Société Anonyme au capital de 518 859,96 €

RCS Antibes B 453 639 932

Siège Social : 2000 route des Lucioles

06410 Biot

DOCUMENT DE PRESENTATION
AUGMENTATION DE CAPITAL

Mars 2010

Avertissement

Ce document d'information est réalisé dans le cadre d'une opération de placement exclusivement réservée aux personnes fournissant le service d'investissement de gestion de portefeuille pour compte de tiers, aux investisseurs qualifiés, ou à un cercle restreint d'investisseurs, sous réserve que ces investisseurs agissent pour compte propre, tels qu'ils sont définis par l'article L. 411-1 et suivants du Code monétaire et financier.

Cette opération d'Augmentation de capital privée ne faisant pas l'objet d'une demande de cotation sur un marché réglementé et étant réalisée en dehors d'une offre au public d'instruments financiers elle ne donne pas lieu à l'établissement d'un prospectus d'information visé par l'AMF en application des dispositions de l'article L. 411-2 du code monétaire et financier et de l'article 211-2 et suivants du règlement général de l'Autorité des marchés financiers (AMF).

Des exemplaires du présent Document d'information sont disponibles sans frais au siège de la société Mobilegov.

TABLE DES MATIERES

Chapitre
1

Chapitre 1: Analyse financière

Le capital social de la Société s'élève à 518 859,96€ et est divisé en 841 619 actions. Il convient de noter l'existence de 203 549 BSAR à 1€ émis en 2008.

L'intégration des primes d'émission des augmentations de capital de 2008 amènera le capital social à 2 113 083€.

L'évolution du cours de bourse depuis l'introduction est la suivante :

Après une chute sévère, le cours semble se stabiliser au dessus de 4€.

Chapitre

2

Chapitre 2: Personnes responsables

2.1. Responsable du Document d'information

Monsieur Michel FRENKIEL, Président de Mobilegov (ci-après « Mobilegov » ou la « Société »).

2.2. Attestation du responsable du Document d'information

« A ma connaissance, et après avoir pris toute mesure raisonnable à cet effet, je déclare que les informations contenues dans le présent Document d'information sont conformes à la réalité ; elles comprennent les informations nécessaires aux investisseurs pour fonder leur jugement sur le patrimoine, l'activité, la situation financière et les résultats historiques de la Société ; elles ne comportent pas d'omissions de nature à en altérer la portée. »

Monsieur Michel FRENKIEL
Président

Chapitre 3

Chapitre 3: Contrôleurs légaux des comptes

3.1. Commissaire aux comptes titulaire

EXPERTS & ASSOCIES INTERNATIONNAL (E.A.I.)

147, boulevard Napoléon III

0600 NICE

Nommé commissaire aux comptes par l'assemblée générale extraordinaire du 5 août 2006, pour une durée de six (6) exercices qui expirera à l'issue de l'assemblée générale ordinaire appelée à statuer sur les comptes de l'exercice clos le 31 décembre 2011.

3.2. Commissaire aux comptes suppléant

Cabinet AUDIAL

21 avenue Ariane

33702 MERIGNAC

Nommé commissaire aux comptes suppléant par l'assemblée générale extraordinaire du 5 août 2006, pour une durée de six (6) exercices qui expirera à l'issue de l'assemblée générale ordinaire appelée à statuer sur les comptes de l'exercice clos le 31 décembre 2011.

Chapitre
4

Chapitre 4: Procédures de l'opération de placement réservée à des investisseurs qualifiés et de l'introduction en Bourse

4.1. Procédure de l'opération

Il sera procédé à un Placement réservé à des Investisseurs Qualifiés qui prendra la forme d'une augmentation de capital qui leur sera réservée.

Le Placement pourra être clos par anticipation sans préavis.

Le Placement sera admis aux négociations sur le Marché Libre, par voie de cotation directe.

Toutefois, l'émission ou la cession d'instruments financiers auprès d'investisseurs qualifiés ou dans un cercle restreint d'investisseurs, ne constitue pas une opération par appel public à l'épargne, sous réserve que ces investisseurs agissent pour compte propre.

Un investisseur qualifié est une personne morale disposant des compétences et des moyens nécessaires pour appréhender les risques inhérents aux opérations sur instruments financiers. La liste des catégories auxquelles doivent appartenir les investisseurs qualifiés est définie par décret. Les organismes de placement collectif en valeurs mobilières sont réputés agir en qualité d'investisseurs qualifiés.

Un cercle restreint d'investisseurs est composé de personnes, autres que les investisseurs qualifiés, liées aux dirigeants de l'émetteur par des relations personnelles, à caractère professionnel ou familial. Sont réputés constituer de tels cercles ceux composés d'un nombre de personnes inférieur à un seuil fixé par décret.

4.2. Cotation Directe

Les actions de la Société sont admises aux négociations sur le Marché Libre d'Euronext Paris, code ISIN FR0010581363 - MLMOB.

L'admission des actions sur le Marché Libre est effectuée par le biais d'une Cotation Directe.

Chapitre

5

Chapitre 5: Principales informations financières et motivations de l'introduction en Bourse

5.1. Evolution du marché de la sécurité

La dépendance de la Société aux Technologies de l'Information et la cybercriminalité associée atteignent un niveau qui inquiète à juste titre nos dirigeants. Des lois nouvelles sont promulguées et des lois anciennes sont mises en application, qui concernent les banques, le e-commerce et tous les prestataires de services en ligne.

Une technologie est recommandée au niveau mondial et progressivement mise en place : c'est l'authentification forte. Là où elle est en place, elle démontre son efficacité. Elle requiert la distribution, par le prestataire, de composants matériels (tokens d'authentification) à tous ses clients, puis la gestion de ces tokens lorsqu'ils sont périmés, perdus ou hors d'usage. Ces tokens sont spécifiques à une application et personnalisés pour chaque client. Lorsque l'authentification forte sera largement déployée, l'usager devra donc avoir autant de tokens qu'il utilise d'applications sécurisées.

Le chiffre d'affaires des vendeurs de tels tokens (Vasco, RSA, Entrust, ActivIdentity, Xiring) explose depuis un an, atteignant 800M€ avec une croissance annuelle de 80%, alors que les utilisateurs se plaignent de la lourdeur des nouvelles procédures et les prestataires du coût induit.

Le déploiement de l'authentification forte est un phénomène mondial en phase de démarrage. Le gouvernement des Etats-Unis a mis de côté 30Mds$ sur 7 ans pour imposer l'authentification forte dans l'ensemble de son administrations. L'ADN du numérique peut s'imposer comme un standard de fait, au moins pour tous les « pure players » du web, à condition de la faire connaître rapidement et d'accumuler les premiers succès commerciaux.

5.2. Evolution de Mobilegov

Jusqu'à présent, Mobilegov vendait des logiciels que ses clients installaient sur leurs ordinateurs et sur leurs serveurs informatiques. L'évolution de la technique ainsi que la demande de plus en plus ciblée dans le domaine de la sécurité tant sur les réseaux privés que sur Internet, incite désormais l'entreprise à distribuer des solutions soit sous forme de machines pré-configurées (des appliances), soit en mode SaaS (software as a service). Cela permet de mettre à disposition de la clientèle des composants embarqués plus puissants et plus faciles à installer sur leurs réseaux informatiques, capables de sécuriser un plus grand nombre d'utilisateurs. Les appliances intègrent notamment des cartes quantiques et des processeurs cryptés, qui n'existent pas sur les serveurs couramment utilisés.

S'appuyant sur son logiciel SAWS, Mobilegov a donc développé une appliance, la Digital DNA ID Box, conforme aux règles de l'authentification forte, qui apporte le même niveau de sécurité que ses concurrents, mais qui utilise comme token d'authentification n'importe quel composant numérique déjà en possession du client (son ordinateur, son téléphone portable, une clé USB ou un appareil photo), authentifié grâce à la technologie brevetée de l'ADN du numérique®.

Après plusieurs mois d'essais chez des prospects, la Digital DNA ID Box est en passe de gagner son premier « win-back » sur les tokens RSA, auprès d'un leader mondial de l'industrie pharmaceutique, et de gagner ses deux premières banques en Italie.

Pour accélérer son développement commercial, Mobilegov a développé un réseau international de Distributeurs exclusifs qui couvre le Royaume-Uni, la Suisse, l'Italie, la Belgique, le Luxembourg, la Corée, l'Afrique de l'Ouest, le Mexique et le Portugal. L'extension est en cours sur Afrique du Nord, Turquie, Espagne, Pologne, Australie, Dubaï, Abu-Dhabi, Hollande, Allemagne.

Les contrats signés engagent les Distributeurs dans une commande immédiate de 100 K€ à 300K€ selon le territoire, et un engagement de vente croissant de 1M€ la première année à 5 M€.

Pour disposer plus vite d'un parc installé significatif, nous allons conclure une opération de croissance externe clairement identifiée et dans des conditions bien définies, financée essentiellement par une émission de titres. Il s'agit d'une entreprise française complémentaire en termes de savoir-faire et de produits.

Cette nouvelle donne oblige Mobilegov à s'approvisionner préalablement en appliances, et à fournir un service avant et après vente renforcé à ses distributeurs, ce qui nécessite un fonds de roulement imprévu dans la trésorerie court terme. Ceci est d'autant plus vrai que les grands donneurs d'ordre exigent de voir tourner un démonstrateur intégré à leur environnement informatique et réseau, mais refusent de payer pour ce démonstrateur un prix aussi élevé que le prix de revient pour Mobilegov de l'appliance nécessaire. Ainsi, la conquête du marché des grands comptes nécessite un investissement significatif, et d'autant plus important ponctuellement que tous les distributeurs ont bien compris le potentiel de ce marché. D'autre part, la croissance du marché à l'international, y compris en Corée, s'accompagne de surcoûts inattendus, tant pour la localisation des produits (support des polices de caractères asiatiques), la traduction des documents, l'extension des brevets à l'Asie. »

MOBILEGOV estime son surcroît de besoin de trésorerie à environ 1 000k€ au cours de l'année 2010. La société ayant entrepris les démarches nécessaire afin de transférer, début 2010, sur le marché ALTERNEXT la cotation des titres représentatifs de son capital, elle aura avec ces deux opérations tous les moyens techniques financiers nécessaires afin d'accompagner son expansion.

La présente levée de fonds permettra

- D'assurer à la Société le fonds de roulement dont elle a besoin pour accélérer sa croissance ;
- D'augmenter sa notoriété et de renforcer sa crédibilité sur les marchés français et internationaux ;
- De valoriser l'entreprise et de renforcer sa présence sur le marché boursier de façon à rentabiliser l'investissement des actionnaires.

Plus précisément, les fonds seront utilisés pour :

- Financer des appliances que l'entreprise doit acheter d'avance.
- Contractualiser avec une entreprise offshore de développement informatique, de façon à disposer d'une marge de manœuvre pour assurer le support clients (hotline, assistance, développements spécifiques)
- Disposer de la marge de manœuvre nécessaire à la nouvelle envergure résultant de notre croissance externe, et poursuivre les développements de produits nouveaux, notamment Mobilegov Document Control.
- Recruter les équipes nécessaires pour accompagner ses Distributeurs sur le terrain.

Enfin, une partie des titres créés permettra la fusion-acquisition d'une entreprise française identifiée, spécialisée dans des produits de sécurité complémentaires.

Mobilegov se tourne donc vers le marché pour trouver de nouveaux partenaires financiers qui apporteront les fonds nécessaires à la réalisation de ses objectifs ambitieux.

5.3. Perspectives financières[1]

Les prévisions 2010 s'appuient sur les contrats de distribution déjà signés pour des produits existants bien connus des distributeurs et sur des prévisions de CA Web correspondant à un marché émergent.

Les revenus provenant de la publicité sur le web (IDissimo) démarrant en mars 2010, suite à la mise en ligne de IDOO, l'année 2010 n'est pas une année pleine, ce qui explique le ratio important entre 2010 et 2011.

Le réel de 2008 et 2009 et les prévisions 2010-2013 s'établissent comme suit :

[1] Période 2009-2012 : données internes non auditées. Les valeurs pour l'année 2009 sont une estimation.

	2008	2009	2010	2011	2012	2013
Revenus (A)	**1 172**	**1 855**	**4 240**	**8 891**	**17 913**	**33 012**
Ventes et locations Licences en direct	495	373	485	630	819	1 065
Revenus des distributeurs exclusifs	0	750	1 100	3 350	7 600	13 350
Revenus IDissimo (service d'authentification forte Internet)	0	0	1 815	4 537	9 075	18 149
Production immobilisée	179	467	515			
Subventions d'exploitation dont crédit impôt recherche	498	266	325	374	419	447
Charges externes	**1 146**	**1 067**	**1 732**	**2 669**	**4 229**	**6 286**
Charges commerciales	32	48	63	82	107	138
Fournitures et consommables	35	47	53	64	64	64
Achat appliances	0	100	475	1 194	2 526	4 325
Loyer	78	120	102	87	87	87
Achat de prestations de services technique	238	108	280	280	280	280
Entretien Brevets, Label FCPI, Intelligence Economique	13	13	13	14	16	17
Honoraires (Comptable, juridique), frais d'actes, assurances	252	262	264	286	329	386
Publicité & Salons	354	177	266	398	558	725
Frais (déplacements, missions, receptions)	110	147	165	202	202	202
Frais de poste, téléphone	34	45	51	62	62	62
Impôts & Taxes	**16**	**20**	**25**	**30**	**33**	**35**
Taxe d'apprentissage	5	6	8	9	10	11
Formation continue	9	11	14	17	19	19
Taxe professionnelle et autres droits	2	2	3	4	4	4
Charges de personnel	**976**	**1 246**	**1 618**	**1 963**	**2 212**	**2 337**
Salaires bruts (salaires nets + parts salariales)	760	930	1 203	1 416	1 571	1 643
PEE/PERCO/Intéressement…	0	14	24	85	126	157
Charges sociales (part patronale)	216	302	391	462	515	537
Charges financières	**217**	**55**	**64**	**74**	**81**	**87**
Intérêts sur emprunts	0	0	0	0	0	1
Dotations aux amortissements & provisions	50	55	64	74	81	85
Charges exceptionnelles	167	0	0	0	0	1
Total des Charges (B)	**2 355**	**2 387**	**3 440**	**4 736**	**6 555**	**8 745**
Resultat avant impôts (A - B)	-1 183	-532	800	4 155	11 359	24 267
Impôt Société (Statut JEI jusqu'à 2012)	0	0	0	0	3 408	7 280
Resultat net comptable	**-1 183**	**-532**	**800**	**4 155**	**7 951**	**16 987**

Pour le marché corporate apporté par les distributeurs exclusifs, il se déduit d'une croissance de CA sur lesquels les distributeurs se sont engagés au cours des 5 premières années :

	2009	2010	2011	2012	2013
Nombre de distributeurs recrutés dans l'année	5	4	3	2	1
Nombre de distributeurs en début d'année	0	5	9	12	14
CA généré k€ pour Mobilegov	0	500	2 900	7 300	13 200
Achat de produits d'avance	750	600	450	300	150
Revenus distributeurs exclusifs	750	1 100	3 350	7 600	13 350

Pour le marché du Web, le CA est réalisé via la publicité qui s'affiche soit à l'enrôlement, soit à l'authentification des usagers. Le service est donc gratuit pour les hébergeurs (ou pour les sites marchands), condition nécessaire au succès de l'introduction d'une telle innovation :

Résultats prévisionnels des sites IDissimo :

	Mars	Avril	Mai	Juin	Juillet	Août	Sept.	Oct.	Nov.	Déc.	CA Annuel Gain Fixe
Nb User	10 000	50 000	60 000	100 000	120 000	150 000	160 000	200 000	300 000	350 000	
Stats Classique Authent J	1 000	5 000	6 000	10 000	12 000	15 000	16 000	20 000	30 000	35 000	
Gains FIXES											
Gain Enrôlement	25 €	100 €	25 €	100 €	50 €	75 €	25 €	100 €	250 €	125 €	
Gain Authentification	42 €	210 €	252 €	420 €	504 €	630 €	672 €	840 €	1 260 €	1 470 €	
Gain CPL	6 000 €	30 000 €	36 000 €	60 000 €	72 000 €	90 000 €	96 000 €	120 000 €	180 000 €	210 000 €	
Gain Pub sur Portail	42 €	210 €	252 €	420 €	504 €	630 €	672 €	840 €	1 260 €	1 470 €	
TOTAUX	6 109 €	30 520 €	36 529 €	60 940 €	73 058 €	91 335 €	97 369 €	121 780 €	182 770 €	213 065 €	**913 475 €**

IDissimo démarre en mars 2010 avec un premier site, IDOO.fr, qui gère 5,7 millions de visiteurs uniques.

Résultats prévisionnels des sites « Identity check »

Certains sites utilisateurs seront recrutés en direct, d'autres par le réseau de distribution. Les prévisions de recrutement en 2010 sont de 5 sites gérant 10.000 utilisateurs, 5 sites gérant 100.000 utilisateurs, etc, comme indiqué dans le tableau suivant pour une année pleine. En 2010, 9 mois seulement sont pris en compte dans le BP.

MOBILEGOV VENTE DIRECTE					MOBILEGOV VENTE RESEAU DISTRIBUTION 50%		
Utilisateurs	**Nombre d'authentifications**	**Nombre de clients**	**CA utilisateur**	**CA authentification**	**Nombre**	**CA utilisateurs**	**CA authentification**
10 000	1 000	5	125 €	1 680 €	10	125 €	1 680 €
100 000	10 000	5	1 250 €	16 800 €	12	1 500 €	20 160 €
1 000 000	100 000	3	7 500 €	100 800 €	6	7 500 €	100 800 €
3 000 000	300 000	1	7 500 €	100 800 €	2	7 500 €	100 800 €
5 000 000	500 000	1	12 500 €	168 000 €	1	6 250 €	84 000 €
			TOTAL	388 080 €		TOTAL	307 440 €

Revenus prévisionnels des sites e-commerce

Les principaux sites de e-commerce et leurs chiffres clés en termes de connexions sont listés ci-dessous :

TOP 15 DES SITES E-COMMERCE EN 2009	NOMBRE DE VISITEURS UNIQUES PAR MOIS (Millions)	Gain mensuel à l'enrôlement	Gain mensuel à l'authentification	Total potentiel sur l'année
1. E-bay	12,954	32 385	47 023	952 896
2. Price Minister	10,472	26 180	38 013	770 320
3. Amazon	8,191	20 478	29 733	602 530
4. Cdiscount	8,026	20 065	29 134	590 393
5. La Redoute	7,714	19 285	28 002	567 442
6. FNAC	7,554	18 885	27 421	555 672
7. Voyages-SNCF.com	7,287	18 218	26 452	536 032
8. 3 suisses	6,793	16 983	24 659	499 693
9. Vente-Privée.com	5,819	14 548	21 123	428 046
10. Pixmania	5,619	14 048	20 397	413 334
11. Kiabi	5,323	13 308	19 322	391 560
12. Rue du Commerce	5,191	12 978	18 843	381 850
13. Carrefour	4,246	10 615	15 413	312 336
14. MisterGoodDeal	4,128	10 320	14 985	303 656
15. Eveil et Jeux	3,495	8 738	12 687	257 092

En 2010, nous faisons l'hypothèse de convaincre un seul de ces distributeurs, par exemple La Redoute, alors que la FEVAD qui les regroupe tous a déjà manifesté son intérêt pour la solution proposée par Mobilegov.

Les prévisions 2011 et au-delà sur les contrats signés ou en cours de signature, et incluent l'adoption, par les distributeurs, du marché web à démontrer en 2010. Ceci confère aux prévisions de vente un bon niveau de confiance.

Chapitre 6

Chapitre 6: Facteurs de risques

Les investisseurs sont invités à prendre en considération l'ensemble des informations figurant dans le présent Document d'information, y compris les risques décrits dans le présent chapitre, avant de se décider à acquérir ou à souscrire des actions de la Société. Les risques exposés dans le présent chapitre sont ceux que la Société considère, à la date du présent Document d'information, comme étant susceptibles d'avoir un effet défavorable significatif sur la Société, son activité, sa situation financière, ses résultats ou son développement. La Société ne peut exclure, toutefois, que d'autres risques puissent se matérialiser à l'avenir et avoir un effet défavorable significatif sur la Société, son activité, sa situation financière, ses résultats ou son développement.

6.1. Risques liés à l'activité

6.1.1. Risques clients

A ce jour, Mobilegov estime ne pas avoir de risque client.

Ses clients sont des Grands Groupes, des Gouvernements, des laboratoires de recherche et des PME en France et à l'étranger. Ils ne présentent donc aucun risque de solvabilité. De plus l'ensemble des encours clients est confié à une société d'affacturage (GE Factbail, l'un des principaux acteurs dans l'affacturage international) garantissant ainsi une protection contre les risques d'impayés.

6.1.2. Risques Fournisseurs

Mobilegov ne présente pas de risque fournisseur.

Grâce à sa forte expérience dans le secteur, l'équipe s'est attachée à développer des produits déployables sur tous les systèmes d'exploitation existants.

De plus, Mobilegov s'est attaché à développer des produits qui ne nécessitent aucune modification des systèmes d'exploitation.

6.1.3. Risques liés à la concurrence et à l'évolution du marché

Mobilegov est présent sur trois marchés principaux :

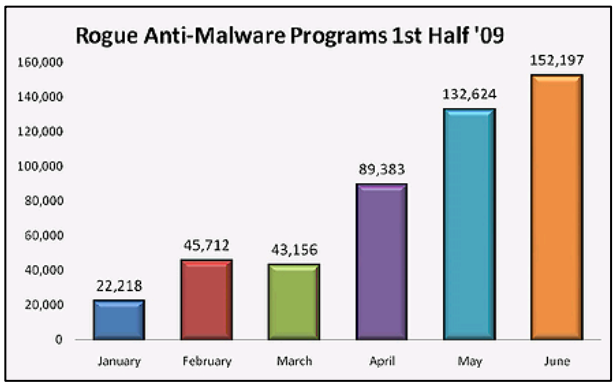
1. Le marché des e*ndpoints* (ou DLP, Data Loss Prevention) : c'est un marché mondial de moins de 250M€ en croissance annuelle de 20%.

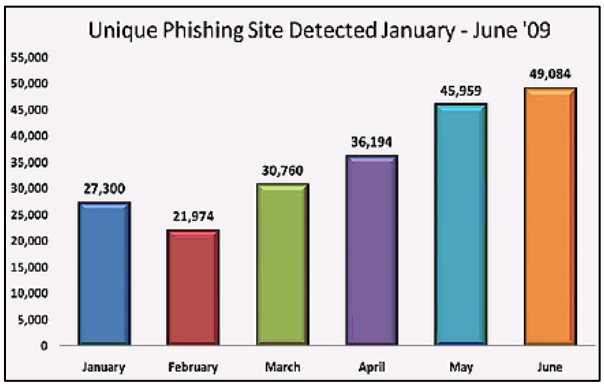
2. Depuis fin 2008, le marché de l'authentification forte : c'est un marché mondial de 800M€ en croissance annuelle de 80%.

3. Depuis début 2010, le marché de la gestion électronique de documents : c'est un marché mondial de 8Mds€ annuels, et Mobilegov s'y introduit via son nouveau produit Mobilegov Document Control qui apporte une solution innovante à la gestion du cycle de vie des documents.

Ces marchés sont liés à la croissance d'une criminalité qui double tous les quatre mois[2] :

[2] Cas des tentatives de fraude bancaire par « phishing », comme le mesure depuis 2 ans la Banque du Canada (www.pwgsc.gc.ca/recgen/colloquium2007/pdf/panel-discussion-jose-navarro-e.pdf)





Mobilegov estime ne pas être exposé à un risque important lié à la concurrence.

En France, sur le marché des Endpoints, la Société n'a pas de concurrent. Ce fait lui donne un avantage stratégique car les logiciels de sécurité sont au cœur des systèmes, et représentent par conséquent un risque important. En Europe, il est plus facile de s'assurer qu'une société européenne n'a pas introduit de Cheval de Troie dans ses logiciels.

Sur le marché des Endpoints, une douzaine de sociétés américaines et israéliennes développent des produits qui visent les mêmes objectifs que Device Control de Mobilegov. En 2008, ce marché s'est restructuré, avec les rachats de plusieurs sociétés spécialisées par les généralistes de la sécurité : Securewave par Lumension, Centennial Software par Frontrange, et surtout Utimaco par Sophos. Restant spécialisé parmi un petit nombre d'acteurs, Mobilegov continue à avoir un rôle à jouer, d'autant plus qu'aucune société n'est focalisée comme Mobilegov sur l'authentification des composants matériels. L'ergonomie et la finesse des résultats du produit de la Société la placent au-dessus de ses concurrents en termes de potentiel de croissance commerciale.

Sur le marché de l'authentification forte, les concurrents sont plus nombreux, les principaux étant ActivIdentity, Entrust, RSA Security, VASCO Data Security, et en France Xiring. Ce marché est né il y a une vingtaine d'années, focalisé sur la lutte contre l'usurpation d'identité sur les réseaux locaux grâce aux tokens de génération de mots de passe à usage unique. La généralisation du Single-Sign-On (SSO), la recrudescence des vols d'identité et les premières décisions réglementaires (banque en ligne au Royaume Uni) ont fait exploser ce marché en 2008. Le marché de l'authentification forte sur le LAN, aujourd'hui mature, est victime de son succès : en effet, à chaque application est liée un token différent, ce qui complique la tâche des usagers. Le marché de l'authentification forte sur Internet est encore émergent, mais avec un potentiel considérable de déploiement dans les 3 à 5 ans :

- fin 2008, une recommandation importante pour la Présidence Obama concerne la mise en place de l'authentification forte dans tous les échanges de l'administration. Un budget de 30Mds$ sur 7 ans est réservé à cet immense chantier, qui va transformer l'Internet : d'un espace de liberté et d'impunité, il va évoluer vers un espace contrôlé où la répudiation d'actions frauduleuses ne sera plus possible.

- De nombreux états se préoccupent de la recrudescence du vol d'identité, et de l'usage frauduleux de ces identités notamment sur Internet, et mettent en place des règles pour le contrer. Ainsi, l'authentification forte est exigée depuis 2007 au Royaume Uni pour les opérations de banque en ligne, elle le sera en France en 2009. La sécurité apparaît aussi dans les opérations de commerce électronique, avec par exemple la norme 3-D Secure de Visa et Mastercard. Le Royaume-Uni a mis en place une cellule de coordination pour lutter contre le vol d'identité (identity-theft.org.uk) qui regroupe une vingtaine d'acteurs (police, justice, finances, cartes grises, banques, industriels). A noter que cette cellule sécurise son site web à l'aide de SAWS.

Sur la marché mature du LAN , la technologie de Mobilegov permet de faire l'économie des tokens et de la logistique liée à leur distribution. SAWS commence à prendre des parts de marchés sur le remplacement des tokens. Sur le marché émergent de l'Internet, la technologie de Mobilegov est la seule compatible avec la philosophie des « pure players ».

Le savoir-faire de Mobilegov sur tous ces marchés est protégé par des brevets robustes qui appartiennent à la Société.

Mobilegov protège juridiquement ses procédés, son savoir faire et ses brevets en vue de vente de licences commerciales et industrielles. Cette stratégie de modèle économique développé en Europe et aux Etats-Unis participe activement à la pénétration rapide de la Société sur un marché mondial.

6.1.4. Risques technologiques

Toutes les solutions de la Société sont protégées par des brevets. Ces brevets concèdent à Mobilegov la technologie la plus adaptée pour la sécurité liée aux composants matériels des systèmes numériques.

Avant de développer un nouveau produit, Mobilegov réalise un « Proof of Concept » technologique et une veille économique et concurrentielle. Cette veille fait appel à un laboratoire spécialisé (e-Novaction, service du CERAM et de la CCI de Nice-Côte d'Azur).

Par contre, il existe une très forte opportunité technologique (voir paragraphe 11.2)

6.2. Risques liés à l'organisation de la société

6.2.1. Dépendance vis-à-vis des collaborateurs clés

Le risque est limité car les postes clés sont occupés par 6 personnes différentes.

1. M. Michel FRENKIEL, co-fondateur de la Société, est Président de Mobilegov,
2. M. François-Pierre LE PAGE, co-fondateur de la Société, est Directeur Général Délégué
3. M. Eric MATHIEU, co-fondateur de la Société, est Directeur Technique.

Ces 3 personnes détiennent à ce jour directement ou indirectement 60% des droits de vote de la Société.

4. M. Olivier LOCUFIER est Directeur Produits
5. M. Mauro ISRAEL est Directeur de la Sécurité Informatique
6. M. Philippe MAZURIER est Directeur Commercial.

6.2.2. Dépendance à l'égard des principaux actionnaires

Co-fondateurs de Mobilegov en avril 2004 et toujours détenteurs de 60% des droits de vote, M. Michel FRENKIEL, François-Pierre LE PAGE et Eric MATHIEU sont les principaux artisans du succès de la Société ; leur objectif demeure le développement de celui-ci.

6.2.3. Aptitude de l'organisation à réaliser la croissance

Les risques liés à la réalisation et à la gestion de la croissance sont inhérents à toute entreprise qui, comme Mobilegov, dispose d'un fort potentiel de développement. La Société considère que savoir gérer la croissance fait partie intégrante du métier et de l'expérience de ses dirigeants.

Sur les trois dernières années, la Société Mobilegov a pu faire la démonstration de sa réactivité et de sa capacité d'adaptation, et de son professionnalisme.

Voici un résumé des prix, concours, partenaires et labels de Mobilegov :

Concours

2005		Sommet international du Capital-Risque 2004
2006		Capital-IT Best Innovation 2005
2007		Lauréat 2007 de l'Entreprise la plus innovante en région PACA
2008		Lauréat du Prix de l'Entrepreneur de l'Année région PACA : Prix de l'entreprise d'avenir.
2008		Prix Speed Starting-up SFR : Entreprise la plus innovante (région PACA)
2008		Winner Red Herring 100 Europe et Red Herring 100 Global

Labels et Subventions

2005		Brevet validé par le Cabinet du Ministre (Fonctionnariat d'Etat aux Nouvelles Technologies), le SGDN et la DCSSI
2006		Aide au Financement de l'Innovation 75 000€
2007		Aide au financement des PME PACA 75 000€

Partenaires

Depuis 2006				
				
2007				
				
				
				

Mobilegov bénéficie du statut JEI et est éligible FCPI. La Société bénéficie également du « Crédit Impôt Recherche ». A ce titre, elle a obtenu 75 000 € pour l'année 2007 et 287 764€ pour l'année 2008. Elle a obtenu en 2008 une Prime d'Aménagement du Territoire de 525.000€ pour la création de 35 emplois sur 3 ans.

6.2.4. Risques liés à la croissance externe

Comme souligné précédemment, la priorité pour Mobilegov est sa croissance organique. Toutefois, anticipant à moyen terme un mouvement de concentration sur son marché de référence, la Société n'exclut pas d'élargir son périmètre par acquisition. Dans cette perspective, elle souhaite se doter des moyens financiers nécessaires à saisir les meilleures opportunités.

6.3. Risques de marché

6.3.1. Risque de liquidité

A ce jour, la Société dispose de la trésorerie et des facilités bancaires suffisantes pour faire face aux besoins et obligations de son exploitation.

A la même date, elle ne détient pas de valeurs mobilières de placement.

