

ALLIANCE POUR LA CONFIANCE NUMÉRIQUE (ACN)



**Les acteurs industriels se mobilisent
pour un avenir numérique de confiance**

19 octobre 2010

Contacts Presse:

Yoann Kassianides - FIEEC
Tél. +33 (0)1 45 05 70 11
Mob. +33 (0)6 26 78 57 55
ykassianides@fieec.fr

Patrick Guérin - GIFAS
Tél. +33 (0)1 44 43 17 50
Mob. +33 (0)6 07 71 86 87
patrick.guerin@gifas.asso.fr



Sommaire

Communiqué de Presse	4
Organisation & Définition	5
Situation actuelle	7
Les enjeux de l'Alliance	8
Thèmes prédominants avec des défis à relever	10
Les acteurs de l'Alliance	16



LES INDUSTRIELS FRANÇAIS S'ORGANISENT POUR RELEVER LE DÉFI DE LA CONFIANCE NUMÉRIQUE AU SEIN DE L'« ALLIANCE POUR LA CONFIANCE NUMÉRIQUE ».

ACN est une instance informelle souple qui :

- **regroupe à la fois des fédérations, des entreprises et des institutionnels ;**
- **se propose d'être l'interlocuteur privilégié sur les questions de sécurité numérique.**

La sécurité est un besoin sociétal fort. La confiance numérique s'appuie sur un ensemble de solutions qui répondent aux risques de sécurité rencontrés par les entreprises, les individus, les administrations. La confiance numérique concerne en particulier la sécurisation des identités, des communications et des flux de personnes et de biens, au bénéfice des usagers.

Face à de tels enjeux :

- Peut-on continuer à sous-traiter la gestion de certaines de nos données les plus sensibles, personnelles ou professionnelles, hors de nos frontières ?
- La sécurité des réseaux physiques (énergie, eau, flux de produits...), numériques (identité numérique, échanges électroniques) et des flux de personnes et de biens, peut-elle être sans risque confiée à des intérêts non européens ?

Les acteurs économiques français disposent de solutions et de compétences de tout premier plan pour répondre à ces enjeux sociétaux et régaliens : systèmes de biométrie, carte à puce, systèmes d'identification ou encore détection d'activité pour la sécurité, management des réseaux numériques et de communications électroniques, cybersécurité, protection des infrastructures critiques....

Mais, en comparaison avec d'autres zones géographiques comme les Etats Unis, qui ont su fédérer l'action publique et mobiliser leur industrie, force est de constater qu'il existe en France un éparpillement des instances de décision et qu'il est nécessaire de renforcer la coordination entre les acteurs tant publics que privés.

C'est pourquoi ACN souhaite mobiliser tous les acteurs concernés afin que se développe une industrie créatrice de valeur, exportatrice et qui réponde aux attentes sociétales.

ACN a identifié, dans un premier temps, trois sujets prioritaires :

- Usage et maîtrise des données sensibles, personnelles et patrimoniales ;
- Confiance sur Internet (Cybercriminalité) ;
- L'apport du numérique sur la sécurité des flux.

Parce que l'investissement dans la confiance numérique répond à une double nécessité citoyenne (maintien de la souveraineté nationale, protection des données privées) et industrielle (maintien des compétences, source de croissance et de création d'emplois non délocalisables), les membres d'ACN s'organisent pour faire des propositions et relever ce défi.



Qu'est-ce qu'ACN ?

L'Alliance pour la Confiance Numérique (ACN) est une coordination des principaux acteurs de la sécurité numérique en France (Fédérations, entreprises, investisseurs...), qui a pour vocation de représenter cette industrie auprès des pouvoirs publics afin de peser dans les débats tant au niveau national qu'europpéen et de coordonner des actions concrètes de développement de marchés et solutions.

L'ACN est une coordination informelle et ouverte qui regroupe aujourd'hui deux grandes fédérations industrielles (la Fédération des Industries Electriques, Electroniques et de Communication – FIEEC et le Groupement des Industries Françaises Aéronautiques et Spatiales – GIFAS), des entreprises industrielles (Bull, CS, Cassidian, Orange, Gemalto, Keynectis, Radiall, Morpho, Siemens, Thales) et un investisseur avisé d'intérêt général (La Caisse des Dépôts). ACN est ouverte aux industriels, groupements et fédérations qui souhaiteraient rejoindre l'initiative.

Initialisée en fin 2009, ACN a répondu en juin 2010 à la consultation gouvernementale sur l'économie numérique.

