

EPCGlobal et Intelligence Economique...

Version 4.3– juillet 2005 - © S.I.A.I.G.E[®] 2005



L'ensemble du contenu de ce mémo (texte, schémas et images) est la propriété exclusive de l'association S.I.A.I.G.E[™]. Tous droits de reproduction ou de représentation sont réservés. Les logos, images et marques relatifs aux autres sociétés, organismes et produits cités ou utilisés dans ce mémo sont la propriété respective de leurs auteurs. Toute mise en réseau, toute rediffusion, sous quelque forme, même partielle, est strictement interdite sans l'accord préalable de l'association S.I.A.I.G.E[™].

Ce droit est personnel et est réservé à l'usage exclusif et non collectif de l'utilisateur. Il n'est transmissible en aucune manière. Tout autre usage est soumis à autorisation préalable et expresse de l'association S.I.A.I.G.E[™]. La violation de ces dispositions impératives soumet le contrevenant, et toutes personnes responsables, aux poursuites pénales et civiles prévues par la loi.

Ce mémo a été déposé sur le site <http://www.copyrightfrance.com/> (acte d'huissier)

Flaq25-07-2005

Constats :

Pour ce qui concerne les principaux acteurs d'EPCGlobal et leurs émules Européens ainsi que le contexte général dans lequel ce sujet s'inscrit, un observateur extérieur pourrait constater que :

- EAN et UCC ont fusionné en « GS1 »
- La société privée VERISIGN opère officiellement la racine de l'ONS depuis plus d'un an
- La société Verisign opère également le « .com » et le « .net » deux « TLD » (Top Level Domains) qui représentent plus de la moitié des domaines enregistrés dans le monde.
- La société Verisign vient d'être reconduite dans la gestion du « .net » (juin 2005) ^{1 et 2}
- Le projet EPCGlobal est activement suivi aux USA depuis 7-8 ans et comporte bon nombre d'acteurs importants qui ne sont pas forcément tous issus de la grande distribution : Département de la Défense, sociétés du secteur des hautes technologies, transport, ...
- La représentation Européenne aux travaux d'EPCGlobal est « symbolique » :
 - 16% du total VS 63% Amérique du Nord (source : EPCGlobal inc.)
 - +136% d'augmentation de la souscription Européenne entre juin 2004 et mai 2005 VS 161% et 410% pour l'Amérique du Nord et l'Asie (source : EPCGlobal inc.)
- EPCGlobal est contrôlé à 50% par GS1 (EAN+UCC) et à 50% par GS1 USA
- Les postes de direction des groupes de travail EPC (SAG – Software action groups) sont principalement occupés par des représentants de firmes Etat-Uniennes. Les recouvrements de fonction sont, en outre, fréquents.
- Une société s'avère particulièrement dynamique s'agissant des aspects liés à l'infrastructure d'EPCGlobal (le squelette et le centre nerveux de l'ensemble du réseau). Cette firme est en effet capable de déléguer plusieurs représentants répartis sur différents groupes de travail EPC et semble également être en lien avec le projet open source parallèle « FREE EPC Software ». Ce projet est destiné à faciliter l'adoption rapide du réseau EPC tout en développant des solutions basées sur les standards et disponibles en libre accès à l'ensemble de la communauté. Il s'agit d'une extension d'un précédent projet de middleware pour la RFID baptisé « Radioactive Software Foundation ».
- Les quelques participants Européens à EPCGlobal constatent régulièrement un manque de transparence dans la communication interne aux groupes de travail. Un récent document interne destiné aux participants d'EPCGlobal illustre ce sentiment et rappelle les règles communautaires de partage et d'ouverture qui doivent caractériser les travaux entrepris et les résultats obtenus.
- Dans l'industrie informatique, plus que partout ailleurs, les standards sont souvent imposés (standards de « fait ») et non issus de travaux de normalisation.

La communauté Européenne des affiliés à GS1 et des acteurs des autres secteurs d'activité concernés par EPCGlobal est donc très peu informée des travaux relatifs au réseau EPCGlobal et compte très peu de représentants dans les groupes de travail.

La plupart des initiatives actuelles sont axées sur l'utilisation des étiquettes à radiofréquences et lecteurs associés dans des projets en **circuit fermé** d'optimisation de gestion des stocks, de traçabilité interne, etc...

