Société Anonyme au capital de 282.993 €

RCS Antibes 453 639 932

Siège Social : 2000 route des Lucioles

06410 Biot

ETUDE FINANCIERE
DOCUMENT D'INFORMATION

Mars 2008

EUROPE FINANCE ET INDUSTRIE
INVESTMENT BANKING

EUROPE FINANCE ET INDUSTRIE
SECURITIES

Avertissement / Warning

Ce Document d'information est réalisé dans le cadre d'une opération de Placement exclusivement réservée à des Investisseurs Qualifiés tels qu'ils sont définis par l'article L. 411-2 du Code monétaire et financier. Cette opération prendra la forme d'une augmentation de capital. Une demande d'inscription au Marché Libre d'Euronext Paris sera demandée.

This Offering Circular is part of a Placement exclusively reserved to "Certified Investors" as defined in article L.411-2 of the French Code monétaire et financier. This placement will take the form of an Increase of Capital. A request for listing on the Marché Libre of Euronext Paris S.A. will be expressed.

Des exemplaires du présent Document d'information sont disponibles sans frais au siège de la société Mobilegov ainsi qu'auprès d'EUROPE FINANCE ET INDUSTRIE.

TABLE DES MATIERES

Chapitre
1

Chapitre 1: Analyse financière

Capital social avant opération : 282 993 € divisé en 459 030 titres d'une valeur nominale de 0,617 €.

1ère cotation prévisionnelle : 29 février 2008
Placement jusqu'au : 14 mars 2008

Prix de souscription : 6,07 €

Valorisation pré-money : 2,79 M€

Flottant post opération : 17,72 % (pouvant aller jusqu'à 41,78 %)

Modalités de l'opération : Augmentation de capital de 600.000 € (pouvant aller jusqu'à 2M€ par autorisation) par émission, dans le cadre d'un placement privé réservé aux investisseurs qualifiés, de 98.846 actions nouvelles (pouvant créer 329.489 nouveaux titres au maximum)

Compte de résultat et bilan résumés après inscription à la cote*

K€	2006	2007e	2008p	2009p	2010p	2011p	2012p
Chiffre d'affaires	68	144	910	3 825	8 060	14 770	18 305
Résultat d'exploitation	-83	-247	-317	324	2 739	7 053	8 881
Résultat net	-65	-250	-323	324	2 739	7 053	5 892
Marge d'exploitation	ns	ns	ns	8,5%	34,0%	47,7%	48,5%
Capitaux propres	42	-53	-286	42	2 781	9 834	15 725
PER	ns	ns	ns	10,5	1,2	0,5	0,6
BPA	ns	ns	ns	0,58	4,91	12,64	10,56
VE/ CA	ns	ns	ns	0,9	0,4	0,2	0,2
VE/ REX	ns	ns	ns	10,5	1,2	0,5	0,4
ROE	ns	ns	ns	ns	66,0%	48,1%	37,8%

Sources : Société, EFI

* Inclut une levée de fonds de 600.000 € prévue par Mobilegov qui servira à financer l'extension de la capacité de production de l'entreprise.

1.1. Valorisation de la société

1.1.1. Préambule

Mobilegov est un éditeur de logiciels qui conçoit, développe et commercialise des matériels de sécurité informatique. Il est le concepteur de l'ADN numérique et pionnier sur le marché des « Endpoint Security ».

La société nous a transmis un business plan qui nous a servi à établir notre valorisation. Nous avons utilisé une méthode classique de valorisation : l'actualisation des cash flows futurs. Cette approche permet de mettre en jeu le RBE, les amortissements, les investissements industriels et la variation du BFR. Le cash flow « libre » annuel est alors actualisé en utilisant comme taux d'actualisation le coût moyen pondéré du capital.

1.1.2. Méthode de l'actualisation des cash flows

Nous avons utilisé le business plan communiqué par la société pour la période 2007-2012 et l'avons prolongé pour qu'il soit adaptable à notre modèle de calcul. Nous avons émis un certain nombre d'hypothèses :

- la croissance du CA ralentit progressivement jusqu'en 2018 pour se maintenir à 3% jusqu'en 2026.
- nous avons retenu un taux de marge d'exploitation de 20%.
- les investissements sont fixés à 6 000 € à partir de 2007
- variation du BFR estimée à 5% du CA

Le taux d'actualisation a été établi à partir du taux sans risque, l'OAT 10 ans à 4,30%, auquel s'additionne une prime de risque que nous évaluons à 3,64%, affectée d'un coefficient bêta de 3,55x.

Taux sans risque	4,30%
Prime de risque	3,64%
Bêta	3,55
Coût du capital	17,23%
WACC (CMPC)	**7,08%**

Source : EFI

En K€	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
CA	144	910	1 274	1 720	2 236	2 795	3 214	3 600	3 888	4 121
Var %	113%	532%	40%	35%	30%	25%	15%	12%	8%	6%
REX	**-247**	**-317**	**-258**	**36**	**345**	**726**	**643**	**720**	**778**	**824**
REX / CA	ns	ns	ns	2,1%	15,4%	26,0%	20,0%	20,0%	20,0%	20,0%
Impôt	0	0	0	12	114	240	212	238	257	272
taux d'impôsition	0,0%	0,0%	0,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%
REX après impôts	**-247**	**-317**	**-258**	**24**	**231**	**486**	**431**	**482**	**521**	**552**
Investiss. Indus.	6	6	6	6	6	6	6	6	6	6
Var BFR	-17	70	49	78	89	140	161	180	194	206
Cash-flow libre	-139	-272	-213	-46	150	355	278	310	335	354
DFCF	**-130**	**-237**	**-173**	**-35**	**107**	**235**	**172**	**180**	**181**	**179**

Source : EFI

En K€	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**
CA	4 286	4 414	4 547	4 683	4 824	4 968	5 118	5 271	5 429	5 592
Var %	4%	3%	3%	3%	3%	3%	3%	3%	3%	3%
REX	**857**	**883**	**909**	**937**	**965**	**994**	**1 024**	**1 054**	**1 086**	**1 118**
REX / CA	20,0%	20,0%	20,0%	20,0%	20,0%	20,0%	20,0%	20,0%	20,0%	20,0%
Impôt	283	291	300	309	318	328	338	348	358	369
taux d'impôsition	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%	33,0%
REX après impôts	**574**	**592**	**609**	**628**	**646**	**666**	**686**	**706**	**728**	**749**
Investiss. Indus.	6	6	6	6	6	6	6	6	6	6
Var BFR	214	112	132	152	241	248	256	264	271	280
Cash-flow libre	368	488	485	484	413	425	438	451	464	478
DFCF	**173**	**215**	**199**	**186**	**148**	**142**	**137**	**132**	**127**	**122**

Source : EFI

En K€	**Taux de croissance à l'infini**				
WACC	0,0%	0,5%	1,0%	1,5%	2,0%
6,38%	3 524	5 024	5 316	5 668	6 100
7,08%	3 295	3 396	3 513	3 652	3 817
7,78%	3 113	3 191	3 281	3 385	3 506
Moyenne	**3 985**				

Source : EFI

1.2. Conclusion

Moyenne des DCF	3 985 469
Valorisation induite	**3 985 469**

Source EFI

La méthode de valorisation que nous avons utilisé aboutit à une valeur de 3,98 M€.

Pour envisager une introduction sur le Marché Libre de la place de Paris, nous estimons raisonnable d'appliquer à cette valeur une décote d'introduction qui peut être estimée à 30%. Dans ces conditions, il ressort que la valeur de Mobilegov se situe à 2,79 M€, soit 6,07 € par action.

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 suivi d'une demande d'admission 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. Caractéristiques du Placement réservé à des Investisseurs Qualifiés

4.2.1. Personnes habilitées à émettre des ordres dans le cadre du Placement réservé à des Investisseurs Qualifiés

Conformément aux dispositions de l'Article L.411-2, alinéa 2 du Code Monétaire et Financier, l'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 de ces investisseurs qualifiés est établie par le Décret n° 98-880 du 1er octobre 1998 :

I – Sont des investisseurs qualifiés au sens du II de l'article 6 de l'ordonnance du 28 septembre 1967 lorsqu'ils agissent pour compte propre :

1. Les établissements de crédit et les compagnies financières mentionnés, respectivement, à l'article 18 et à l'article 72 de la loi du 24 janvier 1984 ;

2. Les institutions et services mentionnés à l'article 8 de la loi du 24 janvier 1984 ;

3. Les entreprises d'investissement mentionnées à l'article 7 de la loi du 2 juillet 1996 ;

4. Les sociétés d'investissement régies par l'ordonnance du 2 novembre 1945 ;

5. Les sociétés d'assurance et de capitalisation, ainsi que les sociétés de réassurance régies par le code des assurances ;

6. Les institutions de prévoyance régies par le code de la sécurité sociale ;

7. La Caisse d'amortissement de la dette sociale instituée par l'article 1er de l'ordonnance du 24 janvier 1996.

II – Sont également des investisseurs qualifiés au sens du II de l'article 6 de l'ordonnance du 28 septembre 1967, lorsqu'ils agissent pour compte propre, et à partir du jour de la publication au Bulletin des annonces légales obligatoires d'une décision prise en ce sens, selon le cas, par le conseil d'administration, par le directoire ou par le ou les gérants :

8. Les sociétés de capital-risque mentionnées à l'article 1er de la loi du 11 juillet 1985 ;

9. Les sociétés financières d'innovation mentionnées au III de l'article 4 de la loi du 11 juillet 1972 ;

10. Les sociétés commerciales régies par la loi du 24 juillet 1966 dont le total du bilan consolidé, ou à défaut le total du bilan social, du dernier exercice, tel que publié et certifié par les commissaires aux comptes, est supérieur à un milliard de francs ;

11. Les établissements publics nationaux à caractère industriel et commercial dont des titres sont négociés sur un marché réglementé d'un Etat partie à l'accord sur l'Espace économique européen ;

12. Les organismes mutualistes régis par le code de la mutualité gérant en leur sein une caisse autonome agréée en vertu des dispositions de l'article L. 321-2 dudit code ;

13. Les sociétés dont un ou plusieurs investisseurs qualifiés mentionnés au I ci-dessus ou aux 8. à 12. du présent II détiennent, ensemble ou séparément, directement ou indirectement, au moins 99 % du capital ou des droits de vote.

La décision prise par le conseil d'administration, par le directoire ou par le ou les gérants rapportant la décision mentionnée au premier alinéa du présent II prend effet à partir de sa publication au Bulletin des annonces légales obligatoires.

Les personnes mentionnées au I ci-dessus ainsi que les sociétés de gestion mentionnées à l'article 12 de la loi du 23 décembre 1988 sont réputées agir en qualité d'investisseur qualifié lorsqu'elles agissent pour le compte d'un organisme de placement collectif en valeurs mobilières ou d'un investisseur qualifié appartenant à l'une des catégories mentionnées au I ou au II ci-dessus.

4.2.2. Ordres susceptibles d'être émis dans le cadre du Placement réservé à des Investisseurs Qualifiés

Les ordres seront exprimés en nombre d'actions ou en montants demandés. Ils pourront comprendre des conditions relatives au prix.

4.3. Demande de Cotation Directe

Une demande d'admission des actions de la Société aux négociations sur le Marché Libre d'Euronext Paris, sera déposée.

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

Chapitre

5

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

5.1. Principales informations financières

(montants en milliers d'€)	30.06.2007*	31.12.2006	31.12.2005
Chiffre d'affaires	60	68	-
Résultat d'exploitation	- 114	- 83	0,4
Résultat Financier	- 0,2	-	-
Résultat net	- 78	- 65	0,2
Actif immobilisé net	113	70	0,2
Capitaux propres	- 36	42	11
Endettement	322	191	17
Disponibilités	24	15	9,4
Total Bilan	296	233	28

* Situation semestrielle

5.2. Usage des fonds levés

La priorité de Mobilegov est d'exploiter sa conception de l'ADN du numérique en développant l'antivol du futur, qui prévient à la fois le vol des données et le vol des équipements. Cette innovation couronne une position de leader à l'international de la sécurisation réseaux de très haut niveau et permet de développer une activité commerciale en plein essor, de gagner des parts de marché et d'aborder la normalisation internationale de notre approche.

A cet effet, les fonds levés seront principalement consacrés :

- Au développement commercial international.
- A la poursuite et à l'amplification de l'effort de Recherche & Développement qui est au cœur de la stratégie de croissance de la Société.

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. Motivations de l'introduction en Bourse

L'inscription des actions de Mobilegov aux négociations sur le Marché Libre d'Euronext Paris marque une étape importante du développement de la Société. Cette opération a pour objectifs :

- De doter la Société des moyens de financement offerts par la cotation en vue d'accompagner son plan de croissance ;
- D'augmenter sa notoriété et de renforcer sa crédibilité sur les marchés français et internationaux ;
- De valoriser la Société et l'acclimater au marché boursier.

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 ou des Gouvernements. Ils ne présentent donc aucun risque de solvabilité. De plus l'ensemble des encours clients est confié à une société d'affacturage (Natixis Factor, N°1 de l'affacturage en France) 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 estime ne pas être exposé à un risque lié à la concurrence.

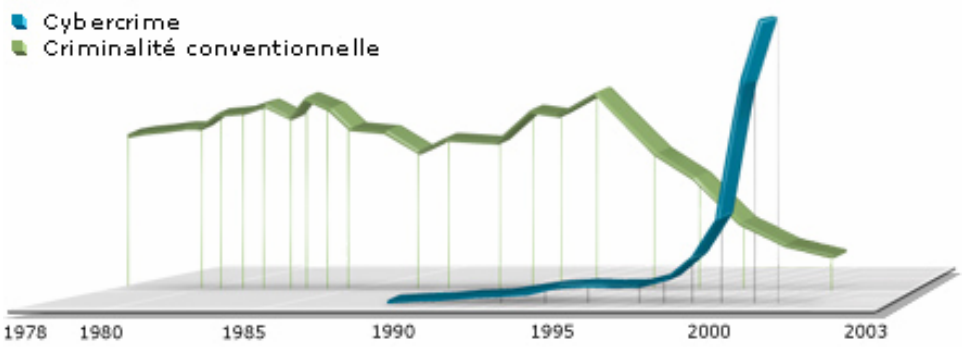
En France, la Société n'a pas de concurrent. Ce fait lui donne un avantage stratégique car les logiciels de sécurité sont au cœur des systèmes, et représentent par conséquent un risque important. En Europe, il est plus facile de s'assurer qu'une société européenne n'a pas introduit de Cheval de Troie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

Une demi-douzaine de société américaines et israéliennes développent des produits qui visent les mêmes objectifs que l'un des produits de Mobilegov. L'ergonomie et la finesse des résultats de la société la placent au-dessus de ses concurrents. Son autre produit n'a pas de concurrents directs.

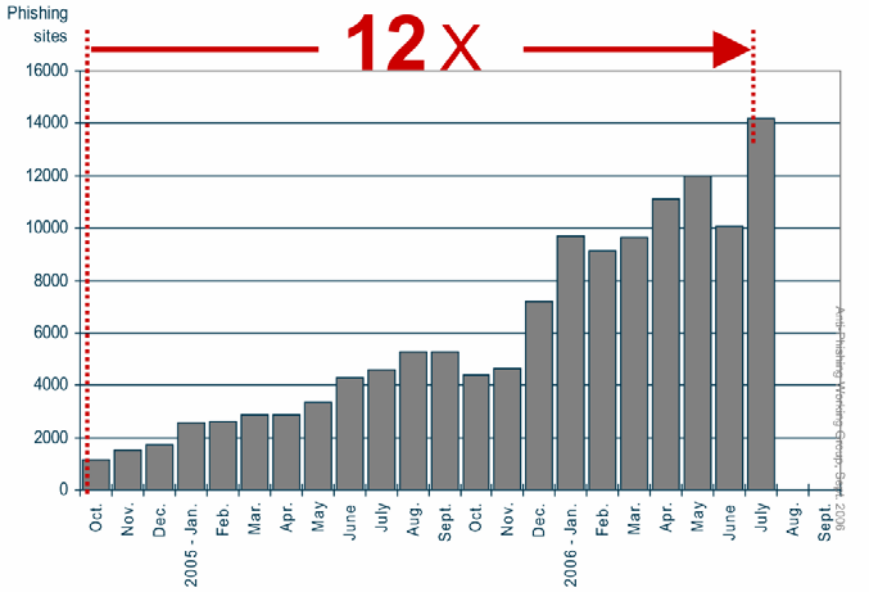
Le savoir-faire est protégé par un brevet robuste qui appartient à la Société.

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.

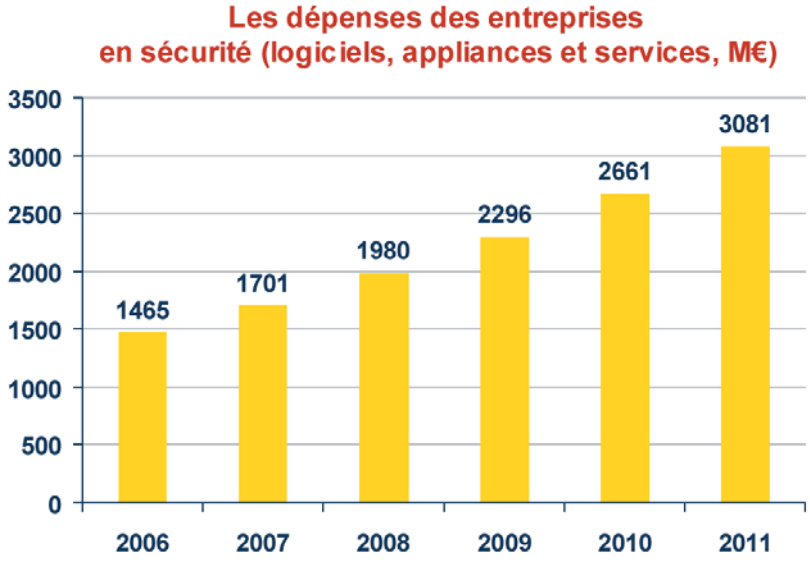
La cybercriminalité augmente fortement depuis plusieurs années. En 2002, le revenu de la cybercriminalité a dépassé celui de la criminalité organisée, comme le démontre l'étude publiée par IBM (http ://www-03.ibm.com/ondemand/ca/fr/pointofview/cybercrime/jul18/ibm_future_crime.html) :



Les tentatives de fraude bancaire par « phishing » (que Mobilegov sait combattre) doublent tous les 4 mois, comme le mesure depuis 2 ans la Banque du Canada (www.pwgsc.gc.ca/recgen/colloquium2007/pdf/panel-discussion-jose-navarro-e.pdf) :



La croissance et les prévisions de croissance du marché de la sécurité sont significatives, de l'ordre de 20% par an, comme le démontrent les études IDC successives (par exemple www.idc.com/france/downloads/about/newsletter_q2_2007.pdf):



Toutefois, la croissance des dépenses de sécurité reste très en deçà de la croissance observée de la criminalité. Notre marché n'est donc pas près de se tarir, il a même grandement besoin de solutions innovantes pour protéger plus efficacement la Société de l'Information attaquée par une criminalité explosive.

6.1.4. Risques technologiques

Toutes les solutions de la Société font l'objet d'un dépôt de brevet. Elle estime disposer de la technologie la plus adaptée pour la sécurité liée aux composants matériels des systèmes numériques.

Avant de développer des produits, Mobilegov a déjà réalisé le « Proof of Concept » en 2005 et fait appel à un laboratoire spécialisé pour mener une veille économique et concurrentielle permanente (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 5 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,
3. M. Eric MATHIEU, co-fondateur de la Société, est Directeur Technique.

Ces 3 personnes détiennent à ce jour directement ou indirectement 75% du capital de la Société.

4. M. Philippe MAZURIER est Directeur Commercial et
5. M. Jean-Bernard LAVAURY est Directeur Projets de Mobilegov.

6.2.2. Dépendance à l'égard des principaux actionnaires

Co-fondateurs de Mobilegov en avril 2004 et détenteurs de 75%, 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.

Mobilegov Ltd. Est une société qui détient 24 % de Mobilegov France SA.

IST Consultants est une société qui détient 4 % de Mobilegov France SA.

Ces deux sociétés sont détenues par les co-fondateurs de Mobilegov.

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	8 INTERNATIONAL VENTURE CAPITAL SUMMIT	Sommet International du Capital-Risque 2004
	Capital-IT DÉMONTRER ET FINANCER L'INNOVATION	Capital-IT Best Innovation 2005
2007	Cap Innovation Méditerranée	Lauréat 2007 de l'Entreprise la plus Innovante en région PACA

Labels et Subventions

2005	Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	Brevet validé par le Cabinet du Ministre (Fonctionnariat d'Etat aux Nouvelles Technologies), le SGDN et la DCSSI
2006	oséo	Aide au Financement de l'Innovation 75 000€
2007	i.a.d.	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 15 000 € pour l'année 2006.

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 240 k€ de disponibilités. A la même date, elle ne détient pas de valeurs mobilières de placement.

La Société considère disposer de la trésorerie et des facilités bancaires suffisantes pour faire face aux besoins et obligations de son exploitation

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 :

2007 : 8 523.,06 €

2008 : 17 046,12 €

2009 : 17 046,12 €

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 :

25 000 € au plus tard le 30/09/2008

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).

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 ne seront pas admis aux négociations sur un marché réglementé et ne bénéficieront donc pas 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. Investissements

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 : +33 492 944 894

Fax : +33 492 944 895

E-mail : info@mobilegov.com

Site Internet : www.mobilegov.com

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.

  Premier contrat de distribution avec SPIE Communication. Suivront 11 contrats de distribution avec des grossistes, des intégrateurs et des distributeurs, en France (Prossi, Quadria-Euralliance's, NextiraOne, IP Vista), Royaume Uni (Onyx Group, RMT, ITPS, LogicaCMG Plc.), Inde (DNP Global) et enfin Accenture.

  Août : sortie de son second produit Device Linker, une clé USB inviolable.

  Contrat CIFRE avec un thésard du CNRS, Laboratoire I3S de Sophia-Antipolis

  Identifiée start-up de croissance et accompagnée par INRIA-Transfert

  Signature d'un NDA avec ORANGE R&D qui étudie l'usage de notre technologie dans ses produits. 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

  Décembre : sortie de la Version PRO de Device Authenticator, présenté à Infosecurity Paris en novembre, et première commande signée.

