

LE DOMICILE NUMERIQUE SECURISE

Les échanges collaboratifs en confiance, anonymes
et personnalisés sur Internet

Xavier Dalloz - Jean-Marc Lévy-Dreyfus

Mars 2007

La genèse du Domicile Numérique Sécurisé

Le Domicile Numérique Sécurisé (ou DNS 2.0) est une architecture de services Internet qui établit une relation de confiance entre usagers, clients potentiels, Administrations et fournisseurs de produits et services du « monde réel », dans un contexte cohérent et maîtrisé. Il transpose le métier des tiers de confiance du « monde réel » au « monde virtuel » (notaires, banques, assurances...).

Le DNS 2.0 permet :

- La sécurisation des échanges basée sur l'identification certaine des usagers, et cela grâce à une gestion centralisée et non pas à une PKI qui peut apparaître comme une usine à gaz.
- La traçabilité des échanges, le stockage et la centralisation des transactions
- Pas de tiers de confiance centralisé, mais un tiers de confiance par métier, par corporation.

Le DNS 2.0 est né de six observations principales

□ Le rôle croissant de la « relation » dans les modèles économiques CtoC et CtoB

Si les modèles B to B et B to C sont impactés par le web, le vrai tournant se trouve dans la montée en puissance des modèles C to C et C to B. Il s'agit pour les entreprises de valoriser les échanges de personne à personne. Aujourd'hui, être mis en relation avec la bonne personne a un prix, comme le prouvent les succès de Meetic (site sur lequel les hommes sont prêts à payer plusieurs euros pour être mis en relation avec la femme de leur vie), de MSN (logiciel de messagerie instantanée permettant aux utilisateurs de communiquer gratuitement entre eux, utilisateurs constituant une audience valorisée par MSN auprès des annonceurs), d'eBay (tiers de confiance proposant aux internautes de vendre leurs produits en ligne, moyennant commission) ou bien encore des sites de petites annonces en direct.

Un autre exemple est celui des applications permettant aux utilisateurs de monétiser leur expertise personnelle telle que la traduction, l'assistance culinaire, les conseils en informatique ou en mathématiques.

Les modèles d'affaires C to C et C to B illustrent l'émergence de ces pratiques mais également leur potentiel économique. Si ces modèles doivent encore travailler à se stabiliser, ils montrent une tendance de fond qui va bien au-delà de l'évolution de la chaîne de la valeur. En effet, le client n'est plus seulement « roi » ou « au cœur », il se situe à l'origine même des flux d'affaires (C to C, C to B) voire des processus d'innovation (innovation ascendante). Les entreprises sont en cela fortement impactées et ne sont plus vraiment maîtres des business models. La dominante « relation » va prendre de plus en plus d'importance, qui réunit tous les acteurs ayant une dominante annuaire : service de courrier électronique, sites de rencontre, services de renseignements, etc.

□ **L'internaute n'est plus passif, il produit lui-même du contenu.**

La troisième vague de l'Internet intègre plus profondément l'interactivité de ce nouveau média. L'utilisateur devient à son tour un producteur de contenu et un créateur de services. Il s'implique. L'échange devient plus riche et n'est plus à sens unique.

De plus le client acquiert un pouvoir de négociation. Les outils tels les blogs, forums, sites de recommandation donnent à celui qui était spectateur accès à plus d'informations, en particulier à l'expérience d'achat des autres clients. Emergent également des sites spécialisés dans la comparaison des offres et des prix, qui influencent considérablement le comportement des clients.

□ **L'importance grandissante de la mobiquité (ubiquité + mobilité)**

Le consommateur désire accéder au service dont il a besoin quand il le souhaite, où qu'il soit et avec l'équipement dont il dispose. Cet équipement peut être un ordinateur, un téléviseur, un téléphone, un PDA, une console de jeu ou multimédia... Nous sommes enfin rentrés dans l'ère de l'**ATAWAD** (*AnyTime, AnyWhere, Any Device*).