¹ Voir : http://www.vnurnet.fr/actualite/tpoepme - business/vie_publique/20050610006 et <http://www.zdnet.fr/actualites/internet/0,39020774,39232810,00.htm>.

² Voir aussi : <http://www.01net.com/editorial/284020/marche/l-icann-libere-les-prix-des-net/>

Or, EPCGlobal définit un principe de fonctionnement en **circuit « ouvert », normalisé** et étant appelé à devenir « **l'Internet des Objets** ». Dans ce contexte, le **réseau EPC** est la raison d'être du projet : les tags RFID ne sont qu'un moyen d'alimenter le système d'information, à l'instar des codes à barres.

A terme, toute velléité d'implémentation des normes EPCGlobal passe donc par une forte implication dans les travaux actuels de normalisation du réseau.

En outre, en matière de concurrence économique, la participation en amont aux travaux de normalisation d'un secteur d'activité octroie à tout « *acteur de la première heure* » un avantage compétitif ultérieur certain.

Ce postulat s'illustre aussi dans le domaine des normes comptables, informatiques, d'audits, légales...

*☞ La communauté des affiliés à GS1 a récemment vécu un tel phénomène avec l'adoption de la norme de transport **EDI INT-AS2**, édictée par un groupe de travail de l'ITF dont le responsable est également le fondateur d'une institution privée délivrant la seule certification officielle pour ce qui concerne les solutions proposées par les éditeurs et supportant ce protocole. Notons au passage que l'un des principaux vecteurs de diffusion de ce protocole fut et reste une entreprise leader du secteur de la grande distribution au niveau mondial qui incite fermement ses partenaires à migrer vers cette solution. Cette entreprise est également très active au sein d'« EPCGlobal ».*

Quelle que soit la participation des acteurs Européens à ce projet, l'adoption d'EPCGlobal à l'échelle mondiale se fera par diffusion de « proche en proche ». En effet, dans une économie où l'interdépendance entre les acteurs permet une adoption des technologies par rebonds successifs, le déploiement des normes EPC au sein d'un acteur majeur du secteur sera, une fois les derniers freins techniques, légaux et administratifs levés (problèmes de lecture et filtrage des numéros EPC, utilisation des fréquences, standardisation d'EPC IS, ...), le signal d'un déploiement généralisé.

Sur ces simples constats, la participation des entreprises Européennes aux standards EPCGlobal est donc primordiale (veille, souscription, ...)

Risques structurels :

Rappel : ONS (*Object naming system*) est un service du réseau EPC qui s'appuie sur la technologie DNS (*domain name system*). Lors de la lecture d'un numéro EPC, le service ONS permet d'obtenir, à partir de l'identifiant « EPCManager », le nom de domaine Internet (affilié au domaine racine, voir ci-après) où se situent les serveur « EPCIS » du fabricant qui dispensent l'information propre au produit concerné.

Le réseau EPCGlobal repose sur Internet : La gestion du réseau EPCGlobal renvoie donc aux problèmes habituellement rencontrés, s'agissant de la **gouvernance du réseau Internet** et des considérations politico-économiques afférentes³.

Historique :

A l'origine (Auto-ID center du MIT) la « *EPC Namespace Authority* » devait être, par principe, un **organisme de normalisation**.

→ Il s'agit, à date, d' **EPCGlobal Inc.** (voir schéma ci-après)

La « *EPC Namespace Authority* » délivre⁴ les identifiants « EPCManager » que l'on retrouve dans les numéros EPC, identifiants propres à chaque fabricant.

La « *EPC Namespace Authority* » ou « EPCGlobal Inc. » définit également l' « **EPC root domain name** » qui sert de suffixe commun aux accès ONS (branches de l'arbre ONS, racine) - (voir schéma ci-après)...

A chaque identifiant « EPCManager » correspond un sous domaine affilié au domaine racine « EPC root domain name ».