6.3.2. Risque de taux

La Société estime être faiblement endettée. A la date du présent Document d'Information, demeure à sa charge un emprunt contracté de 75 k€ en 2007, sous forme d'avance un taux fixe de 5% et un taux variable (à compter de 2008) de 4% de R x P (R = Résultat d'exploitation + amortissements effectués au cours de l'exercice + rémunération nette des Actionnaires Dirigeants détenant plus de 15% du capital ex ante, et P = rapport du solde du prêt participatif de l'I.A.D / fonds propres, les fonds propres étant constitués de capital + réserves + report à nouveau + prêts participatifs + solde des subventions d'équipements) soit les remboursements suivants :

2010 : 17 046,12 €
2011 : 17 046,12 €
2012 : 8 523,06 €

Ainsi qu'une Aide à l'Innovation de 100 000€ contractée auprès de OSEO-ANVAR, sous forme d'avance remboursable à taux nul selon l'échéancier suivant :

35 000 € au plus tard le 30/09/2009
40 000 € au plus tard le 30/09/2010

En conséquence, la Société juge ne pas être exposée de manière significative au risque de taux.

6.3.3. Risque de change

Les transactions de la Société avec ses clients et partenaires européens sont facturées en Euros.

Les transactions de la Société avec ses clients et partenaires américains sont facturées en Dollars.

La Société considère son risque de change négligeable. La Société sera amenée à développer significativement ses relations commerciales libellées en devises, elle prendra donc toutes les dispositions nécessaires en termes de couverture.

6.4. Risques juridiques

6.4.1. Risques liés à la propriété intellectuelle

Mobilegov est titulaire des droits de propriété relatifs à ses marques et brevets. Ils ont tous fait l'objet d'un dépôt auprès de l'Institut national de la propriété intellectuelle (INPI) et de l'*United States Patent and Trademark Office*.

L'ensemble des titres de propriété industrielle liés à ses brevets est géré par le cabinet Thierry Schuffenecker.

6.4.2. Risques liés aux normes et à la réglementation applicable

Mobilegov a pris toute les dispositions liées à réglementation en vigueur sur la protection de la vie privée auprès de la CNIL.

6.5. Risques inhérents à l'opération

Les titres faisant l'objet de la présente opération seront admis aux négociations sur un marché réglementé et bénéficieront des garanties correspondantes.

6.6. Assurances et couvertures de risques

La Société est assurée auprès de la compagnie 3SCI pour des couvertures Multirisque Professionnelle et Multirisque n° 41.760.418.

6.7. Faits exceptionnels et litiges

Il n'existe pas de procédure gouvernementale, judiciaire ou d'arbitrage, y compris toute procédure dont la Société a connaissance, qui est en suspens ou dont elle est menacée, susceptible d'avoir ou ayant eu au cours des douze derniers mois des effets significatifs sur la situation financière ou la rentabilité de la Société.

Chapitre 7

Chapitre 7: Informations concernant la société

7.1. Généralités sur la Société

7.1.1. Dénomination sociale et nom commercial de la société

La Société a pour dénomination sociale « Mobilegov France».

7.1.2. Lieu et numéro d'enregistrement de la société

La Société est enregistrée au registre du commerce et des sociétés d'Antibes sous le numéro 453 639 932.

7.1.3. Date de constitution et durée

La Société a été immatriculée le 24 mai 2004 au registre du commerce et des sociétés d'Antibes.

La Société est constituée pour une durée de 99 ans, sauf prorogation ou dissolution anticipée.

7.1.4. Siège social de la Société, forme juridique, législation régissant ses activités

La société a été constituée sous la forme de Société à Responsabilité Limitée (SARL) le 16 mai 2004 puis elle a été transformée en Société Anonyme (SA) le 5 août 2006. Elle est régie par les dispositions législatives et réglementaires en vigueur et à venir, notamment par le Code de Commerce, le décret n° 67.326 du 23 mars 1967 sur Sociétés Commerciales et leurs textes modificatifs, ainsi que par ses statuts.

Adresse :	2000 route des Lucioles – 06410 Biot
Téléphone :	+33 493 330 666
Fax :	+33 492 944 895
E-mail :	info@mobilegov.com
Site Internet :	www.mobilegov.com
Code ISIN :	FR0010581363 - MLMOB

7.1.5. Origine de la Société

- *2004* En avril, détection par Michel FRENKIEL d'une faille de sécurité touchant potentiellement la plupart des systèmes numériques. Identification avec Eric MATHIEU d'une solution corrigeant cette faille.

- *2004* En mai, création de la SARL Mobilegov à Antibes par Michel FRENKIEL et ses deux associés François-Pierre LE PAGE et Eric MATHIEU. Création simultanée de Mobilegov Ltd. Au Royaume Uni propriétaire de 50% des parts de la SARL.

- *2004* En novembre, dépôt d'un brevet de type « process » pour protéger l'innovation. Le brevet est bloqué par les services de l'Etat car intéressant la Défense Nationale. Validation de l'innovation par le DCSSI.

- *2005* En mars, le brevet est débloqué et publié à l'Office Européen des Brevets.

  En décembre, obtention de la qualification FCPI par l'OSEO-ANVAR.

- *2006* En janvier, la société présente son démonstrateur aux premiers utilisateurs pilotes

  En juin, reconnaissance de la qualité de Jeune Entreprise Innovante par la Direction Générale des Impôts
  Extension du brevet à l'Amérique du Nord
  Adhésion au Pacte PME auprès du Comité Richelieu
  Validation de la technologie par Thales et Unisys

Entrée de Mobilegov dans le Pôle de Compétitivité International « Solutions Communicantes Sécurisées »

- *2007* Janvier : sortie de son premier produit Device Authenticator USB. Premières ventes à un industriel, une administration publique et un organisme de recherche.

  Sortie de son second produit Device Linker, une clé USB inviolable.
  Premier contrat de distribution avec SPIE Communication. Suivront 70 contrats de distribution avec des grossistes, des intégrateurs et des distributeurs, couvrant 14 pays dont la France (Prossi, Quadria-Euralliance's, NextiraOne, IP Vista), Royaume Uni (Onyx Group, RMT, ITPS, LogicaCMG Plc.,), Allemagne (Com-Shack), Inde (DNP Global) et enfin des groupes internationaux comme Accenture, Unisys, Thales.
  Contrat CIFRE avec un thésard du CNRS, Laboratoire I3S de Sophia-Antipolis
  Identifiée start-up de croissance et accompagnée par INRIA-Transfert
  Etude d'opportunités de projets communs avec ST Microelectronics et Gemalto dans le cadre du Pôle SCS. Mobilegov nommé co-président d'un des quatre groupes de travail du Pôle

- *2008* Mars : Introduction au Marché Libre Euronext Paris

  Mai : Présentation de son troisième produit, SAWS (Secured Access Web Service), la seule solution au monde d'authentification forte sans token dédié.
  Contrats de distribution avec des grands distributeurs/intégrateurs étrangers : Insight (UK/US), Com Schack (Allemagne)
  Octobre : participation aux Assises de la Sécurité à Monaco, et présentation de SAWS à plusieurs entreprises du CAC 40.
  Novembre : SAWS plébiscité par le marché

- *2009* Janvier : Vainqueur du Prix RedHerring 100 Global 2008 qui récompense les 100 entreprises privées internationales incontournables dans le secteur des nouvelles technologies, par leur capacité d'innovation.

  Mai : Fin de la levée de fonds de 3M€ décidée en 2007, le cours passe de 6 à 18€.

  Mise sur le marché de solutions globales de sécurité, sur la base SAWS, packagées par métiers, compatibles avec les environnements traditionnels de ces métiers (Radius, VPN, Winlogon, SSO).
  Juin : Sortie de l'appliance Mobilegov Digital ID-BOX (boitier sécurisé multifonctions)
  Mise en place d'un réseau de distributeurs exclusifs en UK, Italie, Suisse, Belgique et création de Mobilegov Corée.
  Dépôt du brevet Mobilegov Device Control.
  Décembre : Lancement de IDissimo, une première solution d'authentification forte pur les applications Internet.

7.2. Investissements

7.2.1. Principaux investissements effectués par la société pendant les 4 dernières années

La politique d'investissement de la Société Mobilegov vise à développer des solutions en phase avec les besoins du marché et des clients et de l'entreprise. Elle vise également le développement de son business model sous la forme de licensing. Au cours des quatre dernières années, ces dépenses d'investissement consacrées à la Recherche et Développement sont mises en évidence par l'évolution du Crédit Impôt Recherche obtenu :

- 2006: 17 085 €
- 2007: 87 026 €
- 2008: 287 764 €
- 2009: 250 000 € (prévision)

La stabilisation des frais démontre la maturité de l'équipe et la possibilité de poursuivre les développements des produits futurs tout en assurant la maintenance des produits disponibles dans des conditions financières contrôlées.

7.2.2. Investissements envisagés

Trois volets d'investissement sont prévus pour 2010 :

1. Achat d'appliances
2. Croissance externe
3. Poursuite des développements de produits

Achat d'appliances

Jusqu'à présent, la Société vendait des logiciels que ses clients installaient sur leurs ordinateurs et sur leurs serveurs informatiques. L'évolution de la technique ainsi que la demande de plus en plus ciblée dans le domaine de la sécurité tant sur les réseaux privés que sur Internet, incite désormais l'entreprise à distribuer des solutions sous forme de machines pré configurées (appliances). Cela permet de mettre à disposition de la clientèle des composants embarqués plus puissants et plus faciles à installer sur leurs réseaux informatiques, capables de sécuriser un plus grand nombre d'utilisateurs. Ces appliances intègrent notamment des cartes quantiques et des processeurs cryptés, qui n'existent pas sur les serveurs couramment utilisés.

Cette nouvelle donne oblige l'entreprise à s'approvisionner préalablement en appliances, ce qui nécessite un fonds de roulement imprévu dans la trésorerie court terme. Ceci est d'autant plus vrai que les grands donneurs d'ordre exigent de voir tourner un démonstrateur intégré à leur environnement informatique et réseau, mais refusent de payer pour ce démonstrateur un prix aussi élevé que le prix de revient pour Mobilegov de l'appliance nécessaire. Ainsi, la conquête du marché des grands comptes nécessite un investissement significatif, et d'autant plus important ponctuellement que tous les distributeurs ont bien compris le potentiel de ce marché. D'autre part, la croissance du marché à l'international, y compris en Corée, s'accompagne de surcoûts inattendus, tant pour la localisation des produits (polices de caractères asiatiques), la traduction des documents, l'extension des brevets à l'Asie. »

Croissance externe

Deux opérations sont en cours, pour lesquelles les cibles ont déjà été contactées :

- une entreprise française identifiée, spécialisée dans des produits de sécurité complémentaires, qui apporterait à Mobilegov à la fois des produits, du savoir-faire et des clients.

- une entreprise offshore de développement informatique, avec qui un contrat permettrait à Mobilegov de disposer d'une marge de manœuvre pour assurer le support clients (hotline, assistance, développements spécifiques)

Poursuite des développements de produits

Il s'agit de maintenir et améliorer les produits existants, notamment ceux mis sur le marché fin 2009 et début 2010, et de terminer le développement d'une première version de Mobilegov Document Control adaptée aux documents PDF.

Chapitre

8

Chapitre 8: Renseignements concernant les activtés

8.1. Présentation générale et métiers de Mobilegov

Créée en 2004 dans le cadre d'un projet Européen de recherche sur la sécurité et les usages des futurs documents d'identité, Mobilegov conçoit, développe et commercialise des solutions innovantes de sécurité informatique.

Fondée sur une technologie propriétaire brevetée dite de l'«ADN numérique», Mobilegov a développé un procédé permettant de détecter et identifier, par des moyens logiciels, tous les éléments d'identification uniques (hard ou soft) des composants intégrés dans un système numérique quel qu'il soit (clé USB, mobile, MP3 …). Une fois extraites, ces données sont assemblées, à partir d'un processus de chiffrement quantique pour en établir une clé unique, encore appelée «l'ADN numérique», laquelle constitue une véritable carte d'identité de l'équipement utilisé. Ce procédé permet donc de reconnaître de façon sûre un équipement numérique parmi des milliards d'autres équipements similaires (même marque, même série de production, même capacité…).A partir de ce procédé, Mobilegov a développé un ensemble de solutions d'avant-garde permettant à ses clients de protéger leurs données sensibles et d'authentifier leurs utilisateurs à un coût très limité.

Jusqu'à présent, l'authentification forte consistait à compléter le contrôle d'accès usuel de type identifiant et mot de passe par la reconnaissance d'un élément matériel dédié détenu par l'utilisateur (dénommé «token»). Ce marché rencontre cependant de nombreux freins dont celui du coût de déploiement qui s'étend de l'achat des tokens, à leur logistique de déploiement et à leur support d'après-vente (hot-line, maintenance). Grâce à l'ADN Numérique proposé par Mobilegov, plus aucun token n'est à déployer, les supports physiques d'authentification sont déjà entre les mains des utilisateurs (PC, disques durs externes, téléphones portables, MP3…). Cette évolution majeure de l'authentification forte devrait permettre un déploiement massif des technologies de Mobilegov.

Destinée dans un premier temps au marché de l'entreprise, l'offre produit de Mobilegov a récemment été déclinée en direction du grand public à travers une offre adaptée aux acteurs du Web. En effet, si Mobilegov peut répondre facilement et à moindre coût, aux problèmes de vol de données sensibles dans les entreprises en proposant d'étendre la sécurité réseau à tous les périphériques amovibles (clés USB, disques, graveurs, etc.), de vol d'équipements numériques en les rendant inutilisables en dehors de l'environnement pour lequel ils ont été configurés, elle permet aussi de protéger les données personnelles sur Internet. Elle offre en effet aujourd'hui une solution de sécurité qui fait défaut à la plupart des applications accessibles via Internet qui touchent le commerce électronique ou les réseaux sociaux. Cette mise en place d'authentification forte sans tokens dédiés, fonctionnant aussi simplement qu'un contrôle de mot de passe, est en pleine conformité avec les normes de sécurité telles que 3-D Secure pour les paiements.

Des premiers contrats majeurs ont été signés, avec des grands groupes industriels (protection VPN, protection des *endpoints*) et avec des organisations publiques (authentification web).

Afin de tirer le meilleur profit de la dimension internationale du marché, Mobilegov s'est attachée depuis 2009 à déployer un réseau de ventes indirectes tant en France qu'à l'étranger. Ainsi, le réseau commercial s'appuie désormais sur des distributeurs exclusifs certifiés (par une formation qualifiante) à l'étranger (Royaume-Uni, la Suisse, l'Italie, la Belgique, le Luxembourg, la Corée, l'Afrique de l'Ouest, le Mexique et le Portugal), ce nombre devant être porté à une quinzaine fin 2010.Forte de son expertise technologique, Mobilegov a d'ores et déjà identifié des déclinaisons de sa technologie afin que l'ADN numérique puisse être utilisé sur de nombreux autres marchés souvent suggérés par les distributeurs eux-mêmes.

Aussi, Mobilegov a pour ambition de devenir rapidement le leader mondial de l'authentification forte, sans token dédié, et généraliser sa technologie de l'ADN du Numérique® au plus grand nombre pour en faire un standard de marché. Grâce à l'ADN du Numérique, Mobilegov estime qu'il sera enfin possible de sécuriser tous les niveaux de l'entreprise et d'apporter enfin, une solution efficace pour lutter contre l'usurpation d'identité en ligne, y compris pour les applications "pure players", rendant ainsi la confiance dans les échanges numériques.

8.2. De nombreux atouts pour devenir un acteur de référence

Mobilegov dispose de nombreux atouts pour s'imposer rapidement comme un acteur de référence sur le marché de l'authentification forte, à savoir :

- Une technologique unique au monde ayant conduit à une offre produits constituée de :
    - Une solution innovante universelle car indépendante de tous les environnements et systèmes d'exploitation et à même de reconnaître la quasi-totalité des équipements numériques existants ;
    - Une solution levant le frein majeur d'un déploiement massif de solutions d'authentification forte, à savoir le coût de déploiement et de gestion d'un parc de tokens. Le facteur sécuritaire de reconnaissance matérielle qualifiant l'authentification forte est assuré à travers tous équipements numériques existants, et concerne à ce jour 2 milliards d'utilisateurs à travers le monde dont l'identité est menacée.
- Une offre produits efficace et économique s'adressant tant au marché des professionnels (corporate et administrations publiques) qu'au grand public à travers une offre dédiée aux acteurs du Web.
- Un contexte de marché particulièrement porteur face à une cybercriminalité croissante et une volonté forte des Etats d'y apporter un coup d'arrêt.
- Un management expérimenté et complémentaire.
- Une barrière technologique à l'entrée grâce à un portefeuille de brevets.
- Une reconnaissance forte de la part de la communauté scientifique à travers la participation de la Société à de grands projets gouvernementaux nationaux et internationaux et l'obtention de nombreux prix et récompenses.
- Des partenariats technologiques avec des acteurs majeurs (Gemalto, Accenture, Orange , Unisys …).
- Des références clients de renom comptant parmi les plus exigeants (Ministère de la Défense France,,Chancellerie autrichienne, Home office britannique, Areva, Sanofi-Pasteur…).
- Un réseau de ventes indirectes mondial est en mesure de déployer rapidement ses solutions et ainsi tirer le meilleur profit de la dimension internationale du marché. Les premiers contacts avec le leader mondial de l'authentification pour intégrer en OEM l'ADN numérique dans son offre démontrent la notoriété atteinte.
- Un spectre très large de nouveaux marchés d'applications. Mobilegov est la première entreprise à proposer une solution à la fois pour protéger les données (en contrôlant mieux les communications) et rendre le vol de composants sans intérêt pour leur voleur (en coupant les communications d'un objet sorti de son contexte). Cette approche novatrice de la sécurité touche potentiellement tous les contextes : la maison, le bureau, la voiture, le bateau mais aussi, la confidentialité des documents ou encore, les téléchargements sur Internet.
- La combinaison d'un modèle économique traditionnel de ventes de licences à même de générer une forme de récurrence et d'un modèle adapté aux acteurs du Web fondés sur des revenus d'affiliation.

8.3. Marché et positionnement concurrentiel de la société

8.3.1. Historique

Des entreprises et des administrations de toutes tailles utilisent des réseaux locaux et Internet, et stockent sous forme numérique leurs informations sensibles. Avec la diversification des technologies (stockage, accès à distance), la banalisation du web et de l'email, la menace qui plane sur les informations sensibles augmente chaque jour.

Les organisations investissent massivement pour contrer les attaques extérieures (Firewalls, filtrage de contenus, anti-virus, détecteurs d'intrusion, etc.) mais investissent très peu en comparaison pour se protéger des menaces de sécurité internes. Le Gartner Group a établi que 80% des crimes et délits liés aux technologies de l'information sont commis par des individus au sein même des organisations. Un périphérique USB peut par exemple contenir 2 GB de données, un disque portable ou un iPod peut stocker 60 GB – plus qu'assez pour emporter les informations vitales de l'entreprise ou introduire un cheval de Troie sur son réseau.

Plus de la moitié des entreprises au Royaume-Uni permettent à leurs employés de se connecter à distance sur leurs réseaux. Beaucoup d'entre elles s'appuient sur des procédés de cryptographie simple à travers des réseaux privés (VPN) tandis que 25% d'entre elles n'ont aucun système de sécurité.

Les Assistants Personnels (PDA) et bien d'autres périphériques comme des téléphones mobiles sont utilisés largement dans le monde professionnel. Ces équipements peuvent se connecter à distance et disposent d'une capacité de stockage importante.

Seule la moitié des entreprises au Royaume-Uni utilisant des PDA ou des téléphones mobiles dispose de systèmes de sécurité élémentaires. L'identification de l'utilisateur par un login et un mot de passe reste prédominante et il a été prouvé que c'était bien insuffisant.

Le besoin d'un système de sécurité efficace a été renforcé par des évènements terroristes dramatiques. Ces évènements ainsi que le crime organisé et l'immigration clandestine ont encouragé les Etats à adopter des documents d'identité biométriques intégrant des cartes à puce.

Les échanges d'informations personnelles ou commerciales sur les réseaux demandent de nouveaux schémas sécuritaires. Diverses solutions sont déjà en place pour contrôler l'accès aux informations sensibles.

Ces solutions sont incomplètes, et elles présentent une faille majeure de sécurité liée aux composants matériels utilisés.

User ID/ Password

Login/password

Ou

Login/passoire ?

Pour chaque application ou système qui demande un accès, il y a un nom et un mot de passe spécifiques à chaque utilisateur. Quand un utilisateur doit accéder à seulement quelques applications dans un environnement restreint, cette approche garantit – jusqu'à un certain point – que l'utilisateur qui demande l'accès est bien autorisé.

Cependant, avec un nombre grandissant d'utilisateurs et d'applications et avec une panoplie d'outils espions apparaissent les failles de sécurité.

Cartes à puce et combinaison User ID/ Password ou code PIN

La combinaison d'un secret (code PIN) avec une carte à puce représente une amélioration significative du contrôle d'accès. La procédure de connexion est partiellement ou complètement remplacée par l'utilisation de la carte à puce.

Cependant, les études ont montré que les cartes à puce peuvent être craquées, soit avec des caméras qui observent la saisie du code PIN, soit en exploitant la naïveté du porteur, soit en mesurant les temps et le courant électrique requis pour certaines encryptions ou décryptions, soit enfin en craquant le générateur de nombres pseudo-aléatoires..

Cette solution ne protège pas contre les modifications de configuration du système qui demande l'accès au service. L'utilisation d'une carte quantique permet de générer des séries de nombres de façon plus sûre.

Biométrie et identification réseau

Les dispositifs d'identification biométriques comme l'utilisation de l'empreinte digitale ou le scan de l'iris, liés à l'examen des paramètres internes de la configuration des utilisateurs (adresse IP et adresse MAC ou IMEI par exemple) sont des approches plus sophistiquées.

Ni ces solutions ni même leur combinaison ne peuvent détecter les modifications matérielles des composants des systèmes utilisés.

Or, même une modification élémentaire comme par exemple ajouter un dispositif de stockage de données USB ou remplacer un lecteur biométrique par un autre dispositif peuvent permettre le vol de données, l'introduction de logiciels malveillants ou le franchissement d'une porte blindée.

Une solution globale pour améliorer la sécurité des réseaux est nécessaire. Cette solution doit être compatible avec la multitude de dispositifs qui existent aujourd'hui dans leurs diverses configurations (systèmes d'opérations), et doit être capable d'évoluer vers les systèmes de demain.

8.3.2. Contexte et enjeux

Le marché de la sécurité informatique et plus particulièrement de celui de l'authentification forte, bénéficie d'un contexte particulièrement porteur avec des enjeux économiques majeurs à la clé.

Les points sensibles des systèmes informatiques sont nombreux :

Le vol ou la perte d'informations sensibles à cause d'intrusions via des supports amovibles de type clés USB, périphériques, ou encore par email avec des pièces jointes infectées de malwares (applications malveillantes : ver, cheval de Troie, virus...) constitue la première faille des systèmes informatiques.

L'usurpation d'identité est un phénomène plus récent qui se développe rapidement. Elle est pratiquée pour arnaquer des particuliers mais également pour voler et utiliser des bases de données, des informations confidentielles d'entreprises. Les moyens d'y arriver sont toujours plus nombreux : attaques keyloggers, phishing, spywares, malwares, « man in the middle», social engineering, etc. En 2008, il s'est créé dans le monde 136 426 nouveaux sites de phishing par mois (Source : PCworld Mars 09), soit une augmentation de 66% par rapport à 2007 générant près de 55 000 nouvelles victimes. Pour mémoire, un site de « phishing » contrefait un site Web de confiance, tels que celui de votre banque ou de votre gestionnaire de carte de crédit. La future victime est amenée sur le site contrefait par un message email (spam) l'informant d'un événement (« vous avez gagné un prix » ou bien « nous mettons en place de nouvelles procédures »). Ces messages, et les sites Web auxquels ils renvoient, sont souvent si proches de l'original que de nombreuses personnes s'y trompent et communiquent leurs numéros de carte de crédit, leurs mots de passe, leurs numéros de compte et autres informations personnelles. On estime que près de 98% du trafic d'email ne concernent que des spams. Les keyloggers constituent une autre menace pour les mots de passe. Un keylogger (littéralement enregistreur de touches) est un dispositif d'espionnage, enregistrant les frappes de touches du clavier à l'insu de l'utilisateur. Certains keyloggers sont capables d'enregistrer les URL visitées, les emails consultés ou envoyés, les fichiers ouverts, voire de créer une vidéo retraçant toute l'activité de l'ordinateur. Des personnes mal attentionnées peuvent ainsi récupérer les mots de passe des utilisateurs du poste de travail. 6191 keyloggers recensés en 2008 représentent 76 % des menaces pesant sur les informations confidentielles (contre 72 % en 2007).

Enfin, tous les outils d'attaque se trouvent facilement sur le Web, apportant une efficacité redoutable aux hackers débutants : il n'est donc plus raisonnable de faire confiance au couple « login-password », devenu en quelques années un «Login-passoire». Ces éléments sont autant d'exemples qui traduisent une complexité d'ensemble qui ne permet plus de garantir un niveau de sécurité en adéquation avec notre dépendance croissante aux technologies de l'information.

Conséquence directe de ces actes de malveillances, la cybercriminalité ne cesse de croître et atteint des sommes records tant sur le marché de la « Sécurité Corporate » que de l'e-commerce au sens large. D'après Symantec (sept 09), la cybercriminalité est une des industries illégales les plus florissantes du monde et dépasserait les revenus du trafic illégal de la drogue. L'évaluation globale des pertes subies par les entreprises, à la suite de la perte de données ou d'actions cybercriminelles, présentée par l'éditeur d'antivirus McAfee, à l'occasion du forum économique mondial de Davos se chiffrerait à 1 000 milliards de dollars. (Source : 01netPro fév 2009). Sur un échantillon de 800 DSI dans quatre pays industrialisés (Etats-Unis, Royaume-Uni, Allemagne, Japon) et quatre pays émergents (Chine, Inde, Brésil, Dubaï), il a été établi qu'en 2008, ces entreprises ont perdu l'équivalent de 4,6 Md$ en données informatiques sensibles (données clients, données financières, brevets, etc.). Ces pertes auraient, par ailleurs, entrainé un coût de 600 M$ pour colmater les brèches de sécurité en question. Ramenées à l'ensemble des entreprises dans le monde, ces pertes de données équivaudraient donc à près de 1 000 milliards de dollars.

En matière d'e-commerce, les e-transactions représentent 5% des transactions mais 32% de la fraude à la carte bancaire, en croissance de plus de 40% par an. (Banque de France, Observatoire de la sécurité des cartes de paiement - Rapport 2007). En France par exemple, il est relevé un taux de fraude sur Internet 6,5 fois supérieur à celui sur les transactions physiques (0,235% contre 0,036%).

8.4. Le marché de l'authentification forte

La cybercriminalité provenant pour l'essentiel d'un vol de données personnelles exploité en usurpation d'identité, l'authentification forte constitue aujourd'hui la meilleure parade. En effet, alors qu'il existe une multitude de moyens de voler des données personnelles, l'authentification forte s'attaque à leur exploitation. L'authentification forte consiste en une sécurité à au moins deux facteurs : le contrôle d'accès par identifiant/mot de passe (« Ce que sait un utilisateur) complété par la reconnaissance d'un élément matériel détenu (ce que possède l'utilisateur), qui peut être un boitier électronique, une liste de mots de passe à usage unique, un téléphone portable, souvent appelé un « token ».

Détournement d'une adresse mail, création d'un faux profil sur Facebook, utilisation de données bancaires volées, etc. : l'usurpation d'identité arrive en tête sur la liste des attaques cybercriminelles. Près de 10 millions de personnes ont été exposées au risque de vol d'identité en 2008, révèle le rapport 2008 Identity Fraud Survey de Javelin Strategy & Research

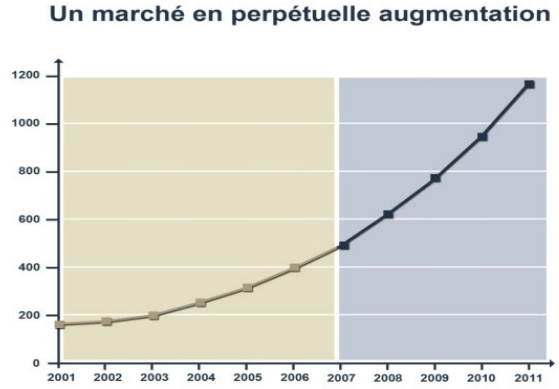
Cette croissance de la cybercriminalité liée au vol d'identité impose l'authentification forte dans de plus en plus d'applications web-based : la banque en ligne, le E-commerce (avec le protocole 3-D Secure), bientôt l'envoi de emails, les accès des webmasters, la protection des enfants…

Limité à un nombre restreint de connaisseurs il y a encore 20 ans, Internet compte aujourd'hui plus d'1,6 milliard d'utilisateurs, et 800 millions supplémentaires pourraient bien arriver d'ici les quatre ans à venir selon Forrester. La cybercriminalité suivra vraisemblablement cette croissance. Un éditeur de solutions de sécurité (PandaSecurity – le Point.fr mars 2009) déclare s'attendre à une croissance mensuelle de 336 % des codes malveillants visant à usurper l'identité des internautes en 2009, une hausse portée par les gains considérables que les cybercriminels génèrent avec cette activité.

Un coup de frein ne sera porté à la cybercriminalité que par l'effet conjugué :

- d'une évolution législative définissant d'une part clairement la notion de délit d'usurpation d'identité et instaurant un cadre répréhensif,
- du déploiement à très grande échelle de solutions d'authentification forte.

Le marché de l'authentification forte est un marché mondial de 800M€, lié à la croissance d'une criminalité elle-même liée au déploiement de l'Internet et du e-commerce. Une croissance de près de 25% par an est anticipée à court terme.



Année	CA (millions de $)	Croissance
2001	165,7	
2002	174,7	+ 5,2 %
2003	199,5	+ 20,5%
2004	248,1	+ 24,3 %
2005	314,5	+ 26,8 %
2006	395,7	+ 25,8 %
2007	494,2	+ 24,9 %
2008	619,9	+ 24,0 %
2009	761,1	+ 24,7 %
2010	948,3	+ 24,1 %
2011	1171,2	+ 23,5 %

Source : Frost & Sullivan

Le passage à l'authentification forte est une priorité pour 2009. Une étude Gartner résume ainsi la situation: "*Organizations that have not deployed stronger authentication methods for local network login by year-end 2009 will be exposed to significant risks.*" La Banque de France impose aux banques françaises de commencer à déployer l'authentification forte pour les opérations de banque en ligne avant juillet 2009 et de la généraliser à tous leurs clients avant juillet 2010. La présidence Obama place la sécurité d'Internet au top de ses priorités et a déjà réservé 30Mds$ sur 7 ans pour imposer l'authentification forte dans tous les services de l'Etat. C'est un chantier estimé à 10Mds€ par an qui s'ouvre aujourd'hui.

Face au besoin d'authentification forte, les motivations sont multiples et se résument ainsi :

Motivations	Prévisions pour les prochaines années		
	1 à 2 ans	3 à 4 ans	5 à 7 ans
1 • La fragilité des mots de passe	●	●	●
2 • Utiliser l'authentification forte pour optimiser le business (type e-banking, e-commerce...)	●	●	●
3 • Coût de gestion des mots de passe	●	●	●
4 • Mise en conformité avec les nouvelles législations	●	●	●
5 • Besoin d'authentifier et de sécuriser les nomades	●	●	●
6 • Protéger les identités lors des opérations en ligne	●	●	●
7 • Prévenir l'usurpation d'identité lors des connexions réseaux	●	●	●
8 • Combattre la prolifération des credentials	●	●	●
9 • ... signature électronique et PKI	●	●	●
10 • Renouvellement de la demande due à l'évolution du marché	●	●	●

● FAIBLE
● MOYENNE
● ELEVE

Mobilegov dispose donc d'une fenêtre d'action de deux ans pour s'imposer sur un marché où le besoin immédiat est considérable.