7.2. Investissements

7.2.1. Principaux investissements effectués par la société pendant les 3 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 trois dernières années, les dépenses d'investissement ont été consacrées à la Recherche et Développement. Pour la majeure partie, elles ont été passées en charge. Le prototype de développement a été immobilisé en 2006 pour une somme de 61 956€ (au compte de résultat clos au 31/12/2006).

La politique d'investissement de la Société Mobilegov vise à développer des solutions en phase avec les besoins du marché, des clients et de l'entreprise. Elle vise également le développement de son business model sous la forme de licensing.

7.2.2. Investissements envisagés

Mobilegov compte poursuivre une politique d'investissement forte et en corrélation avec ses objectifs stratégiques. Le mode de financement de ses investissements prendra la forme de location de longue durée ou « leasing » pour les équipements de tests et mesure nécessaires à la validation produit à l'issue de leur fabrication. Ces investissements incluent également l'achat de matériel et de services pour la qualification (critères communs) de ses produits et la fabrication de produits commercialisables par Mobilegov sur le marché américain. En 2008-2009, les investissements seront centrés sur les objectifs suivants :

- Renforcement des performances de la ligne de produits Device Authenticator, notamment pour supporter les très grands groupes industriels et les grandes administrations (plus de 10 000 postes de travail).
- Généralisation de la technologie Linker aux disques durs, afin de les rendre inexploitables en dehors de l'environnement autorisé. Lancement d'une série de disques durs de haute sécurité.
- Intégration de la technologie Linker dans les microcontrôleurs, de façon à proposer une solution antivol pour les principaux équipements grand public (caméras, appareils photos numériques, etc.).

Chapitre

8

Chapitre 8: Renseignements concernant les activtés

8.1. Présentation générale et métiers de Mobilegov

Mobilegov est un éditeur de logiciel qui conçoit, développe et commercialise des logiciels et des matériels innovants de sécurité informatique.

Présenté par les media comme le concepteur de l'**ADN numérique**, Mobilegov est un des pionniers sur le marché en forte croissance des « Endpoint Security ».

Mobilegov sait détecter et identifier, par des moyens logiciels, tout composant ou toute modification (hard ou soft) de ces composants dans un système numérique. Sa technologie est brevetée en Europe et aux USA. Mobilegov est née d'un projet Européen de recherche sur la sécurité et les usages des futurs documents d'identité.

Mobilegov répond de façon unique au problème du vol de données sensibles dans les entreprises en proposant d'étendre la sécurité réseau aux périphériques amovibles (clés USB, disques, graveurs, etc.). La société améliore la productivité de l'entreprise en permettant l'utilisation des outils nouveaux, souvent bannis par raison de sécurité.

Sa technologie permet aussi de lutter contre le vol (appareils photo numériques, ordinateurs, iPods, disques durs, etc.) en les rendant inutilisables en dehors de l'environnement pour lequel ils ont été configurés.

Sa vision, dans un monde où l'informatique distribuée devient omniprésente, est que la sécurité des composants telle qu'elle est développée par Mobilegov va jouer un rôle prépondérant pour le succès des applications à venir.

La société commercialise ses deux premiers produits Device Authenticator et Device Linker en France et en Europe. Depuis l'été, elle s'appuie sur un puissant réseau de distribution. Sa technologie a été validée par les industriels et les laboratoires les plus exigeants.

Device Authenticator garantit qu'aucun composant non préalablement autorisé, donc potentiellement dangereux, ne puisse être connecté à un PC.

Device Linker garantit qu'un périphérique à mémoire (clé USB) ne puisse être utilisé que dans un environnement déterminé. S'il est perdu ou volé, ses données seront inexploitables.

Mobilegov propose une approche cohérente et mature pour combler une faille de sécurité reconnue, en permettant que seuls des équipements autorisés (PCs, PDAs, téléphones mobiles, etc.) puissent accéder à des données sensibles ou des applications à distance.

Sa technologie est compatible avec la plupart des systèmes existants et ne requiert aucun équipement spécifique. Elle est également compatible avec l'approche du « Trusted Platform Module (TPM) », développée par le Trusted Computing Group.

Avec la convergence des technologies informatique, téléphonie et multimédia, la multiplication de composants puissants et discrets qui s'interconnectent facilement, une opportunité de marché se présente pour Mobilegov qui dispose d'un « time to market » idéal.

En effet, les leaders de la sécurité se sont focalisés sur les attaques logicielles, qui s'appuient sur des technologies de plus en plus sophistiquées. Ils ont ignoré les attaques contre les matériels, qui constituent aujourd'hui la première vulnérabilité des systèmes.

Notre technologie est indépendante du système d'exploitation.

Demain, nous comptons l'appliquer aux domaines autres que les réseaux de PC, et qui dépendent aussi de composants numériques. Nous développons l'**antivol du futur** qui prévient à la fois le vol des données et le vol des équipements, et nous projetons d'en faire un standard international. 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 nouvelle approche de la sécurité touche potentiellement tous les contextes : la maison, le bureau, la voiture, le bateau, etc.. Nous proposons de rendre inutilisables tout composant numérique en dehors du contexte pour lequel (ou lesquels) il a été configuré.

Le surcoût d'une telle protection est négligeable. Nous l'avons démontré dans le cas de la clé USB Mobilegov Device Linker, et nous sommes prêts à généraliser cette solution avec des constructeurs.

8.2. Le marché et les produits futurs

8.2.1. Des « Endpoints » à l'authentification forte

« Endpoint » : traduction littérale de « points de sortie », terme qui définit les points d'entrée et de sortie d'information d'un système informatique comme les ports USB, PCMCIA, FireWire, LPT, infrarouge, COM, mais aussi Bluetooth, Wireless, etc. Le marché des Endpoints comprend l'ensemble des solutions de sécurité qui permettent de contrôler et de gérer ces points de sortie.

La conformité des postes de travail à la politique de sécurité (Endpoint security) et l'administration centralisée portent le marché :

Selon les prévisions de croissance formulées par IDC, les solutions de *Security & Vulnerability Management (SVM)* devraient générer la plus forte dynamique au cours des prochaines années (2005 à 2009) : IDC anticipe une croissance moyenne de 19,3% sur la période (2005 à 2009), alors que le marché des logiciels de sécurité devrait enregistrer une croissance annuelle moyenne de 14,6% sur la même période.

Selon IDC, le marché des SVM sera également porté par les besoins importants des entreprises et des administrations en faveur d'un plus grand niveau de sécurisation du poste client (*Endpoint security*).

Aujourd'hui, le marché entier semble se dépêcher de proposer une forme de sécurité Endpoint. L'enjeu est grand : d'après le Yankee Group, le marché des produits de sécurité Endpoint à distance (REPS) pour les entreprises représentait 20 millions de dollars en 2001 et atteint les 260 millions de dollars en 2006.

De plus, 60% des données d'entreprise sont présentes sur les postes de travail de façon non protégées et le vol de données a coûté USD 50 Milliards aux sociétés américaines en 2004.

La moitié des incidents informatiques sont d'origine interne et 70% des violations de sécurité générant des pertes d'une valeur de plus de USD 100.000 sont effectués depuis l'intérieur des entreprises.

Les nouvelles législations, comme les lois Sarbanes-Oxley et HIPAA aux Etats-Unis, créent de nouveaux standards en termes de confidentialité des données et d'audit. La plupart de ces législations mentionnent explicitement le contrôle des médias amovibles de stockage.

Apple a vendu plus de 11 millions d'iPods, dont certains peuvent stocker jusqu'à 60Go de données, dans les six premiers mois de l'année 2005. Plus d'un milliard de dispositifs USB ont été vendus à ce jour. Cinq millions de dispositifs Bluetooth sont vendus toutes les semaines.

Mobilegov dispose donc d'une fenêtre d'action de trois ans pour s'imposer sur un marché où le besoin immédiat est considérable. Nous offrons une technologie parfaitement adaptée à la demande ainsi qu'une barrière technologique protégée par ses brevets de propriété industrielle. Nous offrons surtout la possibilité d'étendre nos techniques de sécurité à de nouveaux domaines.

A court terme, Mobilegov cible tous les utilisateurs d'équipements informatiques qui nécessitent plus de sécurité. Ceci concerne particulièrement les administrations publiques, les sociétés qui gèrent des flottes importantes d'équipements mobiles, qui souhaitent combattre le vol d'information ou encore qui souhaitent arrêter les modifications matérielles utilisées par exemple pour pirater les jeux vidéo.

A plus long terme, nous travaillons avec le CNRS à la normalisation des couches de sécurité de façon à intégrer la reconnaissance des composants dans les systèmes.

A partir de l'expérience de ses fondateurs dans les équipements mobiles, Mobilegov se focalise en premier lieu sur ces nouvelles niches à forte croissance. Il y a actuellement un nombre croissant et une diversité d'équipements mobiles utilisés par les Entreprises et les Administrations Publiques Européennes pour accéder de manière sécurisée aux informations sensibles.

Mobilegov cible un marché existant mais en croissance rapide, qui démarre son développement et qui explosera en 2008 avec la généralisation des documents d'identité électroniques biométriques.

Les principaux marchés verticaux visés concernent toutes les applications intégrant des composants numériques dont la modification constitue une faille ou un enjeu :

Ordinateurs & périphériques :

postes clients, PDA, serveurs, etc.) et réseaux d'entreprises auxquels ils se connectent.

Téléphonie :

centraux téléphoniques, périphériques téléphonie dont mobiles, Blackberry, etc.). Inclut bien entendu la téléphonie sur Internet, ainsi que les équipements de routage de l'Internet.

Défense/Sécurité/Douanes/ Justice :

futur marché lié aux usages des cartes d'identité électroniques, et notamment biométriques.

D'autres marchés peu prioritaires aujourd'hui seront adressés selon les opportunités et les ressources disponibles :

- Media, vidéo à la demande, set top box, TV interactive...
- Systèmes bancaires, ATM et paiements en ligne aujourd'hui, systèmes basés sur l'authentification forte du client demain
- Jeux, consoles de jeux vidéo, jeux en réseau, bourse en ligne,
- Service de tiers de confiance, ventes/enchères en ligne, etc.
- Automobile (chronotachygraphes, EEPROM...)
- Energie, compteurs électriques, compteurs de gaz, etc.

8.2.2. Canal de distribution

Etant éditeur de logiciel, Mobilegov a mis en place un réseau de distribution Européen, essentiellement constitué de très gros acteurs afin de s'imposer rapidement comme la solution de référence dans son marché et de se doter d'un outil de distribution puissant. Des négociations sont en cours pour étendre ce réseau.

Le réseau de MobileGov s'étend rapidement aussi grâce à des partenariats déjà engagés avec des administrations publiques (Commission Européenne, Europol, Eurojust, le FEDICT belge, Ministère de l'Intérieur Belge, la Chancellerie Autrichienne). Mobilegov étant impliquée dans d'importants projets européens (eJustice et R4eGov qui développent des solutions interopérables à base de cartes d'identité à puce entre ces différents états), la société bénéficie d'une forte crédibilité sur ces marchés.

Aujourd'hui le réseau de distribution de Mobilegov est constitué d'un ensemble de grossistes et d'intégrateurs dont certains sont les leaders sur le marché de la sécurité : IP Vista, SPIE Communication, NextiraOne, Prossi, Quadria-Euralliance (France), LogicaCMG, RMT, Onyx Group, ITPS (UK), DNP Global (Inde), Nexway (Internet). Thales, Accenture et Unisys ont également mis les solutions Mobilegov dans leur boite à outils de solutions de sécurité, en démonstration dans leurs centres d'excellence.

Mobilegov distribue également sa technologie par le biais d'accords d'intégration avec d'autres éditeurs de logiciels.

La technologie Mobilegov est en cours d'évaluation par des grands groupes technologiques (ORANGE R&D, ST Microelectronics, Gemalto) qui envisagent de l'intégrer dans leurs propres produits.

Enfin, Mobilegov démarre le programme de partenariat technologique de Microsoft, IDEES.

MobileGov présente donc des barrières à l'entrée du marché, tant technologiques que légales, positionnant la société en acteur incontournable tant sur le marché des Endpoints que sur le marché de la sécurité des équipements mobiles pour les années à venir.

8.3. Produits commercialisés

Mobilegov commercialise deux lignes de produits :

- Device Authenticator
- Device Linker

Il s'agit de suites logicielles distribuées via un réseau constitué de grossistes, de revendeurs et d'intégrateurs spécialisés dans la sécurité informatique.

La Société propose également la fourniture de solutions sur mesure directement implémentées dans des logiciels ou des équipements existants (cibles : Editeurs de logiciels et fabricants de composants ou d'équipements).

8.3.1. Device Authenticator

Device Authenticator protège un ordinateur ou un groupe d'ordinateurs contre des branchements de périphériques non préalablement autorisés, notamment à mémoire, reliés avec ou sans fil.

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

Le produit 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.

Device Authenticator s'adresse à toute organisation souhaitant protéger ses données informatiques : PME, grand groupe, administrations publiques. Le produit complète (mais ne vise pas à remplacer) les outils de sécurité déjà en place : contrôle d'accès, sécurité réseau, firewall, antivirus, etc.

8.3.2. Device Linker

Device Linker garantit qu'un périphérique (comme par exemple une clé USB) ne puisse fonctionner que sur une configuration définie, rendant ainsi inexploitables les données d'une clé perdue ou volée.

Il existe trois versions commerciales du produit :

- Device Linker Single Edition : le logiciel est livré sur une clé USB (voir photo). Il s'adresse aux particuliers, et il permet de stocker de façon très sûre des données sensibles (mots de passe par exemple). Dans cette version, une clé peut être personnalisée pour fonctionner sur un ou plusieurs ordinateurs, mais un ordinateur ne pourra reconnaître qu'une seule clé Device Linker. Depuis décembre 2007, le logiciel est commercialisé sous forme de téléchargement sur les sites de notre partenaire Nexway nous permettant d'être présent sur les grands sites français de e-commerce : darty.com, fnac.com, pixmania.com, orange.fr, alice.fr, free.fr, etc.
- Device Linker SOHO : le logiciel est livré sur un CD-Rom, et il permet de personnaliser des clés USB de type U3 du commerce. Dans cette version, une clé peut être personnalisée pour fonctionner sur un ou plusieurs ordinateurs, et un ordinateur peut reconnaître plusieurs clés Device Linker. Le produit s'adresse aux PME et aux travailleurs indépendants.
- Device Linker PRO : cette version présente les mêmes caractéristiques que la version SOHO, et offre en outre un logiciel de gestion centralisé des clés de l'entreprise. Le produit s'adresse aux grandes entreprises et aux administrations publiques.

Mobilegov propose la conception et la fabrication de clés USB aux couleurs du client, personnalisées électriquement de façon à faciliter la gestion et le fonctionnement optimisé avec Device Authenticator.

8.4. Technologie Mobilegov

Mobilegov a breveté un procédé et développé un noyau dur technologique. A partir de ce noyau dur, plusieurs produits sont déclinés.

La technologie Mobilegov concerne aussi bien le procédé que sa mise en œuvre pour élaborer des produits commerciaux ergonomique, fiables et efficaces.

Le principe de fonctionnement de la technologie de Mobilegov consiste en deux étapes distinctes, l'enregistrement et l'authentification :

1. Enregistrement : avant qu'un système ne soit déclaré bon pour exécuter une tâche, il passe par une étape, contrôlée par un opérateur habilité, pour produire, chiffrer et stocker la liste des identifiants de ses composants.

Chaque composant d'un système peut être défini comme étant obligatoire, optionnel ou interdit :

- Obligatoire : le composant doit être présent dans le système pour qu'il soit autorisé à fonctionner.
- Optionnel : le composant peut être présent ou pas.
- Interdit : le composant ne peut pas être présent. La détection d'un tel composant interdira le fonctionnement. Par défaut, tout composant non autorisé est interdit.

2. Validation : à chaque fois que le 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.

8.4.1. Principe

Mobilegov s'appuie sur une propriété générale difficilement falsifiable des composants matériels. Sa technologie est donc indépendante des environnements (systèmes d'exploitation) ou des applications. Elle s'applique aussi bien à un PC connecté sur un réseau qu'à une carte d'un central téléphonique ou un chronotachygraphe d'un poids lourd.

Mobilegov développe à partir du noyau dur de sa technologie des logiciels facilement intégrables dans des applicatifs existants grâce à leur structure modulaire. Nous développons également des solutions clé en main (s'appuyant sur ces mêmes composants) avec une interface simple et ergonomique pour gérer des flottes de matériel, comme par exemple les milliers de PC d'un réseau d'entreprise.

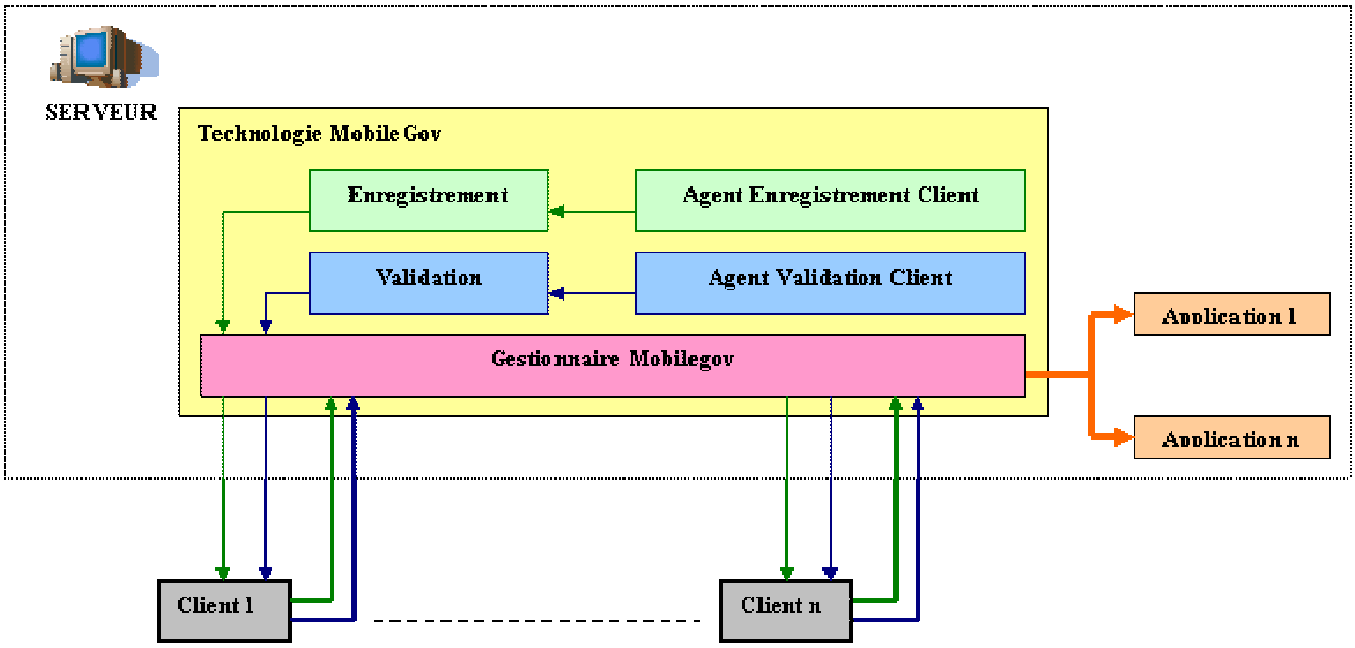
La technologie est portable et permet également de proposer des services en ligne (web services).

8.4.2. Une flexibilité nouvelle pour la sécurité

Des données contextuelles peuvent être intégrées lors de l'enregistrement. Par exemple, si un système ne doit 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).

8.4.3. Utilisation de l'existant

Les agents collectent les identifiants uniques des composants. Ces identifiants sont présents dans la plupart des périphériques matériels et composant logiciels existants : l'IMEI pour les téléphones portables, le numéro de série pour les disques durs, les processeurs, les barrettes mémoire, les lecteurs CDROM, les clés USB, etc..., les Globally Unique Identifier (GUID) et les ClaSs Identifier (CLSID) pour les composants logiciels. Ces identifiants sont utilisés par exemple pour faciliter l'installation de nouveaux périphériques sous Windows, Linux, MacOS, etc. ainsi que pour vérifier la compatibilité logicielle.

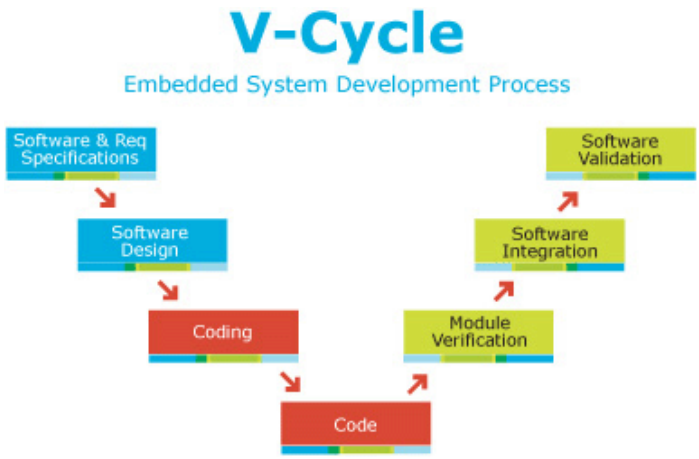
Le processus générant la liste des identifiants est un programme Java qui intègre un système de signature pour sécuriser la tâche demandant une validation. Il est donc très portable et difficilement falsifiable.

En conséquence, Mobilegov est compatible avec la plupart des périphériques (internes ou externes) et systèmes d'exploitation existants (Windows, Linux, MacOS, Solaris, Propriétaires, Embarqués…). Aucune remise en cause d'architecture ou de choix matériel ou logiciel n'est nécessaire.

8.4.4. Le 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 œuvre 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 :



Une road map technique a été développée et suivie avec chaque Beta testeur au cours de nombreuses réunions. 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 certification externes par des organismes de renoms.

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.

8.4.5. Une organisation expérimentée et performante

L'équipe en place possède l'expérience nécessaire pour faire de Mobilegov un succès.

Les trois fondateurs ont précédemment étudié, développé et implémenté une solution mobile innovante utilisée dans la rue par les Forces de Polices des villes de Cannes (France) et de Vintimille (Italie). Ce fut un résultat important des projets Européens pour les Administrations publiques en 2003. Cette expérience leur a permis de bâtir une solide expertise dans l'utilisation, la technologie et la gestion d'applications pour les employés des administrations publiques.

