

## Les investissements d'avenir dans le numérique

*Les réponses ci-après de l'ACSEL à la consultation publique s'appuient sur les contributions de ses membres, qu'elle fait siennes.*

### SECTION 1 - CONTEXTE

#### B - Priorités et principes d'intervention

##### **Q 1B : Comment favoriser les liens entre politique d'investissement très haut débit et développement des services numériques de nouvelle génération**

Au vu du tableau ci-dessous on peut considérer que la pénétration du numérique dans les entreprises n'est pas dépendant des infrastructures lourdes, tous les échanges électroniques pour lesquels la France a un certain retard peuvent être couverts par des investissements minimes. (L'implantation de factures dématérialisées sous format PDF sécurisé avec archivage électronique coûte quelques centaines d'euros + une transaction de 0,40 €). Cette technologie est utilisable par Internet et sécurisée dans de multiples hébergements. Cet exemple peut être décliné sur l'ensemble de la *supply chain* depuis le fournisseur du fournisseur au client du client, jusqu'au particulier. Plus les données à l'intérieur des « tuyaux » circuleront, plus la rentabilité des infrastructures à mettre en place sera rapide.

Mobilisons les CCI et les prestataires, SSII, distributeurs de système métiers, autour des TIC facteurs de compétitivité de leurs adhérents et de leurs clients, par étape, et la diffusion peut se faire très rapidement sans gros investissements. En résumé : *positionnons les usages avant les infrastructures.*

Pourcentage des entreprises de + de 10 salariés échangeant des données électroniques avec des parties tierces (source Eurostat enquête 2007/2008)

Infos produits : Fiche produits	25 %
Banques : instruction de paiement	32 %
Envois commandes aux fournisseurs	22 %
Documents transport	14 %
Réception commandes des acheteurs	18 %
Prévision de stock et production	5 %
Prévisionnel clients sur livraisons	4 %
Prévisionnels échangés avec fournisseurs	9 %
Echange électronique avec fournisseurs sur planning livraison	6 %

Pourcentage moyen : 13%

Rang de la France sur 26 pays européens : 18<sup>e</sup>

Malheureusement les entreprises françaises en retard sont, dans le même temps, enjointes par de nouveaux règlements nationaux ou européens de communiquer électroniquement avec les administrations, et ce sont les PME et les TPE qui en souffrent le plus : ICS, GAMMA EMCS, Empreinte Carbone sur les étiquettes des produits en rayon, Taxe Carbone, Plan Helios de modernisation de l'Etat, OEA sont des nouvelles règles impliquant souvent des liaisons électroniques pour lesquelles les TPE et PME ont du mal à s'intégrer ; il n'est qu'à rapprocher la période de mise en place de ces mesures (2009-2012) des pourcentages du tableau pour se

rendre compte de la marche forcée vers le numérique que l'on impose aux TPE comme aux PME.

## SECTION 2 - DEVELOPPEMENT DU CLOUD COMPUTING

**Q 2.8 : Quels thèmes de R&D vous paraissent prioritaires pour améliorer la compétitivité des opérateurs d'infrastructures ou de plateformes de *cloud computing* ? Quelles sont les caractéristiques de ces thèmes de recherche en termes de verrous technologiques, de proximité du marché (horizon temporel) et de synergies avec les compétences françaises du domaine ?**

Dans le domaine de la dématérialisation, la sûreté et la sécurité des opérations du commerce international est un sujet qui semble fédérateur de nombreux acteurs du logiciel national, tant pour faire évoluer des éditeurs actuels vers un mode SAAS, que pour fédérer des offres existantes qui se doivent d'être interopérables : cela veut dire qu'il faut accélérer le développement de plateformes qui permettent de faire le lien entre les différents systèmes d'information des acteurs de la chaîne logistique et, parallèlement, s'assurer que ces acteurs sont des acteurs sûrs :

1° Les enjeux pour les opérateurs du commerce international :

La mondialisation de l'économie est un phénomène irréversible. Les entreprises françaises accusent un retard tangible dans la dématérialisation de leurs flux :

Pourcentage moyen : 13%

Rang de la France sur 26 pays européens : 18e

Les opérations sont de plus en plus nombreuses et complexes :

- contraintes douanières et sécuritaires (CTPAT Us, OEA et Import control System en Europe)
- contraintes Sanitaires (FDA, AFFSSAPS, ETC)
- Les clients mettent toujours plus de pression sur les coûts, les délais et de la qualité des opérations

La traçabilité totale et l'optimisation des chargements, l'assurance de travailler avec des opérateurs sûrs sont désormais des pré-requis.

Le 1er janvier 2011 les transporteurs doivent fournir 29 données xml dans le système douanier européen ICS : *pas de données = pas de déchargement*.

