Sécurité des appareils et applications mobiles

Auteur
Jean-François Casquet

Editeur
AZERTY Microsystem

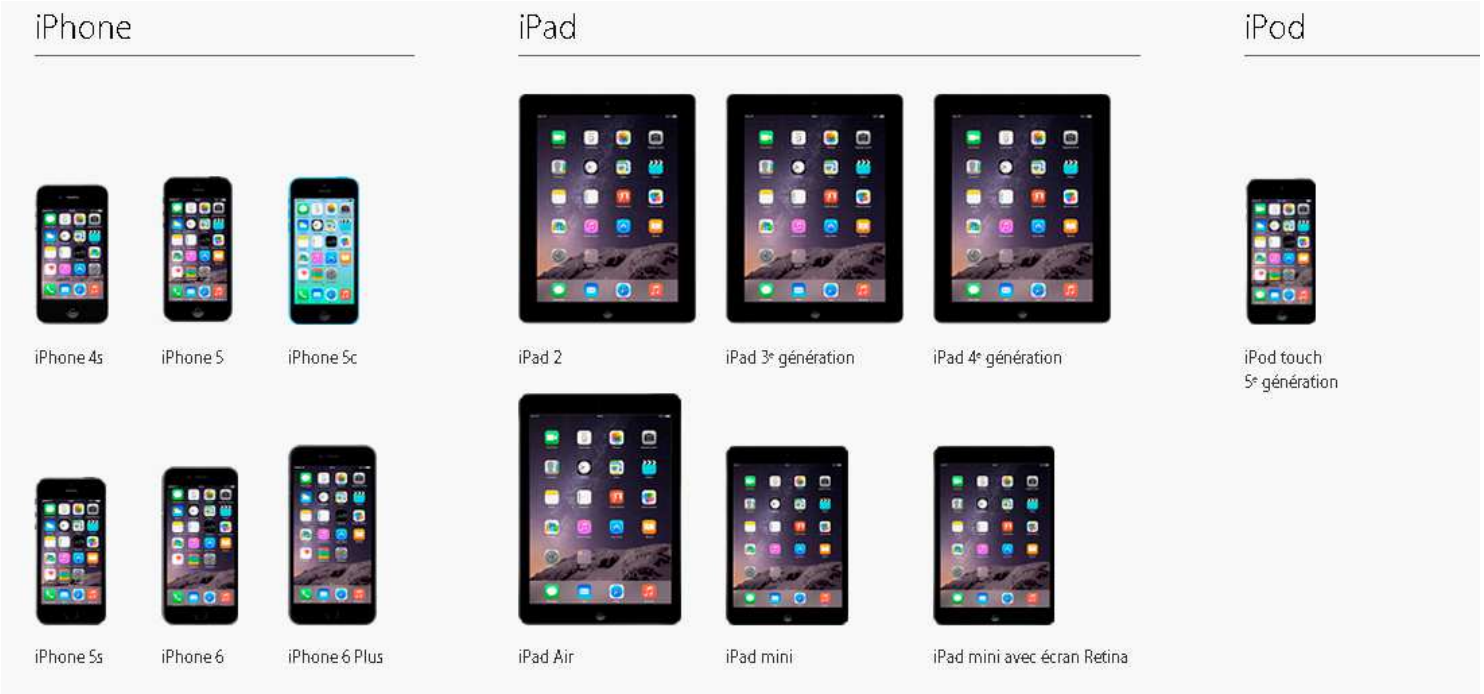
www.65120.net/stage/

iOS (jadis iPhone OS) est le système d'exploitation mobile développé par Apple pour l'iPhone, l'iPod touch, et l'iPad.
Il est dérivé de Mac OS X – basés sur LINUX.
Ce système d'exploitation n'avait aucun nom officiel avant la publication du kit de développement iPhone (SDK) le 6 mars 2008. Jusqu'à cette date, Apple se contentait de mentionner que « l'iPhone tourne sous OS X » une référence ambiguë au système d'exploitation source d'iOS, Mac OS X. Ce n'est qu'à cette occasion que Scott Forstall présenta l'architecture interne du système d'exploitation, et dévoila alors le nom d'iPhone OS5. Ce nom a été changé le 7 juin 2010 pour iOS6.
Le kit de développement en question, disponible pour Mac OS X, propose les outils nécessaires à la création d'une application pouvant tourner sous iOS. Si son téléchargement et son utilisation sont gratuits, la publication (et commercialisation) d'application nécessitent une adhésion et des frais au bénéfice d'APPLE STORE. Il n'en demeure pas moins que cette offre peut s'avérer intéressante pour bon nombre de développeurs, étant donnée la taille du marché créé par iOS.

ANDROID : L'Entreprise d'informatique qui a créé ce système s'appelait Androïd… Google a donc gardé le nom de l'Entreprise qu'ils ont acheté en 2005.
Système basé sur LINUX et fonctionnant sur architecture ARM (au départ). Maintenant, Androïd se voit sur ATOM (Samsung sort ses Galaxy Tab sur ATOM avec Androïd).

Windows Phone : Microsoft a développé ce système d'exploitation sur processeur ARM – Depuis 2016 le projet est arrêté par Microsoft pour s'orienter vers Surface-Phone. Tablette qui téléphone…

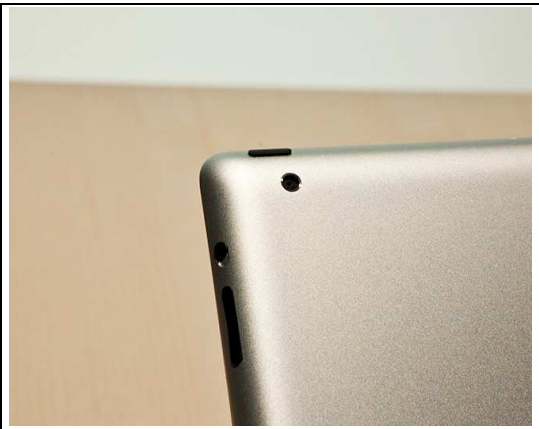
Le iphone est beaucoup moins puissant que le iPad – un processeur plus important a été placé dans les iPad afin de garantir une fluidifier.



Il s'agit d'une « grosse clef USB » qui a les mêmes failles (propagation de virus) et qui peut se faire contaminée (chiffrement des données contenues) – il s'agit d'un ordinateur connecté au réseau presque tout le temps … sans contrôle réel des flux …
En appuyant sur plusieurs touches en même temps (suivant les appareils), nous rebootons l'appareil et nous pouvons prendre le contrôle des données… ou le faire retourner en état d'usine !

2 Modèles différents : WIFI seul et WIFI + 3G/4G **poids :** Wifi : 601g Wifi + 3G : 613 g	
Ecran Est-ce que, demaine, nous serons avec des écrans en réalité augmentée ? ?	Écran Multi-Touch panoramique brillant rétroéclairé par LED de 9,7 pouces (diagonale visible) avec technologie IPS Résolution de 1 024 x 768 pixels à 132 pixels par pouce (ppp) Revêtement oléophobique résistant aux traces de doigt Affichage simultané de langues et de jeux de caractères multiples
Processeur A5 par Samsung Puce A5 bicœur Apple 1 GHz hautes performances et basse consommation	

<table>
<tr>
<td>Caméra arrière :
vidéo en HD (720p) 30 im/s + audio
appareil photo avec zoom numérique 5x
Caméra avant :
vidéo VGA (640p) 30 im/s + audio
appareil photo de qualité VGA

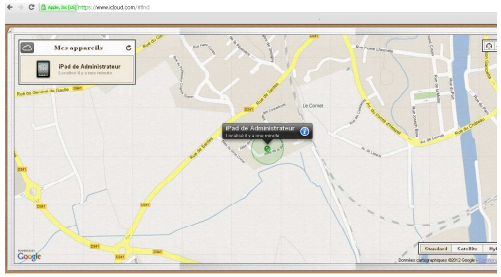
Géolocalisation des photos et vidéos</td>
<td>  
</td>
</tr>
<tr>
<td>Batterie :
lithium-polymère intégrée de 25 Wh
Jusqu’à 10 heures d’autonomie pour naviguer sur Internet en Wi-Fi, regarder des vidéos ou écouter de la musique
Charge via l’adaptateur secteur ou le port USB de l’ordinateur</td>
<td>  </td>
</tr>
</table>

Sorties :

Connecteur dock 30 broches
Prise minijack pour casque stéréo 3,5 mm
Haut-parleur intégré
Microphone
HDMI – Attention, l'écran s'ajuste au iPad (sur un écran panoramique, 2 bandes noires ajusteront l'image)

Capteurs :

Gyroscope à trois axes Accéléromètre Capteur de luminosité ambiante



Géolocalisation :

Wi-Fi
Boussole numérique
Est-ce que la géolocalisation est arrêtée lorsqu'on la lui demande ? *(cf Procès contre Microsoft)*

Vidéos :

Prise en charge du mode Recopie vidéo AirPlay sur Apple TV en 720p

Formats vidéo pris en charge : vidéo H.264 jusqu'à 1080p, 30 images par seconde, profil de référence jusqu'au niveau 4.1 avec son au format AAC-LC jusqu'à 160 kbit/s, 48 kHz, audio stéréo aux formats .m4v, .mp4 et .mov ; vidéo MPEG-4, jusqu'à 2,5 Mbit/s, 640 x 480 pixels, 30 images par seconde, profil simple avec audio AAC-LC jusqu'à 160 kbit/s par canal, 48 kHz, audio stéréo aux formats .m4v, .mp4 et .mov ; vidéo au format Motion JPEG (M-JPEG) jusqu'à 35 Mbit/s, 1 280 x 720 pixels, 30 images par seconde, audio au format uLAW, audio stéréo PCM au format de fichier .avi

Beaucoup d'applications permettent de regarder des contenus … mais ces applications ne sont pas souvent sécurisée !

IPhone :

Écran Retina Écran panoramique Multi-Touch de 3,5 pouces (diagonale) Résolution de 960 x 640 pixels à 326 ppp Contraste 800:1 (type) Luminosité maximale de 500 cd/m^2 (type) Revêtement oléophobe résistant aux traces de doigt à l'avant et au dos de l'appareil Affichage simultané de langues et de jeux de caractères multiples

Appareil photo 8 mégapixels :

Autofocus

Mise au point par toucher

Détection des visages sur les photos – **reconnaissance faciale** !

Est-ce que la caméra est arrêtée ?

Enregistrement vidéo HD (1080p) jusqu'à 30 images par seconde avec audio

Stabilisation vidéo

Photos et vidéos en qualité VGA jusqu'à 30 images par seconde avec la caméra frontale

Géoréférencement des photos et vidéos

Le JailBreak (évasion de prison), sont des logiciels à importer dans l'appareil APPLE (iPhone, iPad …) afin de « casser » les verrous qui empêchent les usagers de se connecter à d'autres logiciels que ceux proposés (validés, « encaissés ») par APPLE (APPLE-STORE).
En réalité, JailBreak ont été développés avant APPLE-STORE et, à l'époque, ces outils étaient incontournables… aujourd'hui, des milliers d'applications (même gratuites) sont sur APPLE-STORE alors pourquoi aller plus loin ?

Avantages du JailBreak :

- Toutes les limitations données par APPLE tombent.
- Bluetooth devient compatible avec tous les appareils.
- Il devient possible d'installer n'importe quel logiciel.
- Un appareil acheté à l'étranger peut être reprogrammé.
- Les compatibilités problématiques sont contournées (flash player fonctionne avec d'autres navigateurs que SAFARI) …

Inconvénients du JailBreak :

- En réalité, il y a des inconvénients étranges – et pourraient être considérés comme des avantages dans certains cas.
- Le logo APPLE est remplacé par un ananas !
- Le déverrouillage permet d'installer n'importe quoi (compatible avec APPLE quand-même) – souvent des applications mal faites qui font ralentir ou planté l'appareil.
- Ouvre certaines fonctions (Bluetooth) – avec aucun contrôle de sécurité.
- L'appareil devient un « serveur SSH » avec nom et mot de passe standard (root / alpine) !
- JailBreak n'est pas désinstallable – il faut vider et repartir à zéro pour retrouver l'état d'origine.

