générer un message : on crée un clé publique de décryption et une clé privée d'encryption.

4) Signature éléctronique

Etape 1 : Alice a un message pour Bob

Alice

Bob

Message

Haché du message

4) Signature éléctronique

Etape 2 : Alice crée une clé publique de décryption et une clé privée d'encryption

Alice

Bob

Message

Haché du message

Clé privée d'encr.

Clé publique décryp.

4) Signature éléctronique

Etape 3 : Alice envoie sa clé publique et encrypte le haché avec sa clé privée

Alice

Message

Haché du message

Clé privée d'encr.

Clé publique décryp.

Haché encrypté

Bob

Clé publique décryp

4) Signature éléctronique

Etape 4 : Alice envoie le message et le haché encrypté

Alice	Bob
Message	
Haché du message	Clé publique décryp
Clé privée d'encr.	Haché encrypté
Clé publique décryp.	Message
Haché encrypté	

4) Signature éléctronique

Etape 5 : Bod décrype le haché et le compare à un haché obtenu à partir du message

Bob

Clé publique décryp

Message → Haché 1

Haché encrypté → Haché 2

4) Signature éléctronique

- Si les deux hachés ne correspondent pas : c'est que soit le message, soit le haché encrypté a été modifié
- Si les deux hachés correspondent alors, le message a été transmis de manière intègre
- Quid de l'expéditeur ?
- Si on est sûr de la source de la clé, on sait qui a envoyé le message ET que le message a été transmis de manière intègre.

4) Signature éléctronique

- Point de vue légal
- Loi du 13 mars 2000 porte modification du Code Civil par légalisation de la signature éléctronique
- La directive européenne 1999/93 définit la signature éléctronique : "une donnée sous forme éléctronique qui est jointe ou liée logiqueemnt à d'autres données éléctroniques et qui sert de méthode d'authentification"

4) Signature éléctronique

- La directive européenne stipule par ailleurs que la signature éléctronique doit :
  - Être liée uniquement au signataire
  - Permettre d'identifier le signataire
  - Etre créée par des moyens que le signataire garde sous son contrôle exclusif
  - Etre liée aux données auxquelles elle se rapport , de sorte que toute modification des données soit détectable

4) Signature éléctronique

- Loi sur la confiance dans l'économie numérique du 21 juin 2004 => modification du code Civil

- Les contrats peuvent être réalisés sous forme électronique.

- EDI / depuis 01/10/2010 : obligation de téléclaration de TVA pour soc à CA>500000€

4) Signature éléctronique

- Nécessité de registre de clés pour s'assurer des identités de l'émetteur d'une clé publique
- Nécessité de certificats.
- Cf également les clés publiques dans le cryptage asymétrique. Il faut être sûr que la clé publique d'encryption soit bien fournie par celui qui le prétend.
- Infrastructures à clé publiques.

4) Architecture de confiance

- Un tiers pourrait se substituer à une entité et envoyer de fausses clés publiques
- Objectif d'établir une communication et d'obtenir des informations
- "Attaque de l'homme du milieu"
- => système de certificats

4) Architectures de confiance

- Architecture de confiance
- IGC : Infrastructure de gestion de clés.

- PKI : public key infrastructure

4) Architecture de confiance

- Les navigateurs modernes intègrent une liste de certificats provenant de différentes **autorités de certification**.

- Lorsqu'une entité X veut mettre en place un serveur web HTTPS : elle crée une clé publique et une clé privé et envoie un **certificat numérique** à une autorité de certification.

4) Architecture de confiance

Certificat numérique :

- 1 clé publique
- Des informations d'identification (adresse, mail, teléphone…)
- 1 signature éléctronique

4) Architectures de confiance

Les services d'une IGC :

- Communication entre serveurs et navigateurs
- Accès aux bases de données
- Accès aux VPN
- Echange par courriers éléctroniques
- Procédures administratives en ligne.
- ….

4) Architectures de confiance

Les fonctions d'une IGC :

- Générer aléatoirement des couples de clés
- Gérer les certificats numériques
- Publier les clés publiques
- Certifier les clés publiques par signature des certificats numériques
- Permettre le recouvrement des clés de cryptage

4) Architectures de confiance

Le fonctionnement de l'IGC :

- Une infrastructure technique (matériel et logiciels adaptés)
- Un ensemble d'acteurs du processus de certification
- Une politique de certification

Sécurité Informatique

1) Contours de la sécurité informatique

2) Les menaces

3) Définir une politique de sécurité

4) Signature éléctronique

5) **Perspectives sur la sécurité informatique**

5) Perspectives

- Les nouveaux risques sur les processus industriels => recherche de points d'entrées pour la manipulation des processus industriels.
- Le cas de l'externalisation des données
- Cryptographie quantique.