Le 1er Janvier 2013, nouveau Code des douanes communautaires. Les opérateurs non certifiés OEA vont avoir plus de difficultés à mener leurs opérations de commerce international

2° Qui sont les opérateurs :

- 35.000 sociétés en France réalisent un volume conséquent de leur chiffre d'affaires grâce à ces opérations internationales :
  - Exportateurs
  - Importateurs
  - Transporteurs (air, mer, route)
  - Transitaires commissionnaires en douane
  - Logisticiens

- Ces opérateurs effectuent aujourd'hui beaucoup de saisies ou de ressaisies d'informations dans de nombreux systèmes, ce qui signifie : perte de temps, risque d'erreurs, pas de traçabilité complète de la chaîne
- Ces opérateurs perdent en moyenne 25 à 30 % sur leurs frais de transport car leurs containers sont insuffisamment chargés, ce qui se traduit par 25 % de dépense carbone en trop !
- Ces opérateurs, leurs fournisseurs, prestataires, sous-traitants doivent répondre à des standards de qualité, sûreté et sécurité (statut opérateur économique agréé douane, sûreté et sécurité) sans lesquels ils risquent des contrôles douaniers renforcés !

## SECTION 5 – DEVELOPPEMENT DES NOUVEAUX USAGES

### 5.C - Sécurité et résilience des réseaux.

Le thème « **sécurité et résilience des réseaux** » est d'une importance primordiale pour le développement de la société numérique dans son ensemble. Le développement des usages numériques atteint un palier. Il ne pourra le dépasser avec des bases solides que grâce à la mise en œuvre de mécanismes de confiance plus avancés et mieux compris par des publics très diversifiés dotés de repères culturels différents.

Les contextes d'évolution professionnels ou territoriaux, les courants d'information contradictoires, les évolutions incessantes des pratiques (sous la poussée d'innovations continues) et la médiatisation d'importance agissent sur le ressenti des besoins en contradiction avec la capacité d'appropriation des acteurs.

Dans ce contexte, il est essentiel d'associer les champs de développement (technologiques, juridiques, ou d'usage) aux utilisateurs pour leur permettre de mieux maîtriser leur usage d'Internet.

L'un des enjeux principaux des évolutions nécessaires pour un utilisateur se situe dans sa capacité à concevoir, gérer et maîtriser les « identités numériques » dont il aura besoin pour vivre pleinement sa vie numérique en confiance. L'authentification des utilisateurs devient un enjeu fondamental à mesure de l'enrichissement des usages possibles. Ceci se vérifie dans tous les types de services en ligne, qu'ils soient marchands ou non, publics ou privés, avec un accès depuis tout type de terminal (fixe ou mobile).

L'Acsel s'est positionnée clairement sur ce thème de l'Identité numérique en créant une Commission idoine ayant déjà permis un premier décryptage des différents aspects du sujet et le rassemblement des acteurs importants dans ce domaine.

Au-delà de cette première phase, elle souhaite promouvoir les conditions de mise en œuvre de services ou de solutions d'authentification et de gestion des identités qui soient interoperables et acceptables largement par l'ensemble des acteurs de l'écosystème. A ce titre, le projet de label « IDéNum » constitue un excellent catalyseur des énergies et devrait être soutenu dans le cadre des investissements d'avenir.

Dans ce domaine, forte d'une large représentativité d'acteurs privés et publics engagés dans des projets, des développements, voire même des offres, l'Acsel apportera son soutien actif à toute initiative européenne, nationale ou territoriale sur les solutions de gestion des identités.

Elle propose de travailler à instaurer un écosystème interopérable, à en définir les règles financières et de responsabilité ainsi que la gouvernance.

**Q 5.c.1 : Avez-vous d'autres objectifs à proposer en matière de sécurité de systèmes d'information**

- Diffuser l'usage de l'identité numérique, ce qui constitue une brique de base à l'approche de la sécurité informatique.
- Permettre des échanges de documents dématérialisés pouvant être légalement probants par des procédés garantissant la signature de l'émetteur, la confidentialité de l'échange et l'intégrité des données transférées.

**Q 5.c.2 : Les thématiques envisagées vous paraissent-elles pertinentes ? Souhaitez-vous en inclure d'autres ?**

La thématique de la biométrie et des technologies associées (capture des données biométrique, conservation, comparaison, protection) et son utilisation dans les thèmes envisagés : authentification, identification, signature électronique, doit être intégrée.

Cette technologie doit être mise en œuvre en accord avec les prescriptions de la CNIL ; à ce titre, la carte à puce sous différents 'facteurs de forme' (ISO, Token..) est un dispositif qui, par la nature personnelle et décentralisée de l'information stockée, est un garant de cette confidentialité des données personnelles.