Des technologies concurrentes existent (voir ci-dessous) mais la plupart d'entre elles présentant des freins que seule la technologie semble à même de lever.

8.5. L'environnement concurrentiel

Plusieurs solutions concurrentes existent sur le marché de l'authentification forte.

Ce segment de l'authentification forte des accès distants, concerne près de 90% du marché actuel de l'authentification forte. Des solutions d'authentification forte concurrentes existent mais contraignent tous les prestataires à distribuer à aux utilisateurs finaux des tokens, électroniques ou non. Ce token matérialise le second facteur sécuritaire caractérisant l'authentification forte, à savoir la reconnaissance matérielle de l'utilisateur (Ce que l'utilisateur « possède » en plus de ce que l'utilisateur « sait »). Il s'agit pour les principales :

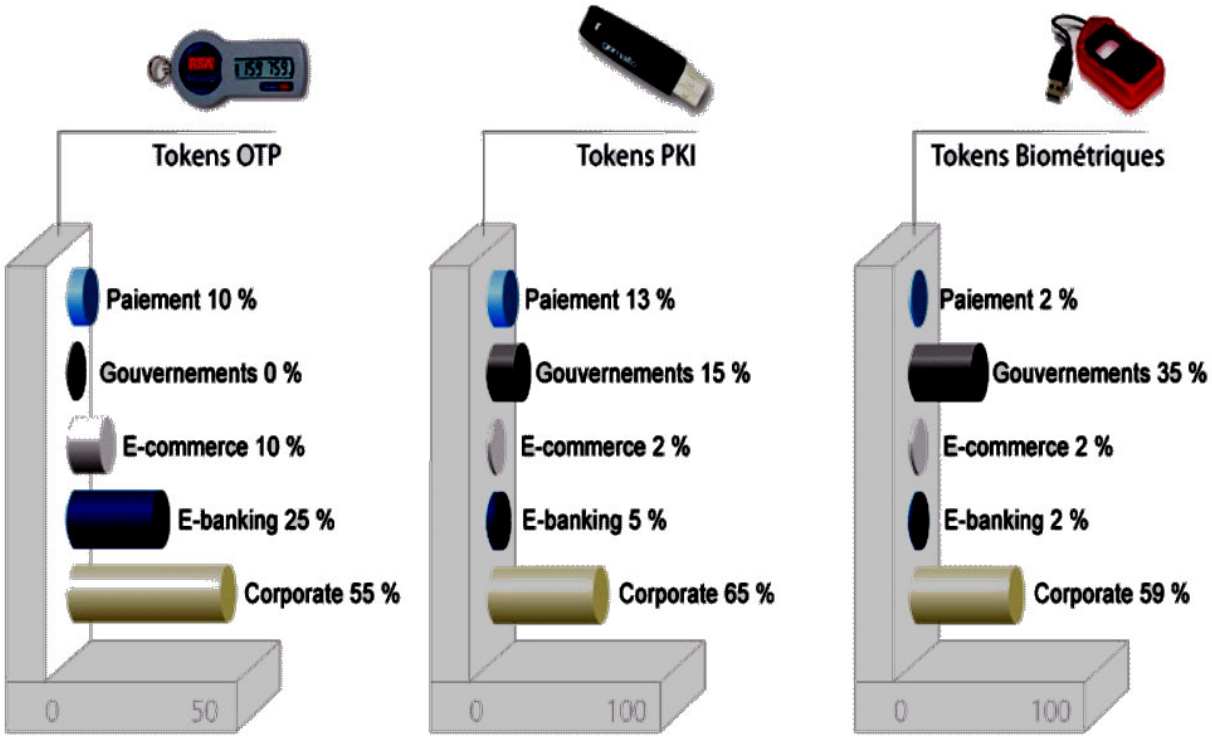
- Token OTP « One Time Passeword » : Il s'agit d'un boitier électronique qui génère un mot de passe à usage unique, dont l'interception est de ce fait sans intérêt.

- Token PKI ou Soft Token : une PKI (public key infrastructure ou infrastructure à clé publique) est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques (wikipédia). La signature électronique qu'elle offre à ses abonnés rend difficile l'usurpation de leur identité.

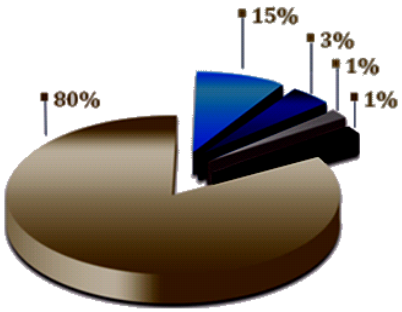
- Token Biométrique : il s'agit d'un boitier électronique capable de vérifier certaines propriétés biométriques de son porteur. Il est protégé contre le vol de ces données et contre diverses falsifications.

La plus répandue de ces solutions d'authentification forte, le token OTP, occupe 75% du marché existant (environ 1,17 Md€ pour 2010/11) alors que la seconde n'en occupe que 15% (Source : Gartner Group – Authentication Market Analysis 2009 / 2010).

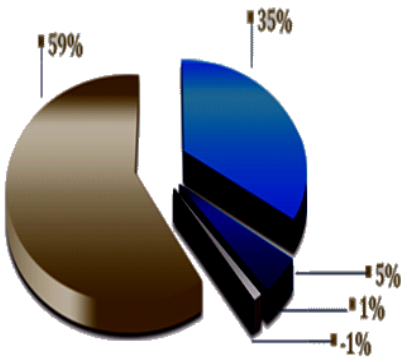
Par secteur de débouchés, la répartition est la suivante :



Il n'en demeure pas moins que malgré le déploiement de tokens, on ne couvre à ce jour que 20% des besoins du marché de la sécurité informatique « Corporate » et encore bien moins sur le Web. Bien que particulièrement sensible, le marché des banques est par exemple encore peu pénétré comme le montrent les schémas ci-dessous :



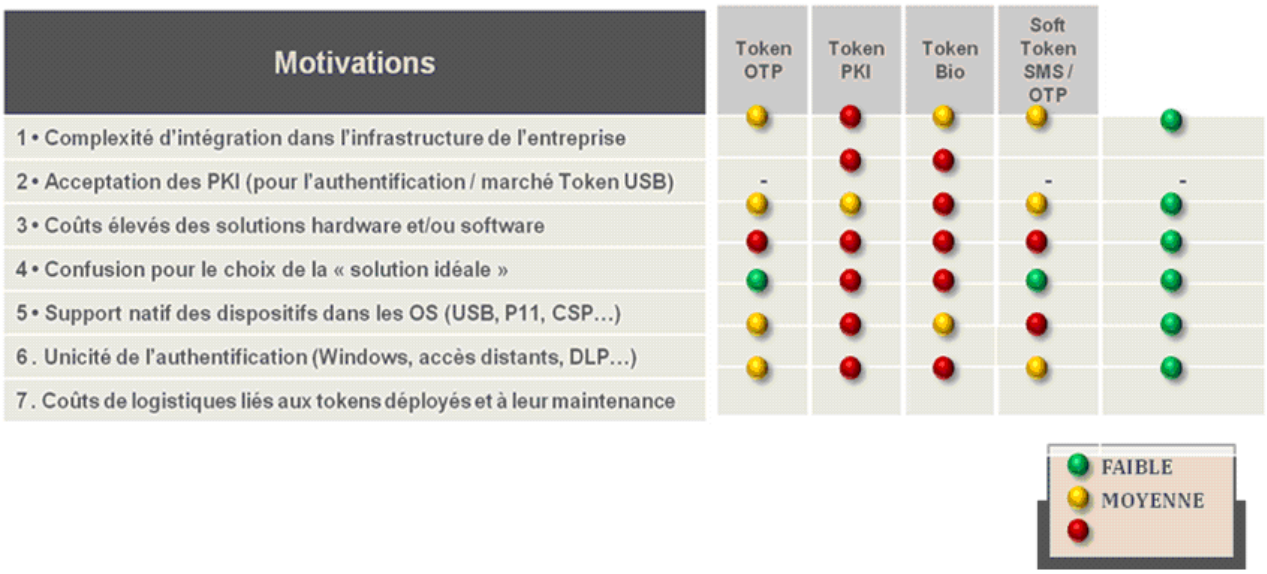
Marché bancaire mondial



Marché bancaire Européen

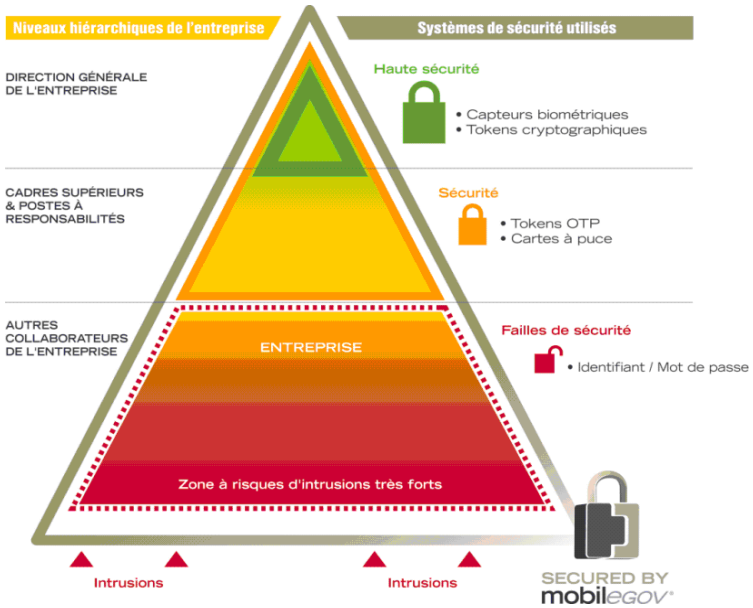
Or, l'authentification forte a fait ses preuves. Au Royaume-Uni, 35% des utilisateurs de banque en ligne sont équipés de solution de type token.(source : APACS-:Association for Payment Clearing Services Juin 2009-Equivalent du GIE Cartes bancaires au Royaume-Uni) et une réduction massive de la fraude a été constatée. En outre, il a été constaté un report des attaques de Phishing sur les banques n'ayant pas déployé de solutions d'authentification forte auprès de leurs clients.

Malgré cette efficacité démontrée, le déploiement de solutions d'authentification forte est très ralenti du fait de l'existence de nombreux freins que résume le tableau ci-dessous.



Du point de vue des sociétés pour le marché Corporate ou des banques pour le e-banking, la problématique clé est que chacun de ces tokens, même s'il ne s'agit pour certains que de format carte de crédit papier avec des codes imprimés, obligent à une logistique complexe et coûteuse. En effet, à leur coût d'achat (d'environ 10 € à 100€ pour les plus complexes) s'ajoutent des coûts de déploiement (intégration au système informatique, envoi aux utilisateurs finaux) et de gestion du parc avec des équipes dédiées au support client et à la maintenance (hot-line pour expliquer le fonctionnement, gérer les pannes, casses ou encore oubli du token lors de déplacements). On estime que le coût d'achat ne représente que 20% du coût total de déploiement.

Le coût unitaire élevé conduit donc les entreprises à ne fortement sécuriser que les postes des collaborateurs de niveau hiérarchique élevé. Or dans les faits, les risques d'intrusion proviennent de tous les collaborateurs, dont les plus nombreux composent la base de la pyramide :



Du point de vue de l'utilisateur enfin, d'une part, les banques font souvent supporter une partie du coût de déploiement, les tokens ne sont pas d'une utilisation aisée pour tous et enfin, vu qu'il n'existe aucun standard, un utilisateur sera rapidement équipé de plusieurs tokens.

Sur ce segment, la concurrence à Mobilegov Access Control consiste principalement en tokens (Vasco, RSA, ActivIdentity, dans une moindre mesure Xiring). Il existe également une autre solution concurrente, qui exploite une PKI (infrastructure à clé publique), aussi appelée « soft token », dont le principal défenseur en France est Mesdisc, avec derrière eux Keynectis.

En revanche, concernant le grand public à travers une offre dédié aux « pure players » Internet, Mobilegov ne dispose à sa connaissance, d'aucun concurrent à ce jour.

Concernant Device Control (Contrôle des périphériques se connectant à un réseau), le marché est plus limité (moins de 250 M€ en 2009). Les principales solutions concurrentes sont DeviceLock, SkyRecon, Devicewall. Seule Mobilegov propose une solution adaptée aux systèmes d'exploitation autres que MS Windows.

Mobilegov estime pour toutes ces raisons que la technologie de l'ADN numérique permet de repousser tous les freins du marché actuel retardant le déploiement massif dans le monde de l'authentification forte en proposant une technologie innovante, économique et évolutive.

En effet, le facteur sécuritaire de reconnaissance matérielle de l'utilisateur se fera à partir d'équipements numériques que possède déjà l'utilisateur et qu'il pourra lui-même choisir, supprimant toute contrainte de déploiement physique de token dédié et toute installation de PKI sur le poste client. Grâce à l'ADN du Numérique, Mobilegov estime qu'il sera enfin possible de sécuriser tous les niveaux de l'entreprise et que la sécurité forte est enfin possible en ligne, y compris pour les applications "pure players". Cette révolution technologique devrait ainsi permettre de toucher le public le plus large.

8.6. Offre commerciale

L'offre de Mobilegov adresse deux marchés : celui de la sécurité informatique de l'entreprise (« Corporate ») d'une part, et celui des acteurs du Web d'autre part. Chacun dispose d'une ligne de produits dédiée.

8.6.1. Produits Corporate

Catalogue de solutions

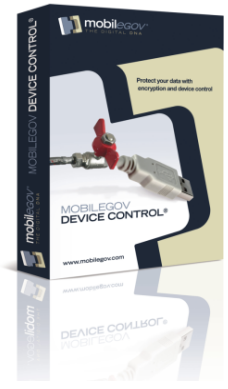
La sécurité Corporate se caractérise par un marché mature, qui s'appuie, pour l'authentification forte, principalement sur des solutions à base de tokens qui ont vu le jour il y a plus de 20 ans. L'offre Mobilegov est mieux adaptée aux nouveaux modes de travail, mal couverts par les solutions existantes, notamment pour les travailleurs nomades et pour le travail collaboratif.

L'offre « Corporate » propose des solutions d'authentification forte couvrant les besoins des organisations souhaitant protéger leurs données informatiques et s'adresse aux PME, grands groupes et administrations publiques.

Mobilegov Device Control® : Cette solution protège l'accès au réseau informatique d'une entreprise en contrôlant les périphériques qui tentent de se connecter. Ainsi, tous périphériques non préalablement autorisés, notamment à mémoire, reliés avec ou sans fil se verront refuser l'accès au réseau, empêchant la fuite de données sensibles Le produit complète (mais ne vise pas à remplacer) les outils de sécurité déjà en place : contrôle d'accès, sécurité réseau, firewall, antivirus, etc.

Le logiciel permet d'imposer la présence opérationnelle d'un composant, par exemple un lecteur d'empreinte ou une clé de certificat.

Le produit s'intègre aux systèmes déjà en place dans les organisations (annuaires LDAP, bases de données). Son architecture permet de gérer la scalabilité, la disponibilité et l'évolutivité de la solution de façon à satisfaire les très grands groupes industriels et les grandes administrations (plus de 10 000 postes de travail).



Mobilegov Device Control® est la seule solution « Corporate » commercialisée sous forme de logiciels. Il comporte deux composants, un logiciel serveur et un logiciel client. Le prix de vente est calculé en fonction du nombre de licences serveur et client nécessaires.

Sur le même principe, mais en logeant la technologie dans le périphérique (clé USB) et non sur le serveur, Mobilegov propose une clé qui ne peut être utilisée que connectée à un ordinateur ou un groupe d'ordinateurs définis, rendant inexploitables les données enregistrées sur une clé perdue ou volée.

Toutes les autres solutions Mobilegov d'authentification requièrent la mise en place d'un serveur d'authentification ID-BOX sur le système d'information de l'entreprise. Toutes fondées sur la technologie dite de l'ADN Numérique en remplacement des combinaisons traditionnelles « Identifiant/ mot de passe », les quatre solutions de contrôle d'accès par authentification forte sont :

- Mobilegov Remote Access : Cette solution a pour objet de sécuriser l'accès aux sites extranet des entreprises. Le recours à ces extranets est croissant du fait de la fluidité des échanges qu'il permet avec les clients, fournisseurs ou collaborateurs nomades des entreprises. Contenant des données de plus en plus sensibles, leur accès doit être mieux sécurisé que par un simple mot de passe

- Mobilegov Secure Webmail : Cette solution a pour objet de sécuriser les accès distants aux webmails de l'entreprise. Les Webmails constituent un outil de travail primordial dans l'efficacité des collaborateurs de l'entreprise, puisqu'ils permettent l'accès au courrier électronique de n'importe quel accès web via des ordinateurs publics (hôtel, cybercafé). Mais ici aussi, la sécurité doit être renforcée.

- Mobilegov Secure VPN : Cette solution a pour objet de sécuriser les accès distants aux réseaux privés d'entreprise (VPN SSL, Virtual Private Network). L'accès au système d'information de l'entreprise est donné aux collaborateurs distants grâce à des connexions au réseau. Or un accès VPN confère à son utilisateur distant les mêmes droits de consultation et de modification de données sensibles qu'à celui qui travaille dans l'environnement sécurisé de son bureau. L'enjeu de l'authentification est là encore primordial.

- Mobilegov WinLogon : Cette solution a pour objet de proposer une authentification renforcée pour accéder à une session Windows. Tous les accès aux fichiers et messageries des entreprises reposent sur l'authentification des collaborateurs à leur session Windows, bien souvent contrôlés par un simple mot de passe.

Chacune de ces applications client/serveur, qui intègre la solution d'authentification forte Mobilegov, est aussi simple à mettre en œuvre qu'un compte protégé par une combinaison « identifiant/mot de passe ».

Afin de simplifier la phase d'installation et de configuration, l'application serveur est livrée sous forme d'une appliance, un boitier qui intègre tous les composants d'un ordinateur fortement sécurisé ainsi que les logiciels système, archivage et sauvegardes, bases de données, chiffrement, réseau et applicatifs nécessaires.

Le modèle économique

Le business modèle repose sur :

- La vente d'une appliance ID-BOX (sauf pour Mobilegov Device Control),

- Puis de la vente de licences logicielles dont les montants sont déterminés en fonction du nombre d'utilisateurs et des modules choisis.

Les applications serveur peuvent également être proposés sous le mode SAAS (Software as a Service), déjà offert aux distributeurs pour réaliser des démonstrateurs.

Des références clients prestigieuses

Le portefeuille clients de Mobilegov compte près de 50 références actives. De nombreux secteurs et tailles d'entreprise y sont représentés. Figurent parmi les clients de grands groupes tels que : AREVA et Sanofi-Pasteur, des administrations telles que Ministère de la Défense France, Chancellerie autrichienne, Home office britannique, des PME et des centres de recherche (Institut Eurécom).

8.6.2. L'offre destinée aux acteurs du Web

La sécurité Internet est caractérisée par son inefficacité, mise en évidence par l'explosion de la cybercriminalité. Depuis 15 ans, la priorité est à l'adoption de l'Internet, encouragée par la légèreté des règles, la faiblesse des contrôles, l'anonymat et la mondialisation des échanges. Aujourd'hui, il est nécessaire d'imposer des mesures de sécurité pour poursuivre ce déploiement.

Les solutions « corporate » sont inadaptées au marché de l'Internet, à cause de la diversité des équipements existants, de l'incompétence et du souci de liberté des usagers.

La technologie de l'ADN numérique, qui permet d'authentifier à distance tout équipement connecté à un poste client, offre aujourd'hui la meilleure solution sur laquelle construire la confiance dans les échanges, qu'ils concernent :

- La banque en ligne

- Le commerce électronique et les achats en ligne

- Les portails et la mise à jour de sites web
- Les sites communautaires
- Les sites de jeux et la protection des mineurs
- Les sites de services, tels que l'envoi de mails et la lutte contre le spam.

En novembre 2009, Mobilegov a mis en ligne son portail IDissimo pour apporter une réponse à ces besoins.

Le portail IDissimo et le moteur d'authentification ID4YOO

Alors qu'une étude de Cybersource (2009) cite comme principales craintes des e-marchands britanniques, le vol des informations sur leurs clients (54%) et la fraude en ligne (52%), le portail IDissimo répond à toutes ces craintes et dispose donc de tous les atouts pour s'imposer rapidement comme la solution d'authentification forte de référence pour les e-marchands.

D'une grande facilité d'implémentation, de configuration et d'utilisation, elle constitue là encore, l'unique solution d'authentification forte qui ne requiert pas la distribution de matériels spécifiques aux usagers ni d'installation spécifique sur le poste client. A l'instar de l'offre Corporate, les coûts de matériel d'authentification sont donc inexistants, la logistique simplifiée et les contraintes d'utilisation pour l'usager réduites au minimum. Ces conditions s'avèrent indispensables pour adresser le grand public ou les services gratuits.

IDissimo intègre un portail de gestion des identités à la norme OpenID sécurisé par l'authentification forte de l'ADN numérique, une interface vers les principaux sites de commerce en ligne, protégeant l'utilisateur contre le risque de phishing, et un web SSO, simplifiant la gestion des mots de passe pour l'utilisateur. Enfin, IDissimo offre une interface d'échange web sécurisée avec le client, ce qui évite l'emploi de mails potentiellement frauduleux, et par conséquent souvent rejetés comme du spam.

IDissimo prépare aussi la mise en place d'authentification forte dans la norme 3-D Secure (standard mondial de paiement e-commerce (Visa et MasterCard) de façon simplifiée.

Côté serveur de commerce en ligne, l'interface IDissimo est l'interface standard d'un serveur OpenID.

Côté client, IDissimo fonctionne soit sans installation préalable (via une applet Java ou un contrôle Activex) soit avec l'installation préalable d'un plugin dans le browser.

Le portail www.idissimo.com est un nouveau support de communication pour le commerce en ligne qui offre une panoplie de services exclusifs tant aux cyber vendeurs qu'aux cyber acheteurs.

Les avantages proposés aux e-marchands sont nombreux:

- Contact des visiteurs : jusqu'à présent, aucune méthode ne permettait à un site marchand de prendre contact avec un visiteur anonyme. Mobilegov offre au site marchand la possibilité de contacter les internautes tout en préservant leur anonymat.
- Garantie de l'identité des Cyber Acheteurs : grâce à l'authentification préalable de l'utilisateur sur le serveur d'identité, les cyber acheteurs sont qualifiés dès leur entrée sur le site marchand (même en mode anonyme).
- Communication ciblée : les analyses montrent que les emails publicitaires ciblés sont jusqu'à neuf fois plus efficaces. Le portail IDissimo propose aux sites marchands des contacts ciblés, en fonction du comportement des utilisateurs.
- Augmentation des revenus : le carnet d'adresses dynamique du portail IDissimo permet de diffuser les campagnes publicitaires et les offres promotionnelles plus rapidement et avec une meilleure visibilité, les rendant plus efficace. De plus, la solution d'authentification par l'ADN du Numérique réduit considérablement les risques de fraudes sur Internet, lesquelles représentent 32% des fraudes sur la totalité des transactions scripturales (soit 33M€ en France l'année dernière).
- Solution Nomade : Plus de Cookies ! Grâce au portail IDissimo et à la technologie de l'ADN du Numérique le site marchand sait reconnaître l'utilisateur quel que soit son lieu de connexion. Celui-ci n'a plus besoin de saisir ses identifiants login/mot de passe, même s'il change d'ordinateur (ou s'il formate son PC).
- Renforcement de la fidélisation : lorsqu'un cyber acheteur décide de dévoiler son identité à un site marchand, il bénéficie automatiquement des différents services (carte de fidélité etc.) en un clic.

- Augmentation de la relation de confiance durant l'achat : aujourd'hui 46% des cyber acheteurs abandonnent leur achat au moment de saisir leur numéro de carte bancaire. IDissimo propose la sécurité de 3D Secure renforcée par l'ADN du Numérique de l'utilisateur pour valider les transactions. En augmentant la confiance, IDissimo facilite le paiement sur Internet.

Les avantages d'IDissimo pour l'utilisateur

- Protection totale de l'identité et de leur vie privée.
- Gratuité intégrale de tous les services offerts
- Anonymat : pouvoir consulter un site, recevoir des informations de celui-ci sans divulguer son identité Inscription en un clic : l'enregistrement et la connexion à un site e-commerce s'effectuent sans saisie préalable « l'inévitable questionnaire » concernant des informations personnelles.
- Authentification matérielle pour bloquer l'usurpation d'identité : les accès aux sites préférés sont sécurisés par l'ADN Numérique, l'utilisateur n'a plus de login ni de mot de passe à mémoriser, son identité est protégée.
- Protection contre le SPAM : le cyber acheteur ne communique plus son adresse e-mail.
- Archivage des documents liés aux transactions : parce qu'il n'est pas forcément évident de gérer les pièces jointes envoyées par les sites e-commerces (bon de commande, message de confirmation, facture, numéro de suivi, historique), les informations sont stockées sur le serveur d'authentification se Mobilegov.
- E-mail gratuit et unique par correspondant.
- Albums photos et vidéos : créations et partage d'albums en parfaite protection de la vie privée.
- Réseaux sociaux : connexion à plusieurs réseaux d'amis tous identifiés par IDissimo permettant de lutter contre l'usurpation d'identité.
- Création de blogs.

IDissimo a déjà été choisi :

- par le portail IDOO de iEurop, utilisé par 5,7 millions de personnes, pour authentifier les usagers et protéger les jeunes, en offrant des accès thématiques adaptés au profil, et notamment à l'âge de l'usager.
- Par le portail Ftopia d'archivage en ligne, pour sécuriser les données sensibles de ses clients.
- Après 3 mois de commercialisation, 37 sites totalisant plus de 10 millions d'utilisateurs potentiels ont commencé à tester le moteur d'authentification ID4YOO.
- De plus, IDissimo permet à un internaute de se connecter à tout site existant ou à venir conforme à la norme OpenID.

Un business model adapté

Le modèle économique offert aux acteurs du Web est double. Les futurs revenus seront constitués :

- Soit de la vente de licences assises sur le nombre d'internautes s'étant enregistré sur le site marchand auxquelles se rajoutera la vente d'une appliance Mobilegov, ou
- Des revenus d'affiliation. Il sera en effet proposé aux e-marchands de bénéficier gratuitement de la solution Mobilegov en échange du droit d'insérer de la publicité sur leurs sites en général, et plus particulièrement, d'adresser une publicité ciblée dès lors qu'un cyber-client entre sur le site.

La déclinaison récente de sa technologie dans une offre packagée destinée au marché du BtoBtoC à travers IDissimo permet aujourd'hui à Mobilegov d'être l'unique acteur du marché, à disposer d'une solution d'authentification forte universelle pouvant s'adresser au public le plus large. Un déploiement massif de la technologie Mobilegov permettrait ainsi à l'ADN du Numérique de rapidement s'imposer comme le standard de marché en matière d'authentification forte.

8.7. Mode de distribution

En tant qu'éditeur de solutions innovantes de sécurité, Mobilegov intervient dans un monde où la vente directe reste très limitée. Les besoins en authentification forte sont mondiaux, c'est pourquoi Mobilegov a opté pour un réseau de ventes indirectes via des distributeurs agréées tant en France qu'à l'étranger, afin de déployer rapidement ses solutions sur le marché mondial.

En France, Mobilegov s'appuie sur son propre service de télémarketing et sur son réseau de distributeurs et d'intégrateurs.

A l'étranger, Mobilegov met en place un réseau de distributeurs exclusifs qui achètent l'exclusivité, forment leurs équipes auprès de Mobilegov France pour ensuite, à leur tour, former leurs propres distributeurs, revendeurs et intégrateurs.

8.7.1. Le réseau de distribution en France

A ce jour, Mobilegov compte en France, une dizaine de distributeurs, revendeurs et intégrateurs. Mobilegov s'attache à développer une sélection qualitative de ses distributeurs dans un souci de satisfaction du client final. Le profil des partenaires de la Société sont des PME spécialisées dans la sécurité informatique, qui voient en l'offre Mobilegov un potentiel de ventes très significatif.

Acquérir le statut de distributeur agréé, suppose de suivre une formation qualifiante (3 jours de cours + cas pratiques) afin de disposer d'au moins un ingénieur certifié MCA (Mobilegov Certified Administrator) et DCA (Device Control Administrator). En contrepartie de cet investissement de formation, le partenaire dispose des avantages suivants :

- Une remise de 30% sur l'offre produits
- Le support exclusif sur les consultations pour des demandes clients spécifiques
- L'accès au portail Partenaire (études de cas …)
- Un accès privilégié à la Hot Line Mobilegov
- Un support Ingénieur Avant Vente privilégié
- Un accès aux tarifs Not For Resale (démonstrations, produits de show-room…).

8.7.2. Le réseau de distribution à l'étranger

Mobilegov a toujours considéré l'international comme un axe prioritaire de commercialisation dans la mesure où les processus de décision des grands acteurs sont très souvent bien plus rapides qu'en France, notamment lorsqu'il s'agit d'adopter des technologies de rupture.

Toutefois, il est apparu que l'animation du réseau d'une soixantaine de membres disséminés dans 15 pays était une tâche lourde.

Debut 2009, il a donc été décidé de mettre en place une structure de décision intermédiaire, par zone géographique : le distributeur exclusif. La stratégie commerciale menée à l'étranger réside désormais en la signature de contrats de distribution exclusive par pays. Outre l'exclusivité territoriale sur les produits qu'il est amené à distribuer, le partenaire local bénéficie d'une assistance technique, commerciale et marketing spécifique (hotline, formations, support commerciaux, etc.) ainsi que d'un programme de formations qualifiantes obligatoires afin d'apporter un service optimum aux clients et utilisateurs finaux de la technologie Mobilegov. Il a la charge du réseau de revendeurs et d'intégrateurs qu'il souhaite mettre en place pour atteindre son quota de ventes.

Les principaux termes d'un tel contrat d'exclusivité territoriale se résument ainsi :

Obligations :

- Acquérir le Package de distribution exclusif comprenant :
    - Des formations qualifiantes pour au moins deux personnes (un ingénieur - MCA et un vendeur - MCS).

- L'achat de licences pour un montant variant en fonction du potentiel de la zone géographique concédée. Ce montant pouvant aller jusqu'à 150 K€, ne constitue pas un droit d'entrée mais un « crédit-licences » venant s'imputer sur les premières ventes réalisées.

- S'engager sur des objectifs de volumes de ventes croissants sur les 5 premières années.

- Assurer le support avant-vente et après-vente de ses clients et de son propre réseau de distribution (revendeurs, intégrateurs…).

- S'investir dans la commercialisation et les événements marketing (séminaires, salons, …).