□ **Le rôle croissant de l'économie de l'attention et de la gestion personnelle du temps**

Le consommateurs/citoyen cherchera de plus en plus à économiser son temps et sous-traiter à des prestataires tout ce qu'il ressent comme une corvée afin de se réserver des plages de loisir. Il appartient aux fournisseurs de produits et de services de comprendre cette attente afin d'agrèger dans un seul endroit ces produits et services issus de filières de production différentes. La mondialisation a radicalement transformé l'organisation des entreprises, appels massifs à la sous-traitance, délocalisation et spécialisation des tâches. De même, l'Internet va transformer l'organisation de la vie quotidienne.

□ **La confiance sera au cœur de tous les modèles économiques**

Le commerce sera d'autant plus efficace qu'il écouterait, donnera la possibilité au consommateur d'exprimer en confiance leurs désirs, de façon individuelle, n'importe où et n'importe quand. Cette situation nouvelle bouscule les hiérarchies sociales, car elle procure un avantage décisif aux utilisateurs chevronnés (agiles) et réduit notablement l'importance du savoir dans les prises de décisions personnelles.

□ **L'offre actuelle de services est inadaptée**

L'architecture actuelle du réseau ne permet pas d'établir la confiance et de sécuriser l'usage de l'Internet pour des activités individuelles et personnelles (Vie Privée).

La limite fondamentale de l'Internet actuel réside dans son architecture:

Comme le dit Lawrence Landweber, "*senior advisor*" (conseiller en chef) de la National Science Foundation (NSF), l'Internet a connu un formidable succès, il est devenu une infrastructure critique pour un grand nombre d'activités, mais on en touche les limites.

L'architecture actuelle a des limites fondamentales. L'Internet n'a aucun mécanisme de sécurité en propre. Il n'a pas été conçu pour être robuste et facile à gérer, pour optimiser la performance et la qualité de service de bout en bout, pour passer à l'échelle rendue nécessaire par la multiplication des objets communicants. L'Internet atteint les limites de son extensibilité. L'Internet n'est pas prêt à remplir son rôle pour l'avenir, et surtout pas dans les conditions de sécurité requises. Nous passons beaucoup de temps à repousser ces limites,

nous continuerons à le faire dans les années à venir, mais à moyen terme, il va falloir les dépasser une bonne fois.

L'architecture de l'internet se fonde en outre sur des hypothèses structurantes et aujourd'hui limitatives :

- Le trafic sur le réseau est "amical"
- Les nœuds finaux sont des ordinateurs, de préférence fixes
- Le réseau n'a rien à dire de lui-même, seules les extrémités communiquent ; le réseau ne peut pas être interrogé, par exemple pour dire en quel état il se trouve
- L'acheminement se fonde sur un principe de "best effort" ("faire au mieux"), pas sur un engagement de résultat.

□ **L'Internet a été pensé pour exploiter la puissance du terminal.**

Dans le cas du téléphone traditionnel, le réseau est « intelligent », alors que le terminal (le vieux poste de téléphone) est « stupide ».

Avec l'Internet et son mécanisme de routage de paquets, le réseau est volontairement simplifié pour être le plus robuste possible, et toute la responsabilité de l'échange repose sur le terminal devenu informatique.

Le système de certification actuel ne peut donc identifier et contrôler que le terminal qui se connecte, et non pas la personne physique. Par défaut, le système ne garantit donc pas que l'interlocuteur est bien celui qu'il prétend être.

Ce contrôle d'identité doit donc être effectué sur le terminal, et il est par définition asynchrone. Les acteurs malveillants ont ainsi tout le temps de simuler les connexions et d'exploiter les failles de sécurité du système bien avant que l'on ait pu en trouver la parade.

□ **L'Internet risque d'atteindre la limite de son développement**

Pour développer les performances il est nécessaire d'améliorer les réseaux, les serveurs, les protocoles,... Il est de plus nécessaire d'avoir des systèmes capables de supporter des architectures hétérogènes mais interopérables. Il devient difficile de surmonter les défauts majeurs des applications qui mettent l'utilisation du réseau en danger:

- Spamming
- Phishing
- Pharming
- La multiplication des ID et mots de passe
- L'impossibilité de gérer sa téléphonie personnelle, de centraliser ses messages, tout ce qui est prévu par les créateurs de SIP par exemple.
- Pas d'anonymat puisque tout est suivi grâce à l'adresse IP

□ **L'Internet n'a pas été conçu pour assurer une qualité de service de bout en bout.**

Comment assurer la qualité de services pour un réseau qui a été conçu selon le principe du « best effort » ? L'IP a été conçu comme cela dès l'origine, c'est en cela qu'il est radicalement différent d'un réseau télécom. Il est basé sur l'empirisme. Il y a des avantages ... mais aussi des inconvénients auxquels il est urgent de remédier. Par exemple, l'Internet ne pourra pas, remplir son rôle pour l'avenir surtout dans les conditions de sécurité requises.