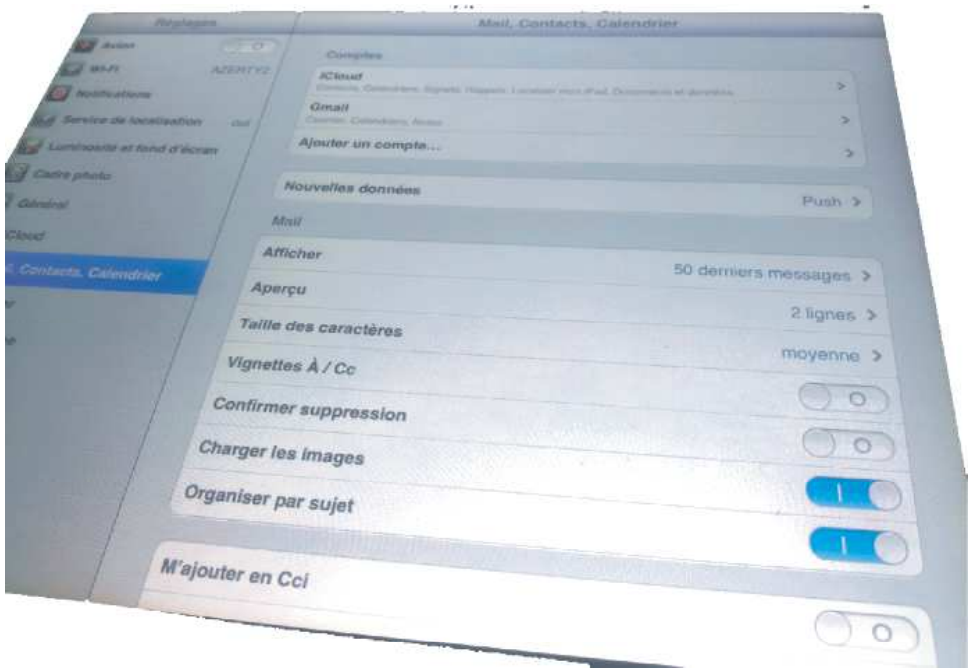
Les failles liées aux **navigateurs** sont moins probantes que sur Windows mais elles existent sous forme d'applications SAFARI existe aussi sous MAC et windows.
IPad et iPhone permettent de surfer avec d'autres solutions (officellement) : OPERA par exemple.

La gestion des mails est très ressemblante maintenant sur tous les systèmes. Ils sont généralement stockés sur une plate forme externe (CLOUD). Que dire de la confidentialité des Mails et des documents ?

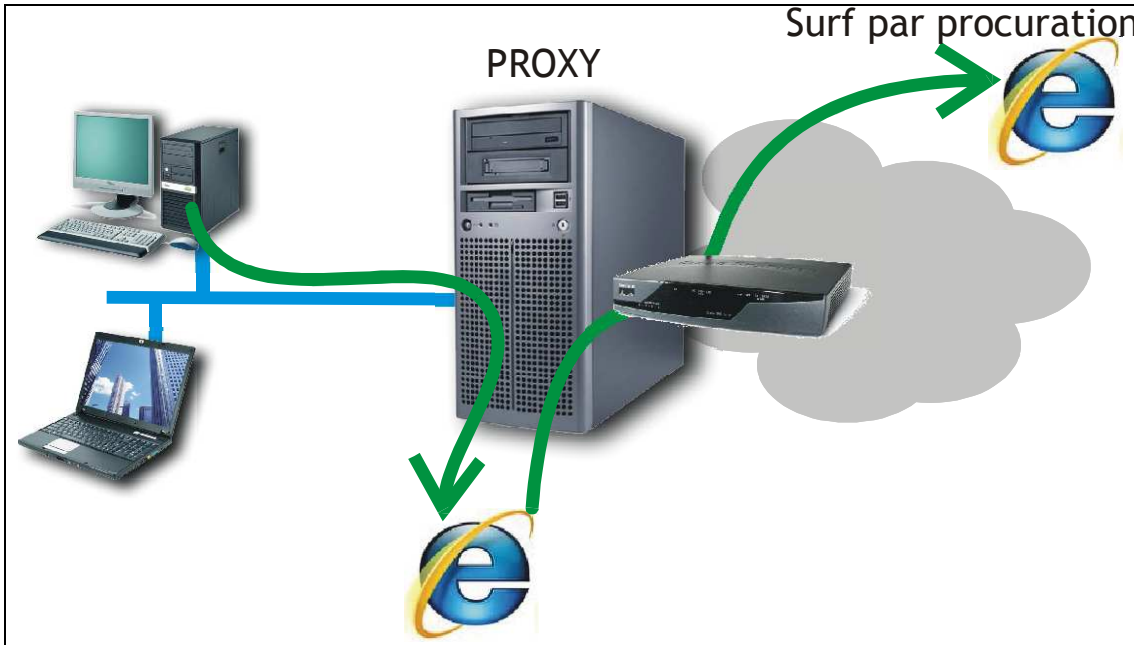
La seule interface autorisée par APPLE est iTunes (produit compatible Windows/Mac et gratuit)

ITunes ne fonctionne pas sous LINUX (sauf sur Wine ou en virtualisation biensûr).

Sur iPad ou iPhone, il suffit d'aller dans les « Réglages »…



Protection par Proxy / Web Mail / Cloud …



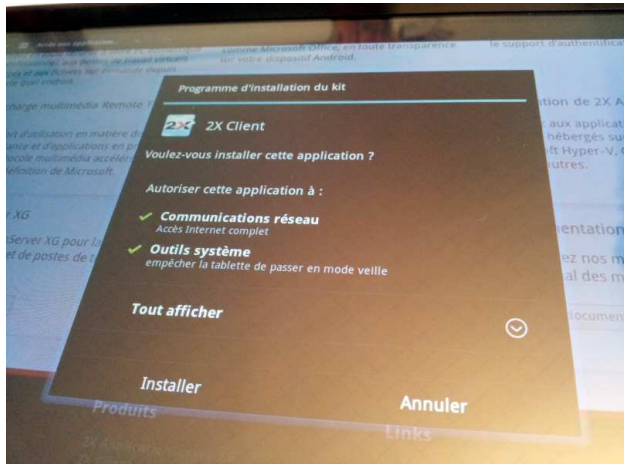
L'utilisation d'un proxy a plusieurs avantages :

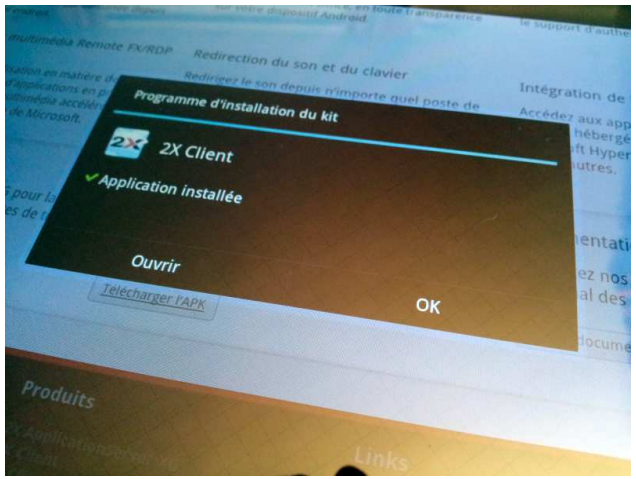
1. Le surf se fait par procuration (nous restons totalement cachés derrière le proxy)
2. Les pages (images…) déjà récupérées ne le sont pas à chaque fois – le proxy met en mémoire les éléments
3. Surveillance des sites visités
4. Protection contre les virus

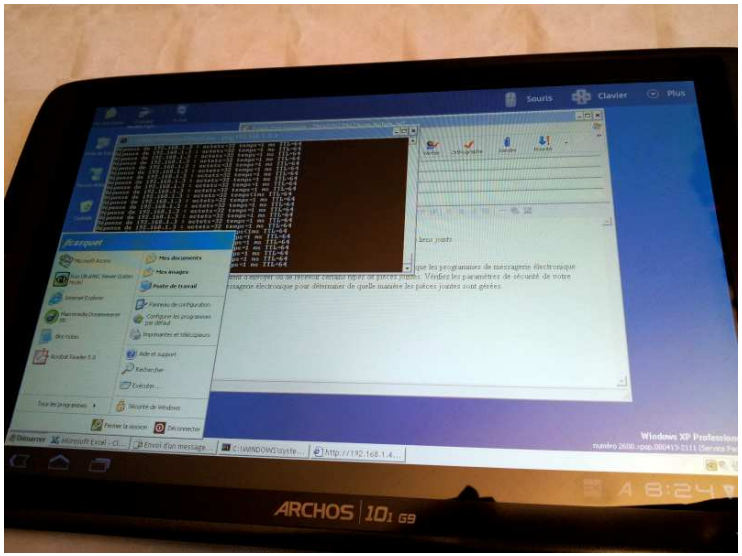
5. Accélération su surf grâce au redimensionnement des images par rapport à l'affichage

6. Permet (en passant de proxy en proxy) de traverser des réseaux qui ne se verraient pas entre eux.
7. cacher son identité réelle (SHADOW)

Ici, nous allons utiliser un client TSE appelé Client 2X (autorisé par tous les market gratuitement … même sur iPad)
Bien sûr, il existe les autres clients du même type – Citrix …



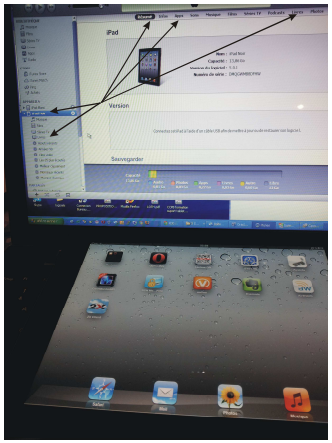




Airwatch, Good Technology, MobileIron, itunes, MaaS360 (IBM)

Les solutions proposées sont des solutions de synchronisations et de validation des échanges sécurisés pour gérer une flotte de tablette …

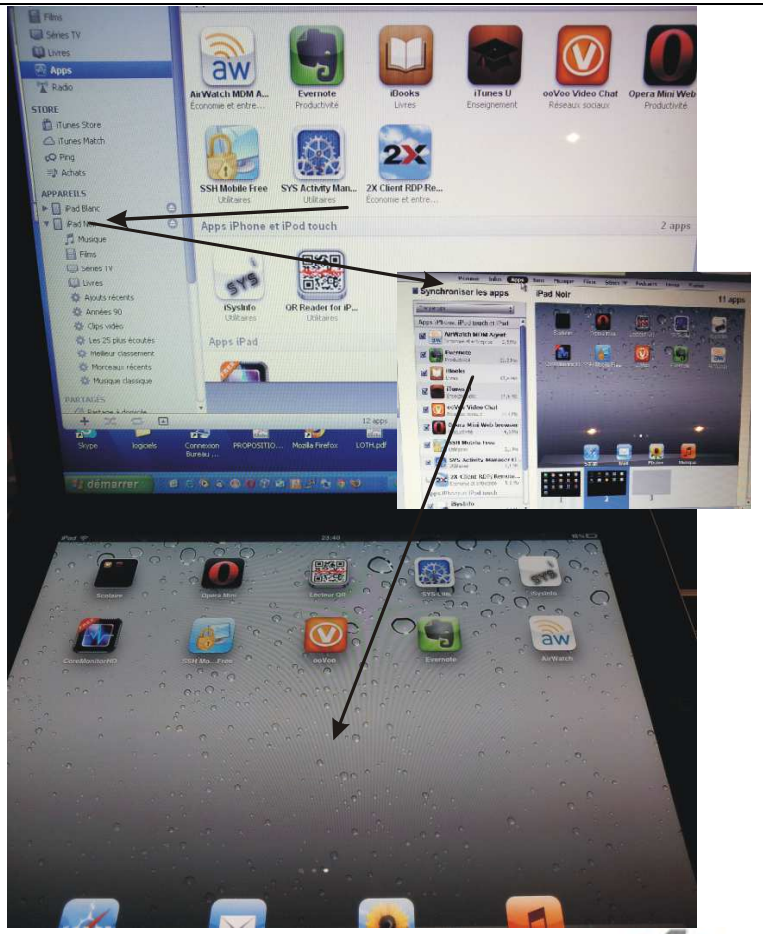
En choisissant iTunes, il faut brancher d'abord l'iPad sur port USB – iTunes exige pour reconnaître la tablette.