L'équipe de Mobilegov dispose d'une compétence prouvée dans les solutions « mobiles ». La technologie créée est le fruit de plusieurs années de recherches et d'expérimentations.

Aux fondateurs se sont ajoutés en 2007 deux cadres de haut niveau :

- Philippe MAZURIER, Directeur Commercial, 40 ans, de formation Ingénieur, expérience internationale, 14 ans d'expérience en tant qu'ingénieur commercial dans des grands groupes (qui distribuent aujourd'hui les produits Mobilegov).
- Jean-Bernard LAVAURY, Directeur de Projets, 49 ans, dont 25 ans d'expérience de R&D au sein du Groupe Thales, et plusieurs années d'expérience commune avec Michel FRENKIEL.

Michel FRENKIEL

Cofondateur & Président (60 ans) :

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 Ingénieur Arts et Métiers et Master of Science de l'Université du Colorado. 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 (39 ans) :

François-Pierre Le Page est diplômé du CERAM Sophia Antipolis et de l'Université de Phoenix Arizona (MBA). Bilingue Français Anglais, M. Le Page est Expert auprès de la Commission Européenne au sein de la Direction Générale de la Société de l'Information, dans les programmes R&D IST, eTEN et eContentplus.

Il 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 », publié par UK International Press au Royaume-Uni et 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 Technique (36 ans)

Eric Mathieu est 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 solution 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/)

8.5. Marchés et positionnement concurrentiel de la société

8.5.1. 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.

L'avancée rapide des technologies sans fil permet de nouveaux services mais aussi des opportunités d'affaires attractives pour les fournisseurs d'accès, les fournisseurs de contenu et les fabricants d'équipements mobiles.

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.

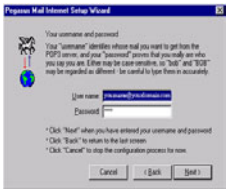
Le besoin d'un système de sécurité efficace a été renforcé par des évènements terroristes dramatiques. Ces évènements ainsi que le crime organisé et l'immigration clandestine ont encouragé les Etats à adopter des documents d'identité biométriques intégrant des cartes à puce.

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



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.

Cette solution ne protège pas contre les modifications de configuration du système qui demande l'accès au service.

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.

Mobilegov a développé une technologie innovante et brevetée, capable de vérifier qu'un périphérique ou un groupe de périphériques (éléments matériels et logiciels) n'a pas été modifié depuis qu'ils ont été autorisés à effectuer des tâches spécifiques. Nous proposons d'adapter cette technologie à un grand nombre de marchés, de façon à leur apporter la sécurité dont ils ont besoin.

8.5.2. Concurrence

Mobilegov a conduit début 2006 une étude de la concurrence en partenariat avec le CERAM Sophia Antipolis. Cette étude menée sur l'ensemble du globe a révélé un certain nombre de concurrents, plus ou moins directs mais uniquement focalisés sur des clones du produit MobileGov Device Authenticator. Il s'agit des sociétés suivantes :

1. SecureWave (Luxembourg) :
2. Centennial Software (Royaume-Uni)
3. Skyrecon (France)
4. Safend (Israël)
5. ControlGuard (Israël)
6. SmartLine (U.S.A)
7. GFI (U.S.A)
8. DaVinsi (Belgium)
9. Toplang (U.S.A)
10. Lync Software (Australia)

Les concurrents les plus proches de la technologie de MobileGov sont :

1. SecureWave (Luxembourg) :
2. Centennial Software (Royaume-Uni)
3. Safend (Israël)
4. ControlGuard (Israël)

Ces sociétés ont pour la plupart effectué des augmentations de capital supérieure à un million d'€ dans les deux dernières années. Malgré leur capacité financière, leur concurrence se limite en général deux aspects essentiels :

1. Focalisation sur les clés USB (alors que Mobilegov s'intéresse à tous les types de composants, internes et externes, avec et sans fil).
2. Focalisation sur la sécurité des PC sous Windows. Aucune de ces sociétés ne dispose d'une technologie portable sur des périphériques et autres environnement (Linux, Mac, etc.).

Ceci donne une avance technologique de deux ans environ à MobileGov, lui permettant de développer une gamme de produits en avance sur ses concurrents.

De plus, Mobilegov a été contactée par SecureWave et Centennial, qui sont les deux entreprises les plus importantes de la liste, et qui souhaitent intégrer sa technologie dans leurs solutions. En effet, la technologie de MobileGov permet d'identifier de façon certaine un périphérique (ce que Centennial ne sait pas faire puisque les solutions proposées ne permettent d'interdire que des familles de périphériques). Elle offre la capacité de gérer les périphériques qui se connectent via un relais tel qu'un PDA (ce que ni SecureWave ni l'ensemble des autres concurrents ne sait faire).

Cependant, étant donné leur taille relativement importante, ces concurrents disposent aujourd'hui d'un réseau de distribution notable et qui ne cesse de grandir en Europe et aux USA.

Malgré les recherches de la société, il est resté difficile d'évaluer la capacité financière exacte de ces concurrents. Ils sont en général mono produit, ce qui donne un avantage essentiel à MobileGov. Nous attaquons leur marché grâce à notre technologie brevetée, qui permet en outre de créer une large gamme de produits à l'opposé des concurrents.

Afin de lutter sur un terrain qui nous est favorable, nous avons identifié des acteurs complémentaires. Ils sont :

- ORANGE R&D
- ST Microelectronics
- Gemalto
- Arkoon (France)

Ces acteurs ont été identifiés pour leur besoin d'identifier des composants numériques afin d'améliorer leurs produits.

Des accords ont été signés avec France Telecom R&D, Criston et Arkoon. ST Microelectronics, Gemalto et Mobilegov, tous trois partenaires dans le Pôle de Compétitivité SCS, ont signé un accord global dans le cadre du Pôle.

Enfin, l'ensemble des offres concurrentes reposant sur l'environnement Windows, l'intégration de la technologie Mobilegov dans Windows Vista, en cours de négociation avec Microsoft, devrait donner à Mobilegov un avantage compétitif certain.

Company	MobileGov	SecureWave	Layton Tech.	SmartLine	Centennial	USB-Blocker	Cynapspro	GFI	Safend	PointSec	Skyrecon	ControlGuard	SafeBoot	Promisec	Senforce
Product	Authenticato	ary Device C	DeviceShield	DeviceLock	DeviceWall		DevicePro	dPoint Secur	Protector	evice Protect	Stormshield	Point Access	Port Control	Spectator Pro	ESS
Tested	N/A	ally (2 compu	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No	No	No
Web	N/A	◇◇◇◇	◇◇◇◇◇	◇◇◇◇◇	◇◇◇◇◇	◇◇◇	◇◇◇◇	◇◇◇◇◇	◇◇◇◇◇	◇◇◇	◇◇◇	◇◇◇◇	◇		◇◇
Danger Rank	N/A	◇◇◇◇◇	◇◇◇	◇◇◇◇	◇◇◇◇◇	◇◇◇	◇◇◇◇	◇◇◇	◇◇◇◇◇	◇◇◇	◇◇◇	◇◇◇◇		◇	
Easy to use															
Install	◇◇◇◇	◇	◇◇◇	◇◇	◇◇◇◇	◇◇◇	◇◇◇	◇◇◇◇							
Interface	◇◇◇◇	◇	◇◇◇	◇	◇◇◇◇◇	◇	◇◇◇◇	◇◇◇◇							
Deploy	◇◇◇◇	◇◇	◇◇◇	◇	◇◇◇◇	◇◇	◇◇	◇◇◇◇							
Size	30 Mb	350 Mb	15 Mb	4 Mb	60 Mb	28 Mb	8 Mb	11 Mb			7 Mb				
Deploy															
Custom (GPO, SMS…)	Yes	No	Yes	No	No	No	No	No	No						
Active Directory	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes		
Novell eDirectory	No	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes		
Policies															
Computers	Yes	No	Yes	No	No		No	No							
Users	No	Yes	No	Yes	Yes	Yes	Yes	Yes			Yes	Yes			
Time Restrictions	No	No	No	Yes	No	No	Yes	No				Yes			
Families Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	USB Only			Yes	Yes
Devices Management	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes				No	Yes
PDA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes							
RT Policy Change	Yes	Yes	???	???	???	???	???	???							
Reports															
Logs & Alerts	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes		Yes		Yes			Yes
Real Time	Yes	Yes	No	Yes	Yes	No	Yes	Yes				Yes			Yes
Search Tools	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes				Yes			Yes
Agent															
Tool	Yes	-	-	-	-	-	-	-	-						
Kernel	-	Yes	-	-	-	-	Yes	-	-		Yes				
Service	-	-	-	Yes	Yes	Yes	-	Yes	Yes			Yes			
Offline Mode	Yes	Yes	No	No	Yes	No	No	No		Yes					
Permissive Mode	Yes	Yes	No	No	Yes	No	No	No							
Security															
Encrypted Data	Yes	No	No	No	No	No	No	No			Yes				
Communications SLL, X509	Yes	No	No	No	No	No	No	No			Yes				
Others															
Computer Internal Integrity	Yes	No	No	No	No	No	No	No							
Password Temporary Unlock	Yes	No	No	No	No	No	No	No							
Backup & Restore	Yes	No	No	No	No	No	No	No					Yes		
File Transfer Control (R/W/Size…)	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes				Yes
Different policies for online/offline	No	Yes	No	No	No	No	No	No							
Restrictions	No	NTFS only	No	No	NTFS Only	No	No	No							
CD/DVD Identification	No	No	No	Yes	No	No	No	No	Yes						
Autorun control	No	No	No	No	No	No	No	No	Yes						
Localizations	EN/FR	12	EN	EN	EN / JP	EN / DE	EN / DE	EN / DE	???						
FireWall	No	No	No	No	No	No	No	No			Yes				Yes
Antivirus	No	No	No	No	No	No	No	No		Yes	Yes				Yes
Keyloggers	No	Yes	No	Yes	No	No	No	No	Yes		Yes				
Customs enduser msgs	Upon Reques	Yes	No	No	No	No	Yes	No							
Vista	No	Yes	No	Yes	No	No	No	No	Yes	No					
DB (SQL Server EE)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes	Yes			
Comment	10M€ Turnover 2006					Scan from Service Agent Reboot				Certified Trainin		Live Update			Suite Logicielle

En conclusion, Device Authenticator surclasse les produits concurrents pour son ergonomie, sa facilité de mise en œuvre et la finesse de son analyse des attaques. En revanche, il peut être amélioré pour s'intégrer plus facilement dans les très grosses configurations.

Il convient de noter que la finesse d'analyse résulte directement de l'exploitation de notre brevet, et peut donc être difficilement améliorée par nos concurrents. En revanche, l'amélioration nécessaire aux grosses configurations s'obtient en intégrant des éléments de l'état de l'art, tels que le support LDAP, et ne présente aucune barrière à l'entrée.

Device Linker n'a à ce jour aucun concurrent. L'intégration de sa technologie dans les disques durs et dans les microcontrôleurs est à l'étude avec des constructeurs de disques et avec des constructeurs de puces et de cartes à puces.

8.6. Forces et positionnement concurrentiel

8.6.1. Forces

Les points forts sont :

- 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

- 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 exceptionnel

8.6.2. Faiblesses

Les points faibles sont :

- Petite taille de la société (résolue en partie par les partenariats)
- Réseau de distribution constitué en 2007, qui n'a donc pas encore généré de chiffre d'affaires significatif
- Réseau de distribution axé principalement sur France et UK à ce jour : nous devons nous positionner sur les marchés Allemand et Américain.

8.6.3. Opportunités

Les opportunités sont :

- Décollage avéré du marché des Endpoints (grande tendance qui va exploser avec l'arrivée de la convergence Informatique, Telecom, Multimédia).
- Le besoin est nouveau, les Entreprises prennent juste conscience qu'une faille de sécurité importante réside dans les matériels.
- Croissance rapide du marché de la sécurité, plus de 20% par an.
- L'environnement politique est favorable (lancement des cartes d'identité à puce et des nouveaux passeports biométriques)

8.6.4. 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 l'entrée sur le marché permet de régler ce problème).
- Le marché des administrations publiques est un marché avec un cycle de vente long (plusieurs mois) mais il est compensé par des cycles plus courts du côté des entreprises et par la mise en place d'une solution d'affacturage.

8.7. 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 ».

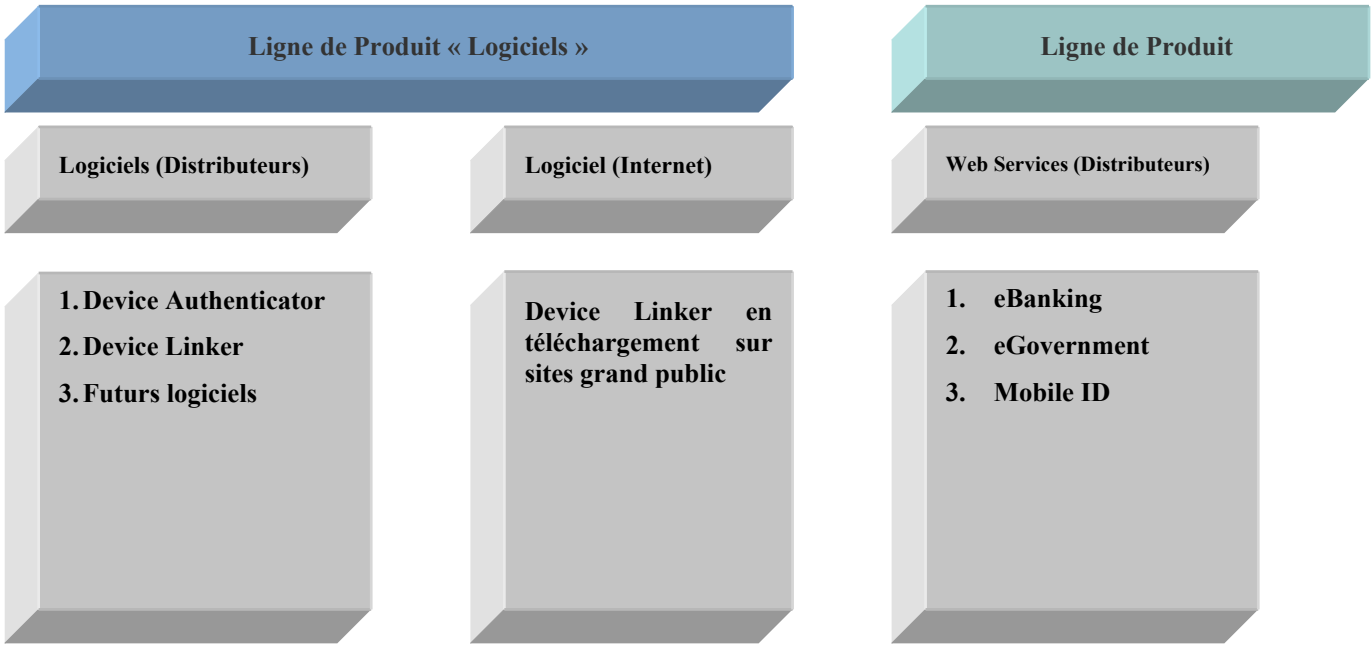
L'identité difficilement falsifiable des composants matériels, que nous appelons leur ADN numérique, est à la base d'une telle solution que nous avons brevetée.

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.

8.8. Stratégie

En tant qu'éditeur de solutions innovantes de sécurité, Mobilegov souhaite développer un réseau Européen et mondial de distributeurs, d'intégrateurs et de revendeurs spécialisés avant 3 ans.

La stratégie utilisée est donc de développer progressivement ces réseaux par grandes zones géographiques et par type de produit.



A ce jour, aucun des concurrents de Mobilegov n'a encore signé avec des grossistes majeurs tels que IP Vista en France (2 000 distributeurs) ou encore d'importants intégrateurs (tels que Unisys ou Accenture) ce qui donne un avantage concurrentiel important à Mobilegov.

Pour développer son réseau, Mobilegov a identifié les distributeurs avec lesquels l'entreprise souhaite travailler et organise depuis septembre 2006 des présentations commerciales aux clients de ses distributeurs. Aujourd'hui, un spécialiste de Mobilegov travaille à mi-temps chez IP Vista pour former et accompagner ses ingénieurs.

Cependant afin de motiver l'adoption des technologies par ces distributeurs, Mobilegov a validé au préalable leur efficacité auprès de prescripteurs importants de l'Industrie, de l'Administration et de la Recherche.

L'objectif est donc de capter des parts de marché après avoir convaincu des distributeurs en Europe et aux USA. Après avoir validé leur potentiel, la société leur offre l'exclusivité, pour une gamme de produits identifiée. Elle développe aussi un maximum d'accords OEM avec fabricants d'équipements, à qui Mobilegov apporte grâce à sa sécurité une valeur ajoutée concurrentielle.

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 Européens de grande envergure (eJustice et R4eGov) et travaille avec le CNRS.

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 à quelques mois.

6. L'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: Organigramme

Michel Frenkiel (Président)	François-Pierre Le Page (Directeur Général)	Eric Mathieu Directeur Technique
	Philippe Mazurier (Directeur Commercial)	Jean-Bernard Lavaury (Directeur des Projets)
Sophia Antipolis (France) - 2 Ingénieurs Commerciaux - 2 Ingénieurs Logiciel Senior - 4 Ingénieurs Logiciel - 1 Ingénieur Qualité - 1 Thésard CIFRE	**Londres (Royaume Uni)** Entreprise créée et accompagnée, à staffer En cours de recrutement : - 1 Business Dev Manager - 1 Chargé de clientèle	**New York (USA)** A créer
Total France : 15	**Total UK : 0**	**Total USA : 0**

Chapitre 10

Chapitre 10: Recherche & Développement et marques

10.1. Recherche et 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.

Les produits de haute technologie Mobilegov sont développés par l'équipe de Recherche et Développement. Cette équipe constituée de sept ingénieurs sous la responsabilité d'un Directeur de Projets et d'un Directeur Technique.

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 le département chargé de la définition des produits, ceci afin d'optimiser les développements, réduire leurs coûts et leur temps de développement pour assurer ainsi une pleine adéquation entre développement et produit.

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 Europol, Eurojust, la Chancellerie Autrichienne.

Enfin, 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.

10.2. Brevets, marques et noms de domaine

Mobilegov a déposé un premier brevet européen fin 2004, étendu début 2006 à l'Amérique du Nord.

Un second brevet est en cours de préparation.

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.

La Société est propriétaire des noms de domaine suivants : 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.

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.

11.2. Tendances et perspectives de la Société

Sur un marché en forte croissance, la Société connaît une progression constante et importante de son chiffre d'affaire.

La tendance du marché qui se dégage actuellement est une forte croissance du besoin en sécurisation des « Endpoints », confirmée par plusieurs affaires retentissantes.

Les indicateurs du marché confirment cette tendance : la progression sera d'au moins 20% par an sur les 5 prochaines années et devraient passer les 400 millions d'euros en 2008 à 744 millions d'euros en 2010.

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 1137, Chemin de Peyniblou 06560 Valbonne	Président
François-Pierre LE PAGE Jardins d'Angélique 801 Chemin du Malvan 06570 SAINT PAUL	Administrateur – Directeur Général
Eric MATHIEU Résidence La Capitainerie 95 avenue des Frères Roustan 06220 Golfe Juan	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

Michel FRENKIEL est gérant de IST Consultants, une SARL immatriculée à Antibes sous le n° 421 714 528 spécialisée dans le conseil en matière de sécurité et de eGouvernement. IST Consultants est particulièrement active dans les projets européens de R&D.

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 2006, Michel FRENKIEL a perçu 0€ 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 26 666,66€, dont 0 euros en part variable.

Sur la même période, les sommes allouées à Eric MATHIEU au titre de ses fonctions s'élèvent à 0€, 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	90 000
François-Pierre LE PAGE	Administrateur	AGE 5 août 2006	31/12/2011	70 000
Eric MATHIEU	Administrateur	AGE 5 août 2006	31/12/2011	70 000

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 Ltd.	110 000	23,96%
Benoît de Maulmin	24 193	5,27%
IST Consultants	20 000	4,36%
Léon Frenkiel	19 000	4,14%
Valérie Podelski	16 129	3,51%
Claude Chausse	12 903	2,81%
Alain Vauthier	9 677	2,11%
Martin Eisenberg	8064	1,76%
Lucile Marsac-Huignard	8 064	1,76%
Nombre total d'actions tous actionnaires confondus		
Total	459 030	**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 cinq principaux actionnaires de la Société, détiennent 75 % du capital avant introduction en Bourse.

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 2006

Mesdames, Messieurs, les Actionnaires,

En notre qualité de commissaire aux comptes de votre société, nous devons vous présenter un rapport sur les conventions règlementées dont nous avons été avisés. Il n'entre pas dans notre mission de rechercher l'existence éventuelle de telles conventions. Nous vous informons qu'il ne nous a été donné avis d'aucune convention visée à l'article L. 225-38 du Code de commerce.