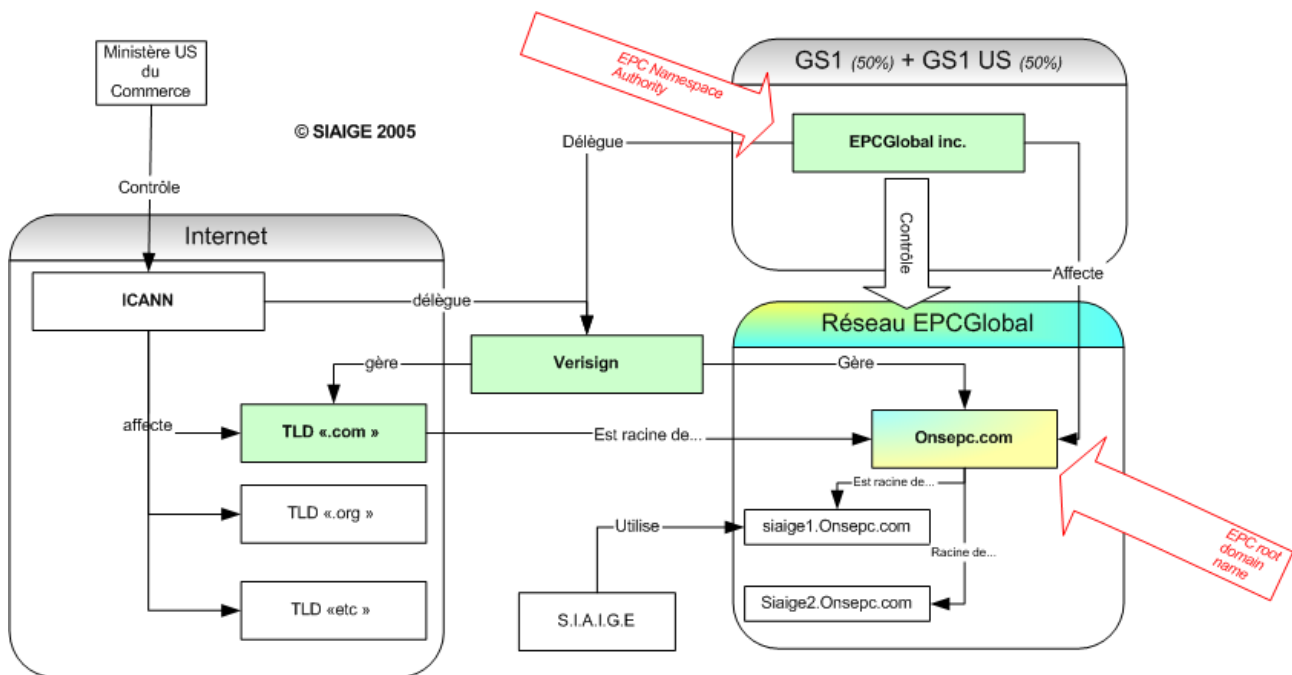
→ A date, la gestion de l' « **EPC root domain name** » : **onsepc.com** est confiée à **Verisign**, société privée Etat-Unienne.

☞ Verisign est une société réputée pour la gestion des infrastructures de réseaux et dispose d'une grande expertise dans ce domaine. Son expertise est donc toute indiquée pour satisfaire au parfait accomplissement de cette tâche. Verisign gère en outre le répertoire principal qui dresse la liste de tous les suffixes actifs sur Internet.

© S.I.A.I.G.E® 2005

³ voir aussi : <http://www.01net.com/editorial/283345/>

⁴ vend ?...



Un (marché) réseau captif ?

Techniquement parlant, le domaine racine (*EPC root domain name*, *Verisign*) est informé de toutes les requêtes non abouties effectuées sur le système ainsi que de toutes les requêtes qui ne sont pas traitées par les caches locaux décentralisés (le système est pyramidal, de type « DNS », mais la gestion est dite « distribuée »).

En outre, sans moyen effectif de contrôle (coercition ?) sa position centrale dans le dispositif lui permet potentiellement de formuler les règles de tout changement, à quelque niveau de hiérarchie que ce soit (coûts d'enregistrement, règles d'admission, ...) et d'exercer son autorité, « de façon directe (domaines du plus haut niveau) ou indirecte (sous domaines) »⁵.

Dans le cas de la mise en place probable d'une infrastructure de clés publiques⁶ c'est aussi l'opérateur du domaine racine qui occupe une place privilégiée pour assurer la délivrance, voire la vente des certificats électroniques (**rôle d'opérateur de certificats**)⁷ - Dans ce contexte, **EPCGlobal Inc.** serait « **autorité de certification** » (voir schéma ci-après).