Qu'appelle-t-on « Confiance numérique »?

La sécurité est un besoin sociétal fort. La confiance numérique s'appuie sur un ensemble de solutions qui répondent aux risques de sécurité rencontrés par les entreprises, les individus, les administrations. La confiance numérique concerne en particulier la sécurisation des identités, des communications, des transactions et des flux de personnes et de biens, au bénéfice des usagers.

ACN a vocation à couvrir les 3 domaines prioritaires cités mais aussi d'autres domaines comme notamment la résilience des infrastructures, la prévention et la gestion des crises et catastrophes naturelles, l'information des populations...

Quelle gouvernance pour ACN ?

- type de structure légère, informelle ;
- une instance de décision ;
- des groupes de travail thématiques à durée limitée ;
- comité stratégique de développement et de soutien à la filière industrielle dédiée à la confiance numérique

Ce comité se réunira au sein de l'ACN avec pour objectif :

- ◆ de partager une vision commune des enjeux économiques et technologiques du secteur en France et à l'international ;
- ◆ d'identifier les segments à soutenir ou à développer dans ce secteur ;
- ◆ de mettre en place avec les industriels et les institutionnels des stratégies concertées, développer des synergies et des alliances dans ce domaine ;



- ◆ d'être un relais vers les investisseurs pour remonter les besoins en financement des projets et des entreprises du secteur/ qualifier les projets prioritaires face aux enjeux technologiques et économiques pour l'industrie française.

Il rassemblera de manière unique des groupes d'experts représentants de l'Industrie, des PME/TPE du secteur, pôles de compétitivité, des institutions et de l'investissement pour agir de manière concrète, concertée et coordonnée.

La Caisse des dépôts qui est un investisseur avisé de long terme au service du développement économique et de l'intérêt général a fait de la confiance numérique un axe stratégique de son action pour le développement de l'économie et la société numérique. Elle sera un interlocuteur privilégié dans ces comités.

ACN se veut un structure réactive, dynamique et performante qui deviendra naturellement le partenaire privilégié de la confiance.



Notre constat

Ainsi que l'a montré le rapport Filière STIC des Etats Généraux de l'Industrie, les technologies électroniques et numériques sont le fondement de la compétitivité globale de l'ensemble du tissu économique, industriel ou de service, et l'un des moteurs puissants d'évolution et de croissance durable de notre société, soucieuse de son impact sur l'environnement. Leur généralisation dans l'ensemble des processus (productifs, de contrôle, informationnels...), permet des innovations de rupture pour tous les secteurs, industriels et de services, mais également dans les usages (santé, administration, éducation...).

Cela implique notamment que les questions de sécurité numérique sont désormais au cœur des futurs enjeux du développement des solutions, services et outils de notre société.

On constate ainsi aujourd'hui que l'ensemble des flux physiques et virtuels (communication, énergie, eau, transports, voyageurs...) devient de plus en plus numérisé grâce à des réseaux intelligents de capteurs et de transmission de données. Les flux physiques ne sont pas numérisés, mais leur sécurité fait appel au numérique. Cette numérisation des flux permet de bâtir de nouvelles formes d'optimisation (par exemple les *smart grids* dans le domaine de l'énergie, le *cloud computing*...), et d'imaginer de nouveaux services et de nouveaux usages. Dans le même temps, ce mouvement introduit de nouveaux enjeux tout particulièrement en termes de sécurité, que ce soit au niveau des personnes (identification, authentification, données personnelles), des entreprises (données patrimoniales), de l'Etat (infrastructures stratégiques et vitales), ou au niveau international (interconnexion des réseaux notamment).

De même, l'utilisation de nouveaux outils et solutions basées sur l'électronique et le numérique (contrôle d'accès, vidéoprotection, cryptage, etc.) permet de répondre plus efficacement à la demande croissante de sécurité des citoyens, des entreprises et des Etats, que ce soit dans le monde virtuel (cybersécurité, identité numérique...) ou réel (contrôle des infrastructures critiques, contrôle des flux...).

Ces nouvelles opportunités existent en France, mais se retrouvent également partout en Europe et dans tous les pays à un degré plus ou moins avancé selon leur stade de développement. Il s'agit d'un marché mondial.