Fait à Sophia-Antipolis, le 14 juin 2007

Le Commissaire aux comptes

Experts & Associés International

Stéphan BRUN

Chapitre
17

Chapitre 17: Informations financières et historiques de la société

17.1. Comptes semestriels au 30 juin 2007

17.1.1. Bilan – Actif

ACTIF	du 01/01/2007 au 30/06/2007 (6 mois)				Exercice précédent 31/12/2006 (12 mois)	
	Brut	Amort. & Prov	Net	%	Net	%
Capital souscrit non appelé (0)						
Actif Immobilisé						
Frais d'établissement						
Recherche et développement	111 263	6 257	105 006	35,49	61 922	26,56
Concessions, brevets, marques, logiciels et droits similaires	1 220	1 220			336	0,14
Fonds commercial						
Autres immobilisations incorporelles						
Avances & acomptes sur immobilisations incorporelles						
Terrains						
Constructions						
Installations techniques, matériel & outillage industriels						
Autres immobilisations corporelles	7 908	2 474	5 434	1,84	5 815	2,49
Immobilisations en cours						
Avances & acomptes						
Participations évaluées selon mise en équivalence						
Autres Participations						
Créances rattachées à des participations						
Autres titres immobilisés						
Prêts						
Autres immobilisations financières	2 159		2 159	0,73	1 905	0,82
TOTAL (I)	***122 550***	***9 951***	***112 599***	38,05	***69 977***	30,01
Actif circulant						
Matières premières, approvisionnements	10 215		10 215	3,45		
En cours de production de biens						
En cours de production de services						
Produits intermédiaires et finis						
Marchandises						
Avances & acomptes versés sur commandes						
Clients et comptes rattachés	58 637		58 637	19,82	87 804	37,66
Autres créances						
. Fournisseurs débiteurs						
. Personnel					6 000	2,57
. Organismes sociaux	3 992		3 992	1,35	4 384	1,88
. Etat, impôts sur les bénéfices	53 201		53 201	17,98	17 085	7,33
. Etat, taxes sur le chiffre d'affaires	28 719		28 719	9,71	29 524	12,66
. Autres	1 644		1 644	0,56	1 544	0,66
Capital souscrit et appelé, non versé						
Valeurs mobilières de placement						
Disponibilités	24 084		24 084	8,14	15 159	6,50
Charges constatées d'avance	2 814		2 814	0,95	1 666	0,71
TOTAL (II)	***183 306***		***183 306***	61,95	***163 166***	69,99
Charges à répartir sur plusieurs exercices (III)						
Primes de remboursement des obligations (IV)						
Ecarts de conversion actif (V)						
TOTAL ACTIF (0 à V)	***305 856***	***9 951***	***295 905***	100,00	***233 143***	100,00

17.1.2. Bilan – Passif

PASSIF	du 01/01/2007 au 30/06/2007 (6 mois)		du 01/01/2006 au 31/12/2006 (12 mois)	
Capitaux propres				
Capital social ou individuel (dont versé : 38 000)	**38 000**	12,84	**38 000**	16,30
Primes d'émission, de fusion, d'apport ...	69 000	23,32	69 000	29,60
Ecarts de réévaluation				
Réserve légale	12	0,00	12	0,01
Réserves statutaires ou contractuelles				
Réserves réglementées				
Autres réserves	210	0,07	210	0,09
Report à nouveau	-65 491	-22,12		
Résultat de l'exercice	***-77 868***	-26,31	***-65 491***	-28,08
Subventions d'investissement				
Provisions réglementées				
TOTAL(I)	***-36 136***	-12,20	***41 731***	17,90
Produits des émissions de titres participatifs				
Avances conditionnées				
TOTAL(II)				
Provisions pour risques et charges				
Provisions pour risques				
Provisions pour charges				
TOTAL (III)				
Emprunts et dettes				
Emprunts obligataires convertibles				
Autres Emprunts obligataires				
Emprunts et dettes auprès des établissements de crédit				
. Emprunts	150 000	50,69	75 000	32,17
. Découverts, concours bancaires				
Emprunts et dettes financières diverses				
. Divers	313	0,11		
. Associés	99 000	33,46	32 000	13,73
Avances & acomptes reçus sur commandes en cours				
Dettes fournisseurs et comptes rattachés	25 350	8,57	19 744	8,47
Dettes fiscales et sociales				
. Personnel	9 611	3,25	10 837	4,65
. Organismes sociaux	35 954	12,15	32 441	13,91
. Etat, impôts sur les bénéfices				
. Etat, taxes sur le chiffre d'affaires	14 828	5,01	15 773	6,77
. Etat, obligations cautionnées				
. Autres impôts, taxes et assimilés				
Dettes sur immobilisations et comptes rattachés				
Autres dettes	-3 014	-1,01	5 616	2,41
Produits constatés d'avance				
TOTAL(IV)	***332 041***	112,21	***191 411***	82,10
Ecart de conversion passif (V)				
TOTAL PASSIF (I à V)	***295 905***	100,00	***233 143***	100,00

17.1.3. Compte de résultat

COMPTE DE RÉSULTAT			du 01/01/2007 au 30/06/2007 (6 mois)		Exercice précédent 31/12/2006 (12 mois)		Variation absolue (6 / 12)	%
	France	Exportation	Total	%	Total	%	Variation	%
Ventes de marchandises								
Production vendue biens								
Production vendue services	39 058	21 331	60 389	100,00	67 762	100,00	-7 373	-10,87
Chiffres d'Affaires Nets	**39 058**	**21 331**	**60 389**	100,00	**67 762**	100,00	**-7 373**	-10,87
Production stockée								
Production immobilisée			49 307	81,65	61 956	91,43	-12 649	-20,41
Subventions d'exploitation			30 600	50,67			30 600	N/S
Reprises sur amortis. et prov., transfert de charges								
Autres produits			336	0,56	194	0,29	142	73,20
Total des produits d'exploitation			***140 633***	232,88	***129 912***	191,72	***10 721***	8,25
Achats de marchandises (y compris droits de douane)								
Variation de stock (marchandises)								
Achats de matières premières et autres approvisionnements			10 215	16,92	1 080	1,59	9 135	845,83
Variation de stock (matières premières et autres approv.)			-10 215	-16,91			-10 215	N/S
Autres achats et charges externes			77 721	128,70	90 930	134,19	-13 209	-14,52
Impôts, taxes et versements assimilés			1 197	1,98	1 964	2,90	-767	-39,04
Salaires et traitements			119 944	198,62	83 790	123,65	36 154	43,15
Charges sociales			45 308	75,03	32 458	47,90	12 850	39,59
Dotations aux amortissements sur immobilisations			7 754	12,84	2 197	3,24	5 557	252,94
Dotations aux provisions sur immobilisations								
Dotations aux provisions sur actif circulant								
Dotations aux provisions pour risques et charges								
Autres charges			2 450	4,06	25	0,04	2 425	N/S
Total des charges d'exploitation			***254 374***	421,23	***212 443***	313,51	***41 931***	19,74
RÉSULTAT D'EXPLOITATION			**-113 742**	-188,34	**-82 531**	-121,79	**-31 211**	-37,81
Bénéfice attribué ou perte transférée								
Perte supportée ou bénéfice transféré								
Produits financiers de participations								
Produits des autres valeurs mobilières et créances								
Autres intérêts et produits assimilés								
Reprises sur provisions et transferts de charges								
Différences positives de change			86	0,14			86	N/S
Produits nets sur cessions valeurs mobilières placement								
Total des produits financiers			***86***	0,14			***86***	N/S
Dotations financières aux amortissements et provisions								
Intérêts et charges assimilées			313	0,52			313	N/S
Différences négatives de change			15	0,02			15	N/S
Charges nettes sur cessions valeurs mobilières placements								
Total des charges financières			***328***	0,54			***328***	N/S
RÉSULTAT FINANCIER			**-242**	-0,39			**-242**	N/S
RÉSULTAT COURANT AVANT IMPÔTS			**-113 984**	-188,74	**-82 531**	-121,79	**-31 453**	-38,10

COMPTE DE RÉSULTAT (suite)	du 01/01/2007 au 30/06/2007 (6 mois)		Exercice précédent 31/12/2006 (12 mois)		Variation absolue (6 / 12)	%
Produits exceptionnels sur opérations de gestion						
Produits exceptionnels sur opérations en capital						
Reprises sur provisions et transferts de charges						
Total des produits exceptionnels						
Charges exceptionnelles sur opérations de gestion			45	0,07	-45	-99,99
Charges exceptionnelles sur opérations en capital						
Dotations exceptionnelles aux amortissements et provisions						
Total des charges exceptionnelles			***45***	0,07	***-45***	-99,99
RÉSULTAT EXCEPTIONNEL			**-45**	-0,06	**45**	100,00
Participation des salariés						
Impôts sur les bénéfices	-36 116	-59,80	-17 085	-25,20	-19 031	-111,38
Total des Produits	***140 719***	233,02	***129 912***	191,72	***10 807***	8,32
Total des Charges	***218 586***	361,96	***195 403***	288,37	***23 183***	11,86
RÉSULTAT NET	**-77 868** *Perte*	-128,93	**-65 491** *Perte*	-96,64	**-12 377**	-18,89
Dont Crédit-bail mobilier						
Dont Crédit-bail immobilier						

17.1.4. Annexes à la situation semestrielle au 30 juin 2007

PREAMBULE

Il s'agit de l'annexe de la situation intermédiaire arrêtée le 30/06/2007 (6 mois).

L'exercice précédent clos le 31/12/2006 avait une durée de 12 mois.

Le total du bilan de l'exercice avant affectation du résultat est de 322 543,81 Euros.

Le résultat net comptable est une perte de 77 867,51 Euros.

Les informations communiquées ci-après font partie intégrante des comptes annuels qui ont été établis le 1/12/2007 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.

3. NOTES SUR LE BILAN ACTIF

3.1- Frais de recherche & de développement = 111 263

Frais recherche & développement	Valeur brute	Amortissement	Valeur nette	Taux
Frais recherche & développement	*111 263*	*6 257*	*105 006*	*20 %*

3.2 - Actif immobilisé

Les mouvements de l'exercice sont détaillés dans les tableaux ci-dessous :

3.2.1 Immobilisations brutes = 122 550

Actif immobilisé	A l'ouverture	Augmentation	Diminution	A la clôture
Immobilisations incorporelles	*63 176*	*49 307*		*112 483*
Immobilisations corporelles	*7 093*	*815*		*7 908*
Immobilisations financières	*1 905*	*214*		*2 159*
TOTAL	*72 174*	*50 376*		*122 550*

3.2.2 – Amortissements et provisions d'actif = 9 951

Amortissements et provisions	A l'ouverture	Augmentation	Diminution	A la clôture
Immobilisations incorporelles	*919*	*6 558*		*7477*
Immobilisations corporelles	*1 278*	*1 196*		*2 474*
Titres mis en équivalence				
Autres Immobilisations financières				
TOTAL	*2 197*	*7 754*		*9 951*

3.2.3 – Détail des immobilisations et amortissements en fin de période

Nature des biens immobilisés	Montant	Amortissement	Valeur nette	Durée
Frais recherche & développement	*111 263*	*6 257*	*105 006*	*5 ans*
Concess. Brevets licences	*1 220*	*1 220*	*0*	*1 an*
Mat. bureau & informatique	*7 908*	*2 474*	*5 434*	*3 ans*
TOTAL	*120 391*	*9 951*	*110 440*	

3.3 – Etat des créances = 158 766

Etat des créances	Montant brut	A un an	A plus d'un an
Actif immobilisé	*2 159*		*2 159*
Actif circulant & charges d'avance	*156 607*	*156 607*	
TOTAL	*158 766*	*156 607*	*2 159*

3.4 – Produits à recevoir par postes du bilan = 57 680

Produits à recevoir	Montant brut
Immobilisations financières	
Clients et comptes rattachés	*57 680*
Autres créances	
Disponibilités	
TOTAL	*57 680*

3.5 – Charges constatées d'avance = 2 814

Les charges constatées d'avance ne sont composées que de charges ordinaires dont la répercussion sur le résultat est reportée à un exercice ultérieur.

3.6 – Informations complémentaires sur le bilan actif

Le montant des créances fait apparaître une créance d'impôt de 53 201 Euros représentant le crédit d'impôt recherche 2006 remboursée le 18/12/2007 (17 085 Euros, ainsi que le crédit d'impôt recherche du premier semestre estimé à 36 116 Euros).

Les produits à recevoir représentent le montant restant dû dans la prestation du projet CEE.

4. NOTES SUR LE BILAN PASSIF

4.1 – Capital social = 38 000

Mouvements des titres	Nombre	Val. Nominale	Capital social
Titres en début d'exercice	*380*	*100,00*	*38 000*
Titres émis ou variation du nominal			
Titres remboursés ou annulés			
Titres en fin d'exercice	*380*	*100,00*	*38 000*

4.2 – Etat des dettes = 339 641

Etat des dettes	Montant total	De 0 à 1 an	De 1 à 5 ans	Plus de 5 ans
Etablissements de crédit	*150 000*	*13 548*	*136 452*	
Dettes financières diverses	*99 313*	*313*	*99 000*	
Fournisseurs	*25 350*	*25 350*		
Dettes fiscales & sociales	*60 393*	*60 393*		
Dettes sur immobilisations				
Autres dettes	*4 586*	*4 586*		
Produits constatés d'avance				
TOTAL	*339 641*	*104 189*	*235 452*	

4.3 – Charges à payer par postes du bilan = 22 276

Charges à payer	Montant
Emprunts & dettes établ. de crédit	
Emprunts & dettes financières div.	*313*
Fournisseurs	*7 595*
Dettes fiscales & sociales	*14 369*
Autres dettes	
TOTAL	*22 276*

4.4 – Informations complémentaires sur le bilan passif

Les emprunts de 150 000 Euros représentent deux prêts participatifs, l'un de l'IAD de 75 000 Euros au taux de 5 % remboursable trimestriellement sur 5 ans ; l'autre prêt d'un montant de 100 000 Euros dont 75 000 Euros déjà versé de l'OSEO ANVAR remboursable sur 3 ans sans intérêts.

5. NOTES SUR LE COMPTE DE RESULTAT

5.1 - Ventilation du chiffre d'affaires = 60 389

Le chiffre d'affaires de l'exercice se décompose de la manière suivante :

Nature du chiffre d'affaires	Montant HT	Taux
Prestations de services	*54 584*	*90,39 %*
Produits des activités annexes	*5 805*	*9,61 %*
TOTAL	*60 389*	*100,00 %*

5.2 – Ventilation de l'impôt sur les bénéfices = -36 116

Niveau de résultat	Avant impôt	Impôt	Après impôt
Résultat d'exploitation	*- 113 742*		*- 113 742*
Résultat financier	*- 242*		*- 242*
Résultat exceptionnel			
Participation des salariés			
TOTAL	*- 113 984*	*- 36 116*	*- 77 868*

5.3 – Autres informations relatives au compte de résultat

Les postes de charges et produits composant le résultat de l'exercice figurent au compte de résultat des états financiers. On pourra s'y reporter ainsi qu'à la plaquette financière annuelle, documents qui fournissent une information plus détaillée.

Le chiffre d'affaires provient de la cession de licences pour 39 058 Euros et pour une prestation de service pour la CEE d'un montant de 15 526 Euros. Le solde dû par la CEE s'élève au 30/06/2007 à 57 680 Euros alors que le projet est terminé.

L'impôt sur les sociétés négatif est représenté par le montant du crédit impôt recherche. Le montant du crédit impôt recherche a été calculé selon les mêmes principes que celui au 31 décembre 2006.

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. Comptes annuels sociaux relatifs à l'exercice clos au 31 décembre 2006

17.2.1. Bilan – Actif

ACTIF	Exercice clos le 31/12/2006 (12 mois)				du 01/05/2004 au 31/12/2005 (20 mois)	
	Brut	Amort. & Prov	Net	%	Net	%
Capital souscrit non appelé (0)						
Actif Immobilisé						
Frais d'établissement						
Recherche et développement	61 956	34	61 922	26,56		
Concessions, brevets, marques, logiciels et droits similaires	1 220	885	336	0,14		
Fonds commercial						
Autres immobilisations incorporelles						
Avances & acomptes sur immobilisations incorporelles						
Terrains						
Constructions						
Installations techniques, matériel & outillage industriels						
Autres immobilisations corporelles	7 093	1 278	5 815	2,49		
Immobilisations en cours						
Avances & acomptes						
Participations évaluées selon mise en équivalence						
Autres Participations						
Créances rattachées à des participations						
Autres titres immobilisés						
Prêts						
Autres immobilisations financières	1 905		1 905	0,82	165	0,58
TOTAL (I)	***72 174***	***2 197***	***69 977***	30,01	***165***	0,58
Actif circulant						
Matières premières, approvisionnements						
En cours de production de biens						
En cours de production de services						
Produits intermédiaires et finis						
Marchandises						
Avances & acomptes versés sur commandes						
Clients et comptes rattachés	87 804		87 804	37,66		
Autres créances						
. Fournisseurs débiteurs						
. Personnel	6 000		6 000	2,57		
. Organismes sociaux	4 384		4 384	1,88		
. Etat, impôts sur les bénéfices	17 085		17 085	7,33		
. Etat, taxes sur le chiffre d'affaires	29 524		29 524	12,66	1 332	4,71
. Autres	1 544		1 544	0,66	17 000	60,16
Capital souscrit et appelé, non versé						
Valeurs mobilières de placement						
Disponibilités	15 159		15 159	6,50	9 435	33,39
Charges constatées d'avance	1 666		1 666	0,71	327	1,16
TOTAL (II)	***163 166***		***163 166***	69,99	***28 095***	99,42
Charges à répartir sur plusieurs exercices (III)						
Primes de remboursement des obligations (IV)						
Ecarts de conversion actif (V)						
TOTAL ACTIF (0 à V)	***235 340***	***2 197***	***233 143***	100,00	***28 260***	100,00

17.2.2. Bilan – Passif

PASSIF	Exercice clos le 31/12/2006 (12 mois)		Exercice précédent 31/12/2005 (20 mois)	
Capitaux propres				
Capital social ou individuel (dont versé : 38 000)	**38 000**	16,30	**11 000**	38,92
Primes d'émission, de fusion, d'apport ...	69 000	29,60		
Ecarts de réévaluation				
Réserve légale	12	0,01		
Réserves statutaires ou contractuelles				
Réserves réglementées				
Autres réserves	210	0,09		
Report à nouveau				
Résultat de l'exercice	***-65 491***	-28,08	***222***	0,79
Subventions d'investissement				
Provisions réglementées				
TOTAL(I)	***41 731***	17,90	***11 222***	39,71
Produits des émissions de titres participatifs				
Avances conditionnées				
TOTAL(II)				
Provisions pour risques et charges				
Provisions pour risques				
Provisions pour charges				
TOTAL (III)				
Emprunts et dettes				
Emprunts obligataires convertibles				
Autres Emprunts obligataires				
Emprunts et dettes auprès des établissements de crédit				
. Emprunts	75 000	32,17		
. Découverts, concours bancaires				
Emprunts et dettes financières diverses				
. Divers				
. Associés	32 000	13,73	2 000	7,08
Avances & acomptes reçus sur commandes en cours				
Dettes fournisseurs et comptes rattachés	19 744	8,47	1 256	4,44
Dettes fiscales et sociales				
. Personnel	10 837	4,65		
. Organismes sociaux	32 441	13,91		
. Etat, impôts sur les bénéfices			136	0,48
. Etat, taxes sur le chiffre d'affaires	15 773	6,77		
. Etat, obligations cautionnées				
. Autres impôts, taxes et assimilés				
Dettes sur immobilisations et comptes rattachés				
Autres dettes	5 616	2,41	13 646	48,29
Produits constatés d'avance				
TOTAL(IV)	***191 411***	82,10	***17 037***	60,29
Ecart de conversion passif (V)				
TOTAL PASSIF (I à V)	***233 143***	100,00	***28 260***	100,00

17.2.3. Compte de Résultat

COMPTE DE RÉSULTAT	Exercice clos le 31/12/2006 (12 mois)		du 01/05/2004 au 31/12/2005 (20 mois)		Variation absolue (12 / 20)	%
	France	Exportation	Total	%	Total	%	Variation	%
Ventes de marchandises								
Production vendue biens								
Production vendue services	17 888	49 874	67 762	100,00			67 762	N/S
Chiffres d'Affaires Nets	**17 888**	**49 874**	**67 762**	100,00			**67 762**	N/S
Production stockée								
Production immobilisée			61 956	91,43			61 956	N/S
Subventions d'exploitation					17 000	100,00	-17 000	-99,99
Reprises sur amortis. et prov., transfert de charges								
Autres produits			194	0,29			194	N/S
Total des produits d'exploitation			***129 912***	191,72	***17 000***	100,00	***112 912***	664,19
Achats de marchandises (y compris droits de douane)								
Variation de stock (marchandises)								
Achats de matières premières et autres approvisionnements			1 080	1,59			1 080	N/S
Variation de stock (matières premières et autres approv.)								
Autres achats et charges externes			90 930	134,19	15 955	93,85	74 975	469,92
Impôts, taxes et versements assimilés			1 964	2,90	642	3,78	1 322	205,92
Salaires et traitements			83 790	123,65			83 790	N/S
Charges sociales			32 458	47,90			32 458	N/S
Dotations aux amortissements sur immobilisations			2 197	3,24			2 197	N/S
Dotations aux provisions sur immobilisations								
Dotations aux provisions sur actif circulant								
Dotations aux provisions pour risques et charges								
Autres charges			25	0,04			25	N/S
Total des charges d'exploitation			***212 443***	313,51	***16 597***	97,63	***195 846***	N/S
RÉSULTAT D'EXPLOITATION			**-82 531**	-121,79	**403**	2,37	**-82 934**	N/S
Bénéfice attribué ou perte transférée								
Perte supportée ou bénéfice transféré								
Produits financiers de participations								
Produits des autres valeurs mobilières et créances								
Autres intérêts et produits assimilés								
Reprises sur provisions et transferts de charges								
Différences positives de change								
Produits nets sur cessions valeurs mobilières placement								
Total des produits financiers								
Dotations financières aux amortissements et provisions								
Intérêts et charges assimilées								
Différences négatives de change								
Charges nettes sur cessions valeurs mobilières placements								
Total des charges financières								
RÉSULTAT FINANCIER								
RÉSULTAT COURANT AVANT IMPÔTS			**-82 531**	-121,79	**403**	2,37	**-82 934**	N/S

COMPTE DE RÉSULTAT (suite)	Exercice clos le 31/12/2006 (12 mois)		du 01/05/2004 au 31/12/2005 (20 mois)		Variation absolue (12 / 20)	%
Produits exceptionnels sur opérations de gestion Produits exceptionnels sur opérations en capital Reprises sur provisions et transferts de charges						
Total des produits exceptionnels						
Charges exceptionnelles sur opérations de gestion Charges exceptionnelles sur opérations en capital Dotations exceptionnelles aux amortissements et provisions	45	0,07	45	0,26		0,00
Total des charges exceptionnelles	***45***	0,07	***45***	0,26		0,00
RÉSULTAT EXCEPTIONNEL	**-45**	-0,06	**-45**	-0,25		0,00
Participation des salariés Impôts sur les bénéfices	-17 085	-25,20	136	0,80	-17 221	N/S
Total des Produits	***129 912***	191,72	***17 000***	100,00	***112 912***	664,19
Total des Charges	***195 403***	288,37	***16 778***	98,69	***178 625***	N/S
RÉSULTAT NET	**-65 491** *Perte*	-96,64	**222** *Bénéfice*	1,31	-65 713	N/S
Dont Crédit-bail mobilier Dont Crédit-bail immobilier						

17.2.4. Annexes aux comptes sociaux relatifs à l'exercice clos au 31 décembre 2006

Préambule

L'exercice social clos le 31/12/2006 a une durée de 12 mois.
L'exercice précédent clos le 31/12/2005 avait une durée de 20 mois.