Les serveurs de cet opérateur sont régulièrement interrogés lorsqu'un contrôle de validité sur un certificat est effectué (listes de révocation) : ce processus permet donc potentiellement d'obtenir indirectement des informations qualifiées sur les flux d'information ainsi observés.

Cette position renforcerait ainsi une situation potentiellement « monopolistique » qui peut avoir un impact sur la qualité de l'offre, les prix et entraîner une dépendance des adhérents GS1.

Pour ne parler que de l'aspect économique, si l'on parle de volumétrie, il s'agit à moyen terme de millions, voire de milliards de certificats...

⁵ voir « Icann et la gouvernance d'Internet » <http://smsi.francofonie.org/IMG/pdf/icann-klein.pdf>

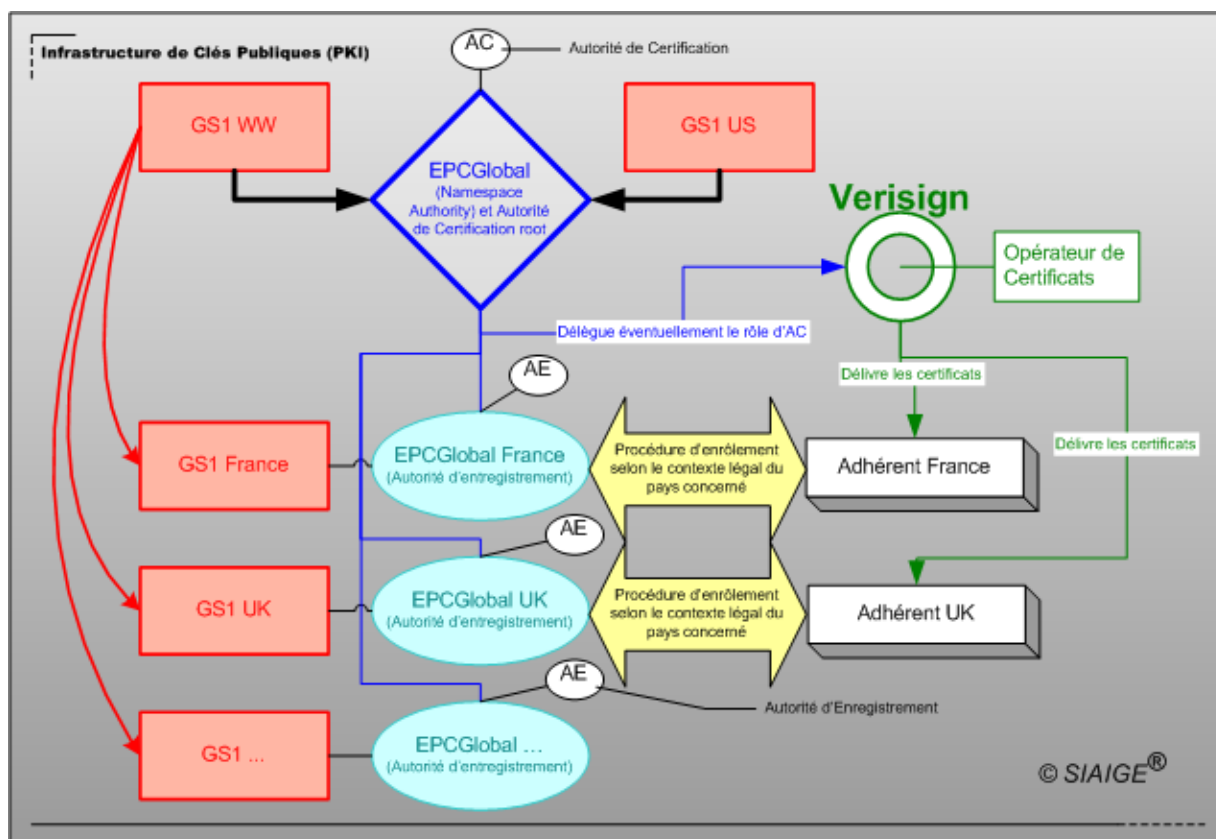
⁶ Les fonctions d'authentification, d'intégrité (et éventuellement de confidentialité et de non répudiation) seront, à priori, assurées par une architecture combinant l'utilisation conjointe du protocole **SAML** et des **certificats X509 V3** (compatibilité Kerberos V5). L'interrogation et la réponse des **services Web** hébergés sur les serveurs EPC IS se fera de façon sécurisée et sur le principe du « SSO » – « Single Sign On ». En outre, l'utilisation d'AS2 pour la partie « transport » est couramment évoquée... Enfin, concernant ONS (Discovery Services), l'utilisation des certificats X509 est également probable à terme :