Prenons l'exemple du mail. C'est une application de l'Internet (couche application) et utilise des protocoles POP et SMTP. Elle n'est pas satisfaisante. La boîte aux lettres est publique et se remplit de spam. Comme la boîte courrier physique, mais le courrier lettre a un coût. Alors que le mail est gratuit. Le serveur SMTP prévient s'il ne parvient pas à livrer le mail au delà de plusieurs tentatives. Mais le serveur SMTP ne garantit pas l'identité de l'émetteur (pourtant identifié par son adresse IP de départ) car il se place en intermédiaire.

Mais rappelons que lorsqu'on reçoit un courrier lettre physique, on ne sait pas non plus qui l'a envoyé. On peut inscrire n'importe quelle adresse au dos de l'enveloppe, cela ne prouve rien. Voir donc quelles sont les professions qui ont besoin d'authentifier leurs interlocuteurs. Mais l'Internet est donc intrinsèquement supérieur car il identifie la machine avec certitude grâce à son adresse IP, ici masquée par le serveur SMTP.

En conséquence, 8,9 millions d'américains sont devenus les victimes de la fraude en 2005, perdant ainsi 56,6 milliards de dollars alors que les cas d'usurpation d'identité et de fraude ne représentent que la partie émergée de l'iceberg. Un grand nombre d'internautes persistent à croire que leur activité sur Internet est anonyme alors que l'utilisation par les sites Web de cookies rend illusoire cette impression.

Les sites qui sont capables d'exploiter différents types d'identification sont les mieux placés pour créer un climat de confiance et gagner des clients : les sites qui exigent des visiteurs qu'ils mémorisent un login sont dissuasifs.

Les consommateurs prennent conscience maintenant que l'identification constitue un véritable enjeu. L'identification doit être au cœur de la stratégie de tous les acteurs concernés par la personnalisation « anonyme ».

L'offre de valeur du DNS 2.0 en 5 points

Dans ce contexte, le Domicile Numérique Sécurisé (ou DNS 2.0) est une architecture qui apporte enfin la solution aux graves problèmes qui obèrent l'avenir du réseau.

Le DNS 2.0 est centré sur l'humain et non sur la machine. Il s'adresse à tous les consommateurs/citoyens en leur proposant un environnement de confiance nécessaire à toute transaction.

L'offre de valeur du DNS 2.0 peut se résumer en quelques points:

□ La simplicité et la richesse des services

- Le DNS 2.0 permet à chaque individu de construire son portail personnel axé sur des services pratiques et de proximité, en fonction de ses besoins, de ses habitudes et de ses désirs. C'est le portail de sa « vie privée ».

□ La mise en relation

- Le DNS 2.0 certifie que chaque message est parvenu à son destinataire
- Le DNS 2.0 rend possible des services opérés par un acteur identifié.

□ **La sécurité**

- Le DNS 2.0 met à la disposition des internautes un dispositif d'intermédiation technique jouant le rôle de tiers de confiance entre les consommateurs et les entreprises *ainsi qu'une personnalisation anonyme*.