Toutes les applications sont dans Apps de la Bibliothèque.

En choisissant l'appareil, puis le menu « apps » en haut de l'écran, nous choisissons les applications de Apps qui doivent être placées sur cet appareil.

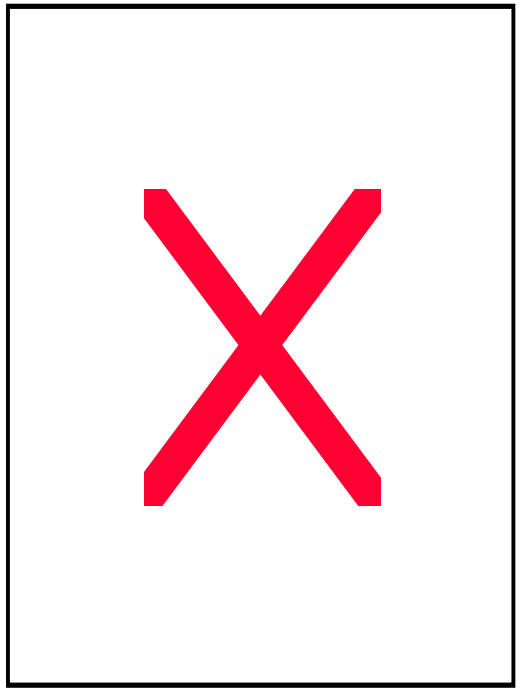
Un soucis, toutefois. Les appareils n'apparaissent QUE s'ils sont connectés (au Wifi ou en USB).
Appareil en veille se connecte toutes les heures.

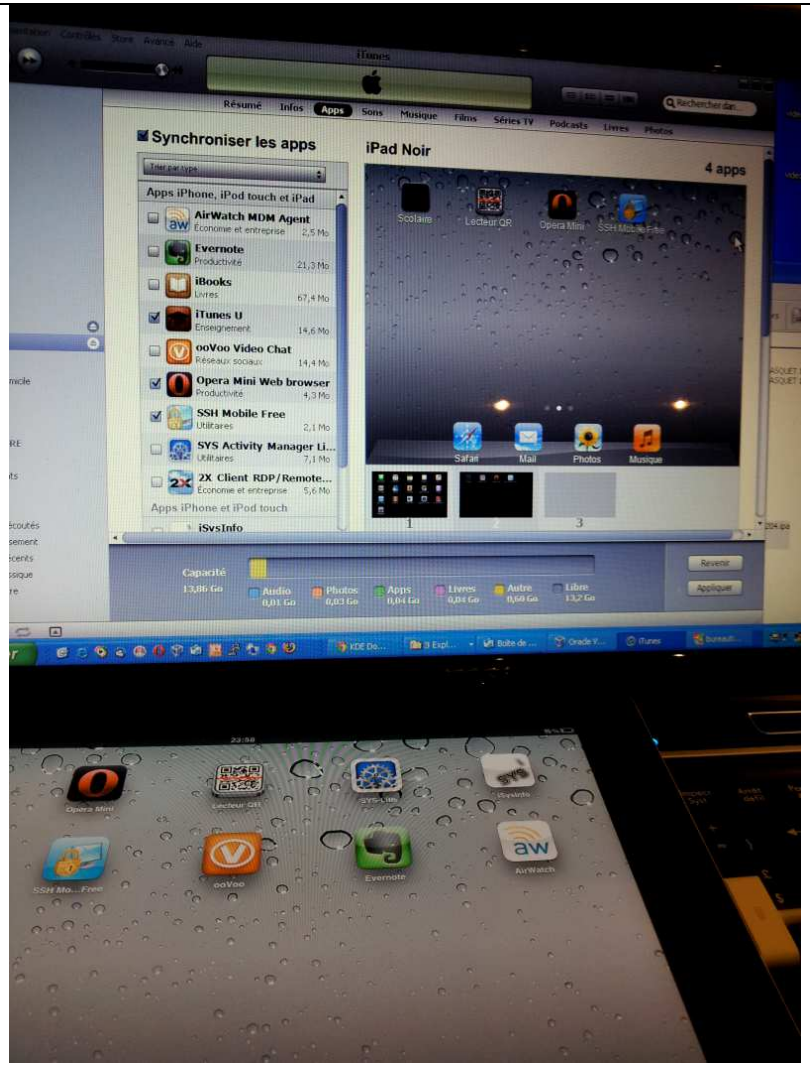


Sélection des Apps à synchroniser.

Les Apps ont celles de la Bibliothèque et il suffit de sélectionner avec des cases à cocher.

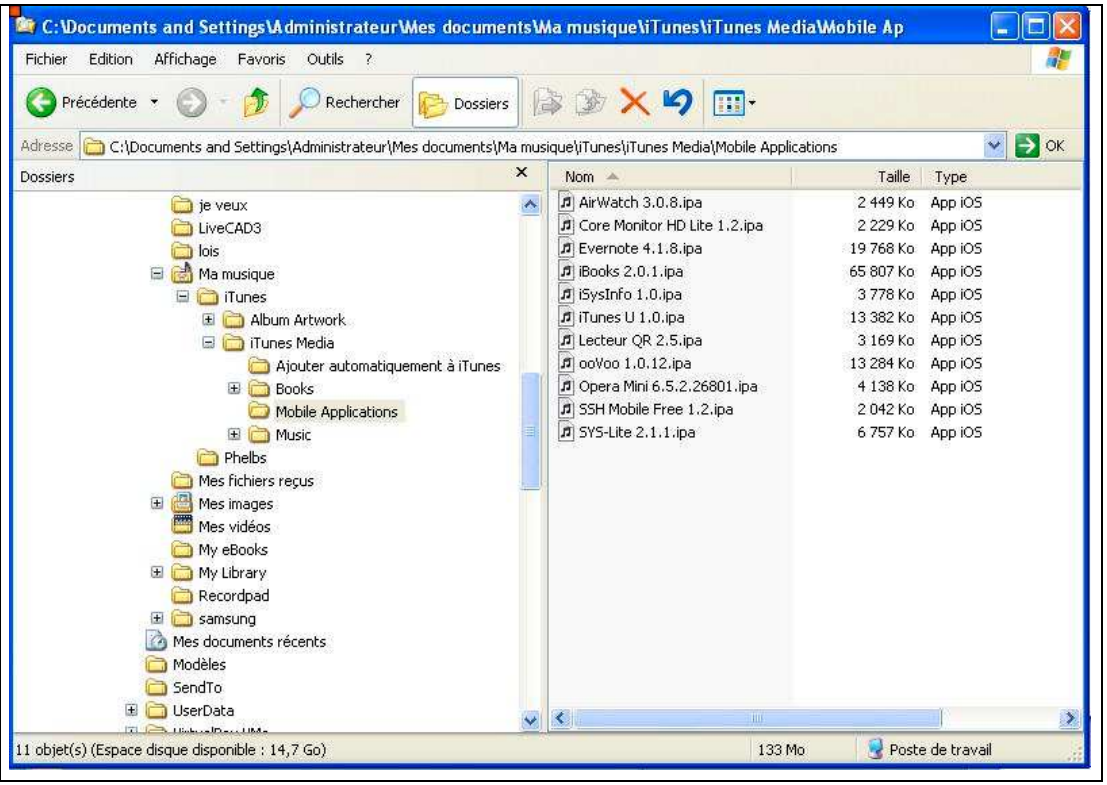
En décochant une Apps, iTunes précise que l'application sera désinstallée avec ses données.

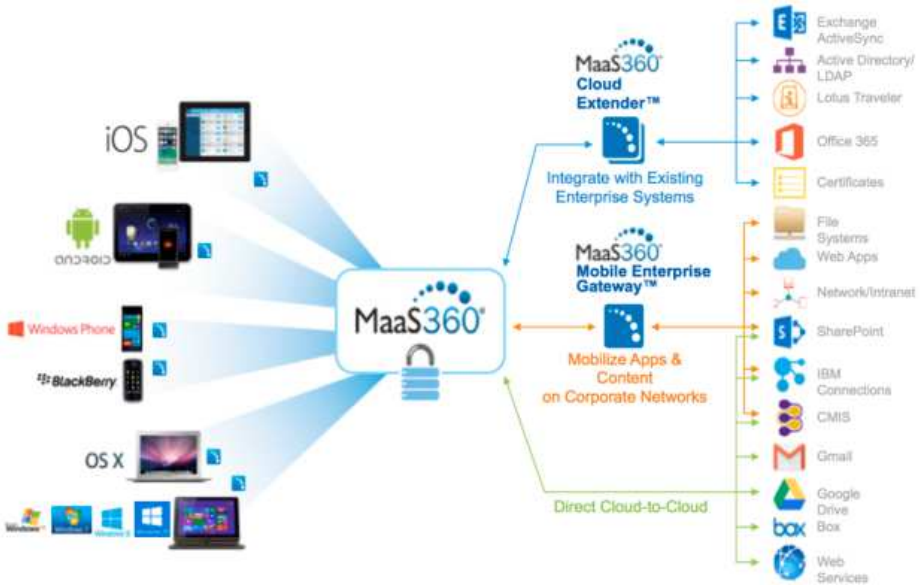




Les fichiers synchronisés sont stockés sur l'ordinateur (ici, un Windows XP)

Un dossier particulier est présent :
« Ajouter automatiquement à iTunes »
Ce dossier permet de signaler au synchronisateur qu'il faut envoyer le contenu à l'appareil (aux appareils).
Nous pouvons y mettre PDF, jpg, ipa (application)…

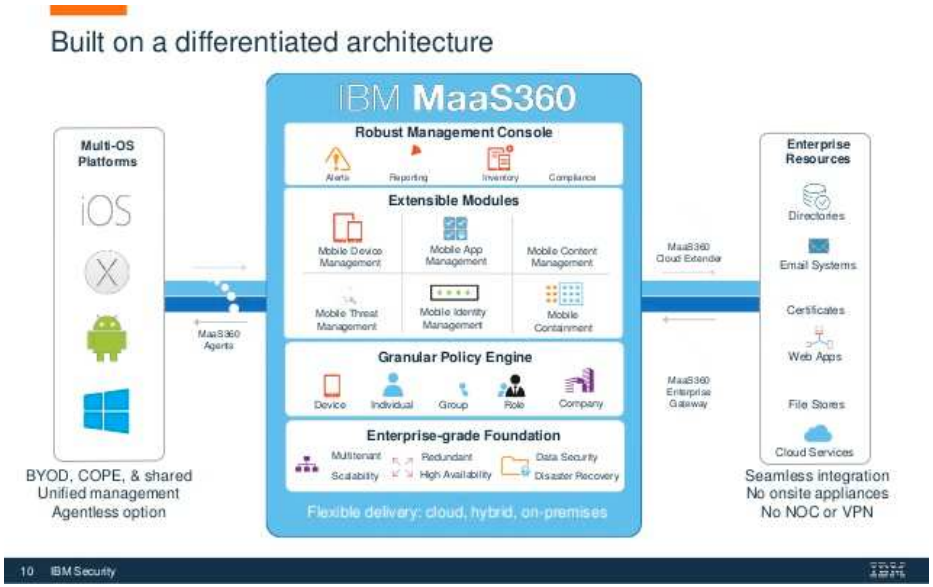




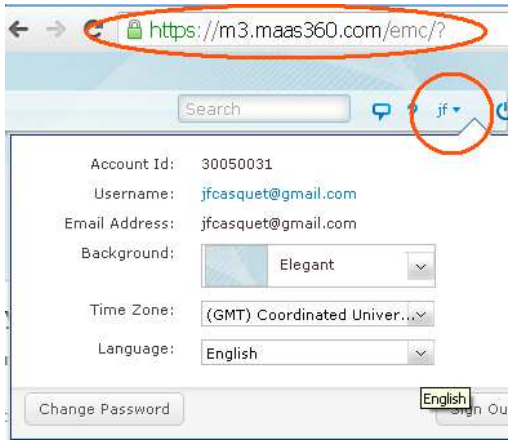
MaaS360 sait gérer aussi les Kindle d'Amazon. Bien sûr avec moindre fonctionnalités.