La sécurité des échanges et requêtes ONS / DNS peut être basée dans un premier temps sur DNSSEC (niveau 4 couche OSI), puis, éventuellement, dans un second, renforcée par IPV6 (niveau 3 couche OSI) qui possède intrinsèquement une gestion standardisée de la sécurité. DNSSEC est une déclinaison sécurisée du DNS (l'outil DNS est BIND, pour rappel) et permet d'assurer, entre autres, les échanges sécurisés entre les serveurs (réplication) ainsi que la propagation des certificats, le cas échéant. Le protocole TSIG pourra être utilisé pour s'assurer que les enregistrements DNS transmis ne sont pas modifiés en route.

→ La mise en place d'une « architecture orientée services » sécurisée entre acteurs / services qui ne se connaissent pas, à priori, implique plusieurs contraintes :

- Une organisation permettant de standardiser les échanges d'identité et d'assurer la notion de « SSO » : Une autorité de certification basée sur le modèle « Liberty Alliance » (partenariat en cours avec EPCGlobal)
- Un système de publication de services : UDDI / WSDL
- Une architecture technique sous-jacente : SOAP + SAML [jetons Kerberos / certificats X509] et une infrastructure de clés publiques (PKI) permettant la délivrance de certificats électroniques.

⁷ ... et occuper le rôle d'**autorité de certification** si d'aventure celui-ci est délégué par EPCGlobal (les deux hiérarchies, « technique » et « sociale » étant structurellement liées)



→ Les problèmes de **souveraineté numérique** soulevés sont également des risques potentiels en termes de **souveraineté économique** si le contrôle des acteurs en présence n'est pas suffisamment [dimensionné / effectué / garanti].

→ Tout va donc dépendre des moyens dont dispose EPCGlobal pour assurer la neutralité de l'ensemble et éviter qu'un déploiement rapide des solutions déjà en place (ONS « compliant », notamment) ne permette l'émergence d'un « standard de fait ».

Une menace pour les standards en place ?

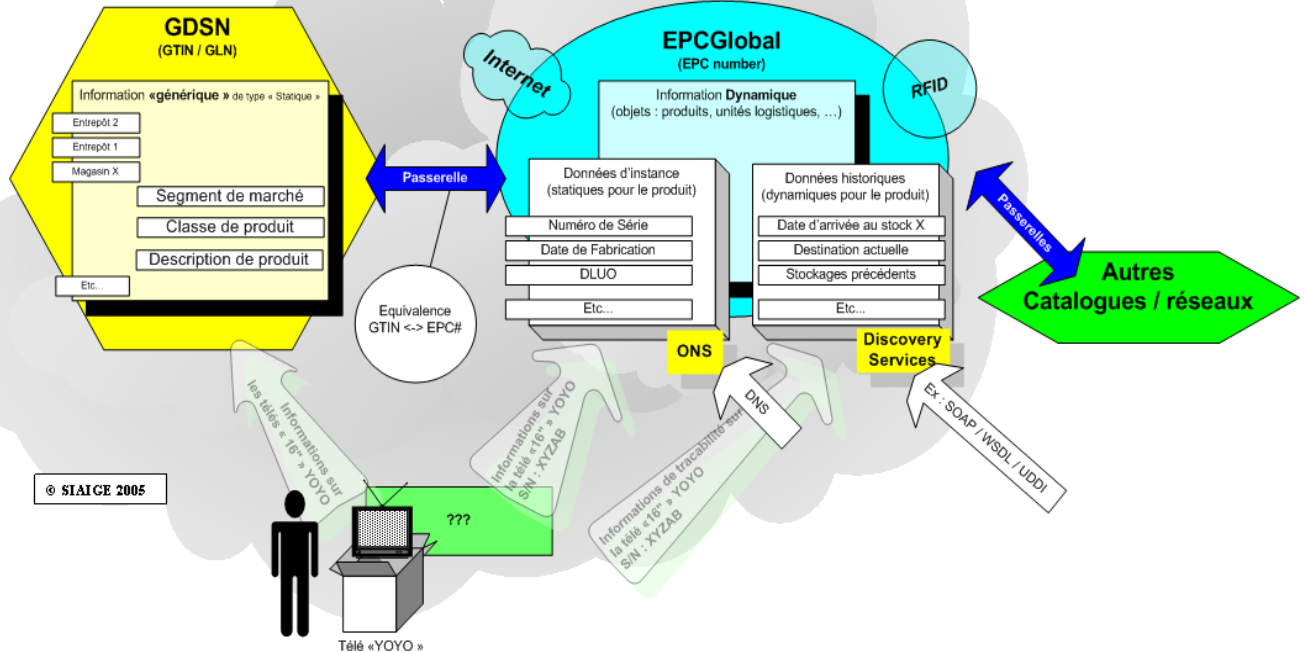
Pour rappel, le « GDSN » (Global Data Synchronization Network) est le Réseau de synchronisation globale des données (secteur de la grande consommation, Supervisé par GS1) qui regroupe trois composants principaux :