□ **La confiance**

- Le DNS 2.0 crée un environnement de confiance garantissant l'authentification de chaque transaction, l'assurance paiement et la caution de partenaires financiers
- Le DNS 2.0 apporte la protection de l'identité numérique de chaque consommateur/citoyen
- Le DNS 2.0 permet l'accès simple, personnalisé, sécurisé avec l'équipement de son choix et en toute confiance à un large éventail de services au quotidien (réduction des contraintes et gain de temps)

□ **La personnalisation anonyme**

- Le DNS 2.0 rend possible une relation permanente avec des services personnalisés qui garantissent l'anonymat.
- Le DNS 2.0 met à disposition des assistants toujours disponibles pour répondre juste à temps à besoins

Les caractéristiques d'un Domicile Numérique Sécurisé

Le **Domicile Numérique Sécurisé** est un espace virtuel qui combine :

- Une **adresse numérique individuelle** (nom de domaine) attribuée par l'autorité qui gère la plate-forme de services.
- Une **Carte de Visite individuelle en ligne** (Home Page) qui présente les détails personnels que l'abonné souhaite afficher et contient des liens vers un kiosque de services de messageries permettant à un visiteur de contacter l'abonné.
- Un **coffre fort de données personnelles**, accessible partout 24h/24 où l'utilisateur range, classe et trace tous les messages, documents, notes, liens, adresses d'amis et données diverses qui ont été reçus et/ou envoyés au Domicile Numérique.

Chacune de ces caractéristiques présente une innovation d'usage, des avantages pour les consommateurs/citoyens et un modèle économique.

Les avantages d'une adresse numérique individuelle

□ **L'innovation d'usage**

Cette adresse indiscutable, non usurpable est attribuée par l'autorité qui gère les inscriptions et en garantit la confidentialité. Elle devient de facto le nom de domaine personnel de l'abonné.

□ **Les principaux avantages**

Les avantages d'une adresse numérique individuelle sont les suivants :

- L'adresse est automatiquement inscrite dans un annuaire sécurisé qui est mis en ligne sur le site de l'autorité de nommage. (exemple : www.postapp.net)
- Chaque annuaire est doté d'un puissant moteur de recherche "à la Google".

- A la différence des moteurs de recherche sur le Web qui n'indexent et par conséquent ne trouvent que des contenus publiés, le moteur de recherche du DNS 2.0 n'indexe et ne retrouve que les adresses des abonnés au service, sans que ces derniers aient le moindre effort à faire pour se référencer ou publier en ligne.
- L'accès aux services de l'annuaire est contrôlé par l'autorité qui peut limiter l'usage de l'annuaire selon des critères de rôle et de profil.
- A partir des résultats d'une recherche (ou en saisissant l'adresse numérique dans la barre d'adresse du navigateur), le visiteur affiche la Carte de Visite Numérique de l'abonné qu'il souhaite contacter ou visiter les liens.

□ **Le modèle économique associé**

Le modèle économique associé à l'adresse numérique individuelle se résume de la façon suivante :

- Les revenus des services associés à l'adresse numérique individuelle sont liés aux possibilités offertes par les annuaires.
- Ces revenus sont une transposition du mode de rémunération des pages blanches et des pages jaunes
- La publicité « ciblée » et le marketing direct profitent de « l'opt in » et de « l'opt out » qui sont à la base du fonctionnement de l'adresse numérique individuelle.
- La commercialisation de panel « sans biais ».
- La protection de l'identité numérique sans aucun risque d'usurpation d'identité.
- L'assurance de ne pas être victime du spam, de Phishing ou du Pharming...

Les avantages d'une Carte de Visite Individuelle en ligne

□ **L'innovation d'usage**

La carte de visite individuelle est une « home page » dans laquelle sont affichés les détails et les liens personnels que l'abonné souhaite faire connaître à ses visiteurs. Les informations affichées sont extraites à la volée, de la base de données au moment de l'affichage de la page, en tenant compte du statut du visiteur (Public, mes proches, moi même).

La grande innovation d'usage réside dans le fait que pour envoyer un message, l'expéditeur¹, n'a même plus besoin de :

- Connaître le numéro de téléphone, l'adresse postale ou l'email du destinataire
- Disposer d'un matériel personnel (ordinateur, imprimante, papier, encre, machine fax, téléphone mobile)
- Manipuler des logiciels ou des fichiers (toutes les opérations dans le DNS 2.0 se font à partir de logiciels de service en ligne Web 2.0)
- Se déplacer ou faire la queue pour affranchir et poster.
- De s'abonner à un service au préalable pour pouvoir expédier en ligne
- De savoir-faire informatique et internet, car le service peut être rendu sur n'importe quel terminal connecté par un agent tiers (postier, banquier, guichetier, bénévole d'association ou tout simplement par un proche)
-

¹ La cible principale est l'expéditeur néophyte ou occasionnel qui se retrouve instantanément doté de services au fil de l'eau qui sont à ce jour difficilement disponibles en entreprise.