Droits :

- Une exclusivité de distribution sur un ou plusieurs territoires ;

- Le droit d'utilisation des marques de la Société sur ce(s) territoire(s) ;

- Des formations qualifiantes gratuites (pour 3 collaborateurs) ;

- L'organisation de formations qualifiantes payantes destinées à son propre réseau ;

- Une appliance Mobilegov Digital DNA ID-BOX en mode NFR ;

- Des accès aux produits en mode SAAS pour les démonstrations ;

- Des tarifs préférentiels sur l'offre de la Société (50% de remise sur le tarif public) ;

- 150 K€ de licences logicielles sur le prix public ;

- Un support avant-vente et commercial avec 1 accès à un Account Manager de Mobilegov ;

L'objectif de la société est d'avoir signé 15 contrats exclusifs d'ici fin 2010 étant précisé qu'à mars 2010, 8 contrats ont été signés (Royaume-Uni, Suisse, Italie, Corée, Belgique-Luxembourg, Afrique de l'Ouest, Mexique, Portugal) et 8 autres sont en négociations avancées (Afrique du Nord, Turquie, Espagne, Pologne, Australie, Dubaï, Abu-Dhabi, Hollande, Allemagne). Le contrat Coréen signé en septembre 2009 est particulièrement important dans la mesure où il étend les activités au continent asiatique, un territoire majeur dans le domaine de la sécurité informatique compte tenu du taux d'équipement et d'utilisation d'Internet habituellement constaté.

Pour cette zone, le distributeur est la société Bluzen Inc., intégrateur et éditeur de solutions de sécurité complémentaires de la technologie développée par Mobilegov. Bluzen Inc. compte parmi ses clients quelques-uns des principaux acteurs économiques du pays tels que Samsung ou encore LG.

La Société est confiante sur ces objectifs car l'enrichissement progressif du réseau international, doublée de la capacité à commercialiser en exclusivité sur un territoire dédié la technologie de l'ADN du Numérique®, sont des atouts majeurs qui contribuent à positionner l'ensemble distributeurs Mobilegov comme des acteurs prépondérants et innovants dans le monde de l'Internet et de la protection des données personnelles grâce à la révolution technologique proposée dans l'offre produits.

L'avantage concurrentiel technologique garantit le succès commercial sur un territoire donné et permettra au membre du réseau de développer son chiffre d'affaires plus rapidement en étant le détenteur unique d'une offre qui répond aux besoins de sécurité grandissant de l'utilisation de l'Internet.

Grâce à son réseau, Mobilegov dispose de plusieurs projets pilote à l'étranger :

- avec Unisys Belgique, pilote impliquant Eurojust, Europol et le FEDICT (Ministère belge des technologies de l'information et de la communication) pour authentifier les acteurs dans les échanges entre police et justice

- Avec Metadat, pilote impliquant la Chancellerie autrichienne pour sécuriser les accès professionnels à la base de données juridiques

- Avec son distributeur exclusif Lab Lateral, pilote impliquant les membres de l'initiative du Home Office pour lutter contre l'usurpation d'identité www.identitytheft.org.uk: Mobilegov sécurise les accès des 17 membres qui comptent les principaux services publics (douanes, police, passeports, réseau bancaire, etc.)

8.8. Technologie Mobilegov

Mobilegov a breveté un procédé et développé un noyau dur technologique. La technologie Mobilegov concerne aussi bien le procédé que sa mise en œuvre pour élaborer des produits commerciaux ergonomique, fiables et efficaces.

8.8.1. Principes de fonctionnement de la technologie Mobilegov

Le principe de fonctionnement de la technologie de Mobilegov consiste en deux étapes distinctes.

- L'enregistrement : avant qu'un système ne soit authentifié afin d'être déclaré bon pour exécuter une tâche, il passe par une étape, contrôlée par un opérateur habilité, pour produire, chiffrer et stocker des informations relatives à ses composants. Dans une application typique de sécurité, chaque composant d'un système peut être défini comme étant obligatoire, optionnel ou interdit. S'il est obligatoire, le composant doit être présent dans le système pour qu'il soit autorisé à fonctionner. S'il est Optionnel, le composant peut être présent ou pas.

  Enfin s'il est interdit, le composant ne peut pas être présent. La détection d'un tel composant bloquera le fonctionnement. Par défaut, tout composant non autorisé est interdit.

- La validation : à chaque fois qu'un système est utilisé pour exécuter une tâche, une étape de validation est lancée afin de comparer le système à celui qui a été préalablement enregistré. Si le système est identique, la tâche est autorisée à s'exécuter. Si le système est différent, la tâche est interdite et des données concernant la tentative sont enregistrées.

8.8.2. L'ADN Numérique

Issues d'une technologie propriétaire, les solutions d'authentification forte de Mobilegov permettent d'identifier tout équipement numérique (ordinateur portable ou non, clé USB, Ipod, disque dur externe mais aussi le tachychronographe d'un poids lourds, un décodeur TNT ou encore un compteur de gaz électrique…). Mobilegov s'appuie sur une propriété générale difficilement falsifiable des composants matériels. Tout composant numérique est unique et reconnaissable parmi des composants semblables. Sa technologie est donc indépendante des environnements (systèmes d'exploitation) ou des applications. Le procédé breveté consiste à :

- Descendre dans les couches basses de l'équipement pour détecter, identifier et extraire par des moyens logiciels des composantes internes et externes uniques, propres à chacun de ces équipements numériques tels que le numéro de série pour les composants (disques durs, processeurs, barrettes mémoire, lecteurs CDROM, clés USB, etc.) les Globally Unique Identifier (GUID) et les ClaSs Identifier (CLSID) pour les composants logiciels, etc.

- Réaliser un assemblage des données extraites, à partir d'un process de chiffrement pour en faire une clé unique, encore appelée « l'ADN numérique », véritable carte d'identité chiffrée de l'équipement numérique.

Ce procédé permet donc de reconnaître un équipement numérique parmi des milliards d'autres équipements similaires (même marque, même série de production, même capacité…). Il s'apparente à la biométrie, avec toutefois quelques avantages :

- L'information initiale est numérique, il n'y a pas de risque de faux rejets ni de fausse acceptation

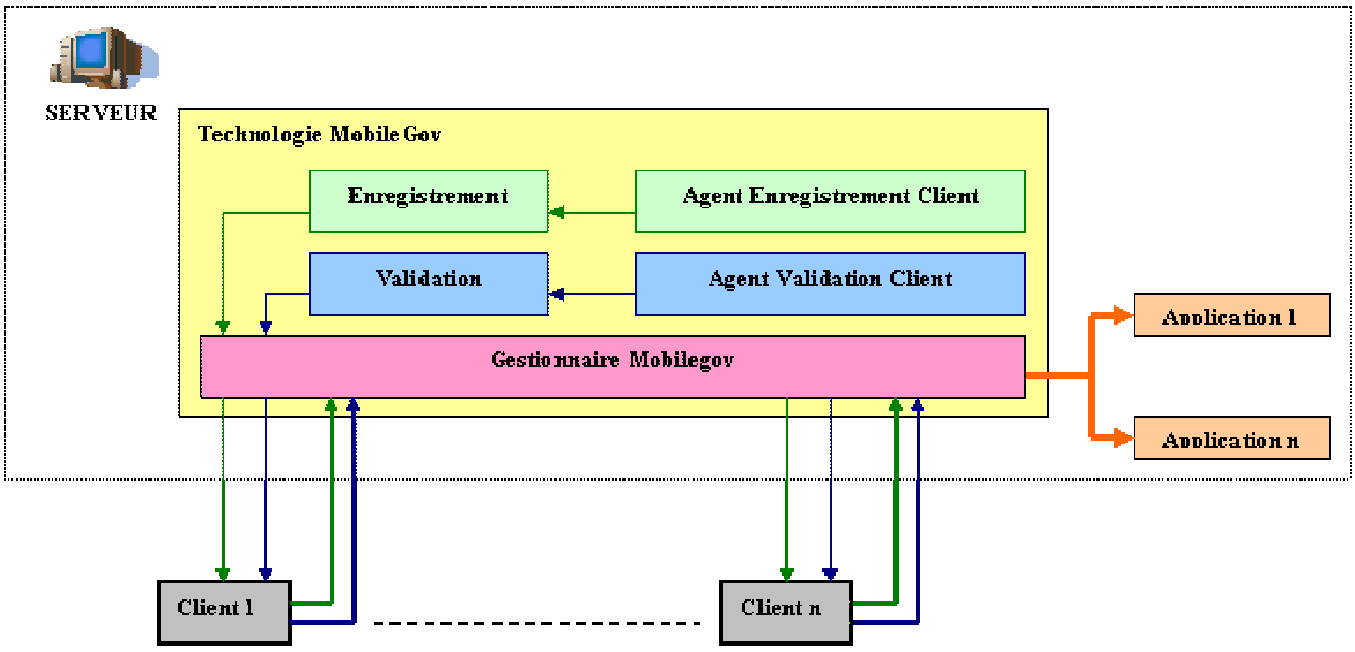
- L'information ne met pas en jeu de données personnelles, elle n'est pas concernée par les règles de la CNIL et plus généralement de la protection de la vie privée

- Selon des modalités à définir par le prestataire de service, l'utilisateur peut changer l'équipement qui sert à l'identifier et il peut même disposer de plusieurs équipements, par exemple au bureau, à la maison, en voyage.

8.8.3. Une flexibilité nouvelle pour la sécurité

Des données contextuelles peuvent être intégrées lors de l'enregistrement de l'équipement numérique Ainsi, pour qu'un système ne puisse être utilisé que dans une zone géographique déterminée, un récepteur GPS lui sera intégré et ses données prises en compte lors de la validation. L'authentification du GPS est un gage de qualité des informations. D'autres capteurs, par exemple biométriques, peuvent être également intégrés. La technologie modulaire Mobilegov permet de mettre en œuvre rapidement ces schémas de sécurité qui demanderaient autrement des développements spécifiques longs et coûteux.

L'exemple ci-dessous, destiné à expliquer la technologie s'appuie sur une architecture Web Service (Trusted Platform) mais les modules peuvent facilement être migrés depuis le serveur vers les clients.



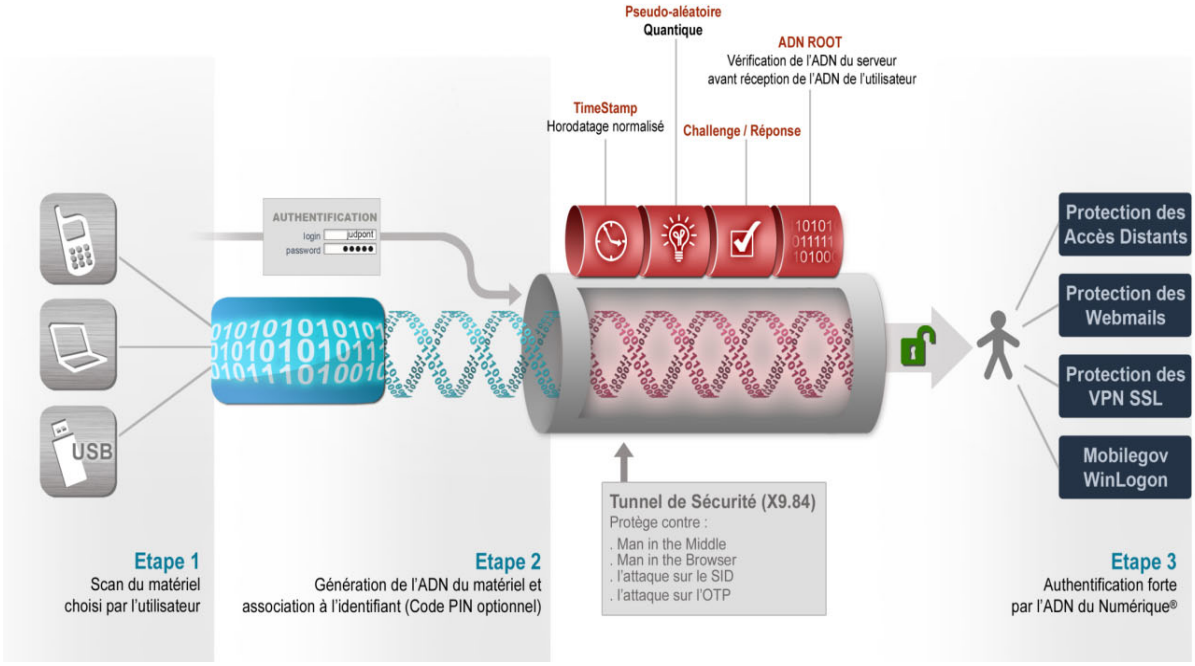
De manière à sécuriser l'accès à des applications (en orange) existant sur un serveur, la technologie Mobilegov (en jaune) initie le lancement d'un agent d'enregistrement des clients à sécuriser (en vert). Le résultat est une signature unique qui est envoyée à l'application Mobilegov. L'agent est ensuite détruit de la machine client.

Lorsqu'un client essaie d'accéder à une application du serveur, la technologie Mobilegov exécute un agent de validation sur la machine client (en bleu) afin de comparer la signature qu'il génère avec celle préenregistrée. Si les signatures sont identiques, l'accès est autorisé, sinon (la machine client a été modifiée), l'accès est refusé.

Ces opérations sont contrôlées et gérées par un gestionnaire propriétaire qui peut être intégré à une solution de gestion de parc existante (en rose).

8.8.4. Le fonctionnement des solutions innovantes Mobilegov

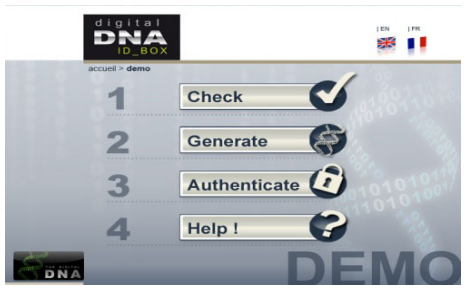
A partir de cette technologie, Mobilegov a développé une gamme de solutions de sécurité informatiques innovantes à destination des entreprises dans un premier temps. Quelle que doit la solution proposée (se reporter au détail de l'offre Chapitre 4), la démarche est identique et comprend étapes réalisées au sein d'une appliance spécifique intégrant la technologie propriétaire de Mobilegov:



L'étape 1 consiste à scanner les composants de l'équipement numérique choisi.

Les étapes 2 et 3 consistent à combiner les éléments scannés pour en établir une clé constituant l'ADN Numérique qui devra être reconnu à chaque tentative d'utilisation,

L'étape 4 correspond à cette phase d'authentification forte.

	
Appliance Mobilegov « ID-Box »	

Ce Serveur AAA (Authentification Administration Audit) innovant et chiffré, dénommé ID-BOX intègre un nouveau processeur qui inaugure une nouvelle ère pour la sécurité intégrée, avec le moteur de sécurité VIA PadLock Security Engine, le moteur de sécurité x86 le plus rapide du monde, disposant de la panoplie d'outils la plus complète pour les opérations de cryptographie. Outre le générateur de nombres aléatoires le meilleur du monde et le moteur de cryptage AES, le moteur de sécurité VIA PadLock du processeur C7 offre le brouillage SHA-1 et SHA-256 et un multiplicateur Montgomery supportant des clés allant jusqu'à 32K de longueur pour accélérer la cryptographie à clé publique. Toutes les opérations de chiffrement et d'échanges à l'intérieur de la technologie ID-BOX sont donc tous chiffrées de manière hardware.

L'ID-BOX est également extrêmement innovant en associant à son serveur de génération d'ADN numérique, un processeur quantique pour toutes les opérations aléatoires. Grâce au processeur intégré dans l'appliance, il est totalement impossible de prévoir le prochain numéro généré par le processeur quantique rendant toute attaque sur faille OTP totalement obsolète. La clé d'authentification correspondant à un équipement numérique enregistré ne peut être « retrouvée ».

Une fois la clé enregistrée, à chaque utilisation, L'ID-BOX envoie cet ADN Numérique à un serveur d'authentification garant de la sécurité et de l'intégration homogène dans un système informatique existant.

8.9. SWOT

8.9.1. Forces

Les points forts sont :

- Technologie de rupture offrant une barrière légale et technologique à l'entrée
- Equipe expérimentée
- Présent au moment où le marché explose
- Résout une faille critique de sécurité pour les eGouvernements et les Entreprises
- Brevet Exclusif
- Partenariats avec des leaders reconnus (Unisys, Accenture, ORANGE R&D, ST Microelectronics, Gemalto…)
- Des premiers clients prestigieux : un leader de l'industrie nucléaire, le Ministère de la Défense, l'Institut EURECOM, la Chancellerie Autrichienne, le National Health Service, britannique, British Telecom qui offre SAWS pour sécuriser ses propres clients.
- Une grande diversité de premiers clients, qui démontre l'étendue du marché : grands groupes, PME, centre de recherche et universités, administrations.
- Un réseau de distribution opérationnel sur 14 pays

8.9.2. Faiblesses

Les points faibles sont :

- Technologie de rupture donc risque pour les primo-adoptants
- Petite taille de la société (résolue en partie par les partenariats).
- Réseau de distribution encore jeune puisque constitué à partir de 2007.
- Réseau de distribution axé principalement sur l'Europe à ce jour : nous devons l'étoffer pour couvrir le globe, et mettre en place une présence locale.
- Le principal marché est encore émergent (lutte contre l'usurpation d'identité sur Internet).

8.9.3. Opportunités

Les opportunités sont :

- Maturité du marché des Endpoints, en croissance de 20% par an
- Maturité du marché de l'authentification forte sur LAN en croissance de 80% par an : besoin de renouvellement face à la technologie des mots de passe à usage unique.
- Décollage de l'authentification forte sur Internet qui commence à équiper les banques, et qui va s'imposer pour sécuriser les applications web
- Le besoin est nouveau, les solutions concurrentes peu adaptées.
- L'environnement politique est favorable (lancement des cartes d'identité à puce et des nouveaux passeports biométriques) qui banalisent la sécurité numérique et nécessitent des équipements relais car ces cartes d'identité ne pourront sécuriser toutes les transactions.

8.9.4. Craintes

Les craintes sont

- Le lobbying des industriels en place (mais résolu avec des Intégrateurs comme ceux de Mobilegov)
- Le manque de financement peut être un frein à la capture du marché par Mobilegov en limitant notre capacité de déploiement (mais une levée de fonds permettra de régler ce problème).
- Le marché des administrations publiques est un marché avec un cycle de vente long (plus d'un an) mais il est compensé par des cycles plus courts du côté des entreprises et par la mise en place d'une solution d'affacturage.

8.10. Notre vision

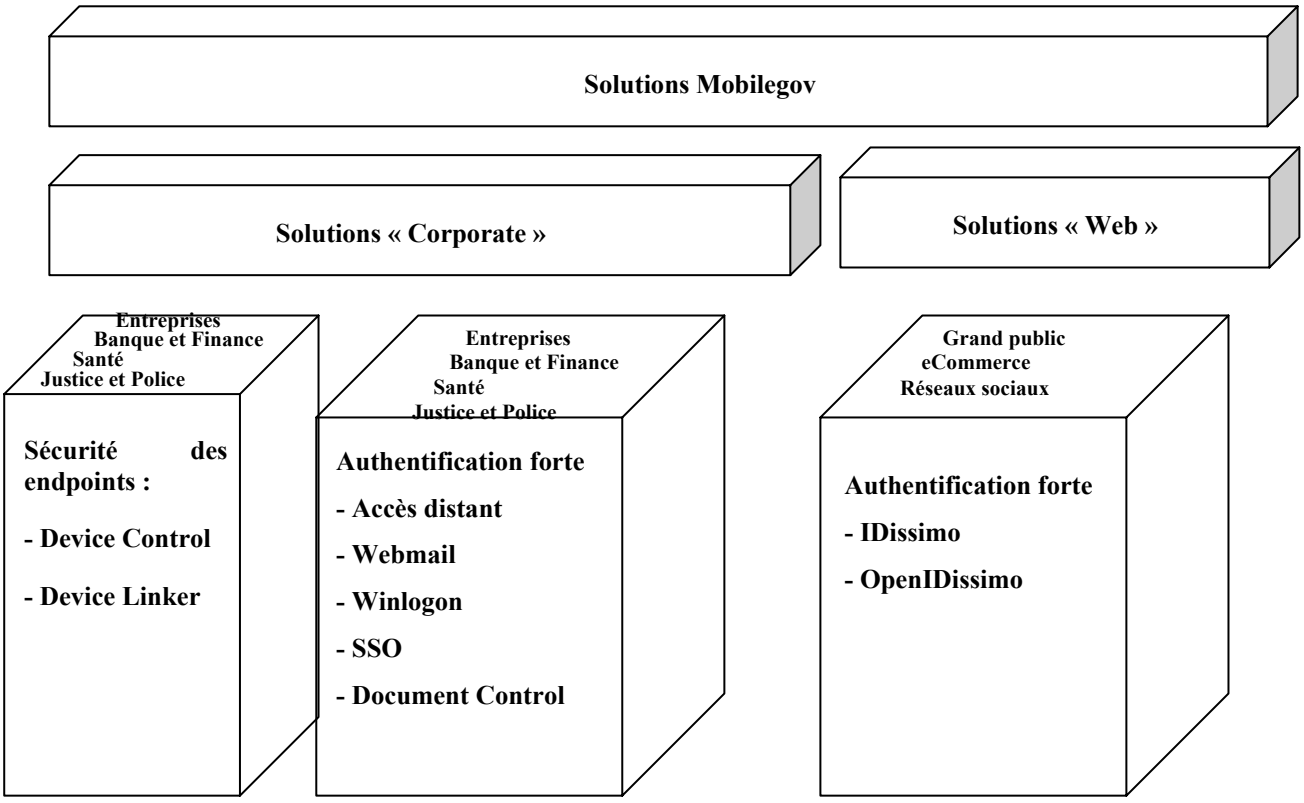
La sécurité aujourd'hui vient toujours en réaction à des attaques réussies. Elle pénalise surtout l'utilisateur honnête, en lui imposant des empilages de mesures toutes contournables par les criminels.

La sécurité doit évoluer vers des solutions proactives. Ces solutions seront génériques, de façon à être bien comprises et applicables dans tous les domaines touchés par la « convergence » informatique-réseaux-téléphonie.

L'identité difficilement falsifiable des composants matériels, que nous appelons leur ADN numérique, est à la base d'une telle solution que nous avons brevetée.

Nous l'exploitons déjà dans nos premiers produits, et nous proposons de la généraliser à tous les domaines où interviennent des composants numériques et dans lesquels existent des préoccupations de sécurité, de protection des droits numériques, de copyright, ou plus simplement pour protéger les appareils contre le vol en les rendant inutilisables en dehors de l'environnement pour lequel ils ont été enregistrés.

En tant qu'éditeur de solutions innovantes de sécurité, dans un monde où la vente directe est limitée, Mobilegov développe et anime un réseau Européen et mondial de distributeurs, d'intégrateurs et de revendeurs spécialisés.



La stratégie utilisée est donc de développer progressivement ces réseaux par grandes zones géographiques et par type de produit, tout en personnalisant par des « solutions métiers » ces produits aux métiers spécifiques des clients des distributeurs.

Aujourd'hui, les spécialistes de Mobilegov travaillent chez ces distributeurs pour former et accompagner leurs ingénieurs afin de les aider à capter des parts de marché. Après avoir validé leur potentiel, la société peut leur offrir une exclusivité, pour une gamme de produits identifiée.

Mobilegov envisage une stratégie de capture de distributeurs agressive via une offre de partenariat motivante basée sur les atouts suivants :

1. La valeur ajoutée de ses produits : Mobilegov ne développe ses solutions qu'avec le concours d'utilisateurs pilotes permettant de créer des solutions qui correspondent à leurs besoins, donc aussi aux exigences du marché.
2. La propriété des brevets d'invention : Mobilegov fait savoir que les entreprises en Europe ou en Amérique du Nord qui copient sa technologie font courir un risque important à leurs clients, puisque Mobilegov a décidé de faire valoir ses droits de propriété industrielle auprès des juridictions compétentes.

3. L'élaboration des futurs standards de sécurité des équipements mobiles : Mobilegov est partenaire du portail Européen de la Biométrie et participe activement en tant que partenaire à plusieurs projets collaboratifs (CNRS, Gemalto, ST Microelectronics).

4. L'approche multi produit : Contrairement à ses concurrents (qui sont mono produit pour la plupart) Mobilegov a une vraie logique de développement de produits à partir de ses brevets et garantit ainsi à ses distributeurs des revenus récurrents, résultant de la vente de nouveaux produits qui dynamisent le marché.

5. L'accélération d'acquisition de distributeurs : Mobilegov entend proposer à ses nouveaux distributeurs des commissions plus importantes que ses concurrents afin d'accélérer la signature d'accords commerciaux, la couverture géographique des ventes et le démarrage de la facturation. Cette période serait limitée aux primo-accédants.

Une approche nationale : à l'heure où le marché de la sécurité est couvert par des sociétés américaines et israéliennes, Mobilegov met en avant son savoir-faire technologique Français et fait jouer le nationalisme économique. La société est déjà accompagnée sur les comptes sensibles par les services de la DST.

Chapitre 9

Chapitre 9: Organisation

9.1. Une organisation souple et réactive

La structure de Mobilegov bénéficie d'une organisation opérationnelle simple dirigée par une équipe de managers expérimentés et complémentaires.

9.1.1. Administrateurs

Michel FRENKIEL - Cofondateur & Président (62 ans) : Ingénieur Arts et Métiers et Master of Science de l'Université du Colorado, Michel Frenkiel est consultant en informatique, expert auprès de la Commission Européenne depuis 1997, spécialiste du gouvernement électronique. Il a organisé dès 2002 un forum Citoyenneté Européenne, d'où est né le projet eJustice, qui facilite la collaboration sécurisée entre les acteurs de la justice en Europe, notamment Eurojust et Europol, organisations internationales de lutte contre le crime organisé. Auparavant, il a dirigé pour Thales le développement logiciel du sonar qui équipe les derniers sous-marins nucléaires Français, l'un des plus gros projets logiciels jamais réalisés. Pour IBM, il mené la stratégie de génie logiciel de télécommunications. Il a travaillé aussi une dizaine d'années aux Etats-Unis, notamment dans la recherche météorologique. Il est un des co-auteurs du Grand Livre Intranet. Durant le projet eJustice, il a identifié une faille de sécurité dans les systèmes d'authentification et il a créé avec ses deux associés la start-up Mobilegov pour exploiter un palliatif qu'il a breveté.

François-Pierre LE PAGE - Cofondateur & Directeur Général Délégué Marketing/Commercial (41 ans) : Diplômé du CERAM Sophia Antipolis et de l'Université de Phoenix Arizona (MBA), expert auprès de la Commission Européenne notamment dans le Programme EUROSTARS – EUREKA, François-Pierre a acquis une expérience internationale d'entrepreneur à travers la création et le développement de son Groupe (implanté à Londres, Paris et Sophia Antipolis), fournissant des services et des applications de eBusiness, de eProcurement et des logiciels à de nombreux grands comptes internationaux (Lucent, Nortel, Accenture, Disney, Infogrames, etc.). En 2003, il a rejoint un fournisseur de services eGouvernement afin de développer la stratégie de la société à l'international et de coordonner l'implémentation de solutions mobiles dans le cadre d'un projet Européen d'équipement des forces de police sur la France et l'Italie. Le projet est un des succès grâce au travail de François, qui avec ses collaborateurs, a réussi à convaincre des forces de police à utiliser sur le terrain des applications mobiles et à en plébisciter l'usage auprès d'autres services d'Administrations publiques.Il fut notamment publié dans le magazine «Traffic Technology International», et dans UK International Press au Royaume-Uni. Il intervient régulièrement lors de conférences ou de débats auprès d'institutions comme la Commission Européenne ou encore auprès du Ministère français de la Recherche et de l'Industrie ainsi que le CERAM Sophia Antipolis.

Eric MATHIEU - Cofondateur & Directeur Général Délégué Technique/Administration (38 ans) : Ingénieur de l'Ecole des Mines (EERIE). Eric a participe à des développements stratégiques classifiés chez Eurocopter (groupe EADS) pour le suivi automatique de cibles sur les hélicoptères "Tigre" et chez Sema Group pour les centrales nucléaires EDF. Il a acquis ensuite des compétences plus larges, et a géré des équipes chez Amadeus (Système de Distribution Global pour les réservations de voyage) et chez LivePicture Inc. (racheté par MGI Software Inc. Puis Roxio Inc., créateur du format d'image multi résolution FlashPix® utilise par Eastman Kodak).Depuis 1999, il travaille sur le marché des assistants personnels de type PDA (Palm, Symbian, Windows CE…).Il a été le responsable du développement et le directeur de produit d'un fournisseur de solution innovante de saisie de texte sur machine nomades (prix INPI de l'innovation en 2000).Il a été Directeur Technique d'un fournisseur de solutions aux eGouvernement. Il a entièrement défini, spécifié, recruté et dirigé une équipe de dix ingénieurs, créé la totalité de la solution technique en place basée sur des appareils nomades et des serveurs de BackOffice. Il a également adapté et déployé cette technologie avec succès à différents pays Européens. Il a également coordonné les relations avec des sociétés sous-traitantes telles que Thalès et Gemalto en Europe, en Asie et aux Etats-Unis. Son expertise est reconnue par de nombreuses conférences auprès d'Universités, d'écoles d'ingénieurs et de salons professionnels. Depuis 2005, il est expert indépendant auprès de l'ENISA (European Network and Information Security Agency http://www.enisa.eu.int/)

9.1.2. Comité de Direction

Forte de 40 collaborateurs, la Société est structurée à travers ses principales fonctions encadrées par un management complémentaire et expérimenté :

- Fondateurs : PDG, DGD, DT
- Direction commerciale
- Direction Produits / Marketing / Communication
- Direction R&D, Qualité / Système / Intégration
- Direction Sécurité Informatique

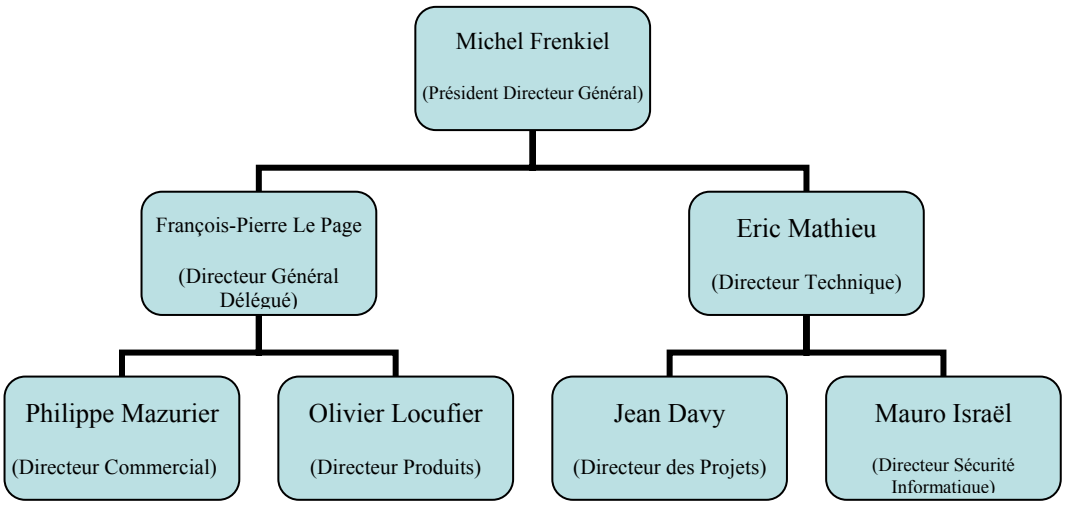
Olivier Locufier : Directeur Produits & Stratégie Marketing Expert en sécurité informatique, cet entrepreneur a créé et développé le Groupe Xelios qu'il a revendu en 2004 à SAGEM. Spécialiste du marché de la sécurité, visionnaire de son évolution, il conçoit des solutions révolutionnaires basées sur la force de l'ADN du Numérique®.