- GTIN – global trade item number
- GLN – global location number
- attributs – données ou caractéristiques d'un produit

GDSN délivrera de l'information générique sur le produit tandis que le réseau EPC permettra l'accès à l'information dynamique (voir schéma ci-dessous). GDSN propose en outre bon nombre d'informations sur les entités qui fabriquent, transportent, conditionnent, stockent et vendent les produits adressés par le réseau EPCGlobal.

© S.I.A.I.G.E® 2005

Communauté GS1



© SIAICE 2005

Télé «YOYO»

Il semble prévu que l'opérateur du domaine racine de l'ONS développe une passerelle entre les deux systèmes (EPC network et GDSN), ce qui n'est, a priori, pas réalisé aujourd'hui (juillet 2005). La correspondance entre les deux systèmes pourrait se faire au niveau du numéro GTIN, le réseau EPC rajoutant la notion de numéro de série au niveau objet (SGTIN).

Il est plausible d'imaginer que GDSN fonctionnera, dans un premier temps, comme référentiel de données (MASTER DATAS) pour l'ensemble du système formé par GDSN/EPCGlobal. Inversement, il est pertinent de se demander si le schéma de données du registre de l'ONS peut être étendu pour incorporer des données complémentaires existant à date dans GDSN seul.

→ Dans cette éventualité, une certaine redondance entre les deux systèmes (EPC Network / GDSN) ne risquerait-elle pas d'exister ?

La valeur ajoutée de GDSN repose actuellement sur la délivrance d'information qualifiée (référentiel faisant autorité). Cet argument, dès l'instant où ONS emploie une méthodologie équivalente pour qualifier l'information (notamment au travers de l'usage des certificats électroniques et de procédures d'enrôlement afférentes rigoureuses), est grandement relativisé. Enfin, au travers de DNS, l'infrastructure supportant ONS est déjà largement déployée et d'un coût de maintenance et de mise en œuvre d'autant plus compétitifs qu'ils sont déjà déployés pour d'autres périmètres techniques ou fonctionnels. Sur ce dernier point, l'avantage revient à EPCGlobal.

D'autres risques habituels, relatifs à l'usage d'Internet...

L'architecture ONS, une fois déployée massivement, pose un problème de volumétrie aux infrastructures Internet actuelles (lié au nombre et au temps passé par les requêtes générées) :

- La « toile » est-elle suffisamment dimensionnée pour supporter un processus industriel de masse en sus du trafic actuel ?...
- Ne faut-il pas en outre attendre une migration vers IP V6 (EPC va « consommer » des adresses IP) ?

L'usage du média Internet expose potentiellement l'ensemble des flux traités au sein d'EPC à divers risques :

- Attaque par « déni de service » - voir précédentes attaques sur les « DNS racines » mondiaux et conséquences qui ont suivi
- Usurpation d'identité
- Détournement des informations, Fausses informations...

→ La position centrale de l'opérateur de la racine l'expose particulièrement dans ces types de scénarii