Le total du bilan de l'exercice avant affectation du résultat est de 233 142,75 E.

Le résultat net comptable est une perte de 65 490,86 E.

Les informations communiquées ci-après font partie intégrante des comptes annuels qui ont été établis le 05/06/2007 par le dirigeant.

1. Règles et méthodes 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.

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.

2. Autres éléments significatifs de l'exercice

La société a été transformée en société anonyme au cours de l'exercice, et a procédé à deux augmentations de capital en date du 13 juillet 2006 et 30 juin 2006. Au cours de l'augmentation de capital du 13 juillet 2006, une prime d'émission d'un montant de 69 000 euros a été versée. Le capital a été augmenté de 11 000 euros à 38 000 euros.

3. Notes sur le bilan d'actif

3.1 - Frais de recherche & développement = 61 956

Frais recherche & développement	Valeur brute	Amortissement	Valeur nette	Taux
Frais recherche & développement	*61 956*	*34*	*61 922*	*%*

3.2 - Actif immobilisé

Les mouvements de l'exercice sont détaillés dans les tableaux ci-dessous :

3.2.1 - Immobilisations brutes = 72 174

Actif immobilisé	A l'ouverture	Augmentation	Diminution	A la clôture
Immobilisations incorporelles		*63 176*		*63 176*
Immobilisations corporelles		*7 093*		*7 093*
Immobilisations financières	*165*	*1 740*		*1 905*
TOTAL	*165*	*72 009*		*72 174*

3.2.2 - Amortissements et provisions d'actif = 2 197

Amortissements et provisions	A l'ouverture	Augmentation	Diminution	A la clôture
Immobilisations incorporelles		*919*		*919*
Immobilisations corporelles		*1 278*		*1 278*
Titres mis en équivalence				
Autres Immobilisations financières				
TOTAL		*2 197*		*2 197*

3.2.3 - Détail des immobilisations et amortissements en fin de période

Nature des biens immobilisés	Montant	Amortissement	Valeur nette	Durée
Frais recherche & developpement	*61 956*	*34*	*61 922*	*5 ans*
Concess.brevets licences	*1 220*	*885*	*336*	*1 ans*
Mat.bureau &informatique	*7 093*	*1 278*	*5 815*	*3 ans*
TOTAL	*70 269*	*2 197*	*68 072*	

3.3 - Etat des créances = 149 912

Etat des créances	Montant brut	A un an	A plus d'un an
Actif immobilisé	*1 905*		*1 905*
Actif circulant & charges d'avance	*148 007*	*148 007*	
TOTAL	*149 912*	*148 007*	*1 905*

3.4 - Produits à recevoir par postes du bilan = 66 874

Produits à recevoir	Montant
Immobilisations financières	
Clients et comptes rattachés	*66 874*
Autres créances	
Disponibilités	
TOTAL	*66 874*

3.5 - Charges constatées d'avance = 1 666

Les charges constatées d'avance ne sont composées que de charges ordinaires dont la répercussion sur le résultat est reportée à un exercice ultérieur.

3.6 - Informations complémentaires sur le bilan actif

Nous avons décidé d'activer les dépenses de frais de recherche et développement comprenant les salaires et charges sociales des ingénieurs, puisque la société remplie les conditions notamment qu'il y a des commandes en cours de logiciels.

4. Notes sur le bilan passif

4.1 - Capital social = 38 000

Mouvements des titres	Nombre	Val. nominale	Capital social
Titres en début d'exercice	*110*	*100,00*	*11 000*
Titres émis ou variation du nominal	*270*	*100,00*	*27 000*
Titres remboursés ou annulés			
Titres en fin d'exercice	*380*	*100,00*	*38 000*

4.2 - Etat des dettes = 191 411

Etat des dettes	Montant total	De 0 à 1 an	De 1 à 5 ans	Plus de 5 ans
Etablissements de crédit	*75 000*		*75 000*	
Dettes financières diverses	*32 000*	*32 000*		
Fournisseurs	*19 744*	*19 744*		
Dettes fiscales & sociales	*59 052*	*59 052*		
Dettes sur immobilisations				
Autres dettes	*5 616*	*5 616*		
Produits constatés d'avance				
TOTAL	*191 411*	*116 411*	*75 000*	

4.3 - Charges à payer par postes du bilan = 22 861

Charges à payer	Montant
Emprunts & dettes établ. de crédit	
Emprunts & dettes financières div.	
Fournisseurs	*7 112*
Dettes fiscales & sociales	*15 749*
Autres dettes	
TOTAL	*22 861*

5. Notes sur le compte de résultat

5.1 - Ventilation du chiffre d'affaires = 67 762

Le chiffre d'affaires de l'exercice se décompose de la manière suivante :

Nature du chiffre d'affaires	Montant HT	Taux
Prestations de services	*67 762*	*100,00 %*
TOTAL	*67 762*	*100,00 %*

5.2 - Ventilation de l'impôt sur les bénéfices = -17 085

Niveau de résultat	Avant impôt	Impôt	Après impôt
Résultat d'exploitation	*-82 531*		*-82 531*
Résultat financier			
Résultat exceptionnel	*-45*		*-45*
Participation des salariés			
TOTAL	*-82 576*	*-17 085*	*-65 491*

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.

6.2 - Autres informations complémentaires

Les engagements de retraite ne sont pas significatifs

17.3. Rapport d'examen limité du commissaire aux comptes - période du 1er janvier 2007 au 30 juin 2007

Mesdames, Messieurs, les Actionnaires,

A la suite de la demande qui nous a été faite et en notre qualité de commissaire aux comptes de la société MOBILEGOV SA, nous avons effectué un examen limité des comptes intermédiaires relatifs au 1er semestre 2007, tels qu'ils sont joints au présent rapport.

Nous précisons que votre société n'étant pas tenue précédemment de communiquer de situation intermédiaire semestrielle, le compte de résultat relatif à la période du 1er semestre 2006 n'a pas fait l'objet d'une revue limitée. Les comptes comparatifs sont les comptes audités au 31 décembre 2006.

Ces comptes ont été établis sous la responsabilité de votre conseil d'administration. Il nous appartient, sur la base de notre examen limité, d'exprimer notre conclusion sur ces comptes.

Nous avons effectué notre examen limité selon les normes professionnelles applicables en France. Un examen limité de comptes intermédiaires consiste à obtenir les informations estimées nécessaires, principalement auprès des personnes responsables des aspects comptables et financiers, et à mettre en œuvre des procédures analytiques ainsi que toute autre procédure appropriée. Un examen de cette nature ne comprend pas tous les contrôles propres à un audit effectué selon les normes professionnelles applicables en France. Il ne permet donc pas d'obtenir l'assurance d'avoir identifié tous les points significatifs qui auraient pu l'être dans le cadre d'un audit et, de ce fait, nous n'exprimons pas une opinion d'audit.

Sur la base de notre examen limité, nous n'avons pas relevé d'anomalies significatives de nature à remettre en cause, au regard des règles et principes comptables français, la régularité et la sincérité des comptes et l'image fidèle qu'ils donnent du résultat des opérations de la période écoulée ainsi que de la situation financière et du patrimoine de la société à la fin de cette période.

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 « Autres éléments significatifs de l'exercice » de l'annexe.

Fait à Sophia-Antipolis, le 07 décembre 2007

Le Commissaire aux comptes

Experts & Associés International

Stéphan Brun

17.4. Rapport général du commissaire aux comptes relatifs à l'exercice clos le 31 décembre 2006

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 2006 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.

I - Opinion sur les comptes annuels

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

Un audit consiste à examiner, par sondages, les éléments probants justifiant les données contenues dans ces comptes. Il consiste également à apprécier les principes comptables suivis et les estimations significatives retenues pour l'arrêté des comptes et à apprécier leur présentation d'ensemble.
Nous estimons que nos contrôles fournissent une base raisonnable à l'opinion exprimée ci-après.

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 « Autres éléments significatifs de l'exercice » de l'annexe.

II - 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, introduites par la loi de sécurité financière du 1er août 2003, 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.

III - Vérifications et informations spécifiques

Nous avons également procédé, conformément aux normes professionnelles applicables en France, aux vérifications spécifiques prévues par la loi.

Nous n'avons pas d'observation 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 juin 2007
Le Commissaire aux comptes
Experts & Associés International
Stéphan BRUN

17.5. Dividendes

17.5.1. 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.

17.5.2. 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 282.993 € et est divisé en 459.030 actions d'un montant nominal égal.

18.1.2. Capital autorisé non émis par décisions de l'Assemblée Générale Extraordinaire du 31 décembre 2007 :

➢ **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 23 janvier 2008, 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 s. du Code de commerce, avec effet au 23 janvier 2008, 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 :

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

(ii) 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 ;

(iii) 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 23 janvier 2008, 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 23 janvier 2008, 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 et part résiduelle
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	Néant
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	Néant
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	Néant

Ces autorisations n'ont pas été utilisées à ce jour, hormis pour la présente opération.

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	Augmentation de capital	Nombre d'actions créées	Valeur nominale	Nombre d'actions cumulées	Capital après opération
19/05/2004	Constitution	1 000 €	10	100 €	10	1 000 €
13/09/2005	Augmentation par incorporation d'une créance	10 000 €	100	100 €	110	11 000 €
23/02/2006	Augmentation par incorporation d'une créance	12 000 €	120	100 €	230	23 000 €
30/06/2006	Augmentation par incorporation d'une créance	9 000 €	90	100 €	320	32 000 €
13/07/06	Augmentation par apport en numéraire	6 000€	60	100€	380	38.000 €
24/12/07	Division du nominal des actions	0	379 620	0,10 €	380.000	38.000 €
24/12/07	Augmentation par apport en numéraire	4 999,90 €	49 999	0,10 €	429 999	42 999,90 €
24/12/07	Augmentation par apport en numéraire	2 903,10 €	29 031	0,10€	459 030	45 903 €
24/12/07	Augmentation de capital par incorporation de la prime d'émission et élévation du nominal des actions	237 090 €	-	0,617 €	459 030	282 993 €

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

Actionnariat[1]

Actionnaires	Nombre d'actions	% capital
Mobilegov Ltd.	110 000	23,96%
Michel Frenkiel	90 000	19,61%
François-Pierre Le Page	70 000	15,25%
Eric Mathieu	70 000	15,25%
Benoît de Maulmin	24 193	5,27%
IST Consultants	20 000	4,36%
Léon Frenkiel	19 000	4,14%
Valérie Podelski	16 129	3,51%
Claude Chaussé	12 903	2,81%
Alain Vauthier	9 677	2,11%
Martin Eisenberg	8 064	1,76%
Lucile Marsac-Huignard	8 064	1,76%
Raymonde Frenkiel	1 000	0,22%
Total	459 030	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.

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

18.2.2. Exercice social

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

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

Néant. La Société n'a pas conclu de contrats importants autres que ceux signés dans le cadre normal de ses activités.

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.

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 :	+33 492 944 894
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 à la fin du document d'information :

NOTE D'INFORMATION DU CERTA, 9/11/2006 : Risques associés aux clés USB

Ce document informe les entreprises sur les risques présentés par les nouvelles catégories de clés USB.

Boursier.com, 18/05/2007 : Alcatel-Lucent : un disque de données salariés de Lucent envolé

Cet article révèle une retentissante affaire de vol de données. Mobilegov propose une solution pour lutter contre de tels vols.

Le Monde Informatique, 05/12/2007 : Les services informatiques, premiers responsables des fuites de données

Selon une étude du cabinet Orthus, 30 % des fuites de données sensibles trouvent leurs origines dans le service informatique de l'entreprise. Et elles auraient toutes pu être évitées en appliquant le règlement intérieur des sociétés.

Mobilegov permet aux collaborateurs d'utiliser leurs outils favoris, mais sans risque pour l'entreprise.

Réseaux-Télécom.net, 24/09/2007 : L'humain reste le maillon faible de la sécurité du SI

Dans son rapport annuel « 2007 Global Security Survey », le cabinet Deloitte Touche Tomatsu montre que les employés et les clients restent le plus grand facteur de risque d'une institution financière.

Site web IP Vista, 28/11/2007 : Communiqué de Presse informant de l'arrivée de Mobilegov

Site web du South-East England Development Agency, 04/12/2007 : Mobilegov opens an office in the 'UK Silicon Valley'

French security software editor Mobilegov launches its UK presence this autumn in Reading at the heart of the Thames Valley following several months of market research and supported by the Thames Valley Economic Partnership (TVEP), South East England Development Agency (SEEDA) and UK Trade & Investment (UKTI) in Paris.

Réseaux-Télécom.net, 21/09/2007 : La cybercriminalité se professionnalise

Selon le dernier Rapport sur les menaces à la sécurité Internet publié par Symantec, la cybercriminalité devient une activité de plus en plus professionnelle et commerciale. Les pirates et autres organisations criminelles cherchent à tirer toujours plus de profit de leurs attaques en ligne.

Zebulon.fr, 30/07/2007 : Device Linker, la clé USB sécurisée

Les clés USB ont depuis bien longtemps pris une place prépondérante dans notre quotidien. Pourtant, en cas de perte ou de vol, nos précieuses données peuvent se retrouver entre de mauvaises mains. De plus, en ce qui concerne les entreprises ou les administrations publiques, ces clés introduisent une nouvelle menace de sécurité où des données confidentielles peuvent facilement être dérobées. Face à ce constat, la société Mobilegov propose une clé USB sécurisée utilisable uniquement sur des PC autorisés.

Site web de la FNAC, 17/12/2007 : Device Linker - single soft

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

01net, 20/12/2007 : L' « ADN numérique » des périphériques sécurise leurs connexions

Mobilegov propose une solution de gestion de la sécurité des équipements amovibles, dont les smartphones et les clés USB.
Avec Device Authenticator Pro Edition, la jeune pousse française Mobilegov fournit une solution élégante à un problème qui prend de l'importance en entreprise : la gestion des périphériques amovibles. Ces équipements sont de plus en plus sophistiqués et donc difficiles à contrôler.

Brochures commerciales Device Authenticator et Device Linker

Ces brochures, comme tous les documents techniques, existent en français et en anglais.

S . G . D . N
Direction centrale
de la sécurité des
systèmes d'information

Paris, le 09 novembre 2006
N° CERTA-2006-INF-006-001

Affaire suivie par :

CERTA

NOTE D'INFORMATION DU CERTA

Objet : Risques associés aux clés USB

GESTION DU DOCUMENT

Tableau 1: Gestion du document

Référence	CERTA-2006-INF-006-001
Titre	Risques associés aux clés USB
Date de la première version	09 novembre 2006
Date de la dernière version	14 novembre 2006
Source(s)	
Pièce(s) jointe(s)	Aucune

Une gestion de version détaillée se trouve à la fin de ce document.

1 INTRODUCTION

Les périphériques USB (pour Universal Serial Bus) occupent actuellement une place prépondérante dans l'univers de l'appareillage informatique. Ils peuvent être de tout type, comme par exemple un support de données amovible (clé USB, lecteur de musique au format MP3, etc).

De par leur facilité d'installation, ces périphériques s'échangent très facilement d'une machine à une autre. Cependant, cette opération présente des risques. Nous montrons dans ce document que ces échanges peuvent aussi bien affecter le périphérique que l'ordinateur d'accueil.

Du fait de la simplicité et de la furtivité des attaques basées sur ces échanges, il est important de prendre des mesures préventives. Il n'est bien sûr pas question de remettre en cause l'utilité de l'USB, notamment les différents périphériques de stockage, mais certaines considérations doivent être prises avant leur utilisation, que ce soit pour l'utilisateur ou l'administrateur. Ce document offre donc quelques recommandations à cet égard.

2 PRÉSENTATION DE L'*UNIVERSAL SERIAL BUS*

2.1 USB 1.0 et 2.0

L'USB (pour Universal Serial Bus) est une interface de connexion définie dans les années 90 et destinée à remplacer les ports série et parallèle sur les ordinateurs. Elle est utilisée de nos jours pour brancher tout type de périphérique, que ce soient les imprimantes, les scanners, les modems, ou des appareils de stockage, comme les clés USB.

Sans rentrer dans les détails fournis par les documents de référence, il existe, à la date de rédaction de cet article, deux standards distincts, USB 1.1 et USB 2.0 :

- L'USB version 1.1 considère deux modes différents, dits lent (1,5 Mbits/s en théorie) et rapide (12 Mbits/s en théorie). Le premier mode, moins sensible aux perturbations électromagnétiques, convient aux petits transferts de données, comme ceux requis par les claviers ou les souris. Le second peut servir dans le cas d'imprimantes, de scanners, de disques durs externes, ou de lecteurs et graveurs CD/DVDs.
- L'USB version 2.0 ajoute un nouveau mode, permettant des échanges théoriques à 480 Mbits/s. La compatibilité entre périphériques USB 1.1 et 2.0 est assurée. Toutefois l'utilisation d'un périphérique USB 2.0 sur un port USB à bas débit limitera celui-ci à 12 Mbit/s maximum. De plus, le système d'exploitation est susceptible d'afficher un message expliquant que le débit est bridé.

Les termes sont parfois utilisés de manière abusive, et la dénomination commerciale USB 2.0 Full Speed fait en réalité référence à la version USB 1.1 en mode rapide, tandis que USB 2.0 High Speed correspond bien au standard 2.0.

L'architecture de type USB a pour caractéristique de fournir une alimentation électrique aux périphériques qu'elle relie, avec une tension maximale de 5V et un courant d'au plus 500mA. Il est enfin possible de connecter jusqu'à 127 appareils à un Bus USB[1] à un temps donné. L'USB se compose de plusieurs couches de protocoles, ou moyens de communication, qui ne seront pas abordées dans ce document.

L'USB, pour résumer, possède les propriétés suivantes :

- la topologie en arbre dont la racine est normalement une machine hôte (PC, Mac, etc.) ;
- les périphériques peuvent être branchés et débranchés sans arrêter l'ordinateur ;
- les périphériques sont alimentés par un bus ;
- il est possible de chaîner jusqu'à 127 périphériques sur un même bus USB (avec l'utilisation d'un *hub* par exemple);
- les périphériques inutilisés sont automatiquement mis en veille ;
- les périphériques sont identifiés et configurés automatiquement par les systèmes d'exploitation.

2.2 La norme *On-the-Go*

L'USB est contrôlé par un hôte, installé sur la machine d'accueil. L'hôte USB a la charge de mener à bien toutes les transactions et de gérer la bande passante.

Cependant, depuis l'USB 2.0, il existe un protocole « au pied levé » (ou *On-the-Go*), qui permet, pour deux périphériques USB, de négocier et d'élire un hôte parmi eux. L'intérêt est le suivant : on peut relier deux périphériques sans ordinateur. Parmi les illustrations les plus courantes, il peut s'agir d'une imprimante et d'un appareil photo numérique reliés entre eux, ou bien d'un lecteur MP3 et d'une clé de stockage USB.

2.3 L'USB sans fil ?

Des projets consistant à porter des caractéristiques de l'USB au domaine du sans-fil tendent à apparaître, l'un en particulier étant déjà très médiatisé : le *Wireless USB* (s'appuyant sur la technologie `uwb`, *Ultra-Wideband*), lancé par un conglomérat de constructeurs, promet des produits commercialisés dans les mois à venir. Nous ne voulons pas nous étendre pour le moment sur cette nouvelle approche USB, mais il sera intéressant, en temps voulu, de vérifier si celle-ci permettra d'éviter les problèmes mentionnés dans les paragraphes suivants et si elle présentera des problèmes spécifiques.

2.4 Génération USB U3

Créée par la société U3 avec le soutien de constructeurs de mémoire flash, cette technologie transforme une clef USB en un système portable contenant des fichiers et des applications favorites.

Une clef USB U3 dispose d'un logiciel, ou `lanceur`, qui s'exécute sur l'ordinateur hôte afin de présenter (le plus souvent) les applications disponibles. Il est facile de gérer son contenu *via* un menu *"Démarrer"* (ou `lanceur`) dédié accessible dans la barre des tâches. Il est alors possible d'afficher à l'écran son *système* personnel sauvegardé sur la clef USB avec son fond d'écran et un accès facile aux différentes applications.

Les inconvénients de la gestion d'applications sur les clefs traditionnelles sont donc effacés : l'accès aux programmes se fait simplement et de manière transparente pour l'utilisateur ; s'appuyant sur un format qui cherche à se standardiser, l'offre logicielle compatible avec U3 ne cesse de se développer.

Autre caractéristique des clefs U3 : elles ne laissent que très peu de traces sur l'ordinateur hôte puisque les documents contenus sur la clef sont ouverts avec des applications elles aussi présentes sur la clef (y compris les cookies récoltés lors d'une navigation sur l'Internet). Les tâches d'écriture se font *via* la mémoire volatile de la machine hôte uniquement, et ces applications ne modifient ni la base de registre, ni la mémoire morte (ROM) de cette dernière.

De nombreuses applications gratuites ou payantes ont désormais des versions compatibles avec U3 : notamment le logiciel de voix sur IP Skype ou le navigateur Firefox. D'autres logiciels sont également disponibles : jeux, bureautique, gestionnaires d'images ou de fichiers audio MP3 ; et cette offre logicielle augmente de jour en jour.

L'USB U3 présente donc un avantage, pour la maîtrise de l'application utilisée ; par exemple, quand une personne est amenée à utiliser un ordinateur dont la configuration et le niveau de sécurité ne sont pas connus (comme dans un cyber-café, un hôtel, un aéroport, etc). Cela permet d'utiliser ses propres applications, plutôt que certaines méconnues, ou aux mises à jour et à la configuration non spécifiées. Elle reste cependant tributaire de la machine d'accueil

pour toute communication, toute saisie, et tout transfert de données vers l'extérieur, et cette opération peut l'exposer à certains risques décrits dans les paragraphes qui suivent.

3 Risques associés à l'USB

3.1 Vol d'informations de la clé

Une clé, ou tout autre support de stockage USB, est, une fois branchée sur une machine, à la merci de celle-ci. Un processus fonctionnant silencieusement, peut très bien attendre que la clé soit branchée (information signalée par le système d'exploitation) pour enclencher une procédure de lecture et de copie du contenu de la clé. Un tel processus, comme la plupart des codes malveillants actuels, ne sera pas facilement décelable sur la machine hôte (dissimulation au niveau de la liste des tâches, des appels système, etc.).

Certains outils plus pernicieux permettent même de faire une image complète de la clé. Outre le vol de documents présents dans celle-ci, ce procédé peut également faciliter la récupération de tout ou partie de documents effacés sur la clé.