Les enjeux de l'Alliance

Les entreprises françaises ont su développer dans la sécurité des compétences très importantes, dans toutes les composantes de la chaîne de valeur (composants, logiciels et services informatiques, services de télécommunication, produits, systèmes...). La France bénéficie ainsi de manière unique d'un écosystème d'innovation qui associe des grands groupes leaders mondiaux, des ETI (Entreprises de Taille Intermédiaire) de croissance et un réseau de PME très innovantes, des laboratoires et des centres de recherche.

Cet écosystème est présent sur l'ensemble des régions en France, notamment dans sa dimension électronique, ainsi que l'a montré l'édition n°2 de l'Observatoire de l'électronique publié par la FIEEC. S'il est difficile à ce stade de quantifier précisément les emplois induits à ce stade, on peut néanmoins affirmer d'ores et déjà que ceux-ci sont de l'ordre de plusieurs dizaines de milliers en France. L'importance stratégique du secteur donne à ces emplois une localisation essentiellement nationale, avec cependant de fortes potentialités à l'export et au développement international. Citons, en exemple, le cas de l'industrie de la carte à puce.

Une très grande partie des outils et des technologies de la sécurité existe déjà et la France a des atouts industriels et de service pour prendre un leadership mondial sur ce marché. En revanche, c'est souvent au stade du déploiement de ces outils et services, sur le territoire national, de son adaptation aux besoins publics ou citoyens que les travaux sont à lancer de façon prioritaire. En effet, si peu de marchés de sécurité s'ouvrent en France c'est parce que le sujet a du mal à émerger au niveau des décideurs de manière structurée. Il est nécessaire de développer un marché structuré et solvable.

Or le rôle des autorités publiques est majeur dans ce secteur. Faut-il citer le *Homeland Security* américain et les dotations budgétaires qui ont ouvert la voie pendant plusieurs années? Une politique industrielle et une politique de soutien de la souveraineté se doit d'être définie si nous souhaitons conserver la mainmise sur nos outils stratégiques. Force est de constater qu'il existe en France un éparpillement des instances de décision qu'il est nécessaire de coordonner que ce soit au niveau public ou privé.

D'autant plus que le déploiement de solutions sur le territoire national aurait pour conséquence d'offrir aux industriels français une vitrine à l'exportation.

Nous pensons par exemple :

- qu'une politique nationale doit être mise en place dans le domaine normatif afin d'éviter l'imposition de normes correspondant à des équipements étrangers ;
- que l'Etat doit mettre en place un outil de soutien aux exportations dans le domaine des systèmes de sécurité, par lequel l'administration servirait de relais d'information sur les besoins des Etats étrangers, de façon similaire au rôle que joue la DGA (Direction Générale de l'Armement) dans le domaine de la défense. La DCI (Direction de la Coopération Nationale) au sein de la DGPN (Délégation Générale de la Police Nationale) pourrait assurer cette mission, parmi d'autres ;
- que l'Etat doit veiller à ce que les projets de recherche, financés sur budget national ou européen, correspondent à des besoins exprimés par les clients (Etat ou opérateurs), et orienter davantage de financement vers les projets de démonstrateurs ;



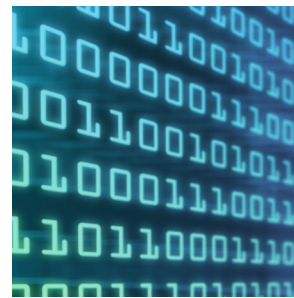
- que l'Etat peut favoriser le rapprochement entre opérateurs privés et industriels fournisseurs de systèmes, pour permettre une réconciliation entre deux mondes qui se connaissent mal ; cela permettra aux deux parties de mieux cerner les besoins en matière de sécurité et les apports de la technologie.

Les outils, technologies et systèmes numériques pour renforcer la confiance et la sécurité de notre société tout en respectant la vie privée des citoyens, existent mais nous en venons souvent à adopter des solutions étrangères alors que la France est très bien placée pour les fournir et les exporter grâce à des technologies reconnues : biométrie, carte à puce, systèmes d'identification ou encore détection d'activité pour la sécurité, management des réseaux informatiques et numériques, télécommunications, cybersécurité, protection des infrastructures critiques...



Thèmes prédominants avec des défis à relever

Thème 1 : Usage et maîtrise des données sensibles, personnelles et patrimoniales



« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Déclaration Universelle des Droits de l'Homme - Article 12.