Mauro Israël : Directeur de la Sécurité Informatique, expert internationalement reconnu en sécurité informatique depuis 15 ans, il a effectué plus de 1000 audits de sécurité et donné de nombreuses conférences à travers le monde. Mauro connaît chacune des problématiques clients et peut les conseiller en apportant la solution la plus adaptée

Philippe Mazurier : Ingénieur commercial depuis 20 ans, Philippe est le directeur commercial de la Société. A ce titre, ildéveloppe et structure le réseau de distribution, dynamise les ventes du groupe à l'international et gère l'équipe commerciale de Mobilegov.

Jean Davy : Ingénieur justifiant de 25 ans d'expérience en développement logiciel, notamment chez Schlumberger et SNECMA, consultant indépendant pour Microsoft, Jean est directeur des projets. Il encadre aujourd'hui les équipes de développements logiciels, structurées autour de projets.

9.2. Organigramme



Chapitre
10

Chapitre 10: Recherche & Développement et Marques

10.1. La Recherche & Développement

La Recherche & Développement est un des axes forts de la stratégie de Mobilegov. C'est en y consacrant la majeure partie de ses investissements que la Société s'est constituée une gamme technologique qui aujourd'hui fait sa différence avec ses principaux concurrents.

Mobilegov s'appuie pleinement sur l'expertise de cette équipe spécialisée dans le domaine des télécommunications, de la sécurité, de l'électronique embarquée pour donner naissance à des produits de haut niveau. La réussite provient également d'une forte synergie entre cette équipe et l'équipe de direction chargée de la définition des produits, ceci afin d'optimiser l'adéquation des produits et le timing de disponibilité.

Sous la responsabilité d'un directeur technique, cette équipe constituée de 15 personnes est répartie en deux pôles :

Le pôle R&D en charge de la sécurisation et de l'enrichissement permanent du cœur de la technologie de l'ADN Numérique. Une veille technologique permanent s'impose afin d'optimiser la capacité de déploiement massif de la technologie de l'ADN. Il est ainsi impératif de veiller à la compatibilité avec l'évolution des différents environnements et des systèmes d'exploitation mais aussi des équipements numériques existants.

Le pôle Test/ Systèmes / Intégration : Certains ingénieurs travaillent plus particulièrement sur les grands domaines de l'offre produits : Internet, VPN …etc. ou à des développements métiers à la demande de certains clients. Les équipes intégration sont pour leur part, en appui des équipes commerciales dans les phases d'avant-vente mais aussi en après-vente afin d'installer les appliances et d'en démarrer la mise en œuvre. Elles assurent également les formations destinées tant aux membres du réseau de distribution qu'auprès de certains clients.

Pour renforcer ses capacités de développement, Mobilegov a su dès la création de la structure en 2004 transformer les projets de collaboration ponctuels en accord de partenariats sur le long terme. On peut citer par exemple l'accord de partenariat renouvelé en novembre 2007 qui lie Mobilegov et le prestigieux CNRS, la participation réussie au projet européen de validation de marché MEMO et aux projets européens de R&D eJustice et R4eGov. Ces accords ont permis à Mobilegov d'élargir son réseau avec des administrations publiques intéressées par les solutions avancées de sécurité. Citons seulement le marché signé en 2008 pour le test de la solution par Europol, Eurojust, la Chancellerie Autrichienne.

Mobilegov co-préside depuis décembre 2007 l'un des quatre groupes de travail du Pôle de Compétitivité International « Solutions Communicantes Sécurisées » et assure la liaison entre la Pôle et les régions Nord-Est (Newcastle) et Sud-Est (Thames Valley) du Royaume Uni, ce qui permet d'espérer des projets collaboratifs intéressants. Fin 2009, Mobilegov est partenaire dans plusieurs propositions de projets de R&D nationaux et européens, notamment dans le programme Eurêka.

Enfin, Mobilegov a vu sa capacité d'innovation récompensée à de nombreuses reprises :

- 2005 : Prix de la meilleure innovation Capital-IT
- 2007 : Lauréat du trophée Cap Innovation décerné par …
- 2008 : Prix de l'innovation TIC-PACA
- Vainqueur du Prix RedHerring 100 Europe
- 2009 : Vainqueur du Prix RedHerring 100 Global 2008 qui récompense les 100 entreprises privées internationales incontournables dans le secteur des nouvelles technologies, par leur capacité d'innovation.

10.2. La propriété intellectuelle

Mobilegov a déposé un premier brevet européen fin 2004, étendu début 2006 à l'Amérique du Nord, et un second brevet déposé en 2009 pour protéger une future application de protection des documents. Grâce à cette application, Mobilegov Document Control, un document (texte, audio, video…) téléchargé d'un serveur ne peut être exploité que sur le matériel utilisé pour le télécharger.

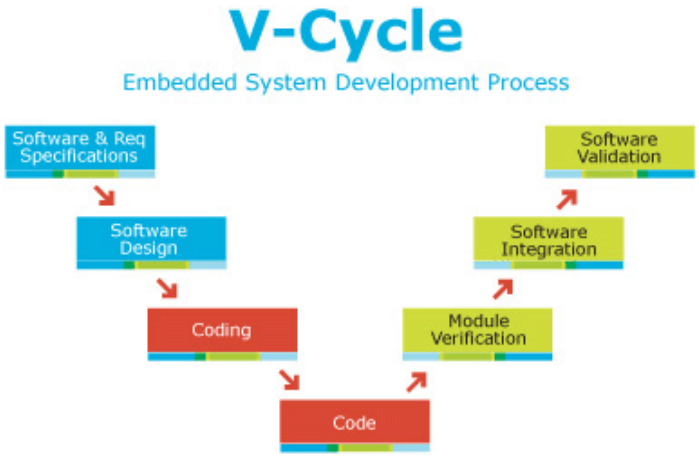
La Société est propriétaire de la marque Mobilegov, dépôt INPI du 28 juillet 2004 sous le N°04 3305673. Elle est propriétaire de son logo et de l'appellation « ADN du Numérique ».

La Société est aussi propriétaire de plusieurs noms de domaine: www.mobilegov.com, www.mobilegov.be, www.mobilegov.co.uk , www.mobilegov.info , www.usbdevicecontrol.com , www.device-authenticator.com, www.device-checker.com , www.device-linker.com , www.deviceauthenticator.com , www.devicechecker.com, www.devicelinker.com.

10.3. Méthodes de développement technique

Le développement technique fait appel aux méthodes éprouvées de développement logiciel, complétées par les technologies les plus à jour de modélisation, d'analyse comportementale des logiciels et de contrôle qualité. La mise en oeuvre de ces techniques de développement est inhabituelle dans une start-up, et résulte de l'expérience des dirigeants dans la mise au point de systèmes complexes de défense.

Le plan de développement a suivi un schéma classique en V où chaque étape a été validée en environnement réel.



Le cycle de développement en V s'appuie sur :

- Des spécifications fonctionnelles et techniques
- Un design UML orienté objet OOM (JAVA, J2EE, SOAP, XML, C++)
- La portabilité (code JAVA Orienté Objet documenté et commenté, une forte adaptabilité aux bases de données mySQL, PostGre, Oracle, DB2,…)
- Un processus qualité renforcé et une méthodologie CMMI
- Des validations et des certifications externes par des organismes de renom.

En se basant sur cette méthodologie, Mobilegov est capable de concevoir des solutions orientées marchés et qui, de surcroît, enrichissent le noyau technologique à chaque étape. Lorsque cela est possible, des solutions génériques sont développées afin de les adapter à diverses applications permettant ainsi de réduire considérablement les phases d'adaptation à de nouveaux périphériques et environnements systèmes. Par exemple, une API (Application Programming Interface) peut être formatée à partir du noyau technique en place pour répondre à un besoin spécifique d'intégration de la technologie dans le produit d'un prospect.Cette approche permet à Mobilegov de proposer des composants logiciels éprouvés qui s'intègrent dans des applications de ses clients. Cette méthodologie s'appuie sur des process éprouvés, en particulier :

- Des sauvegardes sont effectuées de manière régulière et automatisées. Elles sont entreposées dans des lieux sécurisés distincts afin de réduire le risque de catastrophe naturelle (incendie, dégât des eaux…) ;

- Les codes sources sont stockés de manière contrôlée avec un outil CVS permettant de remonter jusqu'à la création du fichier lui-même ;

- Les locaux sont sécurisés (alarme, incendie).

Enfin, Mobilegov met en place la norme de développement CMMI (Capability Maturity Model Integration, Modèle intégré du niveau de maturité), très restrictive, du DoD (Ministère de la défense américain).CMMI est un référentiel d'évaluation de la capacité à gérer et terminer un projet correctement, proposant nombre de bonnes pratiques liées à la gestion, au développement et à la maintenance d'applications et de systèmes. Ces bonnes pratiques sont regroupées en 24 processus, eux-mêmes regroupés en 4 types (Process Management, Project Management, Engineering et Support) et 5 niveaux de maturité. Cette norme met en place une méthodologie complète (des spécifications aux tests de conformités) et éprouvée de documentation. Elle est un gage de fiabilité des produits que Mobilegov fabrique.

Les applications client-serveur telles que Device Control et Access Control apportent l'évolutivité, l'adaptabilité, la scalabilité par plusieurs choix d'organisation :

- l'architecture JEE

- le serveur d'applications, qui apporte l'évolutivité

- l'administration par Web Service exploitant la technologie Flex

- la base de données relationnelle MySQL, qui permet une gestion efficace des données

- l'interface LDAP, qui permet de relier sécurité et annuaire de l'entreprise

- la facilité du déploiement autorisée par IzPack et l'utilisation de l'annuaire d'entreprise.

Chapitre
11

Chapitre 11: Informations sur les tendances

11.1. Principales tendances ayant affecté les ventes, coûts et prix de vente depuis la fin du dernier exercice

La Société n'a pas connaissance de tendances ou d'événements avérés, relatifs à son activité, qui sont raisonnablement susceptibles d'influer de manières sensible et exceptionnelle sur son chiffre d'affaires au cours du prochain semestre.

L'impact négatif de la crise financière de 2008 est contrebalancé par le besoin des organismes financiers de montrer leur détermination à lutter contre les fraudes et à protéger les informations personnelles dont la dissémination accidentelle est à l'origine de plusieurs scandales. Il se traduit cependant par des retards importants dans la prise de décision et la signature de contrats : ainsi, de nombreux POC (« proof of concept », ou démonstrateurs sont en place, mais ils n'ont pas donné lieu aux signatures de commande que nous attendions. Aucun de ces prospects ne s'est non plus tourné vers une solution concurrente. On peut donc s'attendre à concrétiser en 2010 les affaires attendues pour 2009.

11.2. Tendances et perspectives de la Société

Les perspectives de croissance de la Société suivent au moins la croissance de ses marchés :

- 20% de croissance annuelle sur le marché de la sécurisation des « Endpoints », pour un marché mondial de 250M€
- 80% de croissance annuelle sur le marché de l'authentification forte sur les réseaux d'entreprise pour un marché mondial de 800M€
- Le marché émergent de l'authentification forte sur Internet devrait atteindre 10M€ dans les 2 ans, Mobilegov s'y positionne en leader
- Le marché de la gestion documentaire représente 8Mds€, Mobilegov adresse de façon innovante le contrôle du cycle de vie des documents, .

Ainsi, la forte croissance de Mobilegov sera tirée par la gamme de produits pour le Web, conformément au compte de résultat prévisionnel.

Chapitre 12

Chapitre 12: Organes d'administration et de direction

12.1. Dirigeants et administrateurs de la Société

12.1.1. Informations générales relatives aux dirigeants et administrateurs

Nom	Fonction
Michel FRENKIEL	Président Directeur Général
François-Pierre LE PAGE	Administrateur – Directeur Général Délégué
Eric MATHIEU	Administrateur – Directeur Technique

Adresse professionnelle des administrateurs :

- M. Michel FRENKIEL
- M. François-Pierre LE PAGE 2000 route des Lucioles – 06901 Sophia-Antipolis
- M. Eric MATHIEU

L'expertise et l'expérience en matière de gestion de ces personnes résultent des différentes fonctions salariées et/ou de direction qu'elles ont précédemment exercées et/ou qu'elles continuent d'exercer au sein d'autres sociétés ou organismes divers.

Il n'existe pas entre les personnes listées ci-dessus de liens familiaux :

Aucune de ces personnes, au cours des 5 dernières années,

1. n'a fait l'objet de condamnation pour fraude ;
2. n'a été associée en sa qualité de dirigeant ou administrateur à une faillite, mise sous séquestre ou liquidation ;
3. n'a fait l'objet d'une interdiction de gérer ;
4. n'a fait l'objet d'incriminations ou de sanctions publiques officielles prononcées par des autorités statutaires ou réglementaires.

12.2. Autres mandats

Néant.

12.3. Pacte d'actionnaires

Il n'existe pas à la date du présent document un pacte d'actionnaires relatif au capital de Mobilegov.

12.4. Conflits d'intérêts au niveau des organes d'administration, de direction, de surveillance et de la direction générale

A la connaissance de la Société, il n'existe aucun conflit d'intérêts potentiel au niveau des organes d'administration, de direction, de surveillance et de la direction générale.

Chapitre
13

Chapitre 13: Rémunérations et avantages

13.1. Rémunération des membres du Conseil d'Administration et dirigeants

Au cours de l'exercice clos le 31 décembre 2009, Michel FRENKIEL a perçu 80.000€ au titre de ses fonctions, dont 0 euros en part variable.

Sur la même période, les sommes allouées à François LE PAGE au titre de ses fonctions s'élèvent à 80.000€, dont 0 euros en part variable.

Sur la même période, les sommes allouées à Eric MATHIEU au titre de ses fonctions s'élèvent à 80.000€, dont 0 euros en part variable.

La Société n'a pas distribué de jetons de présence à ses administrateurs.

13.2. Sommes provisionnées par la Société aux fins de versement de pensions, retraites et autres avantages au profit des membres du Conseil d'Administration et dirigeants

Il n'y a pas de sommes provisionnées ou constatées par ailleurs par la Société ou ses filiales aux fins du versement de pensions, de retraites ou d'autres avantages au profit des membres du Conseil d'Administration et de Direction.

Chapitre 14

Chapitre 14: Fonctionnement des organes d'administration et de direction

14.1. Direction de la Société

La Société est représentée à l'égard des tiers par son Président, Michel FRENKIEL.

14.1.1. Mandat des administrateurs

Le tableau ci-dessous indique la composition du Conseil d'Administration de la Société à la date du présent Document d'information ainsi que les principales informations relatives aux mandataires sociaux.

Nom	Fonction	Date de première nomination	Date de fin de mandat	Nombre d'actions détenues en date du présent document
Michel FRENKIEL	Président	AGE 5 août 2006 Portant transformation de la SARL en S.A.	31/12/2011	110 000
François-Pierre LE PAGE	Administrateur	AGE 5 août 2006	31/12/2011	59 828
Eric MATHIEU	Administrateur	AGE 5 août 2006	31/12/2011	61 006

14.2. Contrats entre les administrateurs et la Société

Il n'existe aucun contrat de service conclu entre la Société et l'un de ses administrateurs à la date du présent Document d'Information.

Chapitre 15

Chapitre 15: Principaux actionnaires

15.1. Actionnaires significatifs non représentés au Conseil d'administration

Actionnaires	Nombre d'actions	% capital
MOBILEGOV LIMITED	94 405	11,22%
FRENKIEL Raymonde	20 000	2,38%
PODELSKI Valérie	16 129	1,92%
VAUTHIER Alain	9 677	1,15%
KAJLER Norbert	9 290	1,10%
LE MERRER Pascal	6 000	0,71%
SUDRE Dominique	5 554	0,66%
AOSP SARL PIZZA HUT	5 550	0,66%
AUGER Bernard	4 500	0,53%
SUDRE Philippe	4 380	0,52%
LOUCHART BERTELLEMY	3 300	0,39%
ESCURET Edmond	3 000	0,36%
URBAN Henri	2 931	0,35%
CHESSE Claude	2 390	0,28%
JULLIEN François	2 122	0,25%
LE MERRER Hélène	2 000	0,24%
Nombre total d'actions tous actionnaires confondus		
Total	841 619	100%

15.2. Droits de vote des principaux actionnaires

L'article 29 des statuts confère un droit de vote double à toutes les actions entièrement libérées pour lesquelles il sera justifié d'une inscription nominative, depuis deux ans au moins, au nom du même actionnaire.

15.3. Contrôle de la Société

Les principaux actionnaires de la Société, qui sont les fondateurs et leurs familles, détiennent 43% du capital et 60% des droits de vote.

	Nb titres	% Titres	% Droits de vote
Fondateurs	**325 239**	**38,6%**	**54,1%**
Famille	**36 129**	**4,3%**	**6,0%**
Nominatif	**72 068**	**8,6%**	**6,0%**
Autres (public)	**408 183**	**48,5%**	**33,9%**
Total	**841 619**	**100,0%**	**100%**

Chapitre
16

Chapitre 16: Conventions réglementées

16.1. Rapport spécial des commissaires aux comptes sur les conventions réglementées portant sur l'exercice clos au 31 décembre 2008

Mesdames, Messieurs, les Actionnaires,

En notre qualité de commissaire aux comptes de votre société, nous vous présentons notre rapport sur les conventions réglementées.

Conventions autorisées au cours de l'exercice

En application de l'article L. 225-40 du Code de commerce, nous avons été avisés des conventions qui ont fait l'objet de l'autorisation préalable de votre conseil d'administration. Il ne nous appartient pas de rechercher l'existence éventuelle d'autres conventions mais de vous communiquer, sur la base des informations qui nous ont été données, les caractéristiques et les modalités essentielles de celles dont nous avons été avisés, sans avoir à nous prononcer sur leur utilité et leur bien-fondé.

Il vous appartient, selon les termes de l'article R.225-31 du Code de commerce, d'apprécier l'intérêt qui s'attachait à la conclusion de ces conventions en vue de leur approbation.

Nous avons effectué nos travaux selon les normes professionnelles applicables en France ; ces normes requièrent la mise en œuvre de diligences destinées à vérifier la concordance des informations qui nous ont été données avec les documents de base dont elles sont issues.

1. Convention conclue avec la société Mobilegov Ltd

Personne concernée

Monsieur Michel FRENKIEL, Monsieur François-Pierre LE PAGE, Monsieur Eric MATHIEU

(Administrateurs)

Nature et objet

Facturation de licence informatique dans le cadre de l'objet social de la société.

Modalités

La société MOBILEGOV SA a établit des factures de licences et serveurs selon un contrat de « Distribution Partner Agreement » en date du 10/12/2008, à la société Mobilegov Ltd, domiciliée à Reading (Royaume-Uni), pour un montant de 450.000,00 €uros HT au titre de l'exercice clos le 31 décembre 2008.

Fait à Sophia-Antipolis, le 14 septembre 2009

Le Commissaire aux comptes
Expertise & Audit International
Stéphan BRUN

Chapitre
17

Chapitre 17: Informations financières de la société

17.1. Comptes annuels 2008 et 2007

17.1.1. Bilan

AGREMENT DGFIP C5109.10009 — Formulaire obligatoire (article 53 A du code général des impôts). (1) **BILAN - ACTIF** DGFiP N°2050 2009

Désignation de l'entreprise : MOBILEGOV FRANCE — Durée de l'exercice exprimée en nombre de mois * 12

Adresse de l'entreprise LES ALGORYTHMES 2000 RTE DES LUCIOLES 06410 BIOT — Durée de l'exercice précédent * 12

Numéro SIRET* 45363992300012 — Néant ☐*

EXEMPLAIRE À CONSERVER PAR LE DÉCLARANT

			Brut 1	Amortissements, provisions 2	Exercice N clos le 31122008 Net 3	N-1 31122007 Net 4
	Capital souscrit non appelé (I)	AA				
ACTIF IMMOBILISÉ * — IMMOBILISATIONS INCORPORELLES	Frais d'établissement *	AB		AC		
	Frais de développement *	CX	220 047	CQ 34 142	185 905	174 498
	Concessions, brevets et droits similaires	AF	8 887	AG 3 336	5 551	
	Fonds commercial (1)	AH		AI		
	Autres immobilisations incorporelles	AJ		AK		
	Avances et acomptes sur immobilisations incorporelles	AL		AM		
IMMOBILISATIONS CORPORELLES	Terrains	AN		AO		
	Constructions	AP		AQ		
	Installations techniques, matériel et outillage industriels	AR		AS		
	Autres immobilisations corporelles	AT	39 252	AU 12 027	27 226	9 124
	Immobilisations en cours	AV		AW		
	Avances et acomptes	AX		AY		
IMMOBILISATIONS FINANCIÈRES (2)	Participations évaluées selon la méthode de mise en équivalence	CS		CT		
	Autres participations	CU	1	CV	1	
	Créances rattachées à des participations	BB		BC		
	Autres titres immobilisés	BD		BE		
	Prêts	BF		BG		
	Autres immobilisations financières*	BH	21 902	BI	21 902	2 546
	TOTAL (II)	BJ	290 089	BK 49 504	240 585	186 169
ACTIF CIRCULANT — STOCKS *	Matières premières, approvisionnements	BL	4 224	BM	4 224	9 481
	En cours de production de biens	BN		BO		
	En cours de production de services	BP		BQ		
	Produits intermédiaires et finis	BR		BS		
	Marchandises	BT		BU		
	Avances et acomptes versés sur commandes	BV		BW		
CRÉANCES	Clients et comptes rattachés (3)*	BX	521 233	BY 15 500	505 733	95 895
	Autres créances (3)	BZ	738 877	CA	738 877	130 472
	Capital souscrit et appelé, non versé	CB		CC		
DIVERS	Valeurs mobilières de placement (dont actions propres : .....)	CD		CE		
	Disponibilités	CF	1 346	CG	1 346	154 997
Comptes de régularisation	Charges constatées d'avance (3)*	CH	29 783	CI	29 783	3 452
	TOTAL (III)	CJ	1 295 462	CK 15 500	1 279 962	394 297
	Frais d'émission d'emprunt à étaler (IV)	CW				
	Primes de remboursement des obligations (V)	CM				
	Écarts de conversion actif * (VI)	CN				
	TOTAL GÉNÉRAL (I à VI)	CO	1 585 551	1A 65 004	1 520 547	580 466

Renvois : (1) Dont droit au bail : — (2) Part à moins d'un an des immobilisations financières nettes : CP — (3) Part à plus d'un an : CR

Clause de réserve de propriété : * Immobilisations : — Stocks : — Créances :

* Des explications concernant cette rubrique sont données dans la notice n°2032

SAGE Experts-comptables janvier 2009

AGREMENT DGFIP C5109.10009 (2) **BILAN - PASSIF avant répartition** DGFiP N°2051 2009

Formulaire obligatoire (article 53 A du Code général des impôts)

EXEMPLAIRE A CONSERVER PAR LE DÉCLARANT

Désignation de l'entreprise : MOBILEGOV FRANCE — Néant ☐*

				Exercice N	Exercice N-1
CAPITAUX PROPRES	Capital social ou individuel (1)* (Dont versé : 450 382)		DA	450 382	43 000
	Primes d'émission, de fusion, d'apport, ...		DB	1 935 160	218 997
	Ecarts de réévaluation (2) * (dont écart d'équivalence	EK	DC		
	Réserve légale (3)		DD	12	12
	Réserves statutaires ou contractuelles		DE		
	Réserves réglementées (3)* (Dont réserve spéciale des provisions pour fluctuation des cours	B1	DF		
	Autres réserves (Dont réserve relative à l'achat d'oeuvres originales d'artistes vivants*	EJ	DG	210	210
	Report à nouveau		DH	(244 574)	(65 491)
	RÉSULTAT DE L'EXERCICE (bénéfice ou perte)		DI	(1 183 157)	(179 083)
	Subventions d'investissement		DJ		
	Provisions réglementées *		DK		
	TOTAL (I)		DL	958 034	17 646
Autres fonds propres	Produit des émissions de titres participatifs		DM		
	Avances conditionnées		DN		
	TOTAL (II)		DO		
Provisions pour risques et charges	Provisions pour risques		DP	12 000	
	Provisions pour charges		DQ		
	TOTAL (III)		DR	12 000	
DETTES (4)	Emprunts obligataires convertibles		DS		
	Autres emprunts obligataires		DT		
	Emprunts et dettes auprès des établissements de crédit (5)		DU	151 917	190 942
	Emprunts et dettes financières divers (Dont emprunts participatifs	EI	DV		234 000
	Avances et acomptes reçus sur commandes en cours		DW		
	Dettes fournisseurs et comptes rattachés		DX	159 827	38 396
	Dettes fiscales et sociales		DY	226 607	85 536
	Dettes sur immobilisations et comptes rattachés		DZ		
	Autres dettes		EA	12 161	13 946
Compte régul.	Produits constatés d'avance (4)		EB		
	TOTAL (IV)		EC	550 513	562 820
	Ecarts de conversion passif * **(V)**		ED		
	TOTAL GÉNÉRAL (I à V)		EE	1 520 547	580 466

RENVOIS					
(1)	Écart de réévaluation incorporé au capital		1B		
(2)	Dont	Réserve spéciale de réévaluation (1959)	1C		
		Écart de réévaluation libre	1D		
		Réserve de réévaluation (1976)	1E		
(3)	Dont réserve spéciale des plus-values à long terme *		EF		
(4)	Dettes et produits constatés d'avance à moins d'un an		EG	461 087	
(5)	Dont concours bancaires courants, et soldes créditeurs de banques et CCP		EH	7	18 085

* Des explications concernant cette rubrique sont données dans la notice n° 2032.

SAGE Experts-comptables janvier 2009

17.1.2. Compte de résultat

AGREMENT DGFIP C5109.10009

Formulaire obligatoire (article 53 A du Code général des impôts)

3

COMPTE DE RÉSULTAT DE L'EXERCICE (En liste)

DGFiP N°2052 2009

Désignation de l'entreprise : MOBILEGOV FRANCE — Néant ☐*

EXEMPLAIRE A CONSERVER PAR LE DÉCLARANT

			Exercice N				Exercice (N-1)
			France	Exportations et livraisons intracommunautaires		Total	
PRODUITS D'EXPLOITATION	Ventes de marchandises*	FA		FB	FC		
	Production vendue biens*	FD	6 648	FE	FF	6 648	709
	Production vendue services*	FG	29 995	FH	FI	488 701	143 915
	Chiffres d'affaires nets*	FJ	36 643	FK	FL	495 349	144 624
	Production stockée*				FM		
	Production immobilisée*				FN	158 091	125 037
	Subventions d'exploitation				FO	210 703	30 600
	Reprises sur amortissements et provisions, transferts de charges* (9)				FP		
	Autres produits (1) (11)				FQ	6 182	339
	Total des produits d'exploitation (2) (I)				FR	870 325	300 600
CHARGES D'EXPLOITATION	Achats de marchandises (y compris droits de douane)*				FS		
	Variation de stock (marchandises)*				FT		
	Achats de matières premières et autres approvisionnements (y compris droits de douane)*				FU	2 591	10 215
	Variation de stock (matières premières et approvisionnements)*				FV	5 257	(9 481)
	Autres achats et charges externes (3) (6 bis)*				FW	1 137 911	162 774
	Impôts, taxes et versements assimilés*				FX	16 761	3 962
	Salaires et traitements*				FY	759 726	286 745
	Charges sociales (10)				FZ	216 278	92 655
	DOTATIONS D'EXPLOITATION — Sur immobilisations - dotations aux amortissements*				GA	31 815	15 562
	DOTATIONS D'EXPLOITATION — Sur immobilisations - dotations aux provisions				GB		
	DOTATIONS D'EXPLOITATION — Sur actif circulant : dotations aux provisions *				GC	15 500	
	DOTATIONS D'EXPLOITATION — Pour risques et charges : dotations aux provisions				GD		
	Autres charges (12)				GE	1 907	2 533
	Total des charges d'exploitation (4) (II)				GF	2 187 745	564 967
1 - RÉSULTAT D'EXPLOITATION (I - II)					GG	(1 317 421)	(264 366)
opérations en commun	Bénéfice attribué ou perte transférée* (III)				GH		
	Perte supportée ou bénéfice transféré* (IV)				GI		
PRODUITS FINANCIERS	Produits financiers de participations (5)				GJ		
	Produits des autres valeurs mobilières et créances de l'actif immobilisé (5)				GK		
	Autres intérêts et produits assimilés (5)				GL	1 313	
	Reprises sur provisions et transferts de charges				GM		
	Différences positives de change				GN	152	86
	Produits nets sur cessions de valeurs mobilières de placement				GO	5 531	
	Total des produits financiers (V)				GP	6 995	86
CHARGES FINANCIERES	Dotations financières aux amortissements et provisions*				GQ	12 000	
	Intérêts et charges assimilées (6)				GR	3 472	2 353
	Différences négatives de change				GS	152	19
	Charges nettes sur cessions de valeurs mobilières de placement				GT		
	Total des charges financières (VI)				GU	15 624	2 372
2 - RÉSULTAT FINANCIER (V - VI)					GV	(8 629)	(2 286)
3 - RÉSULTAT COURANT AVANT IMPÔTS (I - II + III - IV + V - VI)					GW	(1 326 049)	(266 653)

(RENVOIS : voir tableau n° 2053) * Des explications concernant cette rubrique sont données dans la notice n° 2032.

SAGE Experts-comptables janvier 2009

AGREMENT DGFIP C5109.10009

4 COMPTE DE RÉSULTAT DE L'EXERCICE (Suite)

DGFiP N°2053 2009

Formulaire obligatoire (article 53 A du Code général des impôts)

Désignation de l'entreprise MOBILEGOV FRANCE Néant ☐*

			Exercice N	Exercice N - 1
PRODUITS EXCEPTIONNELS	Produits exceptionnels sur opérations de gestion	HA		
	Produits exceptionnels sur opérations en capital *	HB	3 454	
	Reprises sur provisions et transferts de charges	HC		
	Total des produits exceptionnels (7) (VII)	HD	3 454	
CHARGES EXCEPTIONNELLES	Charges exceptionnelles sur opérations de gestion (6 bis)	HE	24 304	1 723
	Charges exceptionnelles sur opérations en capital *	HF	128 422	
	Dotations exceptionnelles aux amortissements et provisions	HG		
	Total des charges exceptionnelles (7) (VIII)	HH	152 725	1 723
4 - RÉSULTAT EXCEPTIONNEL (VII - VIII)		HI	(149 271)	(1 723)
Participation des salariés aux résultats de l'entreprise **(IX)**		HJ		
Impôts sur les bénéfices * **(X)**		HK	(292 164)	(89 293)
TOTAL DES PRODUITS (I + III + V + VII)		HL	880 774	300 686
TOTAL DES CHARGES (II + IV + VI + VIII + IX + X)		HM	2 063 931	479 769
5 - BÉNÉFICE OU PERTE (Total des produits - total des charges)		HN	(1 183 157)	(179 083)
RENVOIS (1)	Dont produits nets partiels sur opérations à long terme	HO		
(2) Dont	produits de locations immobilières	HY		
	produits d'exploitation afférents à des exercices antérieurs (à détailler au (8) ci-dessous)	1G		
(3) Dont	- Crédit-bail mobilier *	HP	2 234	
	- Crédit-bail immobilier	HQ		
(4)	Dont charges d'exploitation afférentes à des exercices antérieurs (à détailler au (8) ci-dessous)	1H		
(5)	Dont produits concernant les entreprises liées	1J		
(6)	Dont intérêts concernant les entreprises liées	1K		
(6bis)	Dont dons faits aux organismes d'intérêt général (art. 238 bis du C.G.I.)	HX		
(9)	Dont transferts de charges	A1		
(10)	Dont cotisations personnelles de l'exploitant (13)	A2		
(11)	Dont redevances pour concessions de brevets, de licences (produits)	A3		
(12)	Dont redevances pour concessions de brevets, de licences (charges)	A4	1 145	
(13)	Dont primes et cotisations complémentaires personnelles : facultatives A6		obligatoires A9		

(7) Détail des produits et charges exceptionnels (Si le nombre de lignes est insuffisant, reproduire le cadre (7) et le joindre en annexe) :	Exercice N Charges exceptionnelles	Exercice N Produits exceptionnels
PENALITE	304	
OSEO SUBVENTION	24 000	
VNC FRAIS RECHERCHE ET DEVELOPPEMENT	124 967	
REMBOURSEMENT DEPOT DE GARANTIE		3 454
VNC DEPOT GARANTIE	3 454	

(8) Détail des produits et charges sur exercices antérieurs :	Exercice N Charges antérieures	Exercice N Produits antérieurs

EXEMPLAIRE A CONSERVER PAR LE DÉCLARANT

SAGE Expert-s-comptables janvier 2009

* Des explications concernant cette rubrique sont données dans la notice n° 2032.