Les clés disposent de voyants lumineux, montrant les échanges de données. Un clignotement anormal de la clé peut donc être une première indication d'une telle activité de copie. Attention cependant, le voyant peut aussi être manipulé de manière logicielle sur certaines clés. Quelques secondes suffisent enfin pour dérober plusieurs Mo de données avec les performances USB actuelles.

3.2 Exécution d'applications hébergées par la clé

L'action malveillante du paragraphe précédent est perpétrée par la machine d'accueil. Une autre approche, ou action malveillante, se nomme `podslurping` et s'effectue depuis le périphérique. Elle consiste à brancher sur un système un support de stockage, ou aussi un lecteur MP3 (`podslurping` fait référence au produit iPod d'Apple), afin d'en dérober furtivement de l'information.

L'ingénierie sociale, ou la force de persuasion, peut être associée à cette approche, afin de provoquer le branchement, et de perpétrer le vol des informations. Une phrase parmi les dialogues possibles pourrait être :

"Excusez-moi, pourrais-je connecter quelques minutes mon lecteur de musique MP3 sur votre port USB ?... Les batteries sont déchargées, et je ne rentre que demain chez moi. Merci beaucoup !".

Pendant quelques minutes, une partie du disque est copiée sur le lecteur de musique, qui dispose d'un espace de stockage important (de l'ordre de quelques Go à plusieurs dizaines de Go), et dont l'usage ne fait pas obligatoirement penser à un périphérique de stockage.

Ce scénario est aussi valable avec un appareil photo numérique.

Ce problème n'est absolument pas récent, et existait déjà à l'époque des disquettes. Cependant, les supports de stockage ont maintenant une capacité et un débit de transfert beaucoup plus importants, ce qui augmente la quantité de données pouvant être dérobées dans un cours intervalle de temps.

3.3 Problématique des clés USB U3

3.3.1 Mises à jour des logiciels

De nombreux scénarios d'attaques étudiés par le CERTA dans le cadre des incidents qu'il traite au quotidien sont dus à une absence de mises à jour, qui ouvre une brèche au niveau applicatif.

Il en va de même pour clés USB U3, dont le premier point délicat réside dans la maintenance des logiciels compatibles avec U3.

Ces logiciels, comme nous l'avons vu, sont pour la plupart des déclinaisons de ceux manipulés sur des systèmes plus standards (navigateur, client de messagerie, etc). En revanche, ils ont subi quelques modifications pour fonctionner sur le support U3, et quelques sites centralisent ces versions particulières.

Il se pose alors la question des mises à jour de ces dernières. Il n'est pas évident que les sites suivent de manière réactive les modifications des éditeurs officiels. Par ailleurs, la clé ne peut être mise à jour que si l'on dispose d'une connexion Internet.

Imaginons alors le scénario suivant :

1. l'utilisateur possède une clé U3, essentiellement pour un usage bureautique, afin de faire des présentations.
2. l'utilisateur branche sa clé régulièrement pour lire, rédiger et présenter des transparents.
3. la clé n'est pas mise à jour ; elle possède une version du logiciel de bureautique ayant des vulnérabilités permettant une exécution de code arbitraire par le biais d'un document spécialement conçu.
4. la clé peut servir à contaminer les ordinateurs sur lesquels les transparents sont visionnés.

Il est très délicat d'imposer aux utilisateurs d'une clé de se connecter à Internet pour effectuer les mises à jour. Ce n'est pas nécessairement l'usage premier qui est recherché.

Pour résumer, il existe les problèmes suivants, liés aux applications disponibles actuellement :

1. il n'existe pas de mise à jour automatique. Pour effectuer l'une d'elle, il faut supprimer l'application courante, afin d'installer une version plus récente ;
2. les applications compatibles avec U3 sont maintenues par certains sites, mais :
   - les éditeurs légitimes ne donnent généralement aucune garantie sur ces versions ;
   - les versions sont modifiées, et leur configuration est souvent criticable. Par exemple, l'installation d'un navigateur implique une page d'accueil spécifique, une barre de recherche pré-installée et méconnue, une configuration peu regardante sur la sécurité (taille du cache, activation du javascript), des favoris par défaut, etc.
   - certaines applications sont des espiogiciels, voire des troyens. Il peut aussi s'agir de jeux par exemple, compatibles avec U3, mais nécessitant au préalable un enregistrement *via* l'Internet (quel est le but de cette collecte d'information ?).
3. l'utilisateur doit régulièrement surveiller les sites, donc se connecter, pour découvrir les mises à jour.

Il reste possible de développer soi-même les versions de certaines applications (en faisant attention aux problèmes de licences). Plusieurs détails pour opérer se trouvent sur l'Internet, mais cela reste marginal, et nécessite à la fois des connaissances minimales pour compiler du code et une disponibilité des fichiers sources.

3.3.2 Vol d'informations

Compte tenu des applications disponibles, les clés U3 sont susceptibles de contenir des informations personnelles ou confidentielles :

- la configuration du client de messagerie ;
- les contacts stockés par le client de messagerie ;
- les pages en cache du navigateur Internet ;
- les sites favoris installés sur le navigateur ;
- des mots de passe gérés par une application dédiée (application fréquemment offerte par défaut avec la clé).

Le risque du vol de données comme il existe pour les clés classiques reste présent. Malheureusement, l'utilisation d'applications impose de fournir sur la clé U3 un minimum d'informations pour leur bon fonctionnement. D'autres applications U3 incitent également à centraliser des données confidentielles sur le support USB (gestionnaire de mots de passe par exemple). Le vol de celles-ci peut avoir des conséquences variées et génantes.

3.4 Les lanceurs malveillants

Pour finir, il faut noter que les clés U3 sont généralement fournies avec un `lanceur`, qui donne accès aux applications, une fois la clé insérée. Cependant, certains `lanceurs` malveillants sont également disponibles. Ils permettent d'exécuter directement des actions à l'insertion de la clé, et sont fournis avec des outils permettant : de récupérer les tables de mots de passe, d'installer une capture de clavier ou un `rootkit`, difficilement décelables *a posteriori*.

4 Les recommandations du CERTA

4.1 Comptes utilisateurs et droits

La clé ne dispose pas d'autres droits que ceux de l'utilisateur courant sous Windows. Pour limiter les actions que celle-ci peut effectuer sur le système, il est donc important de n'autoriser la connexion de clés que sur des sessions avec des droits limités, et de ne réserver les droits de l'administrateur qu'occasionnellement, pour la maintenance du système. Cette règle de base est également vraie, indépendamment des clés USB.

Sous Windows, pour ouvrir l'outil `Comptes d'utilisateurs`, il faut ouvrir le `Panneau de configuration` à partir du menu `Démarrer`, puis sélectionner `Comptes d'utilisateurs`. La gestion des comptes et des droits associés s'effectue à partir de cette interface.

4.2 Désactivation de la fonctionnalité `autorun`

Les clés U3 profite d'une propriété offerte par les systèmes d'exploitation Windows, nommée `autorun`. Elle consiste à exécuter automatiquement un logiciel lorsqu'un périphérique de stockage qui le contient est connecté. Microsoft autorise par défaut cette fonction pour le périphériques de type CDROM/DVDROM, ou les disques fixes.

Cette fonctionnalité est visible, quand, par exemple, à l'insertion de certains CD, une fenêtre de navigation Internet Explorer, ou une application d'installation s'ouvre. Un périphérique USB classique ne permet pas, lors de son insertion dans une machine fonctionnant sous Windows, d'exécuter automatiquement des programmes ou des commandes qu'il peut contenir. Dans l'objectif de faire exécuter automatiquement du code au cours de l'insertion d'un périphérique USB, certains fabriquants de matériels USB ont développé une astuce, qui consiste à faire passer celui-ci auprès de Windows pour un CD ou/et un DVD. Cette technique existe, et c'est elle qui est utilisée par les produits USB U3. Le principe général est que le périphérique, au moment de l'insertion, se présente comme un lecteur de CDROM USB, permettant *a fortiori* l'exécution d'un `autorun`.

La fonction `autorun` n'est généralement pas indispensable. Pour la désactiver sous Windows, il suffit de modifier la clé suivante dans la base de registres :