Les données personnelles des citoyens comprennent, bien sûr, les attributs officiels d'identité, mais aussi d'autres informations concernant la vie professionnelle, ou la vie privée. A contrario du contrôle de l'identité par des autorités, par exemple au contrôle aux frontières, les usages de la vie courante et notamment pour les services numériques conduisent à diffuser sans contrôle les données personnelles. L'usurpation d'identité est un phénomène important et en forte évolution, causant de graves préjudices.

Le développement de l'économie numérique est vital pour la France. Le numérique n'a pas de frontières. Nos voisins européens ont pris de l'avance, les Etats-Unis d'Amérique ont décidé de normaliser et développer des solutions pour le monde entier. Les pays qui n'auront pas développé la technologie perdront des marchés de technologie et de services, et leur gouvernement de la TVA.

À l'instar des pays industrialisés, la France adopte la notion de sécurité globale qui inclut le monde réel et le monde numérique. L'identité régaliennne et l'identité numérique sont ainsi liées. Forte de ses leaders dans les technologies de carte à puce, de sécurité, d'infrastructures de confiance, la France peut développer un modèle de services numériques sécurisés, en :

- 1 Dotant l'utilisateur d'un objet personnel sécurisé, coffre-fort de ses données personnelles et capable de créer un lien sécurisé d'échange d'informations avec les fournisseurs de service. La Carte Nationale d'Identité Electronique a vocation à être un tel objet.
- 2 Introduire des tiers de confiance pour la validation d'attributs d'identité, et des mécanismes de contrôle de pertinence des accès aux données personnelles.
- 3 Favorisant le déploiement de services numériques publics via des plateformes mutualisées et le *cloud computing* pour les applications :

Citoyen – gouvernement, porteuses d'économies conformément à la RGPP (Révision générale des Politiques Publiques), de meilleur service, de meilleurs délais de réponse à l'utilisateur.

Citoyen – collectivités territoriales, répondant aux besoins d'accès et de sécurisation des transports, des loisirs, du tourisme, de l'éducation, de maintien du lien social, notamment avec l'environnement rural.

Télesanté : l'installation au domicile de systèmes de santé personnels, la nécessité de relier entre eux tous les acteurs du monde médical, de l'assurance sociale et des bénéficiaires sont les clés de l'optimisation des coûts de la santé, tout en apportant une amélioration qualitative et quantitative des soins.



2 propositions majeures :

Déploiement effectif, à court terme, de la Carte Nationale d'Identité Electronique, et des objets sécurisés IDÉNUM (label du Ministère de l'économie numérique), selon la norme IAS ECC déjà validée et développée par les industriels français regroupés au sein du Gixel.

- coordination des projets et initiatives permettant le développement de l'économie numérique sécurisée :
 - ◆ gestion des identités régaliennes ;
 - ◆ labellisation IDÉNUM ;
 - ◆ développement des services numériques conformément aux objectifs définis dans la consultation publique.



Thème 2 : Confiance sur Internet (Cybercriminalité)



Les technologies de l'information, Internet en particulier, prennent une importance grandissante dans notre vie de tous les jours, vie familiale, vie professionnelle, loisirs...

Nous dépendons de plus en plus des réseaux et des services fournis à travers eux. Un foyer moyen dispose d'une grande quantité d'équipements numériques intelligents, connectés et chargés d'informations : téléphones mobiles (Smartphone), PCs, connexion internet haut-débit, accès data-3G mais aussi des équipements domotiques connectés (contrôle de l'énergie, télésurveillance...). Pourtant ces réseaux peuvent être victimes d'attaques informatiques ou d'incidents divers comme le ver Slammer en 2003 qui a littéralement paralysé l'Internet dans de nombreux pays. Des entreprises, des PME, des particuliers sont régulièrement victimes d'attaques ou de chantage à l'attaque informatique.

Ces attaques peuvent viser les données personnelles des internautes et les informations stratégiques des entreprises, ou s'attaquer aux réseaux eux-mêmes (attaque informatique de l'Estonie en avril 2007).

Demain l'Internet des objets (*Machine-To-Machine*) révolutionnera les usages, par exemple dans les domaines de l'énergie, des transports et de la santé mais à condition de garantir sa résilience. Ces enjeux sont considérables : le M2M vise un parc d'équipements estimé entre 50 et 70 milliards de machines, soit entre dix fois le nombre actuel d'abonnés sans fil aux réseaux cellulaires et dix fois celui de la population mondiale actuelle. Et ce pour des systèmes souvent critiques : infrastructures vitales, défense... Récemment, le ver informatique Stuxnet a ainsi été accusé de viser spécifiquement une centrale nucléaire iranienne.