□ **Les principaux avantages**

Les avantages d'une Carte de Visite Individuelle en ligne sont les suivants :

- Le DNS 2.0 garantit la confidentialité des contenus notamment en permettant à l'abonné de choisir quels détails² et quels liens doivent être affichés dans sa carte de visite.
- L'abonné peut décider quel type de visiteur (le public, mes proches ou moi seul) pourra accéder à la fiche et quelles adresses seront affichées en clair ou masquées.
- Chaque détail présente un lien vers un service de messagerie adéquat³.
- Chaque service permet à tout expéditeur de facilement rédiger en ligne, afficher pour contrôle avant envoi, et adresser ses messages à l'abonné.

□ **Le modèle économique associé**

Le modèle économique associé à la Carte de Visite Individuelle se résume de la façon suivante :

- Les revenus des services associés à la carte de visite sont liés aux possibilités offertes de mise en relation dans un environnement de confiance
- Ceux des services qui mettent en jeu, une impression, une expédition et un affranchissement sont facturés en conséquence et payés à l'acte⁴.
- En échange de quoi, le service pilote la transformation du message électronique saisi à l'écran en un document au format classique (fax, SMS, courrier postal simple ou recommandé) et inséré dans le réseau de distribution classique garanti par un opérateur (Poste ou télécoms) référent.
- L'expéditeur est ainsi certain que son message sera délivré à temps au destinataire. De plus, une copie électronique du message est systématiquement enregistrée et indexée dans le coffre de données personnelles du destinataire.

Les avantages d'un coffre fort de données personnelles

□ **L'innovation d'usage**

Le Domicile Numérique offre une fantastique solution à l'abonné pour lui faciliter à partir d'un point d'entrée unique (SSO) la présentation de tous ses liens numériques et l'organisation, la sécurisation et le suivi de tous les contenus résultant de ses échanges et de ses transactions.

La grande innovation d'usage réside dans le fait que pour sécuriser et conserver ses informations au format numérique et surtout les maintenir vivantes et utilisables partout et tout le temps, l'utilisateur n'a plus besoin de :

- Gérer des données éparpillées dans des fichiers, des disques, des clés USB, des backups de stockage

² Adresse postale, Numéros de fax, de téléphone, adresse mail, liens vers des sites et des blogs perso....

³ Il y a 5 services standards : envoyez-moi un courrier postal, envoyez-moi un fax, envoyez-moi un SMS, envoyez-moi un email, laissez-moi un message, et bientôt on trouvera des services pour automatiser l'affranchissement de colis et de courriers manuels.

⁴ Selon la nature du service et l'opérateur, l'affranchissement s'effectue par carte prépayée, appel ou SMS surtaxé, carte bancaire ou par prélèvement sur un compte de téléphonie mobile après signature en ligne autorisant la transaction à l'acte.

- Mettre à jour, synchroniser et transférer ses données d'un appareil et d'un répertoire à un autre à chaque changement de génération ou apparition des nouvelles versions des logiciels.
- S'inscrire dans de multiples services distants, sans garantie de confidentialité, de sécurité et de pérennité
- Se prémunir contre les risques de pertes de données, de vol d'identité et d'obsolescence rapide des supports de sauvegarde

Le Coffre fort propose⁵ à l'abonné son service de messagerie universelle convergente (Meta-webmail) utilisable sur tout terminal, partout et tout le temps. Ce service fonctionne de manière similaire à un Webmail dont il étend la capacité à tous les formats de messages (fax, SMS, courrier postal et email). L'abonné peut ainsi expédier tous ses courriers quels que soient les formats depuis son point d'usage unique en ligne en utilisant l'un des services décrits plus haut. Bien entendu, une copie électronique de chaque message envoyé est systématiquement enregistrée et indexée dans le coffre de données personnelles.

