# Economie numérique : passage d'une économie de copies à une économie de licences, pour de vrai.
# (brouillon)

Aujourd'hui, la plus value utilisateur liée à l'acquisition légale d'œuvres digitalisées, ou de droits d'accès à ces oeuvres, hormis éventuellement une satisfaction personnelle d'honnêteté, est absolument nulle, si ce n'est carrément négative : Liens fichiers licences qui partent en vrille, maintenance de fichiers excel de numéros de licences, perte de ces numéros avec les enveloppes CDs qui vont avec, migration de machines ou installation qui ne marche pas pour une raison x ou y, quand la licence n'est pas liée à la machine (quelle hérésie), règles ésotériques sur ce qu'on a le droit de faire ou pas suite à l'achat, lecteurs obligatoires, etc. A la fin, aucune différence entre acquisition légale ou pas, c'est des CDs/DVDs marqués au feutre indélébile ou de la gestion de disques durs et backups, avec un sentiment de « fragilité » (et non propriété) plus grand que dans le cas du piratage, ce qui n'est pas qu'un sentiment comme décrit plus haut.

On s'intéresse ici à un modèle basé sur l'existence d' « organisations notariales » chargées de gérer des « comptes de licences utilisateurs », permettant en retour à ces utilisateurs d'avoir accès aux œuvres achetées de n'importe quelle machine, ces organisation étant donc garantes des « bibliothèques utilisateurs », avec contraintes de confiance et confidentialité associées.

Cependant, à l'aide de protocoles tri partite, on garantit l' « anonymat global » de l'utilisateur, c'est à dire que les numéros de comptes n'on en rien besoin d'être connus et partagés par les magasins, éditeurs ou fournisseurs de services pour que le système fonctionne.

On note :

- *Mu* la machine de l'utilisateur (une de ses machines, celle qu'il utilise au moment de l'achat)
- *Nu* l'organisation notariale de l'utilisateur (la machine associée)
- *Mag* le magasin en ligne (ou pas) où est acquise l'œuvre ou le droit d'accés (la machine associée)
- *Do* le « distributeur » de l'œuvre, ou responsable de la distribution de copies

Protocole d'achat :

1. L'utilisateur choisit une œuvre sur *Mag*
2. transaction de paiement non décrite
3. transaction de licence :
    1. Génération d'un numéro de session par *Mag,* envoie de ce numéro de session à *Mu*
    2. *Mu* envoie à *Mag* l'identité de *Nu*
    3. *Mu* envoie à *Nu* le numéro de session
    4. *Mag* envoie à *Nu* le session_id, l' identifiant de l'œuvre et le numéro de licence
    5. *Nu* écrit sur le compte de l'utilisateur l'acquisition de la licence

On voit que Nu enregistre une licence sur le compte de l'utilisateur uniquement sur demande de Mag mais jamais de Mu, ce qui garantit l'acte d'achat des deux côtés, d'autre part le magasin n'a à aucun moment besoin de connaître le numéro de compte de l'utilisateur, mais uniquement l'identité de son organisation notariale ou banque de licence. On considère par ailleurs que les numéros de licence sont réellement tirés au sort dans de grands espaces et non sujets à règles algébriques, donc non générables par key generators.

Protocole d'acces à l'œuvre x :

1. Si x est en cache sur la machine utilisée par l'utilisateur, accés direct
2. Si x est pas en cache :
    1. *Mu* demande à *Nu* la génération d'un access_id pour l'œuvre x ainsi que l'identité de *Do* pour x
    2. *Nu* transmet à *Do* l'access_id et l'identifiant de l'œuvre

3. *Mu* transmet à *Do* l'access_id et l'identifiant de l'œuvre
4. l'œuvre est téléchargée sur *Mu* où une session de consultation initialisée (si l'œuvre est un site web par exemple)

Ici, on voit que Do ne déclenche le téléchargement ou la session de consultation que sur un message de Nu, jamais de Mu. Cependant ici aussi, Do n'a à aucun moment besoin de connaître le numéro de compte de license de l'utilisateur, mais uniquement l'identité de son organisation notariale.

Ces principes peuvent être réutilisés pour de nombreux contextes, et on peut imaginer toutes sortes de services ou l' « opérateur du service » délègue la gestion et connaissance des (ou de certaines) données utilisateurs à l'organisation notariale de cet utilisateur, de même un certain service pourra utiliser les données utilisateur lié à un autre service sans jamais en avoir une connaissance effective.

Cela ne veut pas dire que l'utilisateur n'a pas d'identité (ou compte) sur les magasins ou fournisseurs de services, mais aucun « unique ID » de l'utilisateur n'est nécessaire ou partagé entre les intervenants. D'ailleurs la sauvegarde de ces divers comptes et password peut être un des services fournit en délégation vers l'organisation notariale de l'utilisateur.

D'autre services comme des liens vers des espaces de stockage de projets ou données de contenu personnels managés par des FAIs ou autre peuvent être imaginé, et bien sur l'utilisateur doit pouvoir créer des structures ou points de rangements sur son (ou quelques, pas de fétichisme d'unicité à avoir ici) « comptes de licences ».

Les normes nécessaires à la mise en place d'un tel système n'ont à mon avis pas à être « bien grosses », il ne s'agit pas du tout de tout réécrire ou de tout renormaliser, en particulier il n'y a rien à changer dans tous les formats d'œuvres, le compte utilisateur peut tout simplement être vu comme un système de fichier à inodes réellement admistratifs, (ou monde lisp à adresses mémoires administratives), inodes ou adresses à signification globale (directory ou liste de toutes les licences de n'importe quel compte par exemple) ou locale (une structure ou point de rangement d'un tel compte) utilisant des « ISCNs » dont la distribution et l'écriture peut utiliser les procédés décrits dans la proposition de brevet jointe. Par contre de nombreux services pourrait réutiliser cette structure tout comme cela se fait à travers les « cookies », « base de registre », ou autre.