Alors que le numérique est reconnu comme le principal levier de développement des économies de demain, et que sa clé est la confiance, on imagine bien l'enjeu que représente la sécurité Internet, comme le soulignait le Centre d'Analyse Stratégique dans son rapport « La société et l'économie à l'aune de la révolution numérique » à l'horizon 2025.

L'ACN a pour ambition d'identifier et de mobiliser un réseau de compétences cybersécurité qui soient mises au service de tous : citoyens, entreprises, administrations. Cela passe par l'analyse des enjeux et des faiblesses, des champs technologiques à développer (sécurité de bout en bout dans le cyberspace, sécurité de l'Internet des objets, sécurité dans le *cloud computing*...).

Il s'agit aussi d'apprécier les apports d'une meilleure sécurité, d'une plus grande confiance dans les technologies de l'information en termes de développements sociétaux et d'ouverture vers de nouveaux services, de nouveaux business. C'est dans cet esprit que l'ACN se propose d'interpeler les autorités de l'État et les départements ministériels sur la question.



Thème 3 : Apport du numérique sur la sécurité des flux



Contrôle et suivi des flux, de personnes ou de biens, s'imposent de plus en plus aux pouvoirs publics et aux opérateurs économiques. Il s'agit de réponses à des enjeux industriels (suivre des biens périssables ou non afin de s'assurer de leur arrivée à destination dans les délais voulus) ou de sécurité (surveiller des flux de passagers ou de biens, afin de détecter tout risque terroriste ou de malveillance).

Ces enjeux revêtent une acuité de plus en plus importante, avec la mondialisation des échanges, qui induit un allongement des circuits de transport des biens, avec de multiples passages de frontières et phases de transbordement, mais aussi du fait du renforcement du risque terroriste et le développement des mafias et actes d'incivisme. D'où la nécessité pour les pouvoirs publics comme pour les opérateurs économiques, de disposer de la capacité de suivi et d'analyse des flux de voyageurs et de biens, qu'ils soient temporaires ou permanents.

Apport du numérique (exemples)

- contrôle d'accès en mouvement, coopératif ou non, avec reconnaissance faciale ou de l'iris ;
- contrôle d'accès statique, par empreinte ou signature ;
- reconnaissance à la volée, faciale ou de l'iris, avec capacité à identifier et localiser ;
- compression du flux vidéo pour remontée d'information ;
- système de supervision C2 avec fusion des données – moteur d'acquisition des données ;
- gestion de réseaux multi caméras et traitements associés ;
- solutions algorithmiques pour gérer la variabilité des contenus de scène, des conditions de prise de vue, des conditions météorologiques et d'illumination, des qualités d'images.

Ces technologies doivent permettre une surveillance et une identification des flux sans générer d'obstruction à leur écoulement, car le ralentissement de flux, en générant un attroupement en fait une cible de choix pour une attaque terroriste. Les solutions retenues devront maintenir l'équilibre entre les contraintes perçues comme acceptables par la société et les opérateurs, et le besoin d'augmenter le niveau de sécurité.

Actions à lancer (exemples)

Sécurité des flux temporaires

Les solutions technologiques utilisées pour la protection des flux récurrents et temporaires sont très proches. Or la surveillance et la protection des flux ponctuels nécessite de disposer d'un système à architecture modulaire, aisément déployable avec une empreinte limitée vis-à-vis de la population. Cette architecture doit permettre une fusion des données captées et des moyens physiques déployés.



Vidéo-protection

L'amélioration de l'efficacité de la vidéo protection, rendue possible par les progrès de la technologie, nécessite que des actions soient lancées sur cinq techniques jugées prioritaires :

- la gestion des réseaux multi-caméras et les traitements associés ;
- la caractérisation sémantique d'individus pour la recherche sur signalement ;
- la détection d'événements anormaux ;
- le développement de l'exploitation de caméras mobiles, embarquées ;
- la vision nocturne, la prise en compte des conditions environnementales difficiles.



Les acteurs de l'Alliance

La FIEEC

Fédération des Industries Electriques, Electroniques et de Communication

La FIEEC est une grande Fédération de l'industrie qui rassemble 26 syndicats professionnels dans les secteurs de l'énergie, des automatismes, de l'électricité, de l'électronique, du numérique et des biens de consommation. Les secteurs qu'elle représente regroupent plus de 2300 entreprises, emploient près de 400 000 salariés et réalisent plus de 96 milliards d'euros de chiffre d'affaires dont 46 % à l'export. A travers des documents tels que le rapport « Une stratégie industrielle pour les marchés du futur » ou « La contribution des filières stratégiques pour la croissance et l'emploi », la FIEEC souligne depuis longtemps l'importance de bâtir une infrastructure de confiance partagée.