Le Coffre est doté d'un moteur de recherche à la "Google" qui permet à l'abonné de retrouver instantanément⁶ l'information urgente dont il a besoin en recherchant un mot clé dans sa propre histoire numérique.

□ **Les avantages**

Les avantages d'un coffre fort de données personnelles sont les suivants :

- Disposer d'un point d'entrée unique contrôlé par un mécanisme d'identification/authentification. Cette opération permet à l'abonné d'entrer dans son domicile numérique pour accéder à ses services et à ses liens.
- Distinguer nettement entre l'identification de l'abonné à l'entrée dans une session et son identité lors de l'exécution d'une opération qui implique un échange en sécurité avec un ou des tiers.
- Eviter les vols et piratages, le système est conçu pour exiger une signature à l'acte pour chaque transaction dès lors qu'elle met en jeu l'identité de l'abonné.

□ **Le modèle économique associé**

Le modèle économique associé d'un coffre fort de données personnelles se résume de la façon suivante :

- Les revenus des services associés à au coffre fort de données personnelles sont liés aux possibilités offertes pour envoyer (messageries unifiées) et pour retrouver « ses » informations en fonction de leurs contextes.
- Ces services marchands sont comparables à ceux vendus par les assureurs.
- Ces services sont commercialisés sous la forme d'un abonnement annuel avec la possibilité d'une assistance à la constitution de dossiers
- Le commerce électronique, et notamment de « cross fertilisation », lié à chaque domaine de consommation avec la possibilité de vendre avec une continuité de services.

⁵ Sur abonnement payant ou gratuitement selon les décisions de l'opérateur de la plateforme TAPP.

⁶ Par exemple : les coordonnées (malheureusement on les avait notées dans le vieux téléphone) de quelqu'un qui vous a adressé un SMS l'année passée ou la super photo des enfants prise lors des vacances, postée à Mamy depuis un WebCafé avant de se faire voler l'appareil photo.

La technologie au cœur du Domicile Numérique Sécurisé

Le Domicile Numérique Sécurisé s'appuie sur TAPP ou l'Internet transactionnel, une technologie qui adresse aux grands acteurs⁷ qui organisent leur activité autour de répertoires de leurs clients et usagers.

TAPP introduit une méthode et une architecture de services qui permet aux opérateurs du monde réel (Brick and mortar) tout en continuant leurs métiers classiques, de les transposer sur Internet et ainsi de tirer des revenus complémentaires tout en offrant aux clients un fonctionnement et une qualité de services similaires en ligne et dans le réel (Brick and/or Click) .

Les services délivrés par une Plate-forme TAPP sont efficaces et faciles à utiliser car ils sont similaires aux services postaux que nous utilisons quotidiennement depuis des générations.

Ses avantages sont les suivants :

- Les services sont disponibles à la demande partout où un ordinateur connecté à l'Internet est accessible.
- Chaque service paramétré et réalisé automatiquement selon les instructions du client est facturable à l'acte.
- L'utilisation de ces services ne nécessite de la part du client ni implication ni apprentissage ni investissement.
- TAPP transforme la manière dont nous utilisons l'Internet pour en faire un réseau de services garantis de bout en bout, simples et universels.

Le principal différenciateur de TAPP réside dans la manière de s'abonner aux services :

- L'inscription classique sur le Web demande à l'utilisateur d'entrer un identifiant de son choix (généralement son adresse mail) dont le seul critère impératif est de ne pas avoir été déjà utilisé par un autre abonné et d'entrer un mot de passe⁸ de son choix.
- Les solutions basées sur TAPP préenregistrent chaque abonné à partir d'une adresse⁹ (ou d'une immatriculation) qui lui a été déjà attribuée par un tiers référent dans un autre contexte que le Web.