Microsoft s'annonce en direction de surface et surface-phone en abandonnant son Windows-phone qui a été un échec.

MaaS360 touche tous les terminaux et toutes les entreprises !

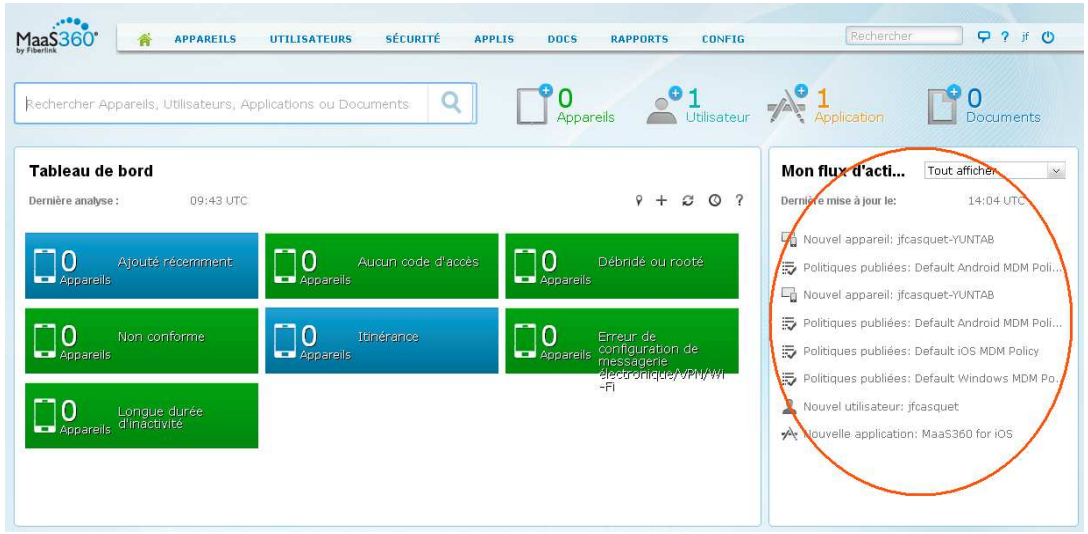


Connexion et interface



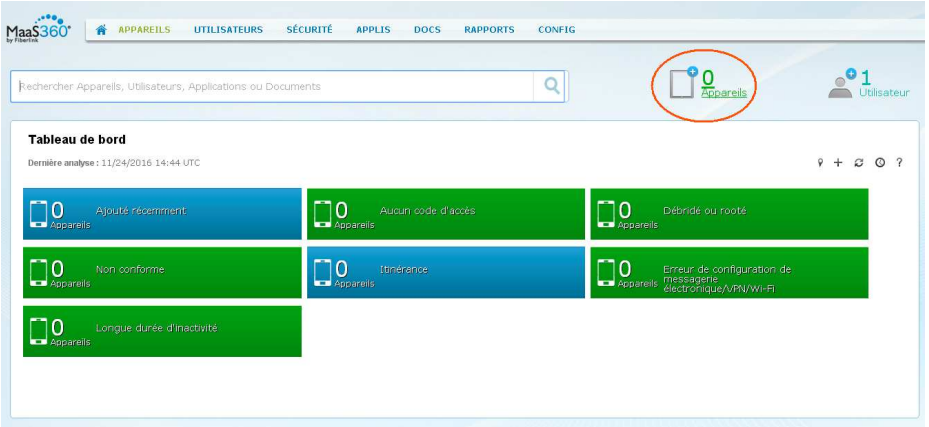
Pour se connecter sur l'interface – tout se passe sur un navigateur.

En haut à droite, nous avons la possibilité de changer quelques informations personnelles. Pour faciliter la navigation.

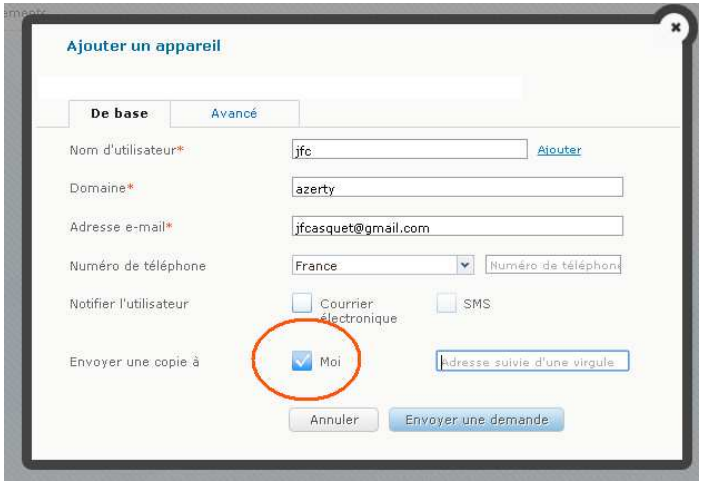


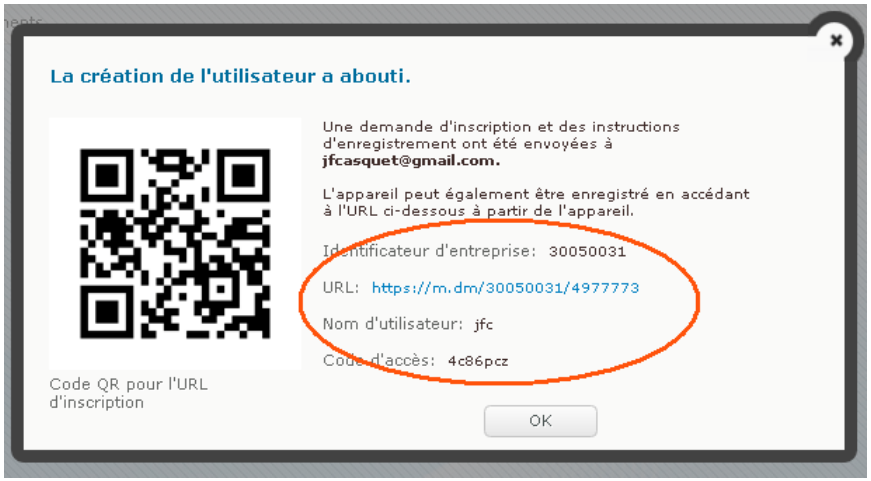
Une interface qui permet de voir toutes les informations principales et le journal des derniers évènements…

Inventaire des mobiles



Sur l'interface, nous choisissons « appareils » puis « inventaire »

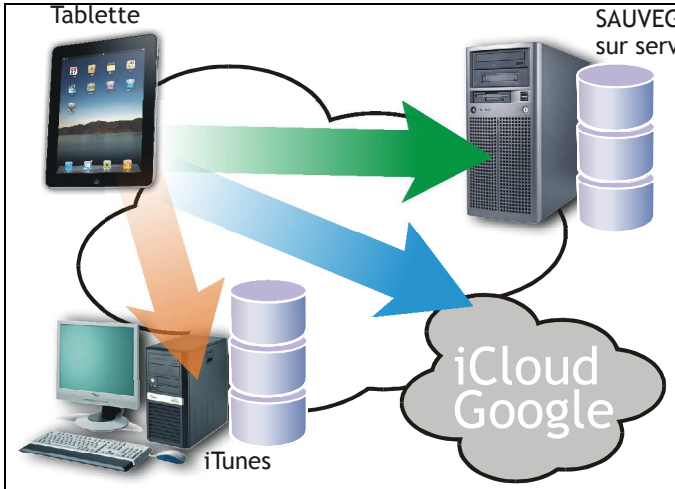
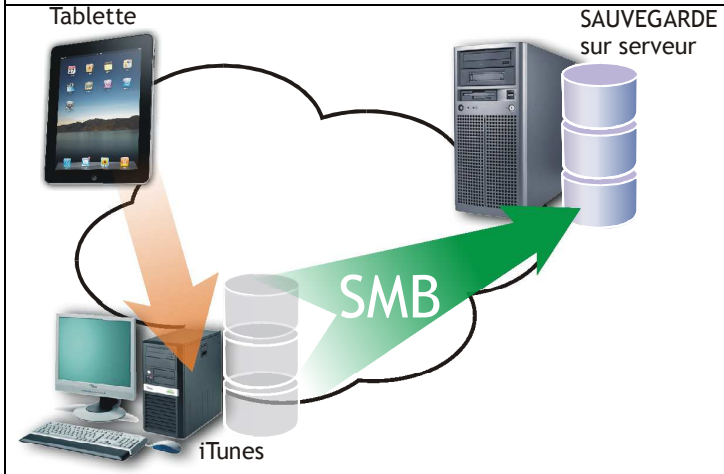


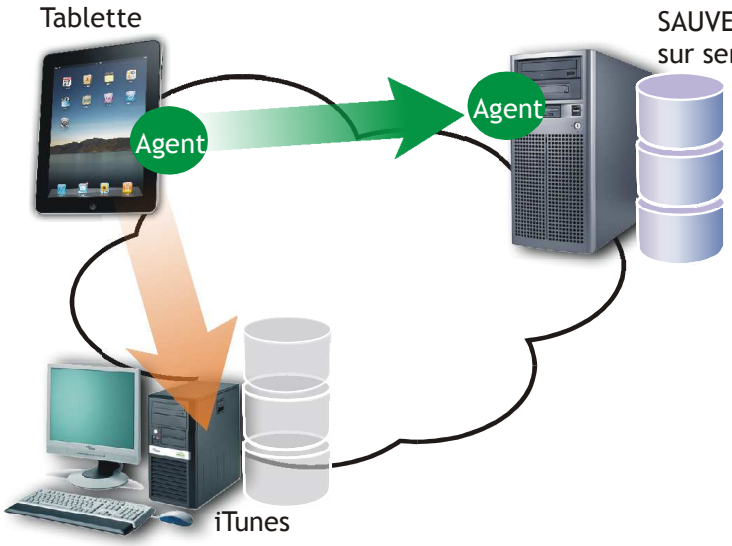


Sur la tablette, il est nécessaire d'avoir un compte GooglePlay.

Avec un lecteur QR-Code ou en tapant l'adresse URL : https://m.dm/{client}/{numéro de tablette}

Notre objectif, dans cette annexe, est de proposer une solution de centralisation des informations stockées sur les tablettes.

	Première solution : Utiliser iTunes en synchronisation vers les 3 solutions habituelles. iTunes qui synchronise vers un PC (ou Mac) et vers le iCloud
	Une autre possibilité simple à mettre en place, utiliser un Serveur NAS auquel est connecté les iTunes de l'entreprise
	La solution professionnelle consiste à installer un produit (agent) sur



les SmartPhones, iPad et andoïd.