Pour plus d'informations www.fieec.fr



Le GIFAS

Groupeement des Industries Françaises Aéronautiques et Spatiales

Créé en 1908, le Groupeement des Industries Françaises Aéronautiques et Spatiales est un organe professionnel qui regroupe 286 sociétés - depuis les grands maîtres d'œuvre et systémiers jusqu'aux PME - spécialisées dans l'étude, le développement, la réalisation, la commercialisation et la maintenance de tous programmes et matériels aéronautiques et spatiaux, civils et militaires, ainsi que des systèmes d'électronique de défense et de sécurité.

Le Gifas dispose en son sein d'une Commission des Systèmes de Sécurité, dont l'un des axes de travail est de faire émerger un éco système de la sécurité. Dans ce but, la Commission travaille étroitement avec le SGDSN et le ministère de l'Intérieur, avec lequel une convention a été signée en 2008. Plusieurs rapports ont été rédigés visant à mieux définir le marché de la sécurité en France, tandis qu'une initiative de rédaction de feuilles de route technologiques destinées à répondre à des besoins capacitaires est en cours de réalisation, en liaison avec des centres de recherche.

Le Gifas représente une profession dont le chiffre d'affaires est de 35,8Mds€, qui exporte 80% de sa production, emploie directement 157000 personnes, dégage un excédent commercial de 14Mds€ et consacre chaque année 15% de son chiffre d'affaires à la Recherche & Développement.

Tous les deux ans, le Gifas organise le Salon International de l'Aéronautique et de l'Espace de Paris Le Bourget, dont la 49^{ème} édition aura lieu du 20 au 26 juin 2011.
8, rue Galilée 75116 PARIS – Tél. +33(0)1 44 43 17 00 – Fax : +33(0)1 40 70 57 36

Pour plus d'informations www.qifas.asso.fr e-mail : infoqifas@qifas.asso.fr



Bull

Bull est une société des technologies de l'information. Notre mission est d'être le partenaire privilégié de nos clients, corporate et administration, en optimisant l'architecture, en opérant et en rentabilisant leur Système d'Information, pour soutenir leur activité et les processus critiques liés à leur métier. Bull est un spécialiste des systèmes ouverts et sécurisés, le seul européen positionné sur les principaux maillons de la chaîne de valeur de l'informatique.

Pour plus d'informations www.bull.fr



La Caisse des Dépôts

Le groupe Caisse des Dépôts est un « groupe public au service de l'intérêt général et du développement économique ».

Le groupe est investisseur de long terme : cette capacité à s'engager financièrement sur le long terme est unique en France. Elle le distingue des autres acteurs de l'économie.

Par ses investissements de long terme, la Caisse des Dépôts laisse le temps à l'innovation et à une croissance durable.

Le groupe investit dans des projets au service du développement de tous les territoires, pour répondre aux besoins que le marché seul ne peut satisfaire. Ce rôle est largement reconnu par les forces politiques et économiques.

Créateur de solutions durables, le groupe Caisse des Dépôts invente en permanence de nouvelles manières d'appuyer les politiques publiques nationales et locales. Il anticipe, innove et s'adapte aux défis de demain.

Pour plus d'informations www.caissedesdepots.fr



Cassidian

CASSIDIAN, an EADS company, est un leader mondial dans le domaine des solutions et systèmes de sécurité intégrés et de l'intégration de grands systèmes, proposant à ses clients civils et militaires dans le monde entier des produits et services à forte valeur ajoutée : systèmes aériens (aéronefs et systèmes de drones), systèmes navals, terrestres et "interarmées", renseignement et surveillance, cybersécurité, communication sécurisée, systèmes de test, missiles, services et support. Avec quelque 21 000 employés, CASSIDIAN a réalisé en 2009 un chiffre d'affaires de 5,4 milliards d'euros. EADS est un leader mondial de l'aéronautique, spatial, défense et des services associés. EADS a enregistré un chiffre d'affaires de 42,8 milliards d'euros en 2009 et emploie plus de 119 000 personnes.



CASSIDIAN, « *Defending world security* » (défendre la sécurité mondiale).