TAPP facilite les services de la vie quotidienne. Par exemple, avec TAPP, il est possible de :

- Envoyer et recevoir son courrier postal ses fax, ses SMS et ses emails de n'importe où à l'aide de n'importe quel ordinateur,
- Bénéficier d'un espace virtuel personnel sécurisé et non usurpable

⁷ Opérateurs de téléphone mobile, Postes, réseaux de Commerçants, Bancassurances, associations, gouvernements, OnG

⁸ Ce qui a comme redoutable effet collatéral de faciliter le piratage car comme la plupart des utilisateurs s'inscrivent avec le même identifiant et le même mot de passe aux différents services. Il suffit à un pirate de s'insérer sur un service en ligne faiblement protégé pour récupérer des binômes (identifiant/authentifiant) utilisables sur des sites bien protégés.

⁹ Ainsi l'identifiant sera initié par un numéro de téléphone mobile (Mobitap), une adresse postale (Postapp), un compte de fidélisation (Buytap) ou une domiciliation bancaire (Paytap).

- Ranger et classer automatiquement ses documents (texte, photos, messages) et ses données et de les retrouver instantanément même des années après.
- Retrouver facilement et au bon moment sur un téléphone mobile, les coordonnées d'un ami, de son dentiste ou de l'école du petit dernier.

Le marché potentiel du Domicile Numérique Sécurisé

En conclusion, le Domicile Numérique Sécurisé (ou DNS 2.0) est une architecture qui met en relation cohérente des usagers, clients potentiels, Administrations et fournisseurs de produits et services du « monde réel ».

Le DNS 2.0 se situe au carrefour des échanges entre producteurs et consommateurs en apportant la simplicité, la richesse des services, la confiance, la sécurité et la personnalisation anonyme. Son objectif est d'abaisser les coûts d'acquisition client, les coûts de transaction et de fidélisation.

Le DNS 2.0 rend donc possible des écosystèmes entre :

- Le client final en quête de confiance
- Les entreprises préoccupées par la gestion de la relation avec leurs clients
- Les partenaires concernées par la construction d'une offre dans la logique du consommateur
-

□ Le client final en quête de confiance

Chacun doit pouvoir constituer au gré de ses besoins, de ses désirs, de ses activités, un espace où il se sente comme chez lui. Son terminal doit devenir la métaphore non plus du bureau, comme l'écran des PC inventés pour des professionnels, mais celle de son chez-soi intime, avec l'avantage supplémentaire et essentiel de l'ubiquité d'intervention. C'est son Domicile Numérique Sécurisé. C'est l'Internet de sa « Vie Privée ».

□ Les entreprises préoccupées par la gestion de la relation avec leurs clients

Pour répondre à ce besoin, le Domicile Numérique Sécurisé permet :

- L'authentification de l'individu quel que soit son mode d'accès : adresse exacte, e-mail exact, profil honnêtement et sérieusement renseigné...
- La sécurisation des paiements
- La réduction des frais d'acquisition et de fidélisation de clientèle

Avec le Domicile Numérique Sécurisé, il est possible de permettre aux entreprises de développer des services rendant beaucoup plus facile, où que l'on soit, l'accès aux services essentiels dont on désire disposer : communication et coopération avec les siens, avec ses communautés, services de la vie quotidienne familiale, personnelle, professionnelle, ressources domestiques, professionnelles, ludiques, éducatives et autres... il s'agit des fonctions de base de la vie quotidienne de la personne.

□ **Les partenaires concernées par la construction d'une offre dans la logique du consommateur**

Aucun acteur isolé ne saurait prétendre seul maintenir un échange avec son client pendant toutes les heures de la journée. Seule l'alliance de plusieurs métiers peut offrir un accès à un éventail assez large de prestations pratiques pour donner envie au citoyen consommateur de garder le contact en permanence.

Le DNS 2.0 permet aux entreprises de se départir de leur logique de producteur ou de distributeur spécialisé, d'entrer dans la logique du client final, de comprendre et de devancer ses attentes contextuelles : l'offre doit devenir globale et proposer des solutions cohérentes à l'ensemble des questions que se pose le client à un moment et dans une situation donnés. Le DNS 2.0 donne naissance à un « marketing contextuel ».

Cette interaction avec le client dans tous les lieux de vie des 24 heures d'une journée va fournir aux acteurs de l'amont une quantité d'informations vivantes qui n'ont rien à voir avec les fichiers classiques et leurs masses d'informations entretenues à grands frais mais pas nécessairement pertinentes pour les exploitations souhaitées.