Absolute MANAGE
airwatch
AMTELNET
Profile Manager
BoxTone
casper
smartMan
DME
FancyFon
MaaS360 by Fiberlink
filewave
Good
McAfee
MFORMATION
MobileIron
MobileNX Enterprise Suite
NOTIFY TECHNOLOGY
ROBOT CLOUD
SOTI.net
SYBASE
Tangoe
TARMAC
ZENPRISE

SÉCURITÉ PAR LA GESTION DES APPAREILS MOBILES (MDM)

Description des caractéristiques communes des solutions MDM (Mobile Device Management) :

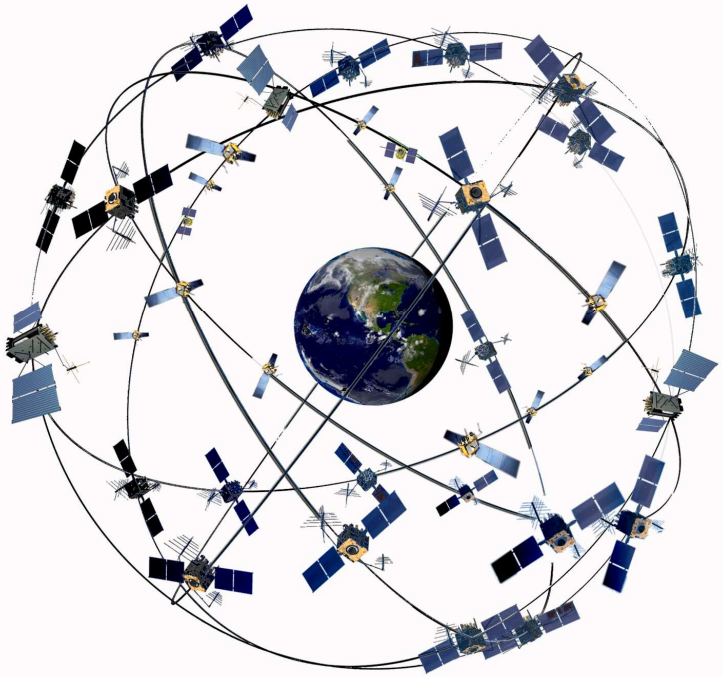
prise en main à distance
géolocalisation des terminaux
vérification de conformité
installation d'applications
Gestion des tailles de disques
Vétusté des appareils
Gestion des versions des OS (Operating System : Systèmes d'exploitation)
Destruction des données à distance
Verrouillage des appareils et des données à distance (en cas de vol)

Renforcement des couches logicielles (SE Android) et création de la Trust Zone (étanchéité)

Un application installée sur un système … en toute volonté … n'a pas forcément le droit de faire n'importe quoi … Car elle pourrait être vulnérable.
La couche SE de linux a été importée sur Androïd. Le noyau ne vérifie pas que le droit de l'utilisateur, mais aussi le comportement de l'application qui veut faire quelque chose.

Suivi de consommation

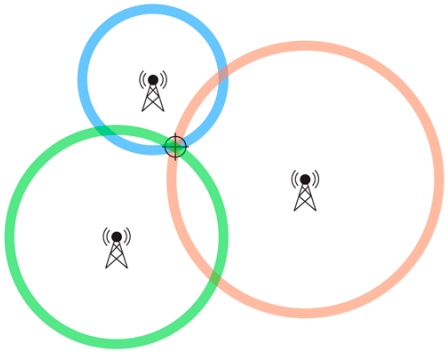
Le suivi des consommations en bande passante (data), en communication téléphonique, SMS, MMS …
La traçabilité des volumes de consommation permet de détecter un changement de comportement : donc, de détecter une intrusion …



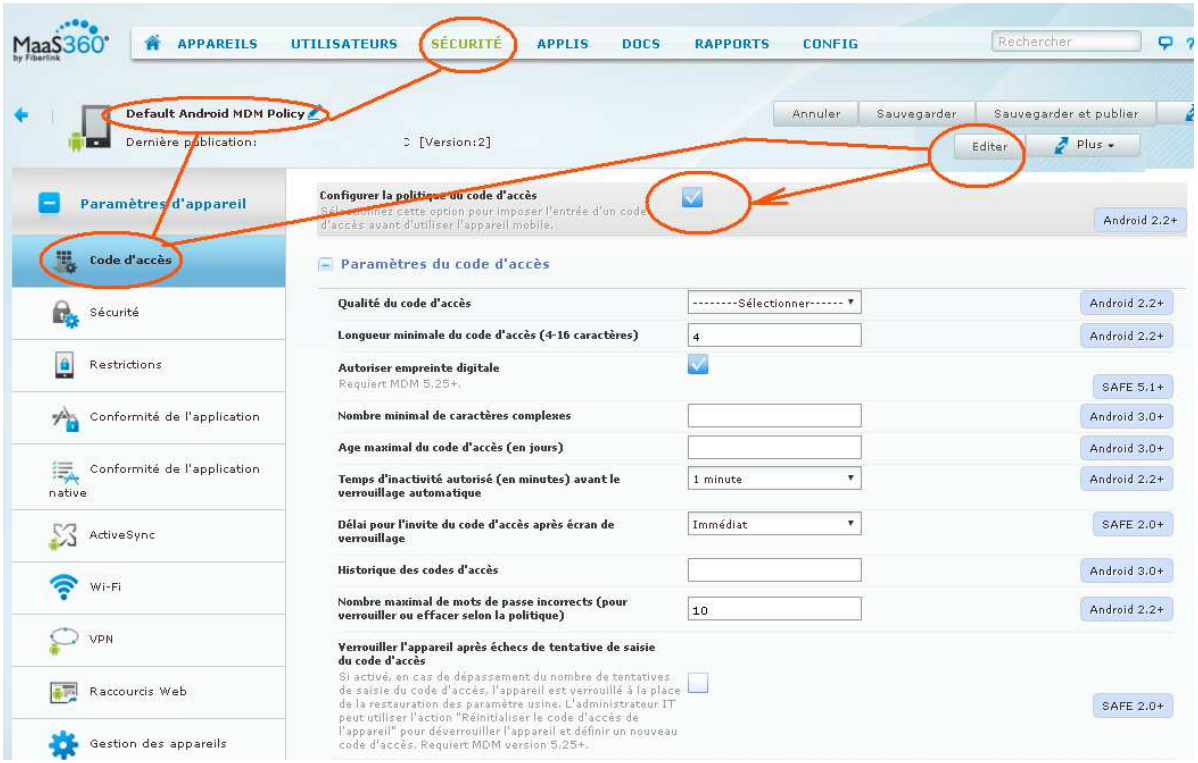
Chaque satellite transmet l'heure et des identifiants.
Ainsi, en recevant l'heure envoyée et l'heure actuelle, le récepteur connaît alors la distance entre lui et ce satellite.
En croisant cette information avec plusieurs satellites, nous trouvons notre position sur la terre.

Mais pour que cette position se transforme en cartographie, il nous faut des cartes terrestres ou des cartes récupérables par 3G/4G chez Google (par exemple).
Google profite de la géolocalisation GPS pour noter (au passage) les niveaux de réception des WIFI alentour. Ainsi, le calcul peut se faire à l'envers .. juste avec du points d'accès wifi ;

Géolocalisation Sans GPS :



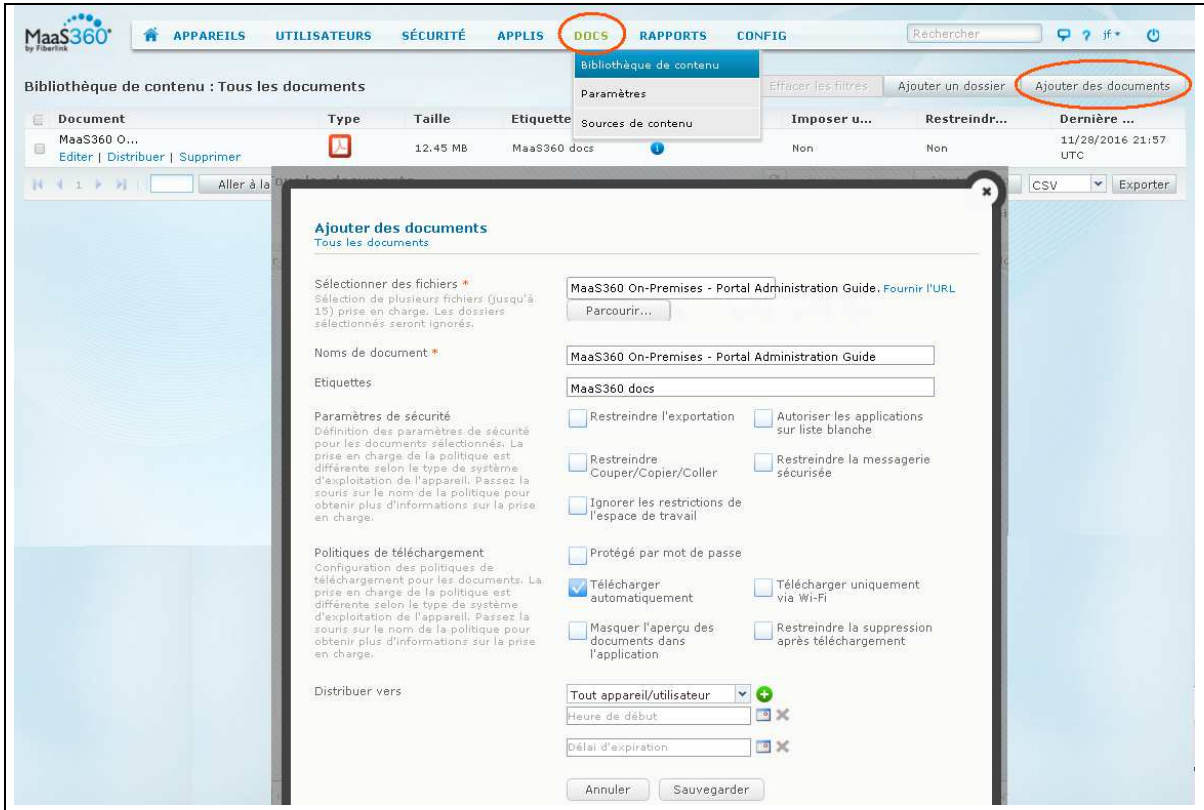
Gestion des restrictions



Il est possible d'imposer une politique de gestion des mots de passe et du verrouillage du terminal

D'autres restrictions se trouvent dans le menu « restrictions »

Gestion des droits sur fichiers et dossiers



Pour charger un document à propulser sur les terminaux, il suffit de l'envoyer sur le serveur MaaS360. Puis, choisir les destinataires et déterminer la politique associée au document.

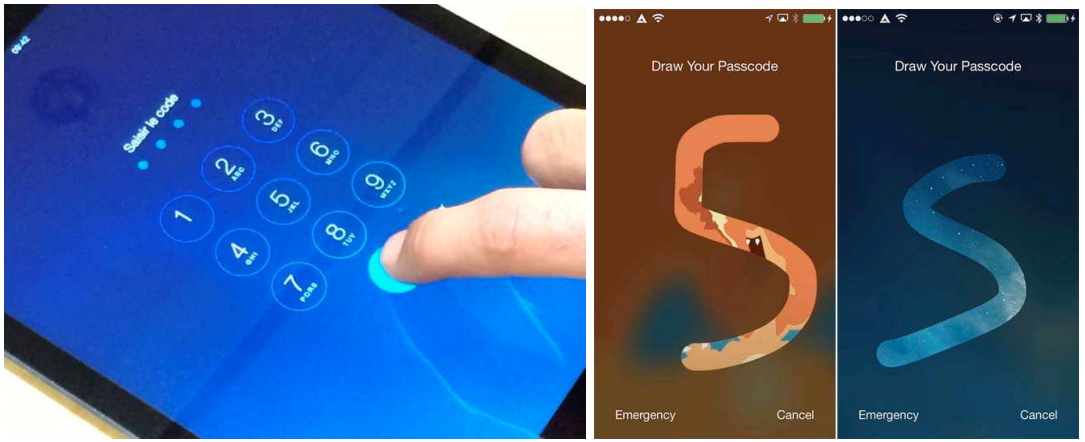
Attention, le document sera donc chez MaaS360.