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/CDRom
```

Pour la désactivation de l'`autorun` :

- Autorun = 0

pour l'activation de l'`autorun` :

- Autorun = 1

Cela fonctionne sur les systèmes Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP et Windows 2003.

4.3 Verrouillage des postes

Afin d'éviter des incidents liés à l'insertion de clés USB sur son système, il est également important de verrouiller son poste de travail : sous Windows, cela peut se régler de manière automatique, après un manque d'activité de quelques minutes sur le système (choisir `Propriétés` après un clic droit sur le fond d'écran), ou de manière ponctuelle (appuyer simultanément sur les touches `Ctrl+Alt+Suppr` ou `Windows+L`).

L'insertion d'un périphérique USB sous Windows ne provoque pas son installation quand l'écran est verrouillé. La partition peut être cependant montée (`automount`) sous Linux malgré le verrouillage[2].

4.4 Clés USB de confiance : une clé par usage

Si une clé doit être insérée dans un système critique, il est important de vérifier son origine. Une solution serait de conserver une clé blanchie, régulièrement formatée, et de réserver l'usage de l'USB à cette seule dernière (ajout de nouveaux matériels/périphériques interdits). En d'autres termes, il faudrait considérer une clé par usage, voire interdire son déplacement hors des locaux liés à son utilisation.

4.5 Bloquer la clé en écriture

Certaines clés présentent un interrupteur physique, qui permet de bloquer l'accès en écriture à la clé. Il ne faut donc pas l'oublier. Si cela ne protège pas du vol d'information, et donc des différentes problématiques de confidentialité, cela empêche des éléments extérieurs de modifier le contenu de la clé, ou de l'effacer à

l'insu de l'utilisateur.

4.6 Nettoyer proprement le contenu de la clé

Les clés peuvent contenir des données sensibles. Avant de les prêter ou de les abandonner, il est important de bien nettoyer leur espace de stockage, ou d'assurer la confidentialité de leur contenu. En fonction des impératifs et des réglementations, certaines opérations doivent être conduites.

4.6.1 Mesures élémentaires

Il n'est souvent pas suffisant de faire `"supprimer"` pour détruire complétement toute trace d'un document. Des résidus peuvent subsister. Certains outils permettent de faire un nettoyage beaucoup plus complet.

- Sous Windows, il existe par exemple :
  - `eraser`

    http://www.bugbrother.com/eraser
  - `BCWipe`

    http://www.jetico.com/bcwipe.htm
- Sous Linux ou MacOS, il existe entre autres la commande `shred` (`Shredit` sous Mac OS) ou l'application :
  - `wipe`

    http://wipe.sourceforge.net/

Il faut cependant bien vérifier que tout l'espace de stockage reste inaccessible. Certains outils se contentent d'effacer des fichiers, mais d'autres temporaires peuvent encore subsister sur l'espace de stockage (cas des documents bureautiques avec Microsoft Word par exemple).

4.6.2 Mesures spécifiques

Dans le cas de données plus sensibles, il existe des mesures plus efficaces que celles précédentes. Elles peuvent s'appuyer sur des méthodes de surcharge, de démagnétisation, etc. Enfin, une dernière mesure consiste à détruire le support de stockage USB.

4.7 Chiffrement et intégrité

Nous n'aborderons pas ce point dans ce document, car les questions de chiffrement et d'intégrité se posent pour tout support de stockage, mais il est bien entendu que si la solution de chiffrement nécessite une clé, celle-ci ne doit pas se trouver sur l'appareil USB. De la même manière, le résultat du test d'intégrité ne doit pas être stocké sur le même support.

D'autre part, les clés actuelles offrent comme contrôle d'accès l'utilisation d'un mot de passe pour accéder aux fonctionnalités U3. C'est une première protection contre le vol, mais il faut garder à l'esprit que :

- si le mot de passe est frappé depuis une machine compromise (contenant une capture de frappe au clavier), ce dernier est récupérable. Or le CERTA observe

dans le cadre de traitements d'incidents que de tels outils malveillants sont fréquemment installés.
- le mot de passe est stocké sur le support amovible. Il peut donc être récupéré, sous une certaine forme, avec le reste des informations contenues (cf. le chapitre 3.1). Des tentatives de récupération par tests exhautifs reste possible, sans disposer de la clé en permanence.

5 Conclusions

Les périphériques de stockage USB offrent beaucoup d'avantages. Outre leur capacité importante, ils étendent actuellement leur champ d'action pour offrir à l'utilisateur des applications et des fonctionnalités multiples. Cependant, ces mêmes technologies peuvent également être utilisées à mauvais escient pour exécuter des actions malveillantes sur le système. *A contrario*, un système malveillant peut tirer profit de la qualité et la quantité des informations contenues sur ces supports, pour en dérober tout ou partie.

Il est important de considérer tout cela, pour un usage approprié de ces périphériques. Certaines mesures doivent être prises, selon le contexte, pour garantir un niveau de sécurité minimal. Etant donné l'usage répandu de ces appareils, un effort de sensibilisation est également nécessaire.

6 Documentation

- Caractéristiques de l'USB U3 :

  http://www.u3.com
- Comment désactiver la fonction autorun sur une machine Windows :

  http://support.microsoft.com/kb/q155217
- Site du standard USB :

  http://www.usb.org
- Documentation en français sur le fonctionnement de l'USB, par B. Acquier :

  http://acquier.developpez.com/cours/USB/
- Cours de Supélec par J. Weiss, "Le protocole USB' :

  http://www.rennes.supelec.fr/ren/fi/elec/docs/usb/usb.html

Gestion détaillée du document

09 novembre 2006
version initiale.
14 novembre 2006
corrections sur la forme.

Notes

... USB[1]
Le bus USB est l'interface matérielle, souvent incluse dans la carte mère d'un

ordinateur, permettant de relier l'unité centrale à un périphérique USB.
... verrouillage[2]
Cette opération est par exemple visible avec l'appel à la fonction `dasg`.

CERTA
2006-12-29

Navigation
Accueil
Accueil Privilèges
Jeu Boursier.com NEW
Broker online
22 Ordres
Cours de Bourse
PARIS
Cours en direct
Indices
Devises
Palmarès
Capitaux échangés
Cours de A à Z
DÉRIVÉS
Warrants
Certificats
Trackers
OPCVM
Sicav et FCP
NEW YORK
Indices US
Palmarès US
Françaises à NewYork
Infos & conseils
News - Paris
News - New York
News - Economie
Interviews
Rumeurs
Conseils Warrants
Introductions
Agenda
Communiqués presse
Accès Abonnés
Portefeuille Boursier
La reco du jour
Conseils Actions
Nos "exclus"
Nos stratégies
Avis des brokers
Valeurs opéables
SERVICES BOURSE
Services mobiles
Orange
SFR
Bouygues Tel.
Audiotel

Alcatel-Lucent — FR0000130007 - ALU

Ajouter à : ma liste mon portefeuille
Articles | Cours | Dérivés | Société | Graphique | Forum | Brokers | Analyse Tech
News | Conseils | Rumeurs | Interviews | Introduction | OST | Conseils warrants

Cotation du 18/05/2007 à 09h45

Dernier	Variation	Ouverture	Plus haut	Plus bas	Volume
9,91 €	+ 0,71 %	9,80 €	9,94 €	9,80 €	549 296

Chiffres
Capi. 22 889 M€
CA '05 13 135 M€
PER détail
RDT '06 1,61 %
Plus de chiffres
Informations
Place Paris
Marché MCA
SRD éligible
PEA éligible
Notre avis
11/05 PAYANT 9,98 €
24/04 PAYANT 9,05 €
26/03 PAYANT 8,67 €
05/03 PAYANT 9,20 €
09/02 PAYANT 10,42 €
Menu
Voir aussi
Toutes les news Paris
Options
Imprimer
Ajouter portefeuille
Ajouter à ma liste
Flash informations
09:58 - Reuters
Alain Juppé nommé numéro deux du gouvernement
09:55 - News
Marchés : le CAC se rapproche de ses meilleurs niveaux annuels
09:52 - News
Gouvernement : Jean-Louis Borloo nommé ministre de l'économie et de l'emploi
09:50 - News
Theolia : un application portant sur 0,53% du capital traitée
09:49 - News
Enel : feu vert du gouvernement espagnol à la montée dans Endesa
09:38 - News
Sorefico Coiffure : en croissance de 4,4% au premier trimestre
09:35 - News
AstraZeneca : feu vert de la FDA à

News

Alcatel-Lucent : un disque de données salariés de Lucent envolé

18/05/2007 - 08h55 | aucun commentaire dans le forum DIVERS

(Boursier.com) - Voilà une affaire qui ne devrait pas avoir de retentissements financiers, mais qui n'arrange pas vraiment l'image du groupe aux Etats-Unis. Alcatel-Lucent a annoncé cette nuit avoir été informé le 7 mai par un prestataire qu'un disque dur contenant des informations personnelles avait été perdu. Le disque contient notamment toutes les données (nom, adresse, numéro de sécurité sociale, salaires, pensions) de salariés actuels et retraités américains de Lucent ainsi que de leurs ayant-droits. Il ne comprend pas en revanche de données comme les numéros de carte de crédit ou les mots de passe.

Le disque disparu avait été préparé par Hewitt Associates pour livraison par UPS à Aon Corporation. Il s'est évaporé ou a été volé lors de son transfert, soit entre le 5 avril et le 3 mai. Alcatel-Lucent a averti les autorités fédérales américaines qui ont ouvert une enquête, et mène en parallèle en interne ses propres investigations. Le groupe assume sa part de responsabilité dans cette disparition et assure les personnes figurant dans le fichier qu'il fera tout pour minimiser la portée de sa disparition.

A.B.

Soyez le premier à réagir à cet article !
Ajouter un commentaire
Les news précédentes

Accueil
Rubriques
Technologie
Economie IT
Développement
Solutions PME
SSII
Emploi/Formation
Micro
Numérique
Agenda
Vidéos
Thèmes
LMI Blogs
Téléchargements
Conférences
Forums
Newsletters
Flux RSS
Zone Directe
Livres Blancs

Sécurité
Inscrivez-vous XML
Consulter le centre de compétences

Version imprimable | Envoyer à un ami | Recevez les news

Les services informatiques, premiers responsables des fuites de données

Edition du 05/12/2007 - par Marie Calzergues

Selon une étude du cabinet Orthus, 30 % des fuites de données sensibles trouvent leurs origines dans le service informatique de l'entreprise. Et elles auraient toutes pu être évitées en appliquant le règlement intérieur des sociétés.

Après plus de 100 000 heures d'activité supervisées, le verdict d'Orthus, un cabinet britannique spécialisé dans la sécurité, est tombé. Les services informatiques sont les principaux responsables des fuites de données (à 30 %) devant les services clients à 22 %. Pour Richard Hollis, directeur d'Orthus : « Cette étude confirme la règle : plus les droits d'accès sont élevés, plus la tentation d'en abuser est grande. Les sociétés doivent considérer l'espion interne comme la première menace pour leurs affaires. Sans cela, aucune sécurité réelle ne peut être atteinte. » De plus, l'enquête a prouvé que dans 68 % des cas, des appareils mobiles (portables, PDA, smartphones, voire des baladeurs MP3 ou des clés USB) ont été utilisés. Parmi les autres outils privilégiés pour la fuite de données se trouvent les webmail, les réseaux sociaux et les logiciels de messagerie instantanée. Dans tous les cas observés, une application plus stricte des règles de sécurité internes auraient suffi à éviter ces fuites.
Cette enquête a été menée en installant des « mouchards » sur les postes de travail et les serveurs des entreprises impliquées, qui ont fourni une liste de mots-clés et de fichiers sensibles spécifiques à leur activité.

En savoir plus
Le site d'Orthus

Rejoignez lemondeinformatique.fr, commentez cet article
Nombre de commentaires postés (0) - Lire tous les commentaires

Pour commenter cet article inscrivez vous ou identifiez vous ci-dessous si vous êtes déjà inscrit :

Email :
Mot de passe : oublié ?
Mémoriser mes identifiants
OK

L'ACTUALITÉ DU JOUR

OPEN SOURCE
Verizon attaqué pour non respect de la GPL
(10/12/2007 12:50) - Les défenseurs des logiciels libres n'hésitent plus à se défendre devant les tribunaux. (...)

FORMATION
Le correspondant informatique et libertés entre à l'université
(10/12/2007 11:42) - Les universités de l'Hexagone viennent d'annoncer la création d'un réseau de correspondants (...)

SÉCURITÉ
Les 10 « pertes de données » les plus surprenantes de l'année
(10/12/2007 10:33) - Décembre est l'heure des bilans et l'informatique n'y échappe pas. D'autant que certains (...)

STOCKAGE
Seagate rachète un spécialiste de la recherche de preuves
(10/12/2007 10:07) - Le fabricant de disques durs Seagate Technology vient de racheter son compatriote (...)

OPEN SOURCE
La Région Ile de France adhère à l'Adullact
(07/12/2007 17:56) - L'Association des Développeurs et des Utilisateurs de Logiciels Libres pour les Administrations (...)

PÉRIPHÉRIQUES
Explosion de la demande en capacité de stockage externe
(07/12/2007 16:57) - Que se passe-t-il ? Au troisième trimestre, IDC a constaté une hausse exceptionnelle (...)

Articles récents SÉCURITÉ

Les 10 « pertes de données » les plus surprenantes de l'année
(10/12/2007 10:33) - Décembre est l'heure des bilans et l'informatique n'y échappe pas. D'autant que certains (...)

Microsoft terminera l'année avec sept correctifs dont trois sensibles

Sondage flash
Pour vos contrats, vous préférez
Un gros acteur pour l'assurance de tout trouver
Privilégier les acteurs locaux et/ou indépendants
Panacher votre panier selon vos besoins
Voter

LMI Vidéo
> Les Entretiens
> Les Webcasts
> Les Reportages

Conférences
29/01/2008
MOBILITE
De 8h30 à 14h00 à l'Automobile Club de France - Paris 8è
s'inscrire
toutes les conférences

Agenda
Du samedi 15 décembre 2007 au samedi 15 décembre 2007
Cap'Tronic 2007
Sélestat (67)
en savoir plus
tout l'agenda

Réseaux-Télécom.net

L'humain reste le maillon faible de la sécurité du SI

Edition du 24/09/2007 - par Marie Caizerques

Dans son rapport annuel « 2007 Global Security Survey », le cabinet Deloitte Touche Tomatsu montre que les employés et les clients restent le plus grand facteur de risque d'une institution financière.

Mené auprès de 169 institutions financières dans le monde, le sondage « 2007 Global Security Survey » du cabinet Deloitte Touche Tomastu (DTT) montre que le facteur humain (employés, clients ou partenaires) reste la faille principale dans la sécurité des systèmes informatiques. Quelque 65 % des entreprises interrogées ont subi au moins une attaque l'an dernier provenant soit de l'intérieur (pour 31 % d'entre elles), soit de l'extérieur (pour 65 % d'entre elles). Les attaques de l'intérieur proviennent de mauvaises manipulations de la part des employés qu'elles soient intentionnelles, ou résultant d'erreurs ou d'ignorance.

Un paradoxe sécuritaire

Si cela inquiète 91 % des participants au sondage, bien peu essaient toutefois d'y remédier. Seules 63 % des institutions financières interrogées disposent d'une stratégie d'information sur la sécurité. Et 22 % d'entre elles n'ont fourni aucune formation à leurs employés sur la sécurité en un an. Du coup, seulement 30 % des sociétés interrogées estiment que leurs employés ont les compétences nécessaires pour faire face à des problèmes de sécurité. « Ces résultats contradictoires soulignent le paradoxe sécuritaire auquel sont confrontées les institutions financières », affirme Adel Melek, dirigeant du groupe sur la gestion des risques et de la sécurité au sein de DTT. « D'un côté, il est clair que les répondants ont identifié les principaux risques et les mesures à prendre pour améliorer leur sécurité. Et de l'autre, de nombreuses organisations financières sont en retard pour mettre ces mesures en place. »

Si les employés représentent un risque majeur, ils ne sont pas les seuls. Les clients des institutions financières restent le risque principal. Ils sont en effet le vecteur privilégié par les cyber-criminels pour mener les trois principales attaques menaçant des institutions financières : virus et vers, spams et phishing. Pour opposer un barrage efficace, la sécurité se heurte à un impératif commercial et au travail de titan que cela représenteraient.
66 % des sociétés interrogées se refusent à tenir leurs clients responsables de ces attaques, et à se sentir concernés par d'éventuelles failles de sécurité sur les ordinateurs de leurs clients.

En savoir plus
Global Security Survey 2007

Url :
http://www.reseaux-telecoms.net/actualites/lire-l-humain-reste-le-maillon-faible-de-la-securite-du-s

Mobilegov, Spin-off du projet européen eJustice (développement des technologies pour la mise en place de la carte d'identité biométrique - www.ejustice.eu.com), a été créée en 2004 en France et au Royaume-Uni.

Mobilegov sait détecter, par des moyens logiciels, toute modification (hard ou soft) dans un système informatique. Sa technologie est brevetée en Europe et aux USA. Alors que pour beaucoup d'entreprises, la sécurité se résume à interdire l'usage de périphériques potentiellement dangereux, par exemple en bloquant les ports USB au détriment de l'efficacité, Mobilegov vous permet d'utiliser les outils les plus performants, mais de façon contrôlée et personnalisée en fonction des besoins des collaborateurs.

Mobilegov répond de façon unique aux problèmes du vol de données dans les entreprises en proposant d'étendre la sécurité du réseau d'entreprise aux périphériques à mémoire (clés uSB, disques, graveurs, etc.), empêchant l'utilisation d'un périphérique hors de l'entreprise.

Link Resource

Mobilegov

TVEP

Mobilegov opens an office in the 'UK Silicon Valley'

French security software editor Mobilegov launches its UK presence this autumn in Reading at the heart of the Thames Valley following several months of market research and supported by the Thames Valley Economic Partnership (TVEP), South East England Development Agency (SEEDA) and UK Trade & Investment (UKTI) in Paris.

A strategic location

Mobilegov is a French company developing original and patented software to protect companies and organisations against the threat from the use of unauthorised equipment (PDAs, Smartphones, USB sticks, external and internal drives etc.). At this stage the company has two main solution offerings, Device Authenticator which protects networks against the use of unwanted removable media devices and Device Linker which allows the use of USB sticks only on authorised configurations. Mobilegov is a global player in Data Loss Prevention helping companies to protect their main asset - their data. Mobilegov has opened an office in GreenPark, Reading next to companies such as Cisco, Symantec and LogicaCMG. Managing Director François-Pierre Le Page has spent much time searching for the ideal location for its UK centre.

"As a leading patented technology owner, we were very strongly encouraged by SEEDA and TVEP to setup in the UK. The fact that Sophia Antipolis, where we have our Head Office, has many similarities with the Thames Valley (Large ICT Community) made our choice easier. We have built a fantastic link between local Government agencies and, at the same time, it is crucial for the development of our network to stay close to our resellers and partners"

Mobilegov has built a significant and impressive network of partners in Europe and starts its operations in the UK with LogicaCMG. The company is supported by the French Government and its solutions are used by organisations within diverse markets such as Military & Defence, Nuclear and Energy, Universities and R&D centres.

Ben Churchill, TVEP's Inward Investment Manager said "We are delighted to welcome MobileGov to the Thames Valley, where it can enjoy the company of some of the world's leading IT companies and join a business community that strongly supports and encourages innovation. MobileGov is ideally placed to develop its position as a technology leader and to engage with new partners and customers in the UK".

Laetitia Régnault, SEEDA's Director of Business Development in France said that "MobileGov's dynamism and confidence to expand into new markets made our job of supporting them by creating introductions and helping build key relationships a pleasure and contributed greatly to their successful arrival in the UK".

About Mobilegov

Mobilegov is a French security software editor providing hardware identification solutions, device access management solutions and USB storage devices having the capacity to recognise the configurations they are connected to. All the Mobilegov solutions are patented. The solutions are distributed by a network of international resellers and Integrators and protect companies and organisations of any size. Mobilegov is a private company, founded in 2004 with its head office in Sophia Antipolis, the French Technopole.

Device Linker, la clé USB sécurisée - Source : zebulon.fr

Par Yann - publié le 30/07/2007 à 14h31

Les clés USB ont depuis bien longtemps pris une place prépondérante dans notre quotidien. Pourtant, en cas de perte ou de vol, nos précieuses données peuvent se retrouver entre de mauvaises mains. De plus, en ce qui concerne les entreprises ou les administrations publiques, ces clés introduisent une nouvelle menace de sécurité où des données confidentielles peuvent facilement être dérobées. Face à ce constat, la société Mobilegov propose une clé USB sécurisée utilisable uniquement sur des PC autorisés. Nous sommes donc allé à la rencontre de cette société afin de pouvoir tester en conditions réelles cette solution de stockage sécurisée.

Introduction

Les clés USB permettent aujourd'hui à tout un chacun de transporter ou échanger facilement ses fichiers, que ce soit des photos de ses dernières vacances ou encore des données confidentielles de première importance. Mais quelque soit le type d'informations contenues sur la clé, sa perte ou son vol peut être problématique.

De même, la prolifération des périphériques de stockage amovible tels que les clés USB, PDA, baladeurs audio ou encore téléphones portables constituent une nouvelle menace de sécurité dans les entreprises où un collaborateur mal intentionné peut voler des données confidentielles sur un support amovible.

Pour contrer ces problèmes de sécurité, il existe différents moyens de protéger les données d'une clé USB. On trouve ainsi des clés intégrant un encryptage matériel AES 128 bits où les données sont cryptées "à la volée". D'autres constructeurs se sont quant à eux tournés vers des clés biométriques. Là encore, les données se voient cryptées et votre empreinte digitale fait alors office de mot de passe.

Si de telles solutions sont très efficaces en cas de perte où de vol de la clé, elles ne répondent pas à la problématique rencontrée par les entreprises : la fuite de données sensibles à l'extérieur de la société.

La solution proposée par *Mobilegov*, **Device Linker**, permet de contrer cette double problématique : en cas de perte ou de vol, les données seront protégées et la fuite des données à l'extérieur sera rendue impossible.

Nous avons donc rencontrés les dirigeants de *Mobilegov* afin de pouvoir tester la solution Device Linker. Nous avons effectué notre test avec la version de 512 Mo qui est proposée au prix de 29.90€.

javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/device-lir

La clé en elle même est tout ce qu'il y a de plus classique et adopte un look plutôt élégant avec une partie en plastique transparent qui laisse apparaître les composants internes et une autre partie en aluminium légèrement brossé du meilleur effet. A noter que le périphérique existe également en version 1Go, 2Go, 4Go et 8Go. Enfin, quelque soit la capacité de la clé, le système de protection utilisé reste le même.

Une clé USB U3

La technologie du Device Linker repose sur la plateforme U3. Avant de voir plus en détail le fonctionnement de la clé de *Mobilgov*, intéressons-nous tout d'abord à l'U3. La plate-forme U3 permet de transformer une clé USB en un véritable bureau virtuel pouvant contenir à la fois des documents classiques mais aussi différentes applications directement utilisables sur le support amovible.

L'U3 est donc un standard créé par la société du même nom. Si à l'origine seules deux sociétés (Scandisk et M-Systems) soutenaient cette initiative, de nombreux autres constructeurs utilisent aujourd'hui la licence U3 afin de proposer des clés USB U3.

Une clé U3 permet donc de transporter aussi bien des données, tout comme le fait une clé USB classique, mais aussi des applications avec leurs paramètres de configuration. Ainsi, un client email conservera ses informations de connexion au serveur email distant et un navigateur web possèdera ses favoris.

Le principe de fonctionnement d'une clé U3 est extrêmement simple : dès son insertion, une interface appelée *Launchpad* est automatiquement exécutée. Cette application, ressemblant à s'y méprendre au menu démarrer de Windows XP, permet de lancer toutes les applications présente sur la clé U3. La partie de droite de Launchpad quant à elle, permet de gérer les applications de la clé.

Concrètement, une clé U3 possède deux partitions : la première, correspondant à une partition

CD-ROM (en lecture seule), contient l'application qui se lancera automatiquement lors de l'insertion de la clé. La seconde partition quant à elle, est privée et protégée par mot de passe. Il existe de nombreuses applications compatibles U3. Ces dernières, facilement reconnaissables car portant l'extension .u3p, sont regroupées sur cette page (http://software.u3.com/) sur le site de l'U3.

Enfin, pour plus de sécurité, chacune des applications créera automatiquement son espace de stockage temporaire sur la clé. Si celle-ci venait à être retirée de la machine, cet espace serait automatiquement effacé.

La technologie utilisée par Mobilegov pour la clé Device Linker prend donc place sur un support U3. Voyons ensemble le principe de fonctionnement de cette clé sécurisée.

Principe de fonctionnement et installation

Le principe théorique de fonctionnement de la clé Device Linker est très simple. Dès l'insertion de la clé, cette dernière va vérifier si la machine utilisée est autorisée. Si oui, l'accès aux données contenues sur la clé sera alors possible. Dans le cas contraire, l'accès sera interdit.

Dès la première insertion de la clé Device Linker, le Launcher U3 s'exécute. En explorant la partition de données de la clé, nous avons les fichiers suivants :

Un double clic sur *DeviceLinkerSetup1_0_Single.msi* permet de lancer l'installation. Cette dernière est tout à fait classique et se déroule sans encombre.

Une fois l'installation terminée, il vous sera nécessaire d'indiquer votre identifiant et le numéro de série correspondant.

Ces informations sont présente dans l'emballage de la clé et sont visibles uniquement après avoir ouvert le blister du Device Linker. Nous avons testé ici la *Single Edition* du Device Linker, l'identifiant que nous indiquons ici est unique. Si cette version est plutôt orientée vers les particuliers, il existe néanmoins une version destinée aux entreprises. Dans ce cas, seul le logiciel est fourni. L'ensemble des clés U3 existantes est alors compatible.

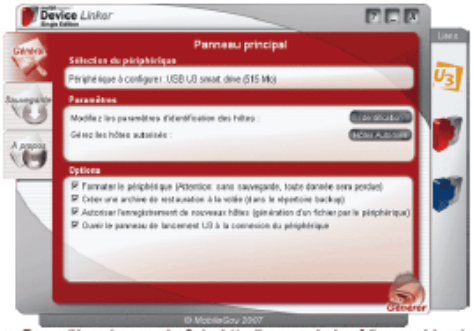
Initialisation du Device linker

Après l'insertion de la clé dans l'ordinateur, cette dernière est automatiquement reconnue et son initialisation commence.

Un double clic sur l'icône du programme va alors nous permettre de configurer la clé USB.

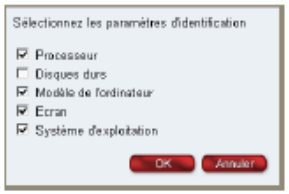
Cette étape permettra à la partie logicielle de fonctionner avec notre clé U3.

La fenêtre principale de l'application permet l'identification et la gestion des hôtes, c'est à dire des ordinateurs qui auront la possibilité d'accéder au contenu protégé de la clé U3.



(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/gen

La configuration de la méthode d'authentification est très simple. Un clic sur le bouton *Identification* permet de sélectionner les éléments de son choix.



Comme nous le voyons, il y a différents paramètres d'identification possible : processeurs, disques durs, modèle d'ordinateur, écran et système d'exploitation. Ces différents éléments seront alors utilisés pour générer (de façon transparente) un identifiant unique correspondant à la machine. Ainsi, le PC hôte pourra par la suite être reconnu et identifié.

Plus le nombre d'éléments pris en compte est important, plus l'identification sera fiable. Il reste néanmoins possible de ne pas prendre en compte certains éléments de la configuration en décochant ceux de son choix. Cela permettra par exemple de ne pas avoir à générer une nouvelle identification de son périphérique si vous changez régulièrement de disque dur ou de système d'exploitation. Cela peut également être utile dans le cas de parc informatique important où l'on peut planifier à l'avance les upgrades des machines en sachant quels éléments seront changés ou non.

Ensuite, il ne nous reste plus qu'à configurer la clé avec les éléments nous venons de choisir en cliquant sur le bouton *Générer* en bas à droite de la fenêtre de l'application.

(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/gen