17.1.3. Annexes à la situation annuelle 2008

PREAMBULE

Les informations communiquées ci-après font partie intégrante des comptes annuels qui ont été établis le 1/12/2008 par le dirigeant.

1. REGLES ET METHODES COMPTABLES

Les conventions ci-après ont été appliquées dans le respect du principe de prudence, conformément aux règles de base suivantes :

- continuité de l'exploitation,
- permanence des méthodes comptables d'un exercice à l'autre,
- indépendance des exercices.

Les principales méthodes utilisées sont les suivantes :

- Amortissements de l'actif immobilisé : les biens susceptibles de subir une dépréciation sont amortis selon le mode linéaire ou dégressif sur la base de leur durée de vie économique.
- Stocks de matières premières : ils sont évalués au dernier prix d'achat connu.

Dans le cadre de la première application des nouvelles règles concernant les actifs, la méthode retenue pour cette première application est la méthode prospective dite simplifiée. Cette méthode s'applique à compter de l'exercice en cours. Le passé n'est pas remis en cause.

Les immobilisations corporelles sont évaluées à leur coût d'acquisition ou de production, compte tenu des frais nécessaires à la mise en état d'utilisation de ces biens, et après déduction des rabais commerciaux, remises, escomptes de règlements obtenus.

Les décisions suivantes ont été prises au niveau de la présentation des comptes annuels :

- immobilisations décomposables : l'entreprise n'a pas été en mesure de définir les immobilisations décomposables ou la décomposition de celles-ci ne présente pas d'impact significatif,
- immobilisations non décomposables : bénéficiant des mesures de tolérance, l'entreprise a opté pour le maintien des durées d'usage pour l'amortissement des biens non décomposés.
- Les frais de recherche et développement ont été activés et amortis sur 5 ans, ils représentent les salaires et charges du personnel affecté aux opérations de recherche & développement.

2. AUTRES ELEMENTS SIGNIFICATIFS DE L'EXERCICE

Le démarrage des ventes ne permettant pas de couvrir l'ensemble des charges d'exploitation, la continuité d'exploitation est assurée par les apports en compte courant des associés.

6. AUTRES INFORMATIONS

6.1 Rémunération des dirigeants

Cette information n'est pas mentionnée dans la présente Annexe, car elle conduirait indirectement à donner une rémunération individuelle.

17.2. Rapport général du commissaire aux comptes relatifs à l'exercice clos le 31 décembre 2008

Mesdames, Messieurs, les Actionnaires,

En exécution de la mission qui nous a été confiée par votre Assemblée Générale du 5 août 2006, nous vous présentons notre rapport relatif à l'exercice de 12 mois clos le 31 décembre 2008 sur :

- le contrôle des comptes annuels de la société MOBILEGOV S.A., tels qu'ils sont joints au présent rapport,
- la justification de nos appréciations,
- les vérifications spécifiques et les informations prévues par la loi.

Les comptes annuels ont été arrêtés par votre Conseil d'Administration. Il nous appartient, sur la base de notre audit, d'exprimer une opinion sur ces comptes.

1 - Opinion sur les comptes annuels

Nous avons effectué notre audit selon les normes d'exercice professionnel applicables en France: ces normes requièrent la mise en œuvre de diligences permettant d'obtenir l'assurance raisonnable que les comptes annuels ne comportent pas d'anomalies significatives.

Un audit consiste à vérifier, par sondages ou au moyen d'autres méthodes de sélection, les éléments justifiant des montants et informations figurant dans les comptes annuels. Il consiste également à apprécier les principes comptables suivis, les estimations significatives retenues et la présentation d'ensemble des comptes. Nous estimons que les éléments que nous avons collectés sont suffisants et appropriés pour fonder notre opinion.

Nous certifions que les comptes annuels sont, au regard des règles et principes comptables français, réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de la situation financière et du patrimoine de la société MOBILEGOV S.A. à la fin de cet exercice.

Sans remettre en cause l'opinion exprimée ci-dessus, nous attirons votre attention sur le point concernant les conditions dans lesquelles le principe de continuité d'exploitation a été apprécié, exposé dans la note « 2- Autres éléments significatifs de l'exercice » de l'annexe.

Il - Justification de nos appréciations

En application des dispositions de l'article L. 823-9 du Code de commerce relatives à la justification de nos appréciations, nous vous informons que les appréciations auxquelles nous avons procédé pour émettre l'opinion ci-dessus, portant notamment sur les principes comptables suivis et les estimations significatives retenues pour l'arrêté des comptes, ainsi que pour leur présentation d'ensemble, n'appellent pas d'autre commentaire que celui exprimé ci-dessus.

Les appréciations ainsi portées s'inscrivent dans le cadre de notre démarche d'audit des comptes annuels, pris dans leur ensemble, et ont donc contribué à la formation de notre opinion exprimée dans la première partie de ce rapport.

III - Vérifications et informations spécifiques

Nous avons également procédé aux vérifications spécifiques prévues par la loi.

A l'exception de l'incidence éventuelle des faits exposés ci-dessus, nous n'avons pas d'autres observations à formuler sur la sincérité et la concordance avec les comptes annuels des informations données dans le rapport de gestion du Conseil d'Administration et dans les documents adressés aux actionnaires sur la situation financière et les comptes annuels.

Fait à Sophia-Antipolis, le 14 septembre 2009

Le Commissaire aux comptes
Expertise & Audit International

Stephan BRUN

17.3. Dividendes

17.3.1. Montants des dividendes versés au cours des trois derniers exercices

Il est rappelé qu'au cours des exercices précédents, la Société n'a procédé à aucune distribution de dividendes.

17.3.2. Politique de distribution des dividendes

La politique future de distribution de dividendes sera déterminée en fonctions de plusieurs critères : les résultats de l'entreprise, le besoin et le niveau des investissements et l'endettement.

La politique de distribution de dividendes est fixée chaque année par l'assemblée générale des actionnaires, lors de l'assemblée générale d'approbation des comptes de l'exercice précédent, au vu, notamment, des résultats financiers et des besoins en investissement.

Chapitre
18

Chapitre 18: Informations complémentaires

18.1. Capital social

18.1.1. Montant du capital social

Le capital social de la Société s'élève à 518 859,96€ et est divisé en 841 619 actions**.**

18.1.2. Capital autorisé non émis par décisions de l'Assemblée Générale Extraordinaire du 30 juin 2009 :

➢ Première résolution

Délégation de compétence à l'effet de procéder, en une ou plusieurs fois, à l'émission d'actions ordinaires et de toutes valeurs mobilières donnant droit à l'attribution de titres de capital de la Société, avec maintien du droit préférentiel de souscription

L'Assemblée Générale, statuant aux conditions de quorum et de majorité requises pour les assemblées générales extraordinaires, après avoir entendu la lecture du rapport du Conseil d'Administration et du rapport spécial du Commissaire aux comptes, et constaté que le capital était entièrement libéré :

délègue au Conseil d'Administration, conformément aux dispositions de l'article L 225-129-2 du Code de commerce, avec effet au 23 janvier 2008, sa compétence en vue, sur ses seules délibérations :

(a) d'augmenter le capital, directement ou indirectement en une ou plusieurs fois, dans les proportions et aux époques qu'il appréciera, pour une durée de vingt-six (26) mois à compter de la présente assemblée, par l'émission, avec maintien du droit préférentiel de souscription des actionnaires, d'actions ou de valeurs mobilières donnant accès au capital de la Société, par émission sous la forme nominative ou au porteur, avec ou sans prime d'émission, dont la souscription pourra être opérée soit en numéraire, soit par compensation de créances, soit, en tout ou en partie, par incorporation de réserves, de bénéfices ou de primes ;

(b) de fixer les conditions d'émission et en particulier le prix de souscription ;

(c) de réaliser l'augmentation de capital et ;

(d) de procéder aux modifications corrélatives des statuts.

Le montant nominal maximal des augmentations de capital social susceptibles d'être réalisées immédiatement et/ou à terme en vertu de cette délégation de compétence, ne pourrait excéder 3.000.000 euros, étant précisé qu'à ce montant global s'ajouterait, le cas échéant, le montant nominal des actions supplémentaires à émettre pour préserver, conformément à la loi, les droits des porteurs de valeurs mobilières donnant droit à l'attribution de titres de la Société.

décide que le prix d'émission des actions ou valeurs mobilières donnant accès au capital de la Société sera fixé en fonction de la valeur d'entreprise de la Société, laquelle devra être déterminée par le Conseil d'Administration en fonction de plusieurs méthodes de valorisation, au nombre desquelles devront figurer, au minimum, la méthode de l'actualisation des flux de trésorerie et la méthode des comparables.

L'Assemblée Générale, **prend acte** de ce que l'émission de valeurs mobilières donnant accès au capital de la Société emporterait renonciation des actionnaires à leur droit préférentiel de souscription aux titres de capital auxquels ces titres ou valeurs mobilières pourraient donner droit.

La somme perçue ou susceptible d'être ultérieurement perçue par la Société pour chacune des actions ordinaires qui serait émise ou créée par souscription, conversion, échange, exercice de bons ou de toute autre manière compte tenu notamment du prix d'émission des valeurs mobilières primaires ou des bons, devrait être au moins égale à la valeur nominale des actions.

autorise et délègue, au Conseil d'Administration, la faculté d'instituer, le cas échéant, un droit de souscription à titre réductible, pour les actions ou valeurs mobilières nouvelles non souscrites à titre irréductible, qui serait attribué aux titulaires de droits de souscription qui auront souscrit un nombre de titres supérieur à celui qu'ils pouvaient souscrire à titre irréductible et ce, proportionnellement au nombre de leurs droits de souscription et dans la limite de leurs demandes.

délègue, en outre, au Conseil d'Administration, dans le cadre des augmentations de capital qui pourront être décidées par ce dernier, la possibilité d'augmenter le nombre de titres à émettre dans le cadre de la présente délégation, dans les trente jours de la clôture de la souscription pour faire face à d'éventuelles demandes supplémentaires de titres. Cette augmentation du nombre de titres à émettre ne pourra toutefois excéder 15 % de l'émission initiale. Les souscriptions complémentaires s'effectueront au même prix que les souscriptions initiales.

décide que le Conseil d'Administration aura tous pouvoirs pour mettre en œuvre, en une ou plusieurs fois, la présente délégation et, notamment, dans le respect des conditions qui viennent d'être arrêtées, pour :

(a) arrêter tous les termes et conditions des augmentations de capital ou émission d'autres valeurs mobilières réalisées en vertu de la présente délégation ;

(b) déterminer les dates et modalités des émissions ainsi que la forme et les caractéristiques des valeurs mobilières à créer, arrêter les prix et conditions des émissions, fixer les montants à émettre, fixer la date de jouissance, même rétroactive, des titres à émettre, déterminer le mode de libération des actions ou autres valeurs mobilières émises ;

(c) fixer les modalités suivant lesquelles sera assuré, le cas échéant, la préservation des droits des titulaires de valeurs mobilières donnant droit à l'attribution de titres de capital et ce, en conformité avec les dispositions légales et réglementaires ;

(d) clore par anticipation toute période de souscription dans les conditions légales et réglementaires en vigueur, procéder, dans les conditions légales et réglementaires en vigueur, à la réception, au dépôt puis au retrait des fonds reçus à l'appui des souscriptions, constater toute libération par compensation avec des créances liquides et exigibles détenues à l'encontre de la Société ;

(e) procéder, le cas échéant, à toutes imputations sur la ou les primes d'émission et, notamment, celles des frais, droits ou honoraires occasionnés par les émissions et prélever, le cas échéant, sur les montants des primes d'émission, les sommes nécessaires pour les affecter à la réserve légale, conformément à la réglementation applicable ;

(f) d'une manière générale, accomplir tous actes et formalités, prendre toutes décisions et conclure tous accords utiles et/ou nécessaires pour parvenir à la bonne fin des émissions réalisées en vertu de la présente délégation et, notamment, pour l'émission, la souscription, la livraison, la jouissance, la négociabilité et le service financier des valeurs mobilières émises, ainsi que l'exercice des droits qui y seront attachés.

Conformément aux dispositions de l'article L. 225-129-2, alinéa 2 du Code de commerce, la délégation de compétence consentie au titre de la présente résolution, prive d'effet, à compter du 30 juin 2009, toutes les délégations antérieures ayant le même objet et notamment, celle octroyée par l'Assemblée Générale Extraordinaire du 24 décembre 2007.

➢ **Deuxième résolution**

Délégation de pouvoirs à l'effet de procéder, en une ou plusieurs fois, à l'émission d'actions ordinaires et de toutes valeurs mobilières donnant droit à l'attribution de titres de capital de la Société, avec suppression du droit préférentiel de souscription

L'Assemblée Générale, statuant aux conditions de quorum et de majorité requises pour les assemblées générales extraordinaires, après avoir entendu la lecture du rapport du Conseil d'Administration et du Commissaire aux comptes, et constaté que le capital était entièrement libéré :

délègue, au Conseil d'Administration, conformément aux dispositions des articles L. 225-129-2, L. 225-135, L. 225-138 et 228-91 et suivant. du Code de commerce, avec effet au 30 juin 2009, sa compétence à l'effet de décider, en une ou plusieurs fois, dans les proportions et aux époques qu'il appréciera, pour une durée de dix-huit (18) mois à compter de la présente assemblée :

(a) d'augmenter le capital, directement ou indirectement, en une ou plusieurs fois, dans les proportions et aux époques qu'il appréciera, par l'émission, avec suppression du droit préférentiel de souscription des actionnaires, d'actions ou de valeurs mobilières donnant accès au capital de la Société, par émission sous la forme nominative ou au porteur, avec ou sans prime d'émission, dont la souscription pourra être opérée soit en numéraire, soit par compensation de créances, soit, en tout ou en partie, par incorporation de réserves, de bénéfices ou de primes ;

(b) de fixer les conditions d'émission et en particulier le prix de souscription, dans les conditions déterminées ci-après ;

(c) de réaliser l'augmentation de capital et ;

(d) de procéder aux modifications corrélatives des statuts.

Le montant nominal maximal des augmentations de capital social susceptibles d'être réalisées immédiatement et/ou à terme en vertu de cette délégation, ne pourrait excéder 3.000.000 euros, étant précisé :

- qu'à ce montant global s'ajouterait, le cas échéant, le montant nominal des actions supplémentaires à émettre pour préserver, conformément à la loi, les droits des porteurs de valeurs mobilières donnant droit à l'attribution de titres de la Société
- que ce plafond s'imputera sur le plafond maximum d'augmentation de capital fixé par la première résolution adoptée par la présente assemblée.

décide que le prix d'émission des actions ou valeurs mobilières donnant accès au capital de la Société sera fixé en fonction de la valeur d'entreprise de la Société, laquelle devra être déterminée par le Conseil d'Administration en fonction de plusieurs méthodes de valorisation, au nombre desquelles devront figurer, au minimum, la méthode de l'actualisation des flux de trésorerie et la méthode des comparables.

décide la suppression du droit préférentiel de souscription des actionnaires au profit des catégories de personnes déterminées ci-après et délègue au Conseil d'Administration toutes compétences à cet effet.

détermine les catégories de bénéficiaires de ces augmentations de capital de la manière suivante :

(a) première catégorie, les investisseurs institutionnels le service d'investissement de gestion de portefeuille pour compte de tiers ;

(b) deuxième catégorie, les Investisseurs Qualifiés, au sens de l'article L. 411-II 4° du Code Monétaire et Financier sous réserve que ces investisseurs agissent pour compte propre ;

(c) troisième catégorie, le cercle restreint d'investisseurs, sous réserve que ces investisseurs agissent pour compte propre.

Etant précisé que :

- un investisseur qualifié est une personne ou une entité disposant des compétences et des moyens nécessaires pour appréhender les risques inhérents aux opérations sur instruments financiers. La liste des catégories d'investisseurs reconnus comme qualifiés est fixée par décret.
- un cercle restreint d'investisseurs est composé de personnes, autres que des Investisseurs Qualifiés, liées aux dirigeants de l'émetteur par des relations personnelles, à caractère professionnel ou familial et dont le nombre est inférieur à un seuil fixé par décret.

délègue en conséquence au Conseil d'Administration le soin de fixer précisément la liste des bénéficiaires au sein de cette ou ces catégories et le nombre de titres à leur attribuer.

L'Assemblée Générale,

prend acte de ce que l'émission de valeurs mobilières donnant accès au capital emporterait renonciation des actionnaires à leur droit préférentiel de souscription aux titres de capital auxquels ces titres ou valeurs mobilières pourraient donner droit.

La somme perçue ou susceptible d'être ultérieurement perçue par la Société pour chacune des actions ordinaires qui serait émise ou créée par souscription, conversion, échange, exercice de bons ou de toute autre manière compte tenu notamment du prix d'émission des valeurs mobilières primaires ou des bons, devrait être au moins égale à la valeur nominale des actions.

délègue, en outre, au Conseil d'Administration, dans le cadre de cette délégation, la possibilité d'augmenter le nombre de titres à émettre dans le cadre des augmentations de capital décidées en vertu de la présente délégation, dans les trente jours de la clôture de la souscription pour faire face à d'éventuelles demandes supplémentaires de titres. Cette augmentation du nombre de titres à émettre ne pourra toutefois excéder 15 % de l'émission initiale. Les souscriptions complémentaires s'effectueront au même prix que les souscriptions initiales.

décide que le Conseil d'Administration aura tous pouvoirs pour mettre en œuvre, en une ou plusieurs fois, la présente délégation et, notamment, dans le respect des conditions qui viennent d'être arrêtées, pour :

(a) arrêter tous les termes et conditions des augmentations de capital ou émission d'autres valeurs mobilières réalisées en vertu de la présente délégation ;

(b) déterminer les dates et modalités des émissions ainsi que la forme et les caractéristiques des valeurs mobilières à créer, arrêter les prix et conditions des émissions, fixer les montants à émettre, fixer la date de jouissance, même rétroactive, des titres à émettre, déterminer le mode de libération des actions ou autres valeurs mobilières émises ;

(c) fixer les modalités suivant lesquelles sera assuré, le cas échéant, la préservation des droits des titulaires de valeurs mobilières donnant accès au capital de la Société et ce, en conformité avec les dispositions légales et réglementaires ;

(d) clore par anticipation toute période de souscription dans les conditions légales et réglementaires en vigueur, procéder, dans les conditions légales et réglementaires en vigueur, à la réception, au dépôt puis au retrait des fonds reçus à l'appui des souscriptions, constater toute libération par compensation avec des créances liquides et exigibles détenues à l'encontre de la Société ;

(e) procéder, le cas échéant, à toutes imputations sur la ou les primes d'émission et, notamment, celles des frais, droits ou honoraires occasionnés par les émissions et prélever, le cas échéant, sur les montants des primes d'émission, les sommes nécessaires pour les affecter à la réserve légale, conformément à la réglementation applicable ;

(f) d'une manière générale, accomplir tous actes et formalités, prendre toutes décisions et conclure tous accords utiles et/ou nécessaires pour parvenir à la bonne fin des émissions réalisées en vertu de la présente délégation et, notamment, pour l'émission, la souscription, la livraison, la jouissance, la négociabilité et le service financier des valeurs mobilières émises, ainsi que l'exercice des droits qui y seront attachés.

Conformément aux dispositions de l'article L. 225-129-2, alinéa 2 du Code de commerce, la délégation de compétence consentie au titre de la présente résolution, prive d'effet, à compter du 30 juin 2009, toutes les délégations antérieures ayant le même objet et notamment, celles octroyées par l'Assemblée Générale Extraordinaire du 24 décembre 2007.

➢Troisième résolution

Limitation globale du montant des émissions déléguées en vertu des résolutions précédentes

L'Assemblée Générale, statuant aux conditions de quorum et de majorité requises pour les assemblées générales extraordinaires, après avoir pris connaissance du rapport du conseil d'administration et du rapport du commissaire aux comptes, et en conséquence de l'adoption des résolutions qui précèdent, décide de fixer à 3.000.000 euros, ou sa contre-valeur, le montant maximum nominal global des émissions d'actions ou de valeurs mobilières donnant accès au capital de la Société qui pourront être réalisées en vertu des délégations octroyées aux termes des résolutions précédentes, étant précisé que (i) s'ajoutera, le cas échéant, à ce montant nominal, celui des actions supplémentaires qui seront émises pour préserver les droits des porteurs de ces titres donnant droit à des actions et que (ii) cette limite ne s'appliquera pas aux augmentations de capital par incorporation de primes, réserves ou autres.

➢Quatrième résolution

Délégation de pouvoirs à l'effet de procéder à l'augmentation du capital social par émission d'actions réservées aux salariés de la Société dans les conditions prévues par l'article L.443-5 du Code du travail en application de l'article L.225-129-6 du Code de commerce

L'Assemblée Générale, statuant aux conditions de quorum et de majorité requises pour les assemblées générales extraordinaires, après avoir pris connaissance du rapport du Conseil d'Administration et du rapport spécial du Commissaire aux comptes et en application des articles L. 225-129-6 et L. 443-5 du Code du travail,

délègue au Conseil d'Administration, avec effet au 30 juin 2009, au regard de l'ensemble des autorisations et décisions d'augmentations de capital données aux termes de la présente assemblée, tous pouvoirs à l'effet de décider d'augmenter le capital social de la Société dans les proportions et aux époques qu'il déterminera mais dans la limite de 10 % du montant de l'augmentation maximale de capital social de la Société de 3.000.000 euros décidée par le Conseil d'Administration et se rapportant aux résolutions ci-avant, au bénéfice des adhérents d'un plan d'épargne d'entreprise ou d'un plan partenariat d'épargne salariale volontaire mis en place ou pouvant être mis en place par la Société, dans les conditions déterminées par l'article L. 443-5 du Code du travail.

Le prix des actions émises sera égal au prix fixé par le Conseil d'Administration conformément aux dispositions des résolutions qui précèdent et ce, dans le respect des règles visées à l'article L. 443-5 du Code du travail.

L'Assemblée Générale,

prend acte de ce que la présente délégation emporte de plein droit renonciation des actionnaires à leur droit préférentiel de souscription aux actions auxquels donnent droit les bons susceptibles d'être émis en vertu de la présente délégation.

La libération des souscriptions pourra être opérée en espèces ou par compensation de créances, dans les délais qui seront déterminés par le Conseil d'Administration dans le respect des dispositions légales et réglementaires.

L'Assemblée Générale,

décide que le Conseil d'Administration disposera de tous pouvoirs pour la mise en œuvre de la présente délégation, à l'effet notamment d'établir, le cas échéant, tout document qui se révélerait nécessaire dans les délais requis, de fixer les dates et modalités de ladite émission, de fixer les prix de souscription et les conditions de l'émission, les montants de chaque émission, le cas échéant, la date de jouissance des titres éventuellement rétroactive, de déterminer le mode de libération des actions, de recueillir les souscriptions et les versements y afférents, de constater la ou les augmentations réalisées en application de la présente délégation, de procéder aux modifications corrélatives des statuts et, d'une façon plus générale, de fixer les conditions, de prendre toutes mesures et d'effectuer toutes formalités utiles à l'émission des actions nouvelles.

Le Conseil d'Administration pourra procéder, le cas échéant, à toutes imputations sur les primes d'émission des frais occasionnés par la réalisation de ces émissions.

Cette autorisation est conférée pour une durée de vingt-six mois à compter de la présente assemblée.

Le tableau ci-dessous synthétise l'ensemble des résolutions d'émission et/ou d'augmentation du capital prises par l'Assemblée Générale extraordinaire des actionnaires le 31 décembre 2007 et dont bénéficie la Société à la date du présent Document d'Information.

Autorisations	Caractéristiques	Utilisation
Emission de titres de capital avec droit préférentiel de souscription	Plafond en nominal de 3.000.000 euros et autorisation pour une durée de 26 mois	Montant levé : 203 549€ au 12/11/2008
Emission de titres de capital sans droit préférentiel de souscription	Plafond en nominal de 3.000.000 euros et autorisation pour une durée de 18 mois	Montant levé :1 830 090€ au 13/10/2008
Emission de titres de capital réservés aux salariés	Plafond en nominal de 10 % du montant de l'augmentation maximale et autorisation pour une durée de 26 mois	3% en 2008

18.1.3. Actions de préférence

Néant.

18.1.4. Titres non représentatifs du capital

A la date du présent Document d'information, il n'existe aucun titre non représentatif du capital de la Société.

18.1.5. Evolution du capital social

Evolution générale du capital social depuis la création de la Société

Date de réalisation	Nature des opérations	Fonds levés	Cumul levées	Nombre d'actions créées	Nombre d'actions cumulées	Cours intro	Valeur nominale après op	Prime émission par action	Augmentation de capital	Prime émission	Compte Primes d'émission	Capital après opération
19/05/2004	Constitution	1 000,00	1 000,00	10	10	100,00	100,00	0,00	1 000,00	0,00	0,00	1 000,00
13/09/2005	Augmentation par incorporation d'une créance	10 000,00	11 000,00	100	110	100,00	100,00	0,00	10 000,00	0,00	0,00	11 000,00
23/02/2006	Augmentation par incorporation d'une créance	12 000,00	23 000,00	120	230	100,00	100,00	0,00	12 000,00	0,00	0,00	23 000,00
30/06/2006	Augmentation par incorporation d'une créance	9 000,00	32 000,00	90	320	100,00	100,00	0,00	9 000,00	0,00	0,00	32 000,00
13/07/2006	Augmentation par apport en numéraire	6 000,00	38 000,00	60	380	100,00	100,00	0,00	6 000,00	0,00	0,00	38 000,00
20/12/2007	Division du nominal des actions	0,00	38 000,00	379 620	380 000	0,00	0,00	0,00	0,00	0,00	0,00	38 000,00
24/12/2007	Augmentation par apport en numéraire	154 996,90	192 996,90	49 999	429 999	3,10	0,10	3,00	4 999,90	149 997,00	149 997,00	42 999,90
24/12/2007	Augmentation de capital par incorporation de la prime d'émission et élévation du nominal des actions	0,00	192 996,90		429 999		0,45		0,00		0,00	192 996,90
21/01/2008	Augmentation par apport en numéraire	89 996,10	282 993,00	29 031	459 030	3,10	0,10	3,00	2 903,10	87 093,00	87 093,00	195 900,00
21/01/2008	Augmentation de capital par incorporation de la prime d'émission et élévation du nominal des actions	0,00	282 993,00		459 030		0,62		0,00		0,00	282 993,00
27/03/2008	Entrée en bourse	1 165 670,66	1 448 663,66	192 038	651 068	6,07	0,62	5,45	118 391,85	1 047 278,81	1 047 278,81	401 384,85
13/10/2008	AK2	664 419,36	2 113 083,02	79 476	730 544	8,36	0,62	7,74	48 997,13	615 422,23	1 662 701,04	450 381,98
12/11/2008	Emission BSAR	203 459,00	2 316 542,02	203 459		1,00	1,00	0,00				
14/04/2009	AK3-T1	664 697,40	2 981 239,42	76 402	806 946	8,70	0,62	8,08	47 102,00	617 595,40	2 280 296,44	497 483,98
27/05/2009	AK3-T2	301 655,10	3 282 894,52	34 673	841 619	8,70	0,62	8,08	21 375,98	280 279,12	2 560 575,56	518 859,96

Aucune autre modification n'est intervenue depuis cette dernière date.

Actionnariat3

Actionnaires	Nombre d'actions	% capital
Mobilegov Ltd.	110 000	13%
Michel Frenkiel	110 000	13%
François Le Page	70 000	8%
Eric Mathieu	70 000	8%
Raymonde Frenkiel	20 000	2%
Valérie Podelski	16 129	2%
Alain Vauthier	9 677	1%
Claude Chesse	2 400	0%
Norbert Kajler	2 400	0%
Public	431 013	51%
Total	841 619	100,00%

18.2. Acte constitutif et statuts

18.2.1. Objet social

La Société continue d'avoir pour objet, en France et dans tous pays : Toute opération non interdite par la loi ou les règlements et notamment, la création de terminaux mobiles communicants, d'applications informatiques et de solutions d'authentification.

Et plus généralement, toutes opérations commerciales, prise ou mise en gérance du fonds, financières, mobilières ou immobilières, pouvant se rattacher directement ou indirectement à l'objet social ou susceptibles d'en faciliter l'extension ou le développement.

La société peut recourir, en tous lieux, à tous les actes ou opérations de quelque nature et importance qu'ils soient, dès lors qu'ils concourent ou peuvent concourir, facilitent ou peuvent faciliter la réalisation des activités visées à l'alinéa qui précède ou qu'ils permettent de sauvegarder, directement ou indirectement, les intérêts industriels, commerciaux ou financiers de la société ou des entreprises avec lesquelles elle est en relation d'affaires.

18.2.2. Exercice social

L'année sociale commence le 1er janvier et finit le 31 décembre.

[3] *A la date du présent Document d'information*

18.2.3. Dispositions statutaires ou autres relatives aux membres des organes d'administration et de direction

Article 15 - Conseil d'administration

1) Composition

La Société est administrée par un Conseil d'administration de trois membres au moins et de dix-huit au plus, sauf dérogation temporaire prévue en cas de fusion où il peut être porté à vingt-quatre.

Les administrateurs sont nommés ou renouvelés dans leurs fonctions par l'Assemblée Générale Ordinaire des actionnaires qui peut les révoquer à tout moment.

Toutefois, en cas de fusion ou de scission, la nomination des administrateurs peut être faite par l'Assemblée Générale Extraordinaire.

Les administrateurs peuvent être des personnes physiques ou des personnes morales. Les administrateurs personnes morales sont tenus lors de leur nomination de désigner un représentant permanent qui est soumis aux mêmes conditions et obligations et qui encourt les mêmes responsabilités civiles et pénales que s'il était administrateur en son nom propre, sans préjudice de la responsabilité solidaire de la personne morale qu'il représente. Ce mandat de représentant permanent lui est donné pour la durée de celui de la personne morale qu'il représente ; il doit être renouvelé à chaque renouvellement de mandat de celle-ci.

Lorsque la personne morale révoque son représentant, elle est tenue de notifier cette révocation à la Société, sans délai, par lettre recommandée et de désigner selon les mêmes modalités un nouveau représentant permanent ; il en est de même en cas de décès ou de démission du représentant permanent.