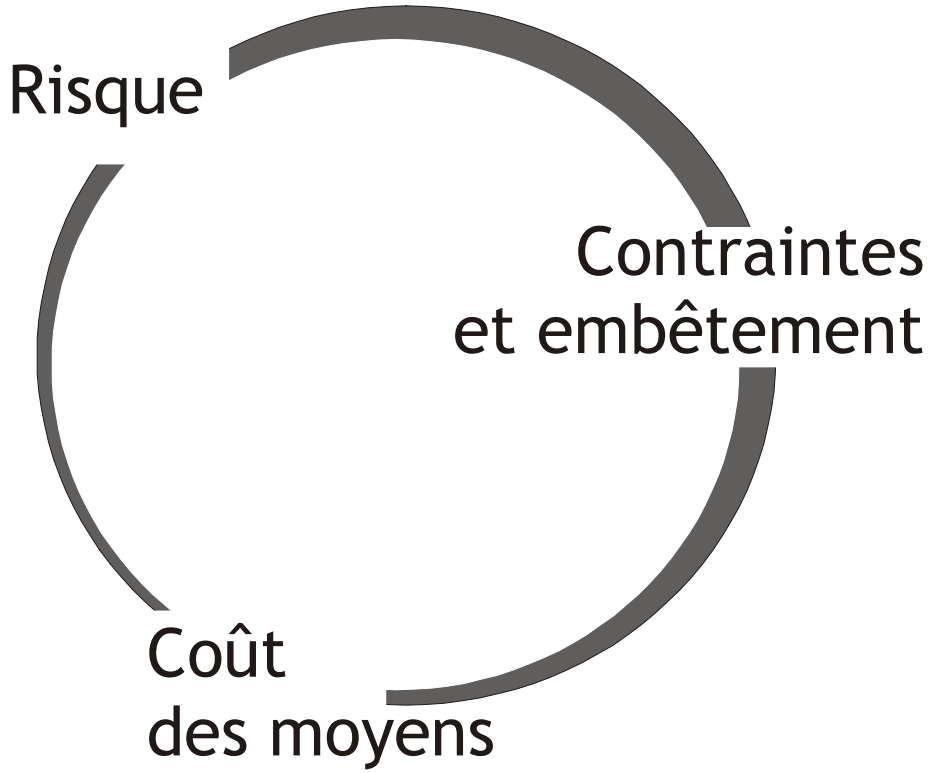
IBM garantit le chiffrement des documents envoyés.
Actuellement, il y a 2 datacenter en Europe :
Irlande et Suède
Il est prévu dans les prochains mois d'avoir un datacenter en France

Utilisation limitée aux zones géographiques (exemple de solution)

Les nouveaux outils utilisent les concepts de « traçabilité ». La position géographique de l'appareil entre de le circuit de validation et d'ouverture des droits à l'utilisation des applications et des données.
Google, par exemple, émet une alerte si l'on se connecte à des distances trop éloignées en un temps trop court.
Les paiements CB sur internet sont soumis aux mêmes vérifications…

Les ouvertures de sessions se font par code PIN au démarrage, mais il faut y ajouter des codes :





Risque : de perte / destruction / divulgation / altération / inaccessibilité …

Contraintes : les moyens mis en place auront-ils de pratiques qui gêneront les usagers ? Si oui , ils contourneront les moyens mis en place !

Coût : nous pouvons toujours TOUT mettre en place. Pourtant, le coût est souvent le phénomène bloquant. Coût financier / Ressources / Moyens humains …

SÉCURITÉ PAR LA GESTION DES APPLICATIONS (MAM)

Description des caractéristiques communes des solutions MAM (Mobile Application Management) :

Le concept tient sur le fait que les applications doivent être autonome dans leur maintien « en vie » :

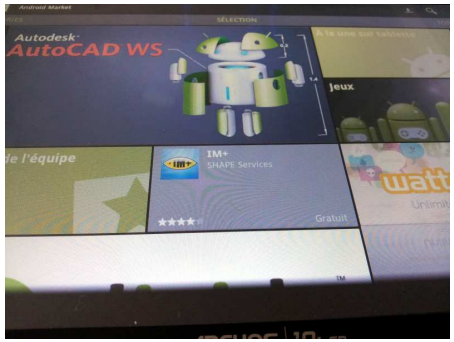
- mise à jour automatique des applications
- Application qui interdit à d'autres de s'installer
- installation interdite des Apps....
- verrouillage de certains fonctions (modification des paramètres réseaux, VPN, firewall …
- bascule de l'écran, connectivité à l'USB …

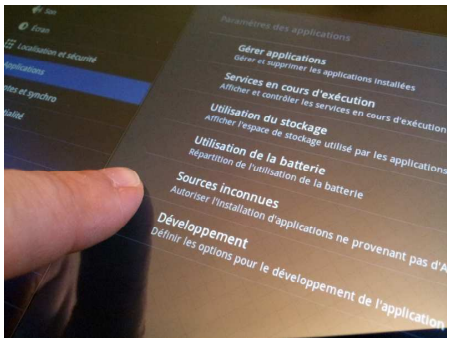
Isolation par les containers

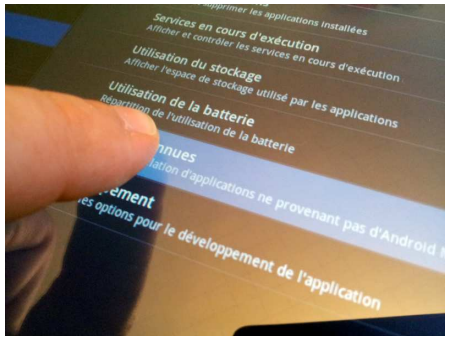
Des applications qui bloquent les autres applications « enfants » sont appelés des « conteneurs ». Ainsi, les applications dites « à risque » peuvent être installées avec moins de risque.

Apps Stores privés et autorisés

Il s'agit d'un endroit où tout le monde peut déposer des applications…
Ce n'est pas un critère de fiabilité !
Mais il est possible de charger des applications « autres » en autorisant la Tablette à le faire :

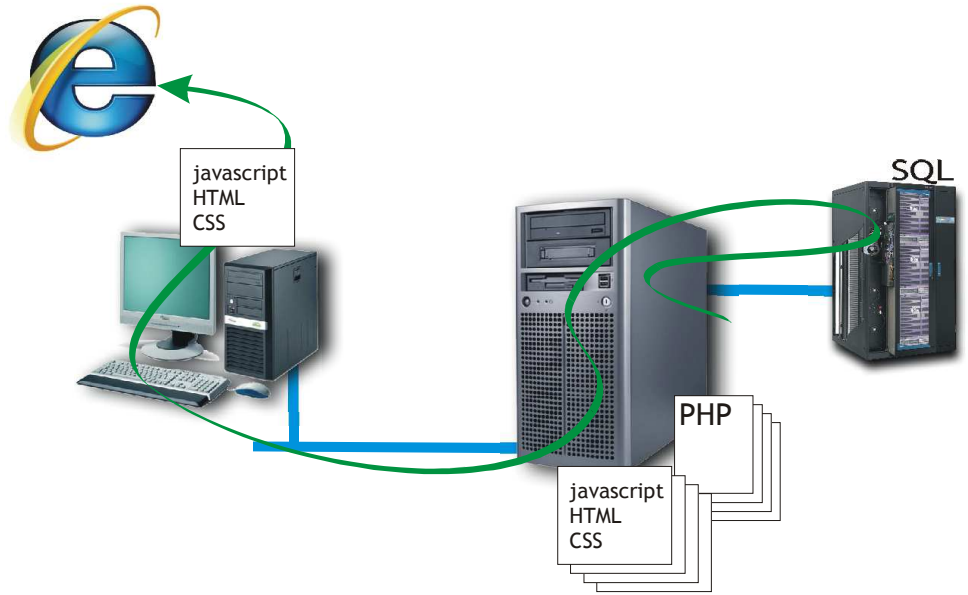






intégration des applications de l'écosystème par des API et connecteurs

Séparation des interactions entre les applications du terminal et du serveur



Métriques de qualité et critères principaux de choix

Le choix se fait souvent à cause d'impératifs :

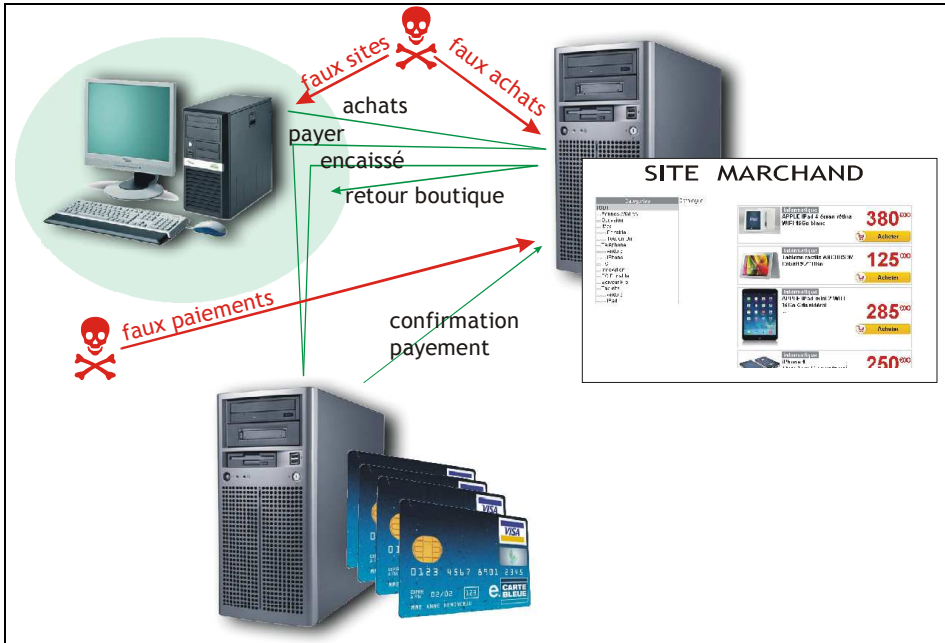
- Connectivité avec un flux constant ?
- Besoin de synchronisation entre la tablette et le serveur
- Besoin de gérer les périphériques directement (USB, GPS, WebCam …)
- Besoin de données totalement synchrone instantanément
- Possibilité de faire fonctionner des versions différentes en même temps
- Tolérance aux pannes et Load Balancing

SÉCURITÉ PAR LA GESTION DES CONTENUS ET DONNÉES (MCM)

Définition du MCM (Mobile Content Management)

Il s'agit de site internet applicatif qui sont adaptés à la taille et aux fonctionnalités des tablettes (et smartphone).
En effet, un lien peut être facilement cliqué mais il est plus agréable d'avoir une zone plus grande pour appuyer avec un doigt.
Cette manière de programmer une application s'appelle un MCM – ou CMS pour mobiles.
Par ailleurs, et à cause des solutions fluide d'aujourd'hui, les MCM utilisent des mécanismes (HTML5) qui évitent que les pages soient chargées à chaque clic mais que les informations bougent à l'intérieur à chaque événement…

Sécurité contre les fuites des données (DLP)



Aujourd'hui, le hacking est simplifié car beaucoup utilisent des CMS ou des outils "publics" avec des failles importantes.
En effet, en connaissant la faille d'un CMS, il est plus simple, voire automatique de le pirater et d'y placer un code de détournement, de la publicité, ou du Hacking pur !