Pour plus d'informations www.cassidian.com

CS - Communication & Systèmes

Maître d'œuvre pour la conception, l'intégration et l'exploitation de systèmes clés en main innovants et performants, CS intervient dans les domaines de la défense, de l'espace & de la sécurité, de l'aéronautique, du transport et de l'énergie, en France et à l'international.

Face à la montée en puissance de la cybercriminalité, de nouvelles menaces apparaissent, favorisées par la complexité croissante des systèmes et des réseaux. CS accompagne ses clients, grandes administrations et entreprises, du conseil à l'élaboration des stratégies de sécurité et à la mise en œuvre de solutions pour la protection des systèmes et la sécurisation des échanges et des données.

Avec 205 M€ de chiffre d'affaires et 2 200 collaborateurs, CS s'impose comme un fournisseur de confiance, reconnu par ses grands clients en raison de sa capacité d'innovation, de l'expertise, de l'engagement et du sens du service de ses collaborateurs.

Pour plus d'informations www.c-s.fr



Gemalto

Gemalto est le leader de la sécurité numérique avec un chiffre d'affaires 2009 de 1,65 Md€, plus de 75 bureaux dans 40 pays et plus de 10 000 salariés dont 1 400 ingénieurs de Recherche & Développement.

Gemalto propose des solutions de sécurité numérique intégrées, depuis le développement de logiciels jusqu'à la création et la fabrication de dispositifs de sécurité numérique comme les cartes à puce, cartes SIM, passeports électroniques ou tokens ou encore le déploiement de services pour ses clients.



Dans le domaine des Télécommunications, représentant plus de 50% des revenus de Gemalto en 2009, Gemalto est présent dans les offres de plus de 450 opérateurs mobiles incluant les 50 opérateurs les plus importants dans le monde avec plus de 40% de part du marché mondial. Le centre mondial de Marketing et de Recherche et Développement des Télécommunications de Gemalto est basé à La Ciotat.

Dans le secteur public, Gemalto dispose d'une expérience pratique considérable avec une participation à plus de 50 programmes nationaux dans le monde, notamment une grande partie des programmes de passeports et cartes d'identité électroniques. Gemalto contribue également aux principaux programmes de santé électroniques, et nombre de réalisations autour du permis de conduire électronique et d'immatriculation des véhicules.

Pour plus d'informations www.gemalto.com

Keynectis

Keynectis est un éditeur français, spécialisé dans le domaine de la sécurité des échanges numériques. Pionnier du SaaS et bénéficiant de plus de 12 ans d'expérience, Keynectis propose une offre globale assurant la gestion des identités numériques et la sécurisation des documents et des communications électroniques, au profit des gouvernements, industriels, institutions financières et in fine au bénéfice des usagers à travers le monde.



Les solutions Keynectis se déclinent dans tous les univers d'utilisation : passeport électronique et biométrique, documents d'identité, signature électronique de documents, sécurisation de transactions, E-Banking.

Avec plus de 20 millions d'identités numériques protégées chaque année, Keynectis est le leader européen de la sécurité des échanges numériques.

Pour plus d'informations www.keynectis.com



Orange

Orange est la marque phare de France Télécom, un des principaux opérateurs de télécommunications dans le monde. Elle compte plus de 131 millions de clients, pour l'internet, la télévision et le mobile dans la majorité des pays où le Groupe est présent. En 2009, le Groupe a réalisé un chiffre d'affaires de 44,8 milliards d'euros (22,1 milliards d'euros au premier semestre 2010) pour l'ensemble de ses activités. Au 30 juin 2010, le Groupe comptait 182 millions de clients dans 32 pays, dont 123,1 millions de clients du mobile et 13,2 millions de clients ADSL dans le monde. Orange est le troisième opérateur mobile et le troisième fournisseur d'accès internet ADSL en Europe et l'un des leaders mondiaux des services de télécommunications aux entreprises multinationales, sous la marque Orange Business Services.

Avec son projet d'entreprise « conquêtes 2015 », Orange s'adresse simultanément à ses salariés, à ses clients, à ses actionnaires et plus largement à la société dans laquelle l'entreprise évolue en s'engageant concrètement sur des plans d'actions. Ceux-ci concernent les salariés du Groupe grâce à une nouvelle vision des Ressources Humaines ; les réseaux, avec le déploiement des infrastructures du futur sur lesquelles le Groupe bâtira sa croissance ; les clients, avec l'ambition de leur offrir la meilleure expérience parmi les opérateurs grâce, notamment, à l'amélioration de la qualité de service ; et l'accélération du développement international.