A cela, il serait utile de rajouter : le routage vers des destinataires partiellement identifiés, la protection de la vie privée lors des échanges et la valeur probante des échanges de données.

**Q 5.c.3 : Selon vous, l'Etat doit-il jouer un rôle particulier vis-à-vis des produits de sécurité et de la création des environnements de confiance dans le numérique ? Si oui, lesquels ? D'autres actions que celles envisagées (aide à la R&D et prises de capital) sont-elles nécessaires ?**

L'Etat devrait jouer un rôle « régalien » de maîtrise et de validation de l'identité numérique des personnes physiques. Il devrait être une autorité de confiance dans ce domaine.

En effet, d'autres actions nous paraissent nécessaires :

Dans la **normalisation** des niveaux de sécurité des produits, la **création de labels de confiance** liés à l'identité numérique (type IdéNum, etc.), la **création d'organismes indépendants ou mixtes** (privés / publics) de fédération des identités sur internet, développement et intégration des documents électroniques sécurisés et de leurs usages dans ce contexte (ex : carte d'identité électronique, passeport biométrique, dossier médical).

La **communication et l'information** de l'Etat pour la mise en place de systèmes de sécurité, d'authentification et d'identification est également un point important, en particulier pour la protection des mineurs sur Internet.

**Généralisation des services numériques (Signature Electronique)** pour les transactions administratives, financières.

**Q 5.c.4 : Il existe une réglementation sur certains produits de sécurité : la connaissez-vous ? Pensez-vous qu'elle est suffisante ?**

Il existe une réglementation RGS, des référentiels de sécurité, des critères communs, des normes SO et des organismes (Agence nationale de la sécurité des systèmes d'information -

ANSSI, COFRAC, ...) consacrés à la certification, qui nécessitent des dispositifs qui nous paraissent lourds. Cela entraîne une application parfois difficile ou incomplète. Un travail de clarification et de simplification pourrait être utile.

**Q 5.c.5 : S'agissant de la résilience, il n'a pas été identifié de projet structurant à ce stade. Partagez-vous cette vision ou avez-vous des projets à suggérer ?**

Au-delà des aspects purement techniques, la résilience des réseaux est basée sur sa stabilité sa capacité à résister aux attaques et la confiance portée par utilisateur dans son fonctionnement. Il est fondamental de gérer l'accès aux réseaux de manière globale, identifier les acteurs des transactions pour lutter contre la cybercriminalité et le terrorisme. A ce titre, l'ensemble des thèmes mentionnés sont de nature à assurer de manière générale le management de l'identité et donc d'assurer une meilleure résilience des réseaux.

Il nous semble pertinent de prendre en compte le travail rapporté par l'ENISA (European Network and Information Security Agency).

### **5.E. Ville numérique**

Le thème « **Ville numérique** » recouvre une réalité très diverse. L'usage du numérique dans les environnements urbains ou métropolitains, que ce soit pour les relations de proximité ou à distance, représente un potentiel de croissance substantiel.

C'est aussi un ensemble d'expérimentation, de cristallisation d'innovations, de diffusion des usages et des pratiques et d'appropriation par des populations en demande dès lors qu'on les associe aux démarches d'innovations qui enrichent leur vie de citoyen et faciliteront leur vie d'administré.

Les collectivités territoriales peuvent et doivent jouer un rôle moteur dans la mise en place d'écosystèmes de confiance. Qu'il s'agisse de services web, mobiles ou de services de proximité (sans contact NFC), la problématique rejoint en partie celle du thème « sécurité et résilience des réseaux », du point de vue de l'Acsel : les services pourront réellement décoller dès lors que les conditions de sécurisation et de confiance seront réunies.

Deux conditions devront être réunies :

- une cohérence des usages proposés.

A titre d'exemple, on peut citer la sécurisation des infrastructures et usages de la mobilité ou l'ensemble des usages « citoyens », de la démarche administrative totalement dématérialisée auprès des mairies (notamment pour des services payants) au vote électronique (local voir national), en passant par les services mobiles basés sur la présence ou la réalité augmentée.

Bien entendu, l'interopérabilité et le modèle économique constituent des défis importants afin d'ouvrir le champ à la panoplie des services qui pourraient émerger.

- En outre, la gestion des identités appliquée aux différentes interfaces (mobiles, ordinateurs, tablettes, bornes, etc.) permettra d'assurer une cohérence dans l'ergonomie et dans les usages. Cette cohérence devrait faciliter l'adoption par les utilisateurs finaux, de même que la mise en place de services réellement multicanaux au bénéfice de l'utilisateur.