Souvent, nous n'avons pas de recul sur le fonctionnement réel du CMS. Il est donc impératif de "courir" après les mises à jour de sécurité et de suivre à la lettre les préconisations de sécurités :

- Gérer le fichier .htaccess
- Supprimer les fichiers d'installation
- Mettre les droits sur les dossiers
- Installer des watchdog
- ne jamais laisser un dossier du site sans "index.php"
- créer vos propres pages d'erreur - pour ne laisser passer aucune info

Sécurité par la surveillance des activités (SIEM)

SEM (security event management)
ou **SEIM** (security event information management)
ou **SIEM** (security information and event management)
ou **SIM** (security information management)

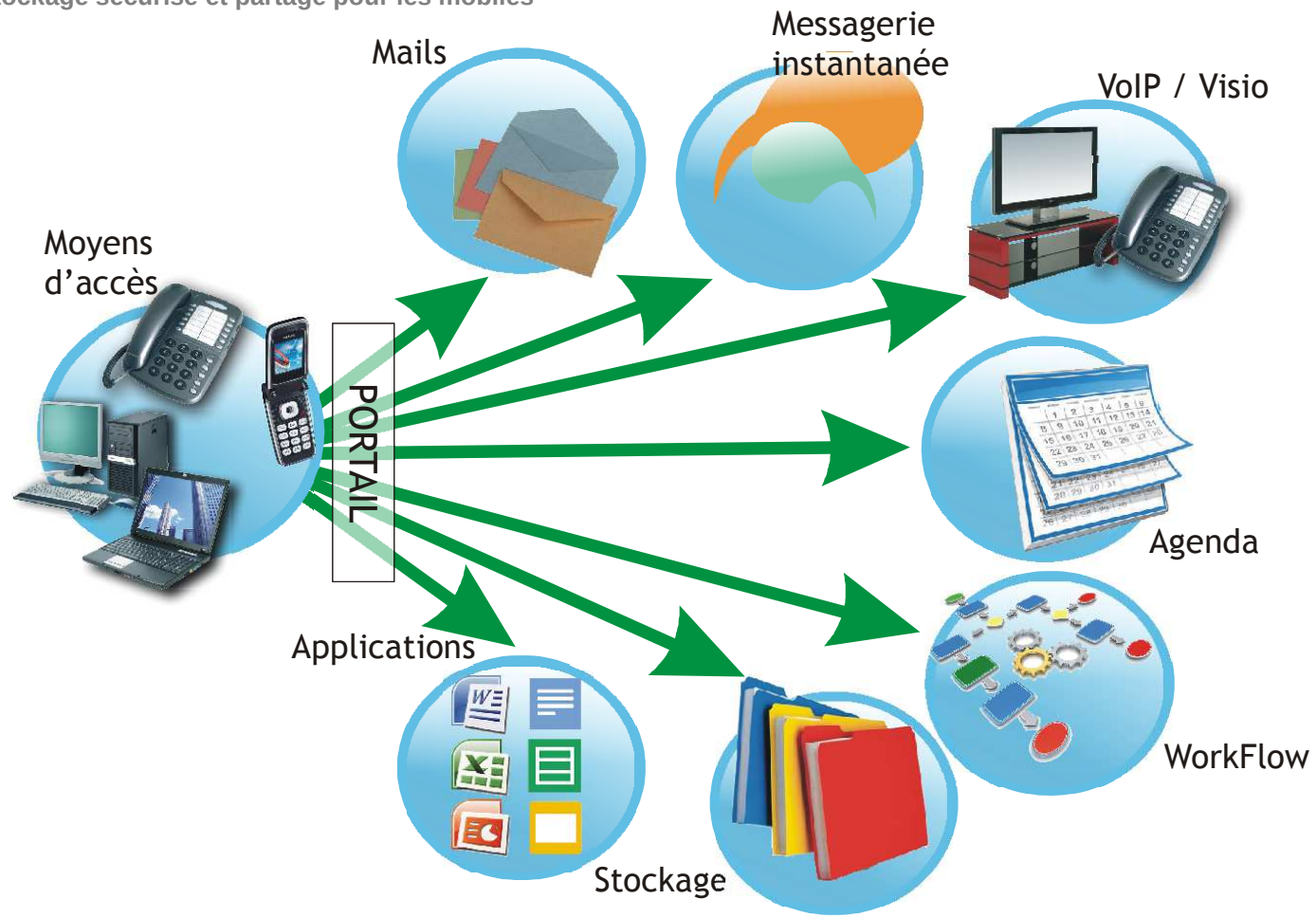
Les SIEM permettent grâce à la gestion des traces, des logs et des journaux :

- la collecte
- l'agrégation
- la normalisation
- la corrélation
- le reporting
- l'archivage
- le rejeu des évènements

Encryptions gérées des données (On Device Encryption FIPS 140-2 (AES))

Federal Information Processing Standard.

Aujourd'hui, la puissance de calcul des terminaux, nous permet d'envoyer des données chiffrées directement vers le navigateur ou l'application qui va déchiffrer à la volée.
Ce mécanisme est plus intéressant que le SSL ou le VPN qui ne chiffrent les données que sur le transport et pas en local sur l'interface.
Les applications peuvent être accréditées FIPS (par l'organisme américain d'accréditation). Tout Bug de sécurité fait perdre cette accréditation – c'est une évidence.



Questions de sécurité : où sont les données / que fait-on des disques HS / quel niveau de chiffrement des données dans le cloud / quelles solutions en cas de crash / sauvegardes et restaurations …

SÉCURITÉ DES MOBILES PERSONNELS DANS LE CADRE PROFESSIONNEL (BYOD)

Définition du concept BYOD (Bring Your Own Device)

Devenu une mode dans le monde entier !
Le principe est de dire « puisque vous avez un terminal et que vous vous en servez dans les transports, pourquoi ne pas s'en servir aussi au travail ? »
Ainsi, la solution technique mise en place serait utilisée en cas de télétravail, crise des transports, grippes …

Quels risques ?

- Terminal non verrouillé – peut-être même Jail-Breaké
- Terminal avec des virus
- Risque de vol de données
- Que faire si le terminal est volé
- Quelles solutions de connectivités sécurisées
- Peut-on installer un logiciel avec une licence Pro sur un matériel Perso

Isolation par la virtualisation du terminal associée aux MDM et MAM

La virtualisation du poste client semble répondre à toutes les problématiques de sécurité.
L'utilisateur lance un « bureau à distance » ou un client CITRIX ou une application « full-web ».
Ainsi, rien n'est installé sur le terminal – nous venons de banaliser le poste client.

Sécurité par la responsabilisation :

fixation d'un cadre légal d'utilisation (charte d'utilisation, confidentialité CNIL...)

a. CNIL et obligations

obligations CNIL :
déclaration du Développement

Indiquer sur le site le pourquoi des cookies
Indiquer sur le site toutes les mentions légales obligatoires.
Garder les logs pas plus 1 mois (le droit à l'oubli)
Attention : HADOPI réclame de garder les logs 12 mois lissants

b. particularité du droit et devoir - (authsecu.com)

1 - Qui est concerné par la loi ?

L'article L. 34-1 du CPCE indique que « les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic (...) ». Le régime juridique applicable aux données relatives au trafic est également opposable aux « personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit (...) ».

Concrètement, l'obligation de conservation des données s'applique aux opérateurs de communications électroniques ainsi qu'à toute autre personne qui fournit un accès Internet dans le cadre d'une activité professionnelle. Les exploitants de « hotspots », tels que les cafés, les restaurants, les hôtels, les centres d'affaires, les cybercafés sont donc concernés, que l'activité de fournisseur d'accès soit effectuée à titre onéreux ou à titre gratuit et sans considération du fait qu'il s'agisse d'une activité principale ou secondaire. Les personnes ainsi désignées sont soumises à l'obligation de principe tendant à effacer et à rendre anonymes les données techniques liées aux communications électroniques.

2 - Quelles sont les données à conserver ?

Le CPCE indique que les données à conserver « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux ».

Tous les opérateurs doivent conserver certaines catégories de données techniques au cas où, dans le cadre d'une enquête judiciaire, les autorités chercheraient à identifier l'usager des services proposés par l'opérateur.

Un décret est venu, le 24 mars 2006, préciser que :

- Les informations permettant d'identifier l'utilisateur ;
- Les données relatives aux équipements terminaux de communication utilisés ;
- Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- Les données permettant d'identifier le ou les destinataires de la communication ;

- doivent être conservées par l'opérateur pendant un an à compter du jour de leur enregistrement.

S'il s'agit du service téléphonique :
L'opérateur doit conserver en plus les données permettant d'identifier l'origine et la localisation de la communication.

3 - Combien de temps doit-on conserver les données ?

Les obligations de conservation ne portent pas sur le contenu des communications échangées. Le cadre juridique a pour objet d'organiser les modalités d'accès aux données relatives au trafic, appelées également données techniques.

En ce sens, les dispositions de l'article L. 32 18° du CPCE indiquent que sont considérées comme données techniques « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation ». L'article R. 10-12 précise à son tour que ces données s'entendent des « informations rendues disponibles par des procédés de communications électroniques susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi ».

Pour autant, le code prévoit un régime juridique dérogatoire qui impose la conservation pendant un an des données relatives au trafic dans le but de faciliter la recherche, la constatation et la poursuite des infractions pénales. La communication de ces données relèvera du mécanisme de la réquisition judiciaire. La conservation des données peut être effectuée par l'opérateur ou confiée à des prestataires externes S'agissant particulièrement de la prévention des actes de terrorisme, l'article L. 34-1-1 du CPCE prévoit le cas des réquisitions administratives qui permettent aux agents de la police et de la gendarmerie nationales habilités à cet effet d'obtenir communication de ces données auprès des opérateurs et des autres personnes mentionnées ci-dessus.

4 - Quels sont les risques encourus pour le responsable légal ?

Il faut se référer à l'article 434-4, selon lequel "est puni de trois ans d'emprisonnement et de 45000 euros d'amende le fait, en vue de faire obstacle à la manifestation de la vérité (...) de détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature à faciliter la découverte d'un crime ou d'un délit, la recherche des preuves ou la condamnation des coupables".

Ce texte concernant les actes d'entrave à la justice, une personne tenue par la loi de communiquer des données techniques à la police, dans le cadre d'une enquête judiciaire, pourrait - si elle refusait de s'exécuter - être poursuivie sur le fondement de cet article.

Par ailleurs, ce dernier augmente les peines applicables lorsque l'infraction a été commise "par une personne qui, par ses fonctions, est appelée à concourir à la manifestation de la vérité". Les opérateurs (ou assimilés) pourraient, dès lors, être considérés comme exerçant de telles fonctions, puisque la loi met à leur charge une obligation particulière de coopération. Il ne peut donc être exclu qu'un juge retienne cette circonstance aggravante, notamment compte tenu du contexte sensible lié à la répression du terrorisme.

Si tel était le cas, la peine serait de cinq ans d'emprisonnement et 75000 euros d'amende.

5 - Quels sont les principes à respecter ?

La collecte et le traitement des logs doivent respecter certains principes, définis dans l'article 6 de la loi Informatique et Libertés. Cette collecte ne peut en effet se faire à l'insu des personnes concernées (principe de loyauté et licéité) et doit répondre à des finalités déterminées, explicites et légitimes. L'entreprise doit également répondre au principe de proportionnalité dans la collecte et le traitement, c'est-à-dire que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas proportionnées au but recherché ». Pour être en conformité avec ces principes, il faut par conséquent que le fichier ait un objectif précis, que les informations exploitées dans ce fichier soient cohérentes par rapport à l'objectif défini et que ces dernières ne puissent être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

Les données doivent également respecter un principe d'exactitude et leur durée de conservation doit être cohérente avec les finalités définies.