France Télécom (NYSE:FTE) est cotée sur Euronext Paris (compartiment A) et sur le New York Stock Exchange.

Pour plus d'informations (sur le web et le mobile) : www.orange.com



Radiall

Leader mondial dans le domaine des systèmes d'interconnexion, Radiall conçoit et industrialise des produits utilisés dans tous les secteurs de l'électronique: Télécommunications, Aéronautique, Défense, Industrie, Instrumentation etc.

L'entreprise est particulièrement sensible à l'évolution de la connectique dans les applications en réseaux où la Sécurité joue un rôle primordial. Avec l'essor de la numérisation des traitements et des communications, la sécurisation des données physiques et également l'intégrité des données privées, sont des paramètres vitaux pour l'exploitation de ces réseaux*Radiall intègre ces éléments dans la conception de ses systèmes et la réalisation de ses produits.

C'est le cas par exemple des nouveaux besoins dans des marchés à forte valeur ajoutée technologique comme la défense et les véhicules électriques où elle développe des solutions à la pointe de l'innovation.

Pour plus d'informations www.radiall.com



Safran Morpho (ex Sagem Sécurité, groupe SAFRAN)

Dans un monde marqué par des besoins grandissants en matière de sécurité, la société Morpho du groupe Safran propose des solutions qui rendent les déplacements, les infrastructures sensibles et les transactions électroniques plus sûres, et facilitent la protection des citoyens.

Leader mondial des technologies biométriques de reconnaissance d'empreintes digitales, de l'iris et du visage, acteur majeur dans les domaines des cartes à puce, des solutions de gestion d'identité, de gestion des droits d'accès et de sécurisation des transactions, leader mondial de la détection tomographique d'explosifs, Morpho répond aux besoins nouveaux de sécurité des citoyens, des entreprises et des Etats. Ses équipements et ses systèmes intégrés contribuent, dans le monde entier, à la sûreté des transports, des infrastructures sensibles et des transactions électroniques, ainsi qu'à l'identification et la protection des citoyens.



Morpho est une société du groupe international de haute technologie Safran. Ces solutions sont déployées dans plus de 100 pays.

Pour plus d'informations www.morpho.com

Siemens

Le groupe Siemens est spécialisé dans l'électronique et la haute technologie dont les activités sont réparties en trois segments : Industrie, Médical et Energie. Siemens Building Technologies est une division du segment Industrie, spécialisée dans le second œuvre électronique du bâtiment.

SBT exerce son activité sur quatre grands marchés : la sécurité incendie, la sûreté électronique, la gestion énergétique et la distribution d'énergie.

Siemens SBT amène une réponse à toutes les étapes des projets qui sont : la fabrication et distribution de ses produits, la conception et l'installation de systèmes et solutions ainsi que le service tel que la maintenance, l'aide au financement et la formation.

Siemens SBT offre des solutions performantes pour tous types de bâtiments à usage professionnel : les établissements recevant du public, les bâtiments tertiaires et l'industrie. SBT intervient également dans le domaine de la sécurité embarquée (flotte Airbus)

Siemens Building Technologies en France ce sont 1949 collaborateurs répartis sur plus de 40 agences pour répondre aux besoins et à la satisfaction de nos 100 000 clients.

Pour plus d'informations www.siemens.com

SIEMENS



Thales

Thales est un leader mondial des hautes technologies pour les marchés de la Défense et de la Sécurité, de l'Aérospatial et du Transport.

Fort de 68 000 collaborateurs dans 50 pays, Thales a réalisé en 2009 un chiffre d'affaires de 12,9 milliards d'euros. Avec 22 500 ingénieurs et chercheurs, Thales offre une capacité unique pour créer et déployer des équipements, des systèmes et des services pour répondre aux besoins de sécurité les plus complexes.

Son implantation internationale exceptionnelle lui permet d'agir au plus près de ses clients partout dans le monde.

Pour plus d'informations www.thalesgroup.com

THALES





Des industriels et investisseurs s'organisent pour relever le défi de la Confiance Numérique au sein d'une instance de coordination baptisée « Alliance pour la Confiance Numérique ».



Alliance pour la Confiance Numérique

11-17 rue de l'Amiral Hamelin, 75783 Paris Cedex 16
Tél : +33 (0)1 45 05 70 48 — Fax : +33 (0)1 45 05 70 37
iboistard@fieec.fr