Un administrateur personne physique ne peut appartenir simultanément à plus de cinq Conseils d'administration ou Conseils de surveillance de Sociétés Anonymes ayant leur siège en France métropolitaine, sauf les exceptions prévues par la loi.

Tout administrateur personne physique qui lorsqu'il accède à nouveau mandat se trouve en infraction avec les dispositions de l'alinéa précédent, doit, dans les trois mois de sa nomination, se démettre de l'un de ses mandats. A défaut, il est réputé s'être démis de son nouveau mandat.

Un salarié de la Société ne peut être nommé administrateur que si son contrat de travail correspond à un emploi effectif. Le nombre des administrateurs liés à la Société par un contrat de travail ne peut dépasser le tiers des administrateurs en fonctions.

2) Cumul de mandats

Une personne physique ne peut exercer simultanément plus de cinq mandats d'administrateur ou de membre du Conseil de surveillance de Sociétés Anonymes ayant leur siège sur le territoire français.

Pour le calcul du nombre de mandats indiqué ci-dessus, ne sont pas pris en compte les mandats d'administrateur ou de membre du Conseil de surveillance exercés par cette personne dans les Sociétés contrôlées au sens de l'article L. 233-16 du Code de commerce, par la Société dont elle est administrateur.

Les mandats d'administrateur ou de membre du Conseil de surveillance de Sociétés dont les titres ne sont pas admis aux négociations sur un marché réglementé et contrôlées par une même Société ne comptent que pour un seul mandat, sous réserve que le nombre de mandats détenus à ce titre n'excède pas cinq.

Sans préjudice des dispositions ci-dessus et de celles de l'article 21 des présents statuts, une même personne physique ne peut exercer simultanément plus de cinq mandats de Directeur Général, de membre du Directoire, de Directeur Général unique, d'administrateur ou de membre du Conseil de surveillance de Sociétés Anonymes ayant leur siège sur le territoire français. Pour l'application de ces dispositions, l'exercice de la Direction Générale par un administrateur est décompté pour un seul mandat.

Tout administrateur personne physique qui, lorsqu'il accède à nouveau mandat, se trouve en infraction avec les dispositions de l'alinéa précédent, doit, dans les trois mois de sa nomination, se démettre de l'un de ses mandats. A défaut, il est réputé s'être démis de son nouveau mandat.

Un salarié de la Société ne peut être nommé administrateur que si son contrat de travail correspond à un emploi effectif. Le nombre des administrateurs liés à la Société par un contrat de travail ne peut dépasser le tiers des administrateurs en fonctions.

3) Limite d'âge - Durée des fonctions

Nul ne peut être nommé administrateur si, ayant dépassé l'âge de 70 ans, sa nomination a pour effet de porter à plus du tiers des membres du Conseil le nombre d'administrateurs ayant dépassé cet âge.

Le nombre des administrateurs ayant dépassé l'âge de 70 ans ne peut excéder le tiers des membres du Conseil d'administration. Si cette limite est atteinte, l'administrateur le plus âgé est réputé démissionnaire.

La durée des fonctions des administrateurs est de six années ; elle expire à l'issue de l'assemblée qui statue sur les comptes de l'exercice écoulé et tenue dans l'année au cours de laquelle expire leur mandat.

Les administrateurs sont toujours rééligibles.

4) Vacance de sièges - Cooptation

En cas de vacance par décès ou démission d'un ou plusieurs sièges d'administrateur, le Conseil d'administration peut, entre deux Assemblées Générales, procéder à des nominations à titre provisoire.

Toutefois, s'il ne reste plus qu'un seul ou que deux administrateurs en fonctions, celui-ci ou ceux-ci, ou à défaut le ou les Commissaires aux Comptes, doivent convoquer immédiatement l'Assemblée Générale Ordinaire des actionnaires à l'effet de compléter l'effectif du Conseil.

Les nominations provisoires effectuées par le Conseil d'administration sont soumises à la ratification de la plus prochaine Assemblée Générale Ordinaire. A défaut de ratification, les délibérations prises et les actes accomplis antérieurement par le Conseil n'en demeurent pas moins valables.

L'administrateur nommé en remplacement d'un autre ne demeure en fonctions que pendant le temps restant à courir du mandat de son prédécesseur.

Article 16 - Actions d'administrateurs

Chaque administrateur doit être propriétaire d'actions dont le nombre est fixé à l'article 7.

Si au jour de sa nomination un administrateur n'est pas propriétaire du nombre d'actions requis ou si en cours de mandat il cesse d'en être propriétaire, il est réputé démissionnaire d'office s'il n'a pas régularisé sa situation dans un délai de trois mois.

Article 17 - Président du Conseil d'administration

Le Conseil d'administration élit, parmi ses membres personnes physiques, un Président dont il fixe la durée des fonctions sans qu'elle puisse excéder la durée de son mandat d'administrateur.

Le Président ne doit pas être âgé de plus de 70 ans. S'il vient à dépasser cet âge, il est réputé démissionnaire d'office.

Le Président du Conseil d'administration organise et dirige les travaux du Conseil d'administration, dont il rend compte à l'Assemblée Générale. Il veille au bon fonctionnement des organes de la Société et s'assure, en particulier, que les administrateurs sont en mesure de remplir leur mission.

Selon décision du Conseil d'administration, il pourra également exercer les fonctions de Directeur Général de la Société.

18.2.4. Droits et obligations attachés aux actions (article 14 des statuts)

1) Chaque action donne droit, dans les bénéfices et l'actif social, à une part proportionnelle à la quotité du capital qu'elle représente et donne droit au vote et à la représentation dans les Assemblées Générales, dans les conditions légales fixées par la loi et les statuts.

Tout actionnaire a le droit d'être informé sur la marche de la Société et d'obtenir communication de certains documents sociaux aux époques et dans les conditions prévues par la loi et les statuts.

2) Les actionnaires ne supportent les pertes qu'à concurrence de leurs apports.

Sous réserve des dispositions légales et statutaires, aucune majorité ne peut leur imposer une augmentation de leurs engagements. Les droits et obligations attachés à l'action suivent le titre dans quelque main qu'il passe.

La possession d'une action comporte de plein droit adhésion aux décisions de l'Assemblée Générale et aux présents statuts. La cession comprend tous les dividendes échus et non payés et à échoir, ainsi éventuellement que la part dans les fonds de réserve, sauf dispositions contraires notifiées à la Société.

Les héritiers, créanciers, ayants droit ou autres représentants d'un actionnaire ne peuvent, sous quelque prétexte que ce soit, requérir l'apposition des scellés sur les biens et documents sociaux, demander le partage ou la licitation de ces biens, ni s'immiscer dans l'administration de la Société. Ils doivent, pour l'exercice de leurs droits, s'en rapporter aux inventaires sociaux et aux décisions de l'Assemblée Générale.

3) Chaque fois qu'il est nécessaire de posséder un certain nombre d'actions pour exercer un droit quelconque, en cas d'échange, de regroupement ou d'attribution de titres, ou lors d'une augmentation ou d'une réduction de capital, d'une fusion ou de toute autre opération, les actionnaires possédant un nombre d'actions inférieur à celui requis, ne peuvent exercer ces droits qu'à la condition de faire leur affaire personnelle de l'obtention du nombre d'actions requis.

18.2.5. Franchissements de seuils statutaires

Néant.

18.2.6. Forme des actions (article 11 des statuts)

1) Les actions sont nominatives ou au porteur, au choix de l'actionnaire.

2) Lorsque les actions sont nominatives, elles donnent lieu à une inscription en compte individuel dans les conditions et selon les modalités prévues par les dispositions législatives et réglementaires en vigueur.

Ces comptes individuels peuvent être des comptes « nominatifs purs » ou des comptes « nominatifs administrés » au choix de l'actionnaire.

18.2.7. Assemblées générales

Article 24 - Nature des Assemblées

Les décisions des actionnaires sont prises en Assemblée Générale.

Les Assemblées Générales Ordinaires sont celles qui sont appelées à prendre toutes décisions qui ne modifient pas les statuts.

Les Assemblées Générales Extraordinaires sont celles appelées à décider ou autoriser des modifications directes ou indirectes des statuts.

Les Assemblées Spéciales réunissent les titulaires d'actions d'une catégorie déterminée pour statuer sur une modification des droits des actions de cette catégorie.

Les délibérations des Assemblées Générales obligent tous les actionnaires, même absents, dissidents ou incapables.

Article 25 - Convocation et réunion des Assemblées Générales

Les Assemblées Générales sont convoquées soit par le Conseil d'administration ou, à défaut, par le ou les Commissaires aux Comptes, soit par un mandataire désigné par le Président du Tribunal de commerce statuant en référé à la demande d'un ou plusieurs actionnaires réunissant le dixième au moins du capital.

Pendant la période de liquidation, les Assemblées sont convoquées par le ou les liquidateurs.

Les Assemblées Générales sont réunies au siège social ou en tout autre lieu indiqué dans l'avis de convocation.

La convocation est faite quinze jours avant la date de l'assemblée soit par lettre simple ou recommandée adressée à chaque actionnaire, soit par un avis inséré dans un Journal d'annonces légales du département du siège social. En cas de convocation par insertion, chaque actionnaire doit également être convoqué par lettre simple ou, sur sa demande et à ses frais, par lettre recommandée.

Lorsqu'une Assemblée n'a pu régulièrement délibérer, faute de réunir le quorum requis, la deuxième Assemblée et, le cas échéant, la deuxième Assemblée prorogée, sont convoquées dans les mêmes formes que la première et l'avis de convocation rappelle la date de la première et reproduit son ordre du jour.

Article 26 - Ordre du jour

1) L'ordre du jour des Assemblées est arrêté par l'auteur de la convocation.

2) Un ou plusieurs actionnaires, représentant au moins la quotité du capital social requise et agissant dans les conditions et délais fixés par la loi, ont la faculté de requérir, par lettre recommandée avec demande d'avis de réception, l'inscription à l'ordre du jour de l'Assemblée de projets de résolutions.

3) L'Assemblée ne peut délibérer sur une question qui n'est pas inscrite à l'ordre du jour, lequel ne peut être modifié sur deuxième convocation. Elle peut toutefois, en toutes circonstances, révoquer un ou plusieurs administrateurs et procéder à leur remplacement.

Article 27 - Admission aux Assemblées - Pouvoirs

1) Tout actionnaire a le droit de participer aux Assemblées Générales et aux délibérations personnellement ou par mandataire, quel que soit le nombre de ses actions, sur simple justification de son identité, dès lors que ses titres sont libérés des versements exigibles et inscrits en compte à son nom depuis cinq jours au moins avant la date de la réunion.

2) Tout actionnaire peut voter par correspondance au moyen d'un formulaire dont il peut obtenir l'envoi dans les conditions indiquées par l'avis de convocation à l'Assemblée.

3) Un actionnaire ne peut se faire représenter que par son conjoint ou par un autre actionnaire en justifiant d'un mandat.

Article 28 - Tenue de l'Assemblée - Bureau - Procès-verbaux

1) Une feuille de présence est émargée par les actionnaires présents et les mandataires et à laquelle sont annexés les pouvoirs donnés à chaque mandataire et, le cas échéant, les formulaires de vote par correspondance. Elle est certifiée exacte par le bureau de l'Assemblée.

2) Les Assemblées sont présidées par le Président du Conseil d'administration ou, en son absence, par un administrateur spécialement délégué à cet effet par le Conseil.

En cas de convocation par un Commissaire aux Comptes ou par mandataire de justice, l'Assemblée est présidée par l'auteur de la convocation. A défaut, l'Assemblée élit elle-même son Président.

Les deux actionnaires, présents et acceptants, représentant, tant par eux-mêmes que comme mandataires, le plus grand nombre de voix remplissent les fonctions de scrutateurs.

Le bureau ainsi constitué désigne un Secrétaire qui peut être choisi en dehors des membres de l'Assemblée.

3) Les délibérations des Assemblées sont constatées par des procès-verbaux signés par les membres du bureau et établis sur un registre spécial conformément à la loi. Les copies et extraits de ces procès-verbaux sont valablement certifiés dans les conditions fixées par la loi.

Article 29 - Vote – Droit de vote double

Le droit de vote attaché aux actions ordinaires est proportionnel à la quotité du capital qu'elles représentent et chaque action donne droit à une voix au moins.

Un droit de vote double de celui conféré aux autres actions, eu égard à la quotité du capital qu'elles représentent, est attribué à toutes les actions entièrement libérées pour lesquelles il est justifié d'une inscription nominative depuis deux ans au moins au nom du même actionnaire.

Ce droit est conféré également dès leur émission en cas d'augmentation du capital par incorporation de réserves, bénéfices ou primes d'émission, aux actions attribuées gratuitement à un actionnaire à raison d'actions anciennes pour lesquelles il bénéficie de ce droit.

Les votes s'expriment soit à main levée soit par appel nominal. Il ne peut être procédé à un scrutin secret dont l'assemblée fixera alors les modalités qu'à la demande de membres représentant, par eux-mêmes ou comme mandataires, la majorité requise pour le vote de la résolution en cause.

Dans certains cas, la loi prive du droit de vote des actionnaires, dont les titres ne sont alors pas pris en compte pour le calcul du quorum et de la majorité. Il en est ainsi notamment de l'apporteur en nature, du bénéficiaire d'un avantage particulier ou du droit de souscription lorsque l'assemblée délibère, selon le cas, sur l'approbation d'un apport en nature, l'octroi d'un avantage particulier ou la réservation du droit de souscription aux titres représentant une augmentation de capital.

Article 30 - Assemblée Générale Ordinaire

L'Assemblée Générale Ordinaire prend toutes décisions excédant les pouvoirs du Conseil d'administration et qui n'ont pas pour objet de modifier les statuts. L'Assemblée Générale Ordinaire est réunie au moins une fois l'an, dans les six mois de la clôture de l'exercice social, pour statuer sur les comptes et éventuellement les comptes consolidés de cet exercice, sous réserve de prolongation de ce délai par décision de justice.

Elle ne délibère valablement, sur première convocation, que si les actionnaires présents ou représentés, ou votant par correspondance, possèdent au moins le quart des actions ayant le droit de vote. Aucun quorum n'est requis sur deuxième convocation.

Elle statue à la majorité des voix dont disposent les actionnaires présents ou représentés ou votant par correspondance.

Article 31 - Assemblée Générale Extraordinaire

L'Assemblée Générale Extraordinaire peut modifier les statuts dans toutes leurs dispositions et décider notamment la transformation de la Société en Société d'une autre forme, civile ou commerciale. Elle ne peut toutefois augmenter les engagements des actionnaires, sous réserve des opérations résultant d'un regroupement d'actions régulièrement effectué.

L'Assemblée Générale Extraordinaire ne peut délibérer valablement que si les actionnaires présents ou représentés, ou votant par correspondance, possèdent au moins, sur première convocation, le tiers et, sur deuxième convocation, le quart des actions ayant le droit de vote. A défaut de ce dernier quorum, la deuxième Assemblée peut être prorogée à une date postérieure de deux mois au plus à celle à laquelle elle avait été convoquée.

L'Assemblée Générale Extraordinaire statue à la majorité des deux tiers des voix dont disposent les actionnaires présents ou représentés, ou votant par correspondance, sauf dérogation légale.

Dans les Assemblées Générales Extraordinaires à forme constitutive, c'est-à-dire celles appelées à délibérer sur l'approbation d'un apport en nature ou l'octroi d'un avantage particulier, l'apporteur ou le bénéficiaire n'a voix délibérative ni pour lui-même ni comme mandataire.

Article 32 - Assemblées Spéciales

S'il existe plusieurs catégories d'actions, aucune modification ne peut être faite aux droits des actions d'une de ces catégories, sans vote conforme d'une Assemblée Générale Extraordinaire ouverte à tous les actionnaires et, en outre, sans vote également conforme d'une Assemblée Spéciale ouverte aux seuls propriétaires des actions de la catégorie intéressée.

Les Assemblées Spéciales ne peuvent délibérer valablement que si les actionnaires présents ou représentés possèdent au moins, sur première convocation, la moitié et, sur deuxième convocation, le quart des actions de la catégorie concernée.

Pour le reste, elles sont convoquées et délibèrent dans les mêmes conditions que les Assemblées Générales Extraordinaires sous réserve des dispositions particulières applicables aux Assemblées de titulaires d'actions à dividende prioritaire sans droit de vote.

Article 33 - Droit de communication des actionnaires

Tout actionnaire a le droit d'obtenir, dans les conditions et aux époques fixées par la loi, communication des documents nécessaires pour lui permettre de se prononcer en connaissance de cause et de porter un jugement sur la gestion et le contrôle de la Société. La nature de ces documents et les conditions de leur envoi ou mise à disposition sont déterminées par la loi et les règlements.

Chapitre

19

Chapitre 19: Contrats importants

Le contrat dont la table des matières est reproduite ci-dessous constitue le fer de lance de la pénétration du marché mondial mis en place fin 2008 et l'une des bases du calcul du prévisionnel de l'entreprise. Il a été signé par 8 distributeurs exclusifs entre juillet 2009 et mars 2010 :

Exclusive Distribution Contract of Mobilegov Products and Services:

Chapitre

20

Chapitre 20: Informations provenant de tiers, déclarations d'experts et déclarations d'intérêts

Toutes les sources relatives aux tableaux, graphiques estimations et pourcentages figurant dans le présent Document d'information, notamment à la Section 7 sont clairement mentionnées.

La Société confirme que les informations visées ont été reproduites fidèlement. Pour autant que la Société le sache et soit en mesure de l'assurer à la lumière des données publiées par ces tierces parties, aucun fait n'a été omis qui rendrait les informations reproduites inexactes ou trompeuses.

On trouve en annexe divers documents qui confirment le bien-fondé du modèle proposé par Mobilegov.

Chapitre
21

Chapitre 21: Documents accessibles

L'ensemble des documents sociaux de la Société devant être mis à la disposition des actionnaires est consultable aux bureaux de la Société :

Adresse :	2000 route des Lucioles – 06901 Sophia-Antipolis
Téléphone :	+33 493 330 666
Fax :	+33 492 944 895
E-mail :	info@mobilegov.com
Site Internet :	www.mobilegov.com

Peuvent notamment être consultés :

(a) l'acte constitutif et les statuts de la Société ;

(b) tous rapports, courriers et autres documents, informations financières historiques, évaluations et déclarations établis par un expert à la demande de la Société, dont une partie est incluse dans le présent Document d'information ;

(c) les informations financières historiques de la Société pour chacun des exercices précédant la publication du Document d'information.

La Société entend communiquer ses résultats financiers conformément aux exigences des lois et réglementations en vigueur.

Chapitre
22

Chapitre 22: Annexes

Les articles et brochures suivants sont reproduits en annexe :

BankInfoSecurity.com 18/12/09 : Heartland Pays $3.6 Million to American Express

First Settlement to Result from Landmark Data Breach

La Tribune 14/11/09 : Mobilegov sécurise les matériels informatiques et les fichiers

En matière de sécurité informatique, le couple « identifiant-mot de passe est dépassé.

PC World 10/03/09 : Forte hausse du cyber-squatting et du phishing

En parallèle de la montée du spam, nous assistons à une montée inquiétante du cyber-squatting et du phishing, d'après le rapport du cabinet MarkMonitor. Il s'agit de pratiques dangereuses pour les utilisateurs et ennuyeuses pour les enseignes.

Le Monde Informatique 8/1/09 : Explosion des pertes de données individuelles aux Etats-Unis

En 2008, bien plus de 35 millions d'Américains ont été indirectement victimes de la perte d'informations personnelles les concernant. Le secteur privé est le principal responsable de la hausse de 47% des pertes de fichiers enregistrés.

The New York Times 9/12/08 : Licence plates may be coming to cyberspace

Un panel d'experts recommande que le gouvernement cesse de faire confiance aux mots de passe et adopte l'authentification forte.

Silicon 28/10/08 : La crise boursière fait-elle augmenter la cybercriminalité ?

PandaLabs va jusqu'à affirmer que les récents pics d'attaques pourraient être mis en relation avec le fait que les cybercriminels disposent de moins de cibles bancaires en raison de la concentration des établissements financiers (depuis le début de la crise, les rapprochements se sont multipliés).

Silicon 07/11/08 : Un ancien d'Intel vole pour 1 milliard de dollars de données

Biswamohan Pani, ingénieur de son état a eu l'idée de télécharger illégalement plus d'une douzaine de fichiers confidentiels de la société Intel pour laquelle il travaillait juste avant son départ chez AMD...

SKY NEWS 04/09/2008 : NHS Could Be Next Data Loss Fiasco

Après plusieurs fuites de données personnelles en 2007 et 2008, NHS est à nouveau dans le collimateur, accusé d'utiliser des supports de stockage peu sûrs.

La Voix du Nord 02/09/08 : Jusqu'à 32 gigaoctets de mémoire dans la poche: les clefs du succès

Ces derniers mois, les performances des clefs USB ont tellement progressé qu'elles ouvrent de nouvelles perspectives : pourquoi encombrer son portable d'un lecteurgraveur, voire pourquoi s'encombrer d'un portable ?

Boursorama 07/08/08 : Le piratage de données bancaires sur Internet dépasse l'imagination

Onze personnes inculpées et accusées d'avoir volé des millions de numéros de cartes bancaires

Telegraph 21/05/08 : NHS disc containing sensitive data lost

Un disque contenant les données de 38.000 patients égaré.

BANK INFO SECURITY®

Heartland Pays $3.6 Million to American Express

First Settlement to Result from Landmark Data Breach

Linda McGlasson, Managing Editor
December 18, 2009

Heartland Payment Systems will pay $3.6 million to American Express to settle charges relating to **Heartland's landmark data breach**.

The payment, Heartland says in a press release announcing the settlement, resolves "all intrusion-related issues between the two parties" regarding the breach of an estimated 130 million credit and debit cards.

"We are pleased to have reached an equitable settlement with American Express," says Bob Carr, Heartland's chairman and chief executive officer. "This settlement marks the first agreement with a card brand related to the intrusion."

The U.S. Department of Justice has charged **Albert Gonzalez** and other accomplices with the Heartland attack, and says that it was only one of several other companies that Gonzalez and the other hackers targeted with SQL injection attacks.

The other companies hacked include 7-Eleven and Hannaford Brothers. Credit card companies, including American Express, Visa and MasterCard, were forced to cancel and reissue credit cards because of the Heartland data breach. Banks and credit unions have also sued the payments processor to recoup the costs of reissuing cards and to cover the cost of fraud that resulted from the breach.

Earlier this year, Heartland said it had put aside more than $12 million to cover the charges related to the breach. Heartland is expected to be fined by other brands, including Visa and MasterCard.

LA TRIBUNE

Business-Techno
Mobilegov sécurise les matériels informatiques et les fichie...

261 mots
14 novembre 2009
La Tribune
TRDS
8
Français

Mobilegov sécurise les matériels informatiques et les fichiers

En matière de sécurité informatique, le couple « identifiant-mot de passe » est dépassé. Les développeurs élaborent des stratégies plus complexes pour sécuriser davantage les données et les ordinateurs. Ce que les professionnels appellent l'authentification forte. **Mobilegov**, un éditeur français de logiciels créé en 2004, a eu l'idée simple mais efficace d'utiliser les numéros de série des composants matériels (PC, clé, téléphone) pour sécuriser les accès informatiques. Ce que le fondateur de **Mobilegov**, Michel Frenkiel, appelle joliment « l'ADN du numérique ». En pratique, cette technologie logicielle permet à un ordinateur de n'accepter que les clés USB enregistrées au préalable. Un PC peut aussi être verrouillé et ne fonctionner qu'avec une clé unique. « Nos solutions sont adaptées aux problématiques des entreprises qui ont besoin de sécuriser des centaines de postes informatiques », observe Michel Frenkiel. **Mobilegov** affiche quelques belles références dans le secteur public, qui constitue 60 % de son activité : le Home Office (ministère de l'Intérieur) britannique, la chancellerie autrichienne. L'entreprise va plus loin dans cette démarche : la sécurisation de fichiers. « Notre nouvelle application garantit qu'un fichier téléchargé sur Internet (texte, image, vidéo) ne pourra être exploité que sur les équipements (PC, téléphone) utilisés pour le télécharger », explique-t-il. À l'heure de la loi Hadopi contre le téléchargement illégal d'œuvres culturelles, cette innovation pourrait séduire. L. P.

l'idée est simple : utiliser les numéros de série des composants matériels pour sécuriser les accès informatiques.

3076014

Forte hausse du cyber-squatting et du phishing

Publié le 10 mars 2009 , par Ludovic DUPUY - dans Internet - Mots clés : Phishing, Cyber-squatting

Il y a une très forte augmentation du cyber-squatting et du phishing...

En parallèle de la montée du spam, nous assistons à une montée inquiétante du cyber-squatting et du phishing, d'après le rapport du cabinet MarkMonitor. Il s'agit de pratiques dangereuses pour les utilisateurs et ennuyeuses pour les enseignes.

Le phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité ; pour cela les fraudeurs ont généralement recours à l'envoi d'e-mails invitant les utilisateurs à se connecter et rentrer leurs identifiants sur de faux sites bancaires afin de leur soutirer des renseignements personnels.

Quant à lui, le cyber-squatting consiste à analyser les fautes potentielles que l'utilisateur pourrait commettre en tapant l'adresse Internet d'une société importante, pour ensuite réserver ces noms de domaines et prendre une part d'audience.

Ce dernier aurait ainsi connu une hausse de 18% au cours de l'année dernière avec 1 722 133 cas répertoriés, et les membres qui en sont à l'origine seraient aussi ceux qui propageraient des attaques de phishing. Les sites frauduleux seraient principalement hébergés aux États-Unis, au Royaume-Uni et en Allemagne.

Celui-ci aurait enregistré une hausse de 122% contre les services de paiement en ligne (Paypal, etc.) et de 51% contre les instituts financiers (banques). Il aurait aussi connu une hausse générale de 66% en 2008, avec 136 426 attaques perpétrées, selon le cabinet RSA Anti-Fraud.

LeMondeInformatique.fr

Explosion des pertes de données individuelles aux Etats-Unis

Edition du 08/01/2009 - par François Lambel

En 2008, bien plus de 35 millions d'Américains ont été indirectement victimes de la perte d'informations personnelles les concernant. Le secteur privé est le principal responsable de la hausse de 47% des pertes de fichiers enregistrés.

Aux Etats-Unis, 656 pertes de fichiers contenant des informations personnelles ont été répertoriées en 2008, selon l'Identity Theft Resource Center (ITRC). Ce type de dommages a augmenté de 47% par rapport à l'an dernier, selon cette association soutenue par le ministère américain de la Justice et qui regroupe divers organismes américains à but non lucratif. Dans près de 83% des cas, il s'agit de fichiers informatiques. Les 17% restants concernent des documents papier.
Bien qu'en baisse par rapport à l'an dernier, la principale cause à l'origine de ces pertes demeure les erreurs des détenteurs (35,2%). Viennent ensuite, dans 30% des cas, les actes malfaisants (attaques de système, piratage et vol par le personnel). Par rapport à 2007, l'ITRC constate un doublement des vols par des salariés des entreprises victimes. Ces actes sont désormais à l'origine de 16% des cas de pertes annoncés.
Précisons que le recensement de l'ITRC n'est rendu possible que par l'obligation légale qu'ont les entreprises américaines de déclarer leurs pertes de données. Il est impossible d'établir ce type de statistiques en France faute d'une telle législation qui contribuerait pourtant à traduire dans la réalité le souci affiché de renforcer la "confiance dans l'économie numérique".

Le secteur privé, champion des pertes de données

L'ampleur du phénomène est pourtant alarmante. Aux Etats-Unis, ce sont les données personnelles (identité, informations financières...) de plus de 35 millions d'individus qui se sont retrouvées dans la nature. Toutefois, ce chiffre est bien en deçà de la réalité, puisque l'ITRC n'a été en mesure de ne connaître le nombre de personnes concernées que dans moins d'un cas sur deux. Sans parler des pertes de fichiers qui n'ont pas été identifiées...
L'analyse sectorielle des données de l'ITRC montre que, sur trois ans, le secteur privé n'a fait aucun progrès dans la protection des données personnelles, bien au contraire. En 2008, 36% des pertes ont été déclarées par des entreprises. En 2006, ce n'était que 21%. Même triste constat pour les institutions financières. Alors que leurs pertes de données ne représentaient que 8% du total en 2006, elles atteignent désormais 12%. A l'inverse, les pertes subies par le secteur public et celui de l'éducation sont passées de 30% à moins de 17%.

En savoir plus:
Le rapport complet de l'Identity Theft Resource Center sur les fuits de données répertoriées en 2008 (PDF de 201 pages, 1,5 Mo).

The New York Times
nytimes.com

December 9, 2008

Panel Presses to Bolster Security in Cyberspace

By JOHN MARKOFF

SAN FRANCISCO — License plates may be coming to cyberspace.

A government and technology industry panel on cyber-security is recommending that the federal government end its reliance on passwords and enforce what the industry describes as "strong authentication."

Such an approach would probably mean that all government computer users would have to hold a device to gain access to a network computer or online service. The commission is also encouraging all nongovernmental commercial services use such a device.

"We need to move away from passwords," said Tom Kellermann, vice president for security awareness at Core Security Technologies and a member of the commission that created the report.

The report, which offers guidance to the Obama administration, is a strong indictment of government and private industry efforts to secure cyberspace to date. "The laissez-faire approach to cyber-security has failed," Mr. Kellermann said.

Restricting Internet access is one of a series of recommendations that a group of more than 60 government and business computer security specialists will make in a public presentation, "Securing Cyberspace in the 44th Presidency," on Monday.

The report has been prepared during the last 18 months under the auspices of the Center for Strategic and International Studies, a Washington policy group, after a number of break-ins into government computer systems.

"The damage from cyber attack is real," the report states. "Last year, the Departments of Defense, State, Homeland Security, and Commerce, NASA and the National Defense University all suffered major intrusions by unknown foreign entities."

The report describes a laundry list of serious break-ins ranging from the hacking of the secretary of Defense's unclassified e-mail to the loss of "terabytes" of data at the State Department.

The group recommends the creation of a White House cyber-security czar reporting to the president and the consolidation of the powers that have largely been held by the Homeland Security Department under the Bush administration. The report argues that cyber-security is one of the most significant national security threats and that it can no longer be relegated to information technology offices and chief information officers.

The commission included the top Democrat and Republican members of the House Homeland Security subcommittee that oversees cyber-security. The chairmen of the commission included Jim Langevin, a Democratic congressman from Rhode Island; and Michael McCaul, a Republican congressman from Texas.

Scott Charney, corporate vice president for trustworthy computing at Microsoft; and Harry D. Raduege Jr.,

a retired Air Force lieutenant general who is chairman of the Center for Network Innovation at Deloitte & Touche, were also on the commission.

The report calls for new laws and regulations governing cyberspace.

“We believe that cyberspace cannot be secured without regulation,” the report said. The proposed regulations included new standards for critical infrastructure providers like the finance and energy industries, as well as new federal product acquisition rules to force more secure products.

The report does not entirely reject the work of the Bush administration. It cites the creation of the Comprehensive National Cybersecurity Initiative, adopted by the government as part of a presidential memorandum issued last January as a good starting point for remaking the nation’s cyber-security strategy.

That effort has led to a commitment by the federal government to spend more than $30 billion in the next seven years to enhance computing security.

La crise boursière fait-elle augmenter la cybercriminalité ?