6 - Pour plus d'informations

Droits et Obligations des opérateurs et fournisseurs de services : Guide juridique pour les opérateurs locaux et les collectivités

Livre Blanc : Conservation des logs : une opportunité pour une sécurité maîtrisée mais aussi une véritable contrainte réglementaire - NSOne, février 2007

Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques

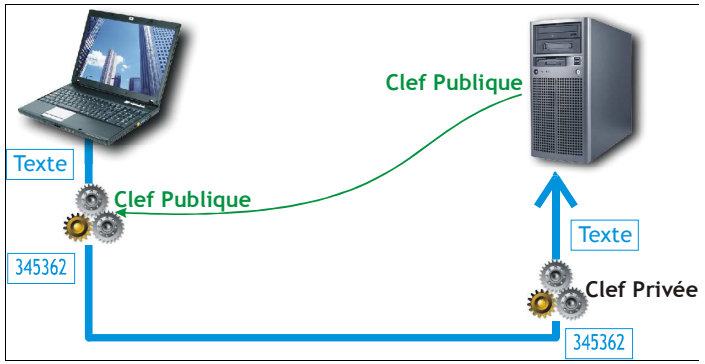
Solutions existantes : VPN SSL, Firewall

Connexion VPN :

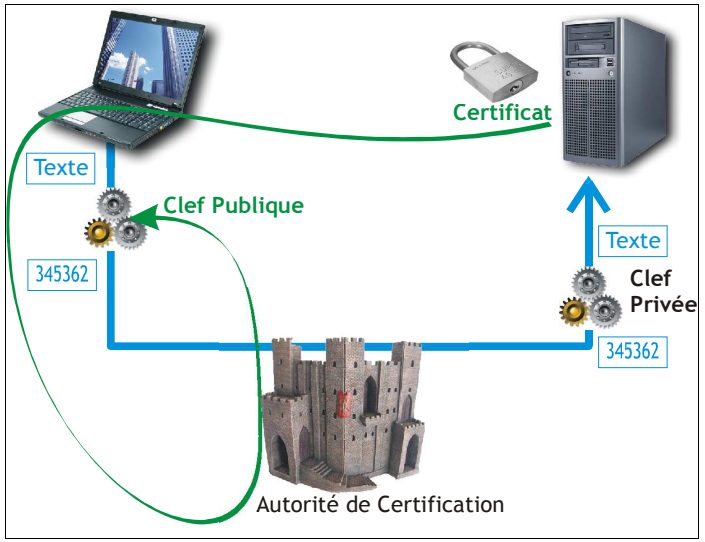
Virtual Private Network – réseau privé par logiciel

Il s'agit du chiffrement du transport des données entre le client et le serveur

Avant tout : une connexion SSL ou un client VPN – comment cela fonctionne-t-il ?

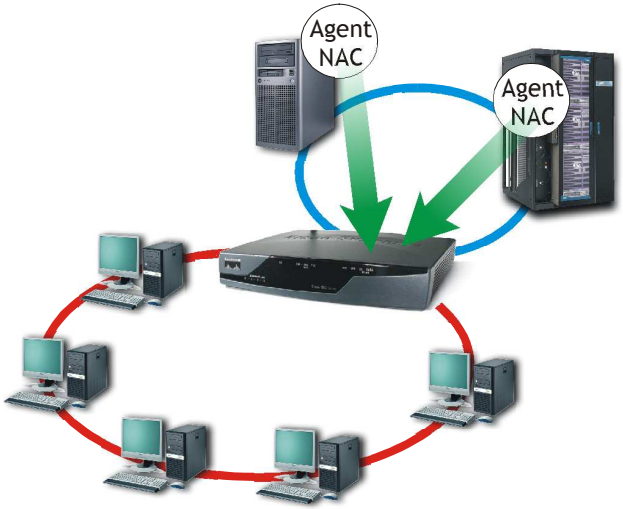


SSL avec certificat

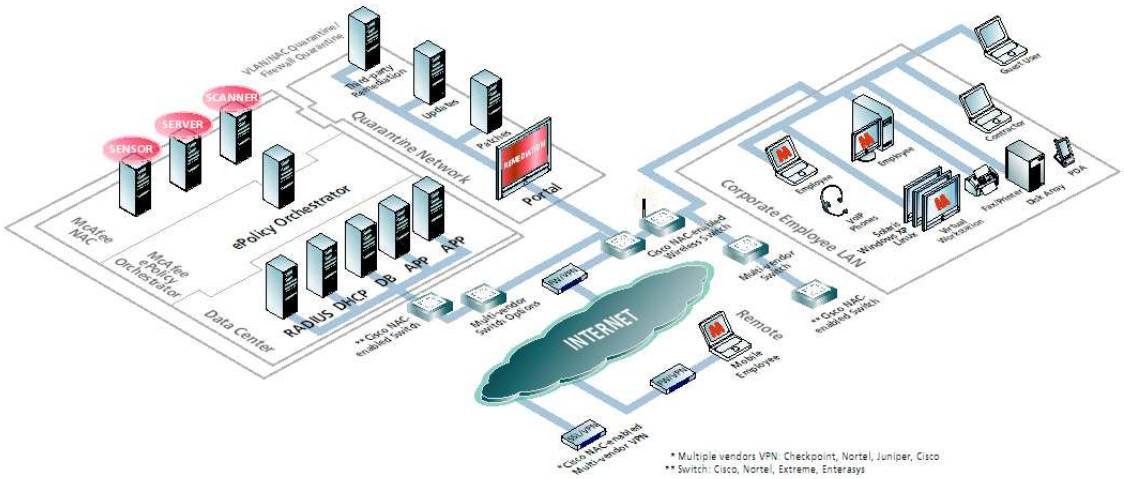


NAC "*Network Access Control*" est une technologie qui permet de gérer les ressources avec une surveillance automatique de type "antivirus".

NAC (Network Access Control) : le réseau n'est ouvert qu'à ceux qui y sont autorisés.
RBAC (Role Based Access Control) : l'accès sera donné aux machines et usagers qui font partie de ceux qui sont autorisés – puis vient la possibilité, pour eux, de se connecter réellement.
Souvent ces solutions sont couplées à une sonde **IDS** (sonde de détection d'intrusion).

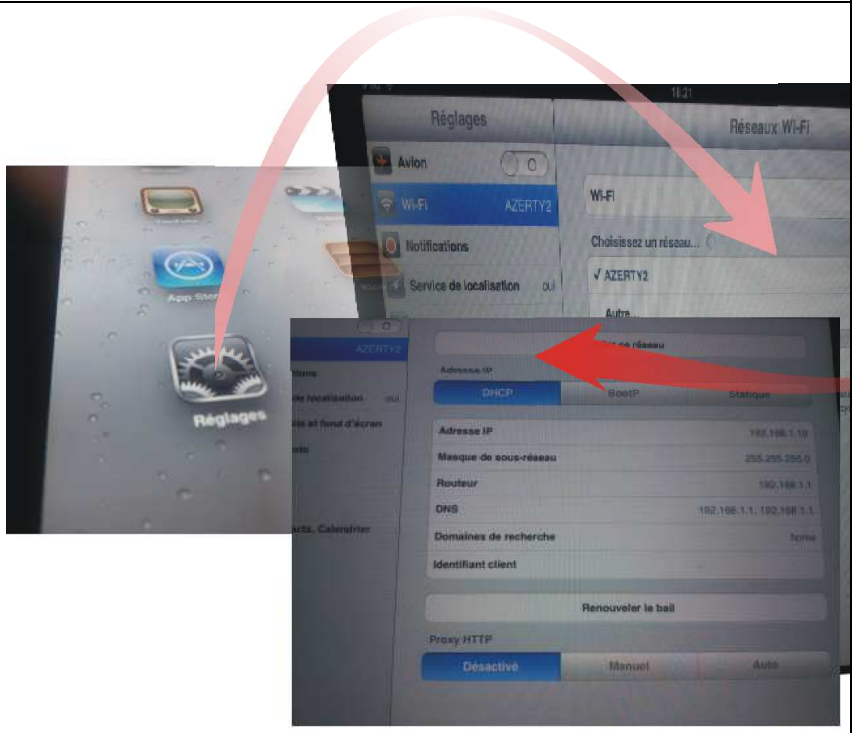


Proposition d'architecture par McAfee :



<table>
<tr>
<td>Réseau de collaboration :
par carte et USB

Ensemble d’éléments connectables en Bluetooth</td>
<td>  </td>
</tr>
<tr>
<td>Connexion WIFI :

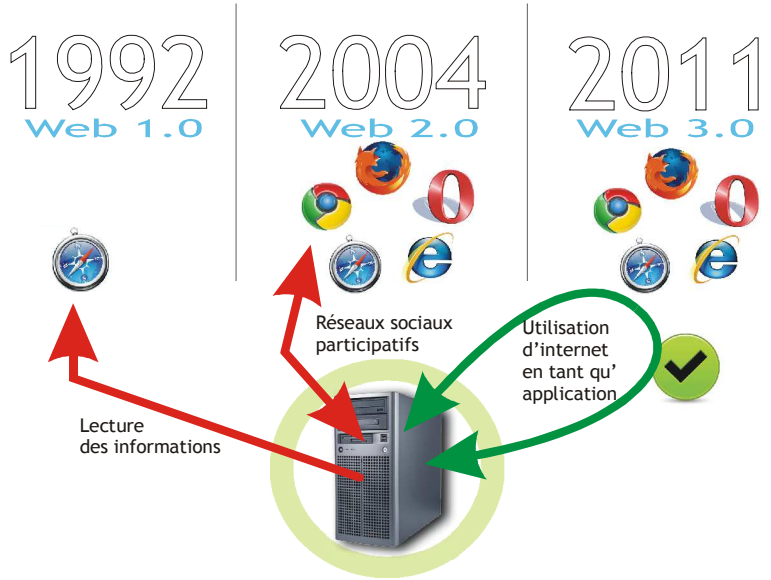
Sur l’écran d’accueil puis « Réglages ».
Nous y trouvons le panneau de configuration de l’iPad.
Sur WIFI, nous aurons la liste de WIFI captés avec celui sur lequel nous sommes connectés.
Grâce à la flèche bleue, nous aurons accès à la configuration avancée (adresse IP …)</td>
<td> 
</td>
</tr>
</table>

Banalisation et abstraction des plates-formes terminales mobiles

Les constructeurs ont bien compris que l'usager avait changé de comportement mais que l'entreprise n'y est pas encore.
Conclusion simple : il faut adapter les devices au monde de l'entreprise : « le client léger ».
Ainsi, par ces technologies, le terminal devient banalisé …
Sachant qu'il y a des milliards de terminaux branchés aujourd'hui : y a-t-il un risque de changement brutal ?

Convergence des solutions mobiles et traditionnelles "fixes"

Le monde de l'entreprise essaie d'évoluer vers le monde du « particulier ». Ainsi, nous voyons fleurir des nouveaux terminaux impensables il y a quelques années :



En 1992 sort le premier moyen pour surfer sur des pages statiques. Des pages publicitaires. Remplacement du minitel !

La messagerie WEB apparaît entre temps. Premier pas vers le Web 3.0
Quelques applications sortent pour le travail collaboratif.

Vers 2004, les premiers réseaux sociaux apparaissent. Il est temps d'entrer des informations dans les pages consultables !
Ce ne sont plus des pages statiques, elles changent avec "mes" données.

Vers 2011 sortent les premières applications sérieuses de travail collaboratif (Mail, Stockage, applications sur navigateur …)

Déjà, plusieurs parlent du **Web 4.0** basé sur les moyens de communication avec une tournure "économie d'énergie" et "protection de l'environnement". **Web 5.0** : nous évaluons tout et commentons tout ce qui se passe et ce que l'on achète.

Aujourd'hui, nous sommes en plein changement :

- Terminaux changent
- La sécurité évoluent
- Il y a de plus en plus de pirates et nous estimons qu'il y a autant de virus connus que d'inconnu
- Les terroristes se mettent à l'informatique
- Les réseaux sociaux vont plus vite que les médias
- IPv6 arrive, et nous ne sommes pas prêts !
- 2 milliards de connectés en 1 an devraient arriver !
- La connectivité au domicile atteint le Giga Bits par seconde ! Et bientôt pour touS !
- Les drones et les imprimantes 3D changent le paysage de la sécurité informatique
- Nous venons d'arriver au 64Bits et l'on nous parle déjà du 128bits
- Les disques sont de plus en plus miniaturisés au point de mettre tout un datacenter dans la poche !