28-10-2008

Par Olivier Robillart

Tous aux abris, semble annoncer l'éditeur Panda Security. Moins de banques favoriserait la concentration des attaques par les hackers

Les chercheurs de PandaLabs ont parfois des idées originales derrière la tête. Le laboratoire d'analyse et détection des *malwares* de Panda Security révèle qu'une **relation directe** existe **entre la volatilité actuelle des marchés boursiers et l'essor des nouvelles menaces.**

PandaLabs va jusqu'à affirmer que les récents pics d'attaques pourraient être mis en relation avec le fait que les cybercriminels disposent de moins de cibles bancaires en raison de la **concentration des établissements financiers (depuis le début de la crise, les rapprochements se sont multipliés).**

La cause serait qu'avec l'incertitude des marchés financiers, les banques représentent des **cibles moins attractives pour les pirates**. Cette situation a occasionné une hausse des autres types de *malwares*, tels que les *adwares* (logiciels de publicités malveillantes).

Panda témoigne de ses découvertes : "*en moyenne, le marché des valeurs américaines a connu une baisse de 3 à 7% entre le 1er septembre et le 9 octobre.* ***L'activité des pirates a connu une évolution inverse*** *: lorsque la bourse a chuté, les* malwares *se sont développés*. De même, *entre le 5 et le 16 septembre, les indices Dow Jones, NASDAQ, S&P 500 et Composite ont tous chuté. Au même moment, nous avons observé une* ***multiplication du nombre de malwares*** *apparaissant chaque jour*". Etc…

Une tendance que confirme l'éditeur G DATA. La société relève une sensible augmentation de certains formes de spams axés sur les offres de crédit venant parfois d'endroits peu exotiques comme l'Ukraine. Les objectifs des criminels semblent alors multiples et vont des arnaques pour le rachat de crédits, au vol de données personnelles via du *phishing* et des logiciels malveillants...

Il semblerait donc que pendant la crise financière, les **spammeurs, voleurs de données** et autres fournisseurs de crédit louches en profitent pour développer leurs activités et pourquoi pas écouler leurs fonds.

Donc un conseil, même en période de vache maigre, évitez de faire confiance lorsqu'il est annoncé : "*Objet :* ***jusqu'à 50.000 € de crédit*** *- sans dossier de crédit - de l'Ukraine*". Même si certains l'aiment chaud, éviter le vol n'a jamais nécessité plus de 7 secondes de réflexion.

Un ancien d'Intel vole pour 1 milliard de dollars de données

07-11-2008

Par Olivier Robillart

Son argument de défense, l'ingénieur voulait progresser plus vite dans la hiérarchie. Raté

Biswamohan Pani, ingénieur de son état a eu l'idée de télécharger illégalement **plus d'une douzaine de fichiers confidentiels** de la société Intel pour laquelle il travaillait juste avant son départ chez AMD...

Sauf que Intel eut la puce à l'oreille en remarquant que Pani **profitait de ses derniers jours de congé pour venir au bureau. Pris la main dans le sac avec des documents sensibles, l'homme de 33 ans risque gros.**

La Cour fédérale du Massachusetts a indiqué qu'il risquait jusqu'à **10 années de prison pour vol de données classées secrètes et 20 s'il est convaincu de fraude.**

Les autorités estiment ces données à **1 milliard de dollars, elles concernent** les coûts de développement, la recherche et les méthodes d'élaboration des microprocesseurs.

Face à ses accusateurs, l'ingénieur s'est défendu en précisant que ces informations étaient destinées à sa femme qui travaillait aussi à Intel. AMD de son côté a immédiatement chercher à éviter toute accusation d'espionnage. : "*AMD n'est pas accusé d'avoir mal agi. Le FBI a d'ailleurs statué qu'il n'existait* ***aucune preuve d'une quelconque implication de l'entreprise dans les actes de M. Pani*****",** affirme-t-elle dans un communiqué.

Ce cas pratique est une illustration parfaite de l'importance des fuites de données internes. KPMG, cabinet français d'audit et de conseil, établissait voilà quelques semaines un baromètre de ces menaces en montrant que **85% de ces employés malhonnêtes sont des hommes et 49% appartiennent au *Senior Management*.** Chose peu surprenante, leurs motivations sont pour 47% d'entre eux l'amélioration de leurs conditions financières, de leur **pouvoir**, voire de leur **influence**.

Un risque énorme d'autant que le coût de ces fuites est établi à **13 millions d´euros dans les seules banques britanniques** au cours de ces douze derniers mois. Avec 1 milliard de dollars, Biswamohan Pani, l'ex-ingénieur d'Intel et d'AMD passe donc pour un " Kerviel " de l'informatique en somme.

L'armée américaine assaillie par… un ver

20-11-2008

Par Olivier Robillart

Le département de la Défense des Etats-Unis a reconnu être la cible d'un ver informatique. Du coup, il vient d'interdire l'utilisation des disques durs externes et autres clés USB dans ses services

Disques externes, clés USB, mais aussi CD et autres supports amovibles sont désormais prohibés chez les militaires américains. La cause de ce bannissement est un simple ver (worm) baptisé ***Agent.btz*****, une variante du ver *SillyFDC*** qui a la particularité de se propager automatiquement dans tous les supports amovibles. Lorsqu'il est alors reconnecté, **le matériel vient contaminer le nouvel ordinateur.**

Cette interdiction a été décidée par le commandant de la division stratégique du Pentagone. Il comprend, à en croire le site wired.com les fichiers classés secrets **SIPR** et ceux non-classifiés **NIPR**. Une mesure qui ne comprendrait que quelques inconvénients dans la plupart des sociétés mais qui revêtent une dimension particulière dans ce cas.

Les services américains préfèrent **considérer les réseaux comme "hors de confiance"**, ils utilisent alors régulièrement des supports amovibles pour sauvegarder leurs données. Un usage appelé à cesser selon les responsables : "*toute utilisation de matériel de stockage est désormais interdit jusqu'à ce qu'il soit* ***analysé et approuvé comme étant libre de tout malware***". Les équipes de sécurité du gouvernement promettent donc de vérifier quotidiennement l'état de l'éventuel reflux du ver dans ses systèmes.

Un type d'attaque qui montre combien certaines **grandes structures sont vulnérables aux malwares**. Carlos Solari, le Monsieur sécurité de la Maison-Blanche entre 2002 et 2005, nous révélait qu'il en était souvent ainsi. Il nous expliquait qu'il y a encore peu de temps : ***"toute l'infrastructure informatique avait été négligée*** *et même reléguée à des rangs et intérêts inférieurs. Nous avions les personnes et les compétences, restait à les organiser entre elles et à leur donnée une ligne de conduite*". C'est désormais chose faite, l'armée américaine nettoie ses virus à la main.

SKY NEWS

NHS Could Be Next Data Loss Fiasco

11:53am UK, Thursday September 04, 2008

The NHS could be next in line to face an embarrassing data loss fiasco unless "urgent action is taken", clinicians are warning.

NHS could be next in wave of Government data loss fiascos

A survey released by the **Health Service Journal** has found that unsecured memory sticks containing the medical details of thousands of NHS patients could easily go missing.

Of the 92 memory sticks carried by the surveyed doctors 79 sticks held confidential patient information - yet only five were password protected.

Clinicians who conducted the study among colleagues at an unnamed teaching hospital in London said there is "no reason why this lack of security would not be mirrored in surveys across every hospital in the UK and beyond".

One of the clinicians - a surgical registrar - said the sticks contained patient names and dates of birth alongside medical information such as X-ray results, diagnoses and treatment.

A spokeswoman for the Department of Health said: "The NHS locally has legal responsibility to comply with data protection rules.

The survey warns NHS doctors

"Any breach of patient security is unacceptable. We have urged the HSJ to provide details of their survey to the relevant trust so they can take appropriate action to protect patient confidentiality."

Responding to the results of the survey, shadow health minister Mike Penning said: "The Government's shocking record on data losses demonstrates for itself how vitally important it is that we maintain the security of the public's data, particularly when it is of such a sensitive clinical nature.

"Patients rightly expect their personal details to be protected. Unfortunately, this survey exposes the chaos inherent in Labour's approach to data security."

The Government has been hit by numerous missing data scandals in the past year.

An inquiry was launched last month after a computer memory stick containing information on thousands of criminals **was lost** by private contractor PA Consulting.

Home Secretary Jacqui Smith said the contractor appeared to have downloaded the data contrary to the rules of its contract.

On November 20 last year Chancellor Alistair Darling admitted to MPs that computer discs holding personal information on 25 million people and 7.2 million families had gone missing.

Mr Darling told Parliament that the details included names, addresses, dates of birth, child benefit numbers,

La Voix du Nord - Edition du mardi 2 septembre 2008

<<< Retour au sommaire

Jusqu'à 32 gigaoctets de mémoire dans la poche: les clefs du succès

Ces derniers mois, les performances des clefs USB ont tellement progressé qu'elles ouvrent de nouvelles perspectives : pourquoi encombrer son portable d'un lecteur-graveur, voire pourquoi s'encombrer d'un portable ?

PAR FRANCK BAZIN

fbazin@lavoixdunord.fr Depuis quelques mois, on trouve sur le marché des clefs USB d'une capacité de 32 gigaoctets (Corsair - Flash Voyager, 99,99 E), presque dix fois plus de mémoire que les ordinateurs de bureau, il y a une dizaine d'années ! Avec de telles quantité de données, on peut envisager de nouveaux usages.

Combinée à un ordinateur ultraportable, comme le fameux Asus EeePC, la clef USB apporte la mémoire qui fait défaut sur ces machines (une quinzaine de Go).

On peut partir avec ses films ou y stocker les photos prises lors du déplacement. Toutefois, les nouvelles machines de cette catégorie, parallèlement à une légère augmentation de prix, offre une capacité de stockage bien plus importante. Le nouveau Medion Akoya Mini E1210 (actuellement vendu chez Orange et le 10 septembre chez Aldi) dispose d'un disque dur de 80 Go pour moins de 400 E.

Mais, même avec des clefs plus petites, on peut déjà… s'en mettre plein les poches. D'autant que les prix ont terriblement baissé : une clef 2 Go coûte entre 5 E et 10 E et on trouve des clefs 4 Go pour moins de 12 E ! La Sony Micro Vault 4 Go est facturée un peu moins de 25 E mais une Essentiel B 4 Go de chez Boulanger ne coûte que 17,99 E. Cette dernière est livrée avec trois coques (noire, verte, transparente). Mais ce qui fera vraiment la différence d'une clef à l'autre, c'est la différence de vitesse en lecture et en écriture, des informations pas toujours facile à trouver.

Pourtant, une bonne vitesse est essentielle lorsqu'il s'agit de transférer des fichiers volumineux, voire d'utiliser des logiciels directement sur la clef. Une simple clef (au moins 2 Go) permet d'avoir en poche sa suite bureautique, son navigateur Internet, son logiciel de messagerie…, et gratuitement en plus : « *La Framakey est une compilation de logiciels libres pour Windows, (…) préinstallés et prêts à être utilisés directement depuis votre clef USB. L'utilisation des logiciels se fait de façon sécurisée et sans laisser d'informations personnelles sur les machines sur lesquelles vous utilisez votre Framakey* », peut-on lire sur le site Framasoft (www.framasoft.net), le portail du monde libre. Même plus besoin de portable : on peut « squatter » sans risque n'importe quel PC !

Quant à ceux qui serait inquiet à l'idée de perdre une clef avec autant de données personnelles, il existe diverses solutions de sécurité. Une des plus innovantes semble être celle de Mobilegov avec sa clef Device Linker. Cette clef ne peut fonctionner que sur les ordinateurs pour lesquels elle a été préalablement configurées en « mémorisant » l'ADN de ces machines, leurs composants. (70 E pour une clef de 4 Go.)

Communiqués sociétés

Mobilegov déploie sa solution d'authentification forte.

juillet 2008

Juillet 2008

Mobilegov, éditeur de solutions de sécurité basées sur la technologie brevetée de l'ADN du Numérique® (reconnaissance de la signature unique de chaque composant informatique), annonce le démarrage de projets pilotes avec deux organismes bancaires majeurs en Europe, en partenariat avec de grands opérateurs internationaux.

Malgré les alertes lancées par l'APACS et la CNIL dès 2005, les solutions d'authentification forte, qui complètent la reconnaissance du couple Identifiant/Mot de passe (ce que l'on sait) par la reconnaissance d'un élément matériel (ce que l'on a) tardent à s'imposer. D'après Michel Frenkiel, Président de Mobilegov, il y a deux raisons à cela : de tels objets compliquent la vie des banques, qui doivent les gérer, et compliquent également la vie des clients, qui doivent les avoir sous la main pour effectuer une transaction. La solution SAWS (Secure Access Web Service) de Mobilegov utilise comme élément matériel d'authentification forte n'importe quel objet numérique déjà détenu par le client, authentifié à distance par son ADN Numérique, qui est unique, comme notre propre ADN. L'utilisateur peut donc enregistrer auprès de sa banque l'élément matériel de son choix (son téléphone mobile, une clef USB ou même son ordinateur…) afin d'être authentifié lors de sa transaction sur Internet.

« Un certain nombre de solutions ont récemment été testées au Royaume-Uni dans le secteur bancaire pour diminuer les risques de vol en ligne mais celles-ci reposent sur des solutions telles que l'accès par identifiant/mot de passe, complétées par des cartes à puces ou encore des « tokens » (boîtier générant des mots de passe à usage unique, synchronisés avec le mécanisme de contrôle d'accès en ligne de la banque). Cependant, ces objets peuvent être aisément oubliés, perdus ou volés et imposent alors une solution de secours lourde. Dès lors, le coût de possession des objets est élevé : au prix d'achat s'ajoute les coûts de, logistique et de maintenance, au final assumés par le client » commente David Hawksworth, Directeur Général de Torotech, l'un des intégrateurs britannique qui implémente la solution de Mobilegov.

Dans un climat de manque de confiance dans les services sur Internet, Mobilegov apporte une solution innovante et simple dans la sécurité des accès sur Internet et dispose déjà d'un réseau de partenaires dans plus de 14 pays. Pour plus d'information, merci de visiter : www.mobilegov.com

Mobilegov

Boursorama
Votre partenaire pour investir

Associated Press le 07/08/2008 05h16

Le piratage de données bancaires sur Internet dépasse l'imagination

Les autorités américaines estiment que c'est la plus grosse affaire de vol d'identité sur Internet jamais découverte jusqu'ici. Onze personnes ont été inculpées cette semaine et sont accusées d'avoir volé des millions de numéros de cartes bancaires.

Cela ne devrait pourtant pas beaucoup affecter le monde souterrain qui exploite ce type de fuites de données. Les participants à une conférence sur le vol de données sur Internet réunis à Las Vegas estiment que le pillage de cartes de paiement est une activité florissante.

"Ces types ont juste fait preuve d'obstination et ils ont été chanceux, a estimé Jim Christy, un enquêteur spécialisé dans la criminalité en ligne, qui travaille maintenant pour la Défense. "Il y a probablement beaucoup plus de vols de données qui ne sont pas rapportés. Cela touche de petites entreprises dont les systèmes sont forcés sans même qu'elles le sachent".

La portée des vols d'identité sur Internet est à couper le souffle: plus de 41 millions de numéros de cartes bancaires ont été soustraits à de grandes compagnies comme la chaîne de librairies Barnes&Noble. Et cela coûte de l'argent. Une société de vente de vêtements bon marché, JTX, a dû débourser près de 200 millions de dollars (129,6 millions d'euros) pour couvrir ces fuites, qui ont commencé en juillet 2005.

Parmi les personnes inculpées, des Américains, des Estoniens, des Ukrainiens et des Biélorusses, des Chinois, une variété d'origines qui reflète la dimension internationale du crime organisé sur Internet. Le business porte sur des millions de dollars, et il montre que des failles existent dans la sécurité des entreprises.

Les criminels en col blanc circulent par exemple en voiture autour des boutiques avec un ordinateur connecté sur un réseau Wifi pour trouver des opportunités de détournements. Ils parviennent à intercepter des flux de données de paiements.

La personne au centre du réseau démantelé est un ancien informateur des services secrets, installé à Miami, déjà arrêté pour des fraudes. Il risque la prison à vie si toutes les charges retenues contre lui sont prouvées. AP

xo/v734/ma

Les membres réagissent à l'article
Soyez le premier à réagir à l'article

Software Applications News

08 July 2008

Digital DNA touted for better security

By Matthew Broersma, Techworld

UK security integrator Torotech has begun offering a new take on securing online transactions such as banking acces a digital fingerprinting system that uses the uniqueness of a piece of user hardware as an authentication token.

Torotech's "Digital DNA" offering takes advantage of the fact that even mass-produced hardware is never completel homogenous. This means that a particular PC, or even a peripheral such as a USB stick or mobile phone, has a uniq profile that can be used in the authentication process.

For instance, the system can identify individual devices of the same brand, model and capacity, using supposedly non-forgeable data such as serial numbers, according to Mobilegov, the Franco-British firm that developed the underlying Digital DNA technology.

Mobilegov originally intended Digital DNA for controlling the access of peripheral storage devices to corporate networks, but Torotech argued the system could be ideal for applications such as banking, e-commerce and secure remote working.

Under Torotech's system, the first time a user logs onto a bank or e-commerce site, the site takes a fingerprint of c user-supplied hardware device, whether the PC itself or a peripheral.

Each time the user subsequently logs on, that device is needed to complete the authentication process.

Users who want to log on from multiple locations could use a peripheral device such as a mobile phone or PDA for authentication, said Torotech managing director David Hawksworth.

The technique gets around limitations in the use of ordinary authentication tokens such as smartcards or single-use generators, according to Torotech.

For instance, if a peripheral device is used for authentication, it matters less if that device is lost or stolen, since its role in authentication is not evident to anyone aside from the user, the company pointed out.

The Digital DNA system also cuts the costs that can be associated with maintaining systems that rely on smartcards tokens or readers, Torotech said.

"Digital DNA is so unique, like our own DNA, that it is impossible to duplicate and therefore can be used to protect personal data and financial information to a much higher level than ever before," Hawksworth said in a statement.

The system covers a range of devices, including removable storage but also network cards, Bluetooth modems, keyboards, monitors and others hardware.

Mobilegov, which developed the underlying technology, is a 2004 spin-off of the European eJustice project, which aimed primarily to develop biometric authentication technologies.

Vídeos Computerworld

Informativo semanal de IDG TV (31/07/08)

Buscar

SECCIONES
Especial elecciones 08
CW Vídeo
PYMES
E-Business
ERP-CRM
Seguridad
Mobility
Almacenamiento
Outsourcing
Sector TI
Biz Intelligence
Networking
Gestión TI
Profesionales
Tecnología
Portada
SIMO 2007

SERVICIOS
Vídeo Móvil
Partnerzone APC
Especial Green IT
Partnerzone Seguridad
Blogs Computerworld
Webcasts ComputerWorld
Eventos CW
Empleo
Tienda ComputerWorld
Knowledge Center
Newsletter

IDG .es COMPUTERWORLD

Contactar Publicidad Suscripciones Perfil Acta de Privacidad

ADN digital para una mayor seguridad

Votar esta noticia (14 votos) Versión impresora

El integrador de seguridad británico Torotech ha empezado a comercializar un nuevo sistema para garantizar la seguridad de las transacciones online tales como el acceso a entidad financieras: un sistema de toma de huellas digitales que utiliza el rasgo distintivo de una pieza de hardware del usuario como forma de autenticación.

La oferta ADN Digital de Torotech tiene la ventaja de que incluso el hardware fabricado a gran escala nunca es completamente homogéneo, lo que significa que un PC e incluso un periférico, como un USB o teléfono móvil, tiene un perfil único que puede utilizarse en el proceso de autenticación."El ADN digital es único, al igual que nuestro ADN.Es imposible que haya dos iguales, por lo que da un mayor nivel de seguridad a nuestra información financiera y datos personales", afirma David Hawksworth, director general de Torotech.

Por ejemplo, el sistema puede identificar los dispositivos personales de la misma marca, modelo y capacidad, utilizando datos que no pueden falsificarse como el número de serie. Así, la primera vez que el usuario se registra en un banco o en un sitio de comercio electrónico, el sitio toma una huella de su dispositivo de hardware, ya sea el propio PC o un periférico, para autenticar al usuario. Este proceso tiene que completarse cada vez que el usuario se registra.

El sistema de ADN digital evita además las limitaciones implícitas en el uso de otros sistemas de autenticación como smartcards o los generadores de PIN de uso único que, en el caso de robo o pérdida, pueden ser utilizados para un uso fraudulento, algo prácticamente imposible con el sistema de ADN digital, ya que pocos saben que pueden utilizar el hardware como sistema de autenticación. Asimismo, con el ADN digital se reducen los costes asociados al mantenimiento, como los que van parejos a las smartcards o los lectores; y posibilita el registro del usuario desde múltiples ubicaciones, utilizando dispositivos como el teléfono móvil o la PDA.

El sistema cubre un amplio rango de dispositivos, entre los que se incluye hardware desmontables, tarjetas de red, módems Bluetooth, teclados, monitores y otros.

Mobilegov, una spin-off del proyecto europeo de eJustice para el desarrollo de tecnologías de autenticación biométricas, ha sido la encargada de desarrollar la tecnología subyacente al ADN digital.

Natalia Mosquera [09/07/2008 09:37:20]

NOTICIAS MÁS VOTADAS

ING Nationale-Nederlanden integra sus herramientas de monitorización TI ...

Jorge Dinarés dimite como director general de Panda Security ...

Felix del Barrio sustituye a Miguel Milano al frente de Oracle Ibérica ...

[+]

WEBCASTS

Telegraph.co.uk

NHS disc containing sensitive data lost

A computer disc containing the medical records of more than 38,000 NHS patients went missing when it was sent to a software company to be backed up - in case the records got lost.

By Caroline Gammell
Last Updated: 2:20AM BST 21 May 2008

The information, which dates back 10 years, was mislaid somewhere between London and Sandown Health Centre on the Isle of Wight.

It was given to courier company City Link in March, but the health centre only spotted it was missing in May.

A spokesman for the South Central Strategic Health Authority said the courier company - which is supposed to track every item at every stage - demonstrated a “clear failure” by losing all record of the disc once it passed into their hands.

City Link, which won “Courier of the Year” last year for reliability and customer service, is searching all its 92 depots nationwide, while all 38,650 past and present patients are being notified of the loss.

A spokesman for the courier company said: “We are naturally very concerned by the loss of our customer’s consignment and a rigorous search for the parcel continues.

“We are doing everything in our power to resolve the matter and return the package as quickly as possible.”

A Department of Health spokesman insisted the chances of someone being able to access the information - which is stored on specialist software and password-secured - is “pretty slim”.

The disc is the latest piece of sensitive data to go astray in the last 12 months after details about child benefit applicants, national insurance numbers and driver’s licences got lost en route to their destinations.

The latest parcel was sent to the London-based software company In Practice Systems on March 10.

A spokesman for the Isle of Wight Primary Care Trust said: “They carry out checks on computer back-up tapes to make sure they could be used effectively to restore information to the practice computer system in the event of a system failure or other emergency such as a fire.”

Having checked the back-up records, the disc was given to City Link to return to Sandown on March 11, but the health centre was not notified that the tape was back in transit.

It was not until May 1 that they realised that the records were missing and further 11 days before the Isle of Wight PCT was notified.

The system of sending sensitive medical data by courier or post is now being reviewed by all PCTs and the SHA has called for mechanisms to be put in place “to alert when data is not received by the expected date”.

Margaret Pratt, interim chief executive of the Isle of Wight PCT, said: “Although there is very little chance of anyone being able to do anything untoward with this tape, should they find it, it is potentially a very serious loss of confidential information.”

Dr Peter Randall, senior partner at Sandown added: “We have another copy of the back-up tape and our main computer records system is not affected by this, so we still have access to all the information we need and patient care is not compromised in any way.”

MICHEL FRENKIEL

Sans aucune expérience entrepreneuriale, il crée sa première entreprise et la mène en Bourse en deux ans.

MobileGov, la réussite effrontée !

MobileGov entre en Bourse en mars 2008. C'est la première entreprise à franchir le pas cette année là, première également à réaliser toutes les étapes en 4 mois seulement, et contre toute attente, MobileGov lève1,5 millions d'euros au lieu des 600.000 escomptés. D'un calme olympien, Michel Frenkiel ne masque pas plus longtemps son excitation tout intérieure. « Nous sommes très fier, confie-t-il. Il ne nous aura fallu que 2 ans pour réaliser cette entrée en Bourse, alors que l'entreprise a vraiment démarré ses activités que courant 2006 ». Grand sorcier de la finance, Michel Frenkiel ? Gourou incontesté de l'entrepreneuriat ? Chasseur d'opportunités hors pair ? Pas du tout. C'est même tout l'inverse. Cet ingénieur informaticien de formation a un parcours bien balisé dans de grands groupes comme IBM ou Thalès. Des projets d'envergure, motivants, captivants et confortables, le maintiennent encore à distance de toute idée entrepreneuriale. Une charrette en 2004 de son employeur du moment le conduit à la Commission Européenne où il travaille sur les failles de sécurité informatique et y détecte une lacune majeure. C'est là qu'il découvre un univers étonnant, celui de la cybercriminalité. « La fraude est énorme sur Internet, s'exclame-t-il, les enjeux sont immenses. J'ai senti comme un défi se poser à moi, une lute permanente qui ne connaît pas de vainqueur ». Ce passionné de montagne va jusqu'à comparer son challenge aux sommets himalayens dont on ne voit pas les cimes. Michel Frenkiel n'est pas casse-cou pour autant. S'il accepte le risque, il veut poser des jalons et enrôle avec lui deux amis de longue date ayant fait partie de la même charrette.

L'équipe fondatrice et co-présidents : Eric Mathieur, François-Pierre Lepage, Michel Frenkiel.

Le processus est en marche... Une réponse est trouvée au problème de sécurité, un brevet déposé, MobileGov créée dans la foulée. A cet instant, l'équipe n'a encore aucune idée du marché. Une étude réalisée par l'Arist identifie quelques concurrents et d'authentiques opportunités de business. « Nous avions des moyens très limités à cette époque, poursuit-il. Nous nous voyions une fois par semaine lors d'un déjeuner, mais l'étude à été un fougueux déclencheur ». Nous sommes en 2005, nos trois complices s'engouffrent dans la voie et sortent un premier produit fin d'année. Les premiers prospects sérieux s'annoncent début 2006, suivi des premières embauchent, puis deux nouveaux produits de sécurisation. La suite est une montée en puissance rapide et frénétique, faites de remises en question permanentes et de réussites exemplaires. « Je n'étais pas préparé à cette aventure, avoue-t-il, modeste. Etre trois nous a permis de répartir la charge du doute ». La proximité du Ceram (Ecole de commerce Nice Sophia-Antipolis), l'accompagnement du service "Inria transfert", un groupe motivé et très soudé, tous ces paramètres ont très vite forgé une culture entrepreneuriale indiscutable. De plus Michel Frenkiel peut s'appuyer sur un vrai savoir-faire dans l'industrialisation de projet développé lors de son parcours professionnel. « Les idées ne manquent pas en France, assure-t-il. La difficulté vient plutôt de la faisabilité. Où comment transformer une innovation en produit commercialisable ». Et de fait, pour être passé par là, Michel Frenkiel en sait quelque chose. Arrivé dans le monde de l'entreprise (presque) par hasard, il est aujourd'hui cité en exemple, et un professeur en entrepreneuriat du Ceram, Michel Bernasconi, a fait de MobileGov un cas d'école pour sa vitesse d'exécution.

JEAN-PHILIPPE THIRION

Plus qu'un besoin de reconnaissance social, de défi ou d'autonomie, l'entrepreneuriat est d'abord un acte créatif.

L'entreprise, coûte que coûte !

Quantificare développe une méthode de quantification et d'observation de l'évolution des maladies à partir d'analyse d'images, pour le compte de sociétés pharmaceutiques et biotech. L'objectif est stratégique, il consiste à prouver l'efficacité d'un médicament avant sa mise sur le marché. Les économies réalisées sont vertigineuses. Dans ces secteurs du médical, et particulièrement la pharmacie, tout est démesuré : la taille des entreprises, le nombre de salariés, le chiffre d'affaires, la R&D, les enjeux... Pourtant, lorsqu'il créé Quantificare, Jean-Philippe Thirion n'est pas impressionné. Ce Normal Sup, Ponts et Chaussés et Inria, peintre à ses heures perdues, n'a pas d'autre objectif que de créer son entreprise.
Une première expérience de 4 ans dans une jeune entreprise lui donne l'occasion d'appréhender toutes les étapes de croissance, avant de fonder Quantificare. C'est sa seule expérience du monde de l'entreprise qu'il ait eu. De conseils d'experts, il n'en a pas voulu. « Ce sont les rencontres de terrain qui ont forgé ma culture d'entreprise, précise-t-il. Bien sûr je me suis documenté sur les processus économiques, mais l'écoute de gens d'expérience a été plus formatrice que l'étude des mécanismes de marché ».
Très motivé par la création, il n'explique pas ce besoin inné, presque vital, ce penchant naturel à faire les choses par lui-même comme une expression de lui-même. « Je n'ai pas le souci d'exister socialement, poursuit-il, la création d'entreprise, c'est ancré plus profondément en moi que l'apparence sociale ». Un père entrepreneur n'est sans doute pas étranger à cette disposition... Mais malgré cette force viscérale, il reconnaît l'extrême difficulté à contrôler tous les aspects d'une affaire. « Mieux vaut être calme, on nous demande de prendre tous les risques, vis-à-vis des financiers, de l'administratif, du personnel ». Après sept années intenses, Jean-Philippe Thirion savoure un de ses plus beaux succès, la conquête du marché américain et la création d'une filiale sur ce territoire le plus business au monde.

>> EN BREF

L'Auvergne crée des résidences pour entrepreneurs

Pour compenser un baisse démographique, le Conseil Régional de l'Auvergne a mis en place le dispositif innovant des résidences d'entrepreneurs. Directement inspirées des résidences d'artistes, les résidences d'entrepreneurs visent à offrir à un créateur ou à un repreneur d'entreprise le cadre et les conditions matérielles qui lui permettront de mener à bien son projet. En charge du projet, l'Agence régionale du développement du territoire s'appuie sur les acteurs locaux pour proposer une aide complète, portant à la fois sur le projet professionnel et sur le projet de vie.
Contact : 04 73 31 84 84

Couveuse d'entreprises dans le 06

L'idée repose sur le test et la faisabilité d'un projet. Dès l'entrée en couveuse, l'entrepreneur bénéficie d'un hébergement juridique, mais il conserve son statut social et ses revenus. Il peut produire, facturer, encaisser avec le numéro de Siret de la couveuse. Les paiements sont faits à l'ordre de Creative 06, jusqu'à ce que l'entreprise atteigne une viabilité. Parvenu à ce stade, l'entreprise procède alors à son inscription au CFE. Le bénéfice est reversé au chef d'entreprise sous forme de rémunération, la couveuse, elle, touche 10 % de la marge brute.

Tous les types d'entreprises ne peuvent pas être couvés. Le fait d'avoir la responsabilité juridique empêche d'accueillir un certain nombre d'activités, notamment celles qui doivent disposer d'un bail commercial et celles qui exigent une garantie décennale.

Créative 06. Tél. 09.63.22.03.52 et www.creative06.com

Un forfait pour les entrepreneurs

Christine Lagarde a annoncé pour le prochain projet de loi de modernisation de l'économie le remplacement des charges fiscales et sociales d'un entrepreneur par un forfait mensuel ou trimestriel de 13% du chiffre d'affaires pour les commerces et de 23% dans les services.