Le programme nous rappelle alors les différents paramètres d'identification des hôtes que nous avons choisi ainsi que les machines autorisées à accéder à la clé. Un clic sur le bouton *Lancer* permet alors la génération de la clé qui prendra quelques secondes (voir minutes en fonction de la puissance de la machine).

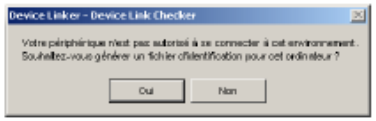
Une fois la configuration de la clé terminée, vous pouvez la retirer. Le contenu de la partition cryptée sera alors accessible uniquement sur notre machine.

Gestion des hôtes

Toujours dans la fenêtre principale de l'application, il est possible de consulter les hôtes autorisés. Un simple clic sur le bouton correspondant permet de sélectionner les machines pour pourront accéder au contenu de la clé :

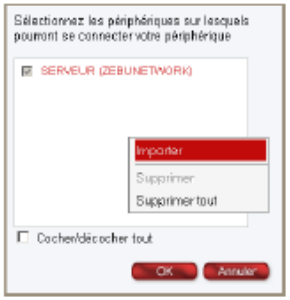
Par défaut, seule la machine sur laquelle l'application a été installé est autorisé. La machine principale (le "*Master Host*") est ici indiquée en rouge. C'est cette machine qui va gérer les autorisations de la clé. Il est bien entendu possible d'ajouter d'autres machines par la suite de façon très simple : l'insertion de la clé U3 sur un autre PC va automatiquement proposer la création d'une nouvelle identification.

Ainsi, lors de l'insertion de la clé sur une machine inconnue, la fenêtre suivante apparaîtra :



Si vous acceptez, un fichier ayant pour extension *.qki* sera automatiquement généré. Pour autoriser la machine, il faut ensuite rapatrier le fichier *.qki* sur la machine principale. Ce rapatriement du fichier d'identification peut se faire par email, réseau ou à l'aide d'un autre équipement de stockage. On ne peut bien entendu pas encore utiliser notre clé U3 car celle-ci n'étant pas encore autorisé, il n'est pas possible d'y copier un quelconque fichier.

Sur le poste maître, il est maintenant possible d'importer simplement le fichier d'identification en effectuant un clic droit dans la fenêtre de gestion des hôtes. Dans le menu contextuel qui apparaît, il suffit simplement de choisir l'option *Importer* puis, à l'aide d'un bouton parcourir, d'aller chercher le fichier d'identification généré par notre machine inconnue.

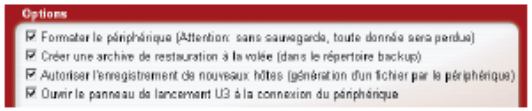


Après avoir ajouté la (ou les) machine(s) autorisée(s), il suffit simplement de régénérer la clé pour que celle-ci soit acceptée sur les nouveaux hôtes.

Sauvegarde, restauration et options

L'interface de gestion de la clé propose également différentes options ainsi que la possibilité de créer une sauvegarde du contenu de la clé. En cas de perte, il sera donc toujours possible de créer une nouvelle clé à partir de notre machine principale.

Les options disponibles sont les suivantes :



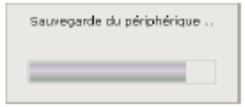
Il est donc possible de formater la clé, de créer une sauvegarde automatique lors des générations, d'autoriser l'enregistrement de nouveaux hôtes ou encore de lancer ou non le *LauchPad* lors de l'insertion de la clé.

A noter que si l'on n'autorise pas la création de nouveaux hôtes, aucune demande d'identification de sera effectuée lors de l'insertion de la clé sur une machine inconnue.

Enfin, pour sauvegarder l'ensemble de données contenues sur la clé, il suffit simplement d'aller dans l'onglet *Sauvegarde* de l'application.

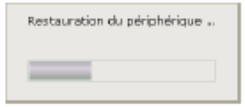
(javascript:ShowPopup('/pop-image.php?pic=http://www.zebulon.fr/images/dossiers/device-linker/sau

Après avoir choisi le chemin et le nom du fichier de sauvegarde, un clic sur le bouton *Sauver* lance la sauvegarde des données.



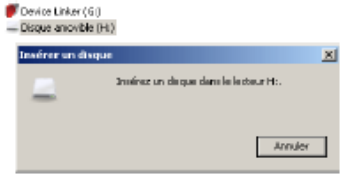
Le fichier généré sera une simple archive au format .zip.

Concernant la restauration, il suffit d'aller sélectionner une archive de sauvegarde sur notre disque dur puis de cliquer sur le bouton *Restaurer* afin que l'arborescence complète et les fichiers soient restaurés sur la clé.



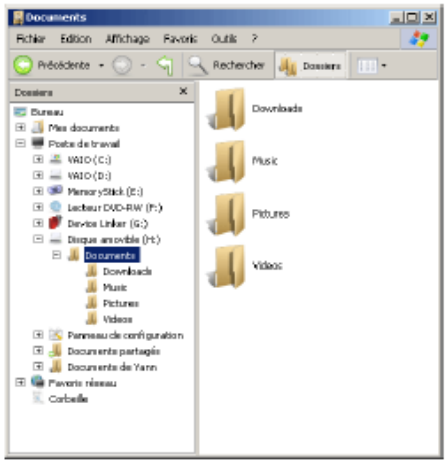
Conclusion

Si le principe de la clé Device Linker est simple en théorie, son fonctionnement l'est tout autant dans la pratique. Ainsi, lors de l'insertion de la clé sur une machine inconnue, nous n'avons pas pu accéder à la partition de donnée.



Si la clé est bien détectée et que la partition en lecture seule est visible, la seconde partition de la clé U3 est inaccessible. Windows la reconnaît comme un lecteur dans lequel aucun disque n'aurait été inséré.

Après avoir régénéré le périphérique en y ajoutant l'identification de notre nouvelle machine, l'insertion de la clé laisse apparaître l'ensemble du contenu de la seconde partition.



Cette partition est bien entendu accessible en lecture et écriture.

Pour le particulier, la version *Single Edition* permettra de protéger efficacement ses données contre la perte ou le vol en toute simplicité. Après avoir autorisé sa (ou ses) machine(s), l'utilisation de la clé sera totalement transparente. Le point fort du système est qu'il ne sera pas nécessaire pour l'utilisateur de mémoriser un quelconque mot de passe puisque celui-ci est généré automatiquement et reste inconnu de l'utilisateur. Tout se fait de façon transparente et en toute simplicité.

Pour l'entreprise, le bénéfice est double si la logique de sécurité réseau est respectée. Non seulement les données sont protégées contre la perte ou le vol mais toute tentative de fuite de données par un collaborateur peu scrupuleux est interdite. Bien sûr, rien n'empêche alors l'utilisation d'une clé USB classique pour récupérer des données confidentielles. Dans ce cas, il est alors nécessaire d'utiliser la solution *Device Authenticator* conjointement à Device Linker. Cette solution, que nous n'avons pas testée, permet de gérer tous les équipements se connectant à un réseau d'entreprise. Ainsi, un périphérique non autorisé ne pourra fonctionner sur une machine donnée. En interdisant alors l'utilisation des autres périphériques de stockage externe, le réseau est donc protégé contre la fuite de données.

Pour conclure, nous avons été séduit par le fonctionnement du Device Linker. Les données sont protégés de façon simple et efficace et surtout, de façon totalement transparente. Une fois nos différentes machines autorisées, on oublie que nous avons entre les mains une clé où nos données sont en sécurité !

Nous pouvons par contre distinguer deux bémols : tout d'abord, la clé ne fonctionne que sous Windows XP. Si l'on peut se douter qu'une telle solution ne soit pas multi plateforme, on regrette toutefois l'absence du support de Vista. Même s'il ne s'agit pas d'un besoin urgent

pour les entreprises, Windows Vista commence petit à petit à s'implanter dans les foyers. Fort heureusement, le fonctionnement de Device Linker est prévu sous cet OS pour 2008.

Enfin, le type même du fonctionnement de la clé oblige l'utilisateur à repasser par le poste maître pour gérer les autorisations. Si ce principe de fonctionnement est tout à fait logique, il peut empêcher l'utilisation de la clé si vous n'avez pas accès au poste maître pour ajouter l'identification de la nouvelle machine.

Malgré ces deux éléments gênants, force est de reconnaître que le Device Linker fonctionne très bien. Sa technologie (qui est brevetée) permettant d'identifier une machine fonctionne à merveille, la distinction des équipements se faisant de manière totalement unique. Même deux configurations exactement similaires seront différenciées. C'est là une alternative originale et efficace face aux autres clés USB sécurisées du marché.

Pour plus d'informations, vous pouvez consulter le site Device Linker (http://www.devicelinker.com/) de Mobilegov.

Source : Zebulon.fr (http://www.zebulon.fr/dossiers/78-cle-usb-securisee-device-linker.html)

Réseaux-Télécom.net

La cybercriminalité se professionnalise

Edition du 21/09/2007 - par Eddye Dibar

Selon le dernier *Rapport sur les menaces à la sécurité Internet* publié par Symantec, la cybercriminalité devient une activité de plus en plus professionnelle et commerciale. Les pirates et autres organisations criminelles cherchent à tirer toujours plus de profit de leurs attaques en ligne. Aujourd'hui elles n'hésitent pas à développer leurs propres réseaux de pirates. « Les dernières observations de Symantec montrent que le cybercriminel d'aujourd'hui est extrêmement compétent et intelligent », explique Lee Sharrocks, directeur commercial grand public de Symantec au Royaume-Uni.

D'autant que des outils simples et clés en main circulent sur le Web. Conçus par des cybercriminels, ces kits quasi *plug and play* sont vendus entre 35 et 75 euros et permettent même à des personnes non expérimentées d'organiser, en quelques clics, des campagnes de phishing par exemple.

Depuis plusieurs semaines, l'éditeur de solutions de sécurité recense un nombre croissant de serveurs commerciaux clandestins. Ces plates-formes permettent aux pirates de vendre et d'acheter tout type d'information susceptible d'être monnayée : cartes de crédits, comptes bancaires, mots de passe de boîtes électroniques, etc (voir encadré).

Au cours du premier semestre 2007, les Etats-Unis hébergeaient le plus grand nombre de serveurs commerciaux clandestins, avec 64% du total identifié par Symantec. « L'Internet clandestin se développe à une vitesse inquiétante », alarme Lee Sharrocks. Selon les dernières tendances le nombre de sites d'enchères au marché noir continue d'augmenter. « Il s'agit d'un marché illégal de plusieurs milliards de dollars », conclut-il.

Répartition des articles mis en vente sur les serveurs commerciaux clandestins

Rang	Article	% de tous les articles proposés	Prix moyen
1	Cartes de crédit	22 %	0,35€ - 3,62€
2	Comptes bancaires	21 %	22€ - 290€
3	Mots de passes de boites e-mail	8 %	0,73€ - 254€
4	Mailers	8 %	5,8€ - 7,3€
5	Adresses e-mails	6 %	1,4€/Mo - 2,9€/Mo
6	Proxies	6 %	0,35€ - 2€
7	Identités complètes	6 %	7,3€ - 108€
8	Scams	6 %	7,3€/semaine
9	N° de sécurité sociale	3 %	3,6€ - 5€
10	Shells sous Unix	2 %	1,4€ - 7,3€

Source: Symantec Corporation

Url :
http://www.reseaux-telecoms.net/actualites/lire-la-cybercriminalite-se-professionnalise-17147.html

Mon panier Téléchargement
Votre panier est vide

Téléchargement de logiciels

Actualités
Nouveautés
Affaires de Fnac

Catégories
Arts et culture
Bureautique
Educatif
Internet
Jeux détente
Jeux enfants
Jeux Vidéo
Loisirs / Vie Pratique
Multimédia
Sécurité
Traduction
Utilitaires

Services Fnac
» Aide au téléchargement
» Extension de téléchargement
» Conditions générales de vente

nexway
www.nexway.fr

Rechercher | Logiciels à télécharger | OK

Accueil >> Téléchargement de logiciels >> Sécurité >> Sauvegarde

Device Linker - single soft

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

Editeur : MOBILE GOV
En téléchargement

Durée de téléchargement -512Ko / 07mn -2Mo / 01mn -8Mo / 00mn

29.90 €

Disponibilité immédiate

Télécharger ce logiciel

En détail | Configuration

Description

Pour que vos périphériquesde stockage de données ne fonctionnent que sur vos machines !

Device Linker® vous protège contre le vol de vos données sauvegardées sur votre clé U3 en cas de perte ou de vol. Tant que votre clé USB U3 ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible ! Device Linker® ne nécessite aucune modification de votre environnement informatique.

Protégez-vous contre :

L'UTILISATION DE VOS PERIPHERIQUES USB U3 SUR DES PCs NON AUTORISES
La technologie Linker® rend vos périphériques USB U3 inutilisables en dehors de l'environnement que vous choisissez (réseau de l'entreprise, pool de machines).

LA PERTE OU LE VOL DE VOS CLES USB U3
La clé USB reste inaccessible tant qu'elle ne reconnaît pas l'ordinateur sur lequel celle-ci est connectée. Device Linker® ne nécessite aucune modification de votre environnement informatique. La protection s'applique à tous les périphériques U3 existants.
Une interface d'administration simple vous permet de configurer vos périphériques et les hôtes sur lesquels ils fonctionneront.

Principales fonctionnalités :

Définition dynamique des environnements : sélection des paramètres d'identification d'une machine hôte à partir d'une liste préétablie (CPU/ OS/ cartes mère/ etc.).

Gestion des machines hôtes : enregistrement direct sur une machine non identifiée et gestion des listes de machines autorisées.

Enregistrement des modifications sur la clé et gestion transparente et sécurisée (mot de passe généré inconnu de l'utilisateur) d'une partition chiffrée et cachée.

Options de backup et de restauration des clés

Peut s'utiliser conjointement avec Device Authenticator® les clés Device Linker pouvant ainsi être intégrés à la logique de sécurité réseau.

Comment fonctionne Device Linker®

1. Au cours d'une première étape de configuration, le périphérique est connecté à n'importe quel PC du Réseau afin de définir l'environnement sur lequel il pourra être utilisé : ce PC, un groupe de PC, le LAN sur lequel le PC est lui-même connecté.

2. Il faut ensuite définir les mesures à prendre si le périphérique est connecté à un environnement imprévu : rendre le périphérique illisible, transmettre discrètement des informations sur l'environnement, détruire les données ou demander une autorisation d'usage temporaire.

Principaux matériels compatibles :
Certifié U3, Device Linker® reconnaît les matériels informatiques USB U3

Configuration requise :

- OS : Windows 2000/2003/XP/VISTA (administration sous XP)
- Processeur : Pentium II
- Espace disque dur : 40 Mo d'espace libre
- Mémoire vive : 256 Mo RAM

[SÉCURITÉ]

L' « ADN numérique » des périphériques sécurise leurs connexions

Mobilegov propose une solution de gestion de la sécurité des équipements amovibles, dont les smartphones et les clés USB.

Gilbert Kallenborn , 01net., le 20/12/2007 à 15h55

Avec Device Authenticator Pro Edition (DAPE), la jeune pousse française Mobilegov fournit une solution élégante à un problème qui prend de l'importance en entreprise : la gestion des périphériques amovibles. Ces équipements sont de plus en plus sophistiqués et donc difficiles à contrôler.

Clé USB, smartphone dernier cri ou simple iPod, tous peuvent servir au vol de données ou à la corruption du système d'information. *« En particulier, les clés USB U3, qui sont dotées d'un véritable microprocesseur, sèment la terreur dans les bureaux, car elles permettent de lancer des applications sans que le service informatique ne s'en rende compte »*, explique François-Pierre Le Page, directeur général et cofondateur de Mobilegov.

Vingt-trois types de périphériques identifiés

Pour endiguer cette marée d'objets non sollicités, Mobilegov propose d'affecter à chaque équipement un identifiant unique, qu'il baptise Qualification Key Identifier (QKI). Cet « ADN numérique » est obtenu à partir des qualités intrinsèques du matériel : les paramètres de fabrication, les dimensions, la catégorie, etc.

Ces données issues des couches basses des équipements sont agrégées selon un procédé breveté en 2005, pour obtenir le QKI. Mobilegov peut reconnaître 23 types de périphériques différents, du stockage USB au moniteur en passant par la webcam, les cartes Bluetooth et les tablettes graphiques.

A partir de là, la solution DAPE permet de définir des règles de sécurité millimétrées. Basée sur un serveur et des agents logiciels, elle peut ne permettre sur certains postes que la connexion de certains périphériques, voire d'un seul en particulier. Le branchement d'un périphérique inconnu bloque automatiquement toute communication avec lui et l'administrateur est informé en temps réel. L'entreprise peut également définir des plages horaires pour certains types d'utilisation.

Le contrôle de l'intégrité des équipements en prime

Mais ce n'est pas tout. Comme le QKI est généré à partir des composants d'un matériel, il permet aussi d'assurer son intégrité physique. Si dans un PC un disque dur a été remplacé ou une barrette de mémoire subtilisée, l'ADN numérique ne correspond plus. Une notification est envoyée au service informatique.

Mais que faire si un périphérique autorisé est utilisé pour transférer des données sur un ordinateur externe, non géré par DAPE ? Là encore, Mobilegov propose une solution.

Les clés USB Device Linker du fournisseur embarquent la même technologie d'identification et permettent de limiter leur fonctionnement à certains ordinateurs pré-définis. Au moment de la connexion, la clé scanne le poste et vérifie simplement son « code génétique ». Le fournisseur envisage d'intégrer ce procédé dans d'autres équipements comme les disques durs.

Enfin, les tarifs de DAPE restent abordables. La solution coûte autour de 25 euros par poste protégé, plus 15 % sur le contrat global en service de maintenance.

FORUM : soyez le premier à vous exprimer !

L' « ADN numérique » des périphériques sécurise leurs connexions

Réagir

Le test des hébergeurs

Semaine du 12 au 18 décembre 2007

Internet FR, une remontée fulgurante

Après plusieurs semaines de chute, qui l'ont mené à l'avant-dernière place du classement, Internet FR est 1er cette semaine. Cette remontée spectaculaire est due au remplacement de But - qui plombait les résultats d'Internet Fr - par Veolia dans la liste des sites hébergés par Internet Fr et testé par IP Label...

moyenne du 18 11 au 18 12 2007

rang	hébergeurs	dispo. sites (sur 100)	performance d'accès aux sites (sur 100)	qualité globale (sur 100)	tendance
1	Internet FR	99.68	96.20	98.81	▲
2	Omis	99.54	96.47	98.77	▼
3	Pictime	99.91	95.18	98.73	▼
	Moyenne	98.88	93.04	97.28	

› 01net.com, en partenariat avec ip-label, mesure chaque semaine les performances des hébergeurs

> tous les classements des hébergeurs

Le test des opérateurs

Pour retrouver tout le test des opérateurs VoIP
› Cliquez ici

Agenda

A ne pas manquer !
› Salon Les jeudis-Emplois informatique & ingénierie le 10/01/2008
› Moteurs de recherche et intranet le 10/01/2008
› Conférence APE2008 du 22/01/2008 au 23/01/2008
› Progilog du 22/01/2008 au 24/01/2008

> tous les salons et séminaires


“ Sécurité du poste de travail ”
mobilegov®
Device Authenticator
PRO Edition
“Maîtriser l’usage des équipements amovibles dans l’entreprise
et prévenir les fuites des données.”
www.mobilegov.com

Garantir l'intégrité des postes clients : le défi des organisations

Le maintien de l'intégrité du Système d'Information est un ENJEU CAPITAL car une défaillance de celui-ci peut entraîner la perte de l'entreprise d'aujourd'hui.

La prolifération des ports sur ces postes de travail (USB, WIFI, BlueTooth, Firewire, HDMI, lecteurs de cartes multi formats, …) et les capacités de stockage grandissantes des périphériques amovibles (clefs USB, cartes, Disques externes, PDA, Smartphone, lecteurs MP3,…) sont un réel problème pour la sécurité des entreprises car ce sont autant de portes ouvertes non surveillées.

Malgré des investissements coûteux, la simple utilisation de périphériques amovibles fait tomber l'entière protection déployée sur vos réseaux et permet à tout un chacun "d'emprunter" des données sensibles ou d'introduire virus ou autres malwares potentiellement catastrophiques pour votre organisation.

Les solutions de protection traditionnelles, efficaces contre les attaques logicielles (Antivirus, Firewall, Anti-Spyware, Cryptage, etc.), ne sont plus suffisantes. Le vol d'informations confidentielles ou sensibles représente une réalité quotidienne (avec ou sans la complicité de l'utilisateur).

Le changement ou la modification de composants internes du poste de travail est également un danger, car ceci permet de passer au travers des solutions de sécurité mises en place par l'entreprise à son insu.

Les solutions traditionnelles ne sont plus suffisantes : 62% des entreprises qui sont infectées par un virus informatique avaient un antivirus installé.(source : Yankee Group, Forrester)

70% des attaques d'ordinateurs, des failles de sécurité ou du vol de données provient de l'intérieur des organisations. (Source : Yankee Group Security Leaders)

76% des entreprises reconnaissent qu'augmenter la sécurité de leurs systèmes les rend plus efficaces et leur donne un avantage compétitif sur leur marché.
(Etude Pen, Shoen & Berland Associates pour Business Software Alliance)

Les lois et régulations internationales telles que Sarbanes Oxley (contrôle des flux d'informations au sein des sociétés) ou l'HIPAA (vie privée des patients) imposent aux société de sécuriser les informations sensibles ainsi que leurs flux et transferts.

Autorisez l'utilisation des périphériques amovibles tout en maîtrisant les dangers.

Protéger votre entreprise et vos collaborateurs.

En complément de vos systèmes de protection actuels, indispensables, notre solution Device Authenticator PRO Edition permet de contrôler et de gérer les flux d'informations à travers les composants/périphériques internes et externes des entreprises et des organisations mais aussi d'auditer l'utilisation de ces périphériques.

- Sécurisez vos réseaux contre le VOL DE DONNEES et l'introduction de MALWARE au travers des ports de vos postes de travail (USB, bluetooth, Wifi, firewire, …)
- Contrôlez les CONNEXIONS INTERDITES et éviter le divertissement au travail (musique, vidéo, jeu) par des connexions d'iPods, de clés USB, de disques, etc…
- Garantissez la CONFORMITE AVEC LES LOIS ET REGULATIONS INTERNATIONALES (Sarbanes Oxley, HIPAA, …)
- Contrôlez les MODIFICATIONS MATERIELLES tels que les changements ou les modifications de composants internes (piratage des matériels, vol de pièces détachées, …)

La Solution

mobilegov
Device *Authenticator*
PRO Edition

Maîtriser l'usage des périphériques et profiter des gains de productivité qu'ils apportent.

Parce que l'ajout ou le changement d'un composant dans votre environnement informatique constitue une menace :

- **Protégez les postes clients contre le branchement de périphériques non autorisés.**
- **Définissez, gérez et appliquez facilement vos politiques de sécurité.**
- **Recevez sur votre serveur des notifications en temps réel des "mauvais usages".**
- **Etendez votre politique de sécurité à tous les périphériques amovibles avec ou sans fil.**

Authentifier, sécuriser, déployer…

Comment fonctionne Device Authenticator ?

Grâce à notre technologie, Device Authenticator PRO Edition permet l'identification forte et unique de tous les sous ensembles électroniques (clef, disques, PDA, smartphones, postes de travail, …) en utilisant des "protocoles de couches basses". Cette technologie unique est brevetée depuis 2005.

1. L'administrateur identifie les périphériques autorisés ou interdits, par famille ou individuellement.
2. Il spécifie les actions à entreprendre lors du branchement d'un périphérique non autorisé.
3. Ces règles sont déployées automatiquement depuis le serveur sur tous les postes qu'il souhaite protéger.
4. Les agents de Device Authenticator veillent régulièrement de manière transparente pour l'utilisateur, bloquant toute communication avec un périphérique non autorisé et informent l'administrateur en temps réel de toute infraction.
5. La solution permet de déterminer des plages horaires pour les politiques (horaires de bureau, salons, présentations clients, ...)
6. Les agents ont la connaissance des politiques, le Poste de Travail est protégé même lorsqu'il n'est plus sur le réseau de l'entreprise.
7. L'agent ne peut pas être désactivé par l'utilisateur.

Prenez l'avantage :

- Notre technologie repose sur l'utilisation de couches basses et non sur des services Windows.
- Gère les périphériques au niveau des paramètres de fabrication infalsifiables (n° de série, type et famille).
- Communications Agents/Serveur sécurisées et cryptées (certificats X509, cryptage RSA).
- Vérifie l'intégrité des composants internes d'une machine afin d'empêcher l'usurpation d'un poste de travail sur un réseau (création d'une identification unique de la machine).
- Détecte tout changement de configuration matérielle sur les postes clients et réagit selon la politique définie (désactivation du périphérique incriminé, alerte email, logoff…)
- Permet une gestion unitaire ou par classe.
- Fonction de Sauvegarde et de restauration incluse
- Permet l'association utilisateur/périphériques.
- Fonctionne sous Windows (XP Home et Pro, 2000, 2000 PRO, 2003)
- Recherche et tri avancé des alertes et logs.
- Fichiers de données cryptés
- Documentation en ligne intégrée
- Grande facilité d'installation et d'exploitation

EVOLUTIF

Puissant, fiable, intuitif

- Seul Device Authenticator PRO Edition permet de sécuriser les équipements mobiles tels que PDAs ou smartphones en évitant de les utiliser comme passerelle.
- L'architecture client/serveur rend Device Authenticator évolutif quelque soit le nombre de pc dans l'entreprise.
- Fonctionne sous Windows (Linux, Mac, autres sur demande).
- Echanges sécurisés (certificats X509, cryptage MD5, RSA, SHA1)
- Disponible en Anglais et Français.
- Impacte les performances de façon minime.
- Protection active: le poste client reste protégé même s'il n'est pas connecté au réseau.

TECHNOLOGIE PORTABLE

Grâce à la technologie unique d'identification matérielle de Mobilegov, Device Authenticator n'est pas dépendant du système d'exploitation.
Notre solution peut être adaptée à une multitude d'environnements et peut supporter un réseau hétérogène.

CLASSES DE PERIPHERIQUES IDENTIFIES

1. Stockage USB - Clé USB, Disque dur externe USB,
2. Stockage IEEE 1394 - Disque dur externe FireWire,
3. Stockage SCSI - Disque dur SCSI,
4. Stockage IDE - Disque dur IDES,
5. Lecteur de disquettes - Lecteur de disquettes 3.5/5.25,
6. Disque Optique - Lecteur CDROM/DVD, Graveurs,
7. Port Parallèle,
8. Port Série - COM,
9. Infrarouge - Port IrDA,
10. PCMCIA,
11. Periphérique Biométrique - Lecteur de carte à puce, lecteur d'empreintes.
12. Périphérique d'imagerie USB - Appareil Photo, Scanner,
13. Webcam,
14. Périphérique TV USB - Périphérique TV USB à base de composants 28xx.
15. Son - Carte Son, Microphone,
16. Imprimante,
17. Carte Réseau - Carte Ethernet, Carte WIFI,
18. Modem RNDIS,
19. Bluetooth - Carte Bluetooth,
20. PDA - PDA, Smartphone,
21. Clavier,
22. Pointage - Souris, Tablette Graphique,
23. Moniteur.

mobilegov
Device *Authenticator*
PRO Edition

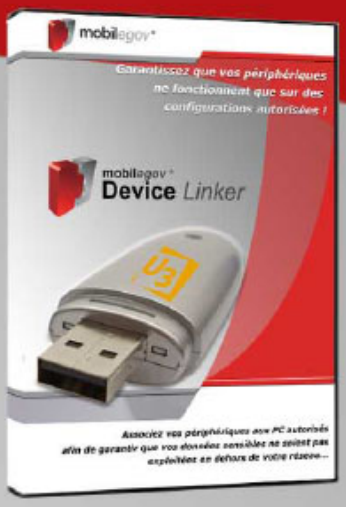
Mobilegov France
2000, route des Lucioles - Les Algorithmes
06901 Sophia Antipolis
France

Tel : +33 492 944 894
Fax : +33 492 944 895

Mobilegov UK
200 Brook Drive - Green Park
Reading RG2 6UB
United Kingdom

Tel : +44 118 949 7000
Fax : +44 118 949 7001

mobilegov
Device Linker



Pour que vos périphériques de stockage de données ne fonctionnent que sur vos machines !

La prolifération de périphériques de stockage de grande capacité tels que Clés USB, iPod®s, PDAs, Graveurs, Caméras et autres gadgets avec ou sans fil, introduit une nouvelle menace de sécurité dans les entreprises et les administrations publiques où des données sensibles peuvent être dérobées.

Device Authenticator® vous protège contre ce risque.

D'autre part, vous stockez des données sensibles sur vos périphériques amovibles.

Etes-vous protégé en cas de perte ou de vol du périphérique ?

Les protections à base de mot de passe ou de biométrie sont sans effet face à des personnels consentants ou menacés.

Device Linker® vous protège contre :

▶▶ Le vol de données informatiques, en rendant vos données illisibles en dehors de votre environnement (vos machines, votre réseau).

▶▶ Le vol de périphériques de stockage, en les rendant inutilisables.

Protégez-vous contre :

L'UTILISATION DE VOS PERIPHERIQUES USB U3 SUR DES PCs NON AUTORISES

La technologie Linker® rend vos périphériques USB U3 inutilisables en dehors de votre environnement (réseau, pool de machines).

LA PERTE OU LE VOL DE VOS CLES USB U3

Tant que la clé USB ne reconnaît pas la configuration sur laquelle elle est connectée, elle reste inutilisable et l'accès aux données qu'elle contient est impossible !

Device Linker® ne nécessite aucune modification de votre environnement informatique. La protection s'applique à tous les périphériques U3 existants.

Une interface d'administration simple vous permet de configurer vos périphériques et les hôtes sur lesquels ils fonctionneront.

U3 smart

www.devicelinker.com

mobilegov
Device Linker

Device Linker® intègre la technologie de sécurité brevetée de MobileGov. U3 fournit des clés USB sécurisées ayant deux partitions : une partition CDROM (lecture seule) lançant un logiciel dès l'insertion de la clé et une partition privée, protégée par un mot de passe (sans ce mot de passe, cette partition est inaccessible en lecture et en écriture).

Device Linker® permet à une clé U3 d'être utilisée sur un groupe de machines préalablement autorisé et d'être inutilisable sur les autres machines.

Device Linker® régit l'accès à la partition protégée (contenant vos données).

Fonctionnement schématisé :

Comment fonctionne Device Linker®

1. Au cours d'une première étape de configuration, le périphérique est connecté à n'importe quel PC du Réseau afin de définir l'environnement sur lequel il pourra être utilisé : ce PC, un groupe de PC, le LAN sur lequel le PC est lui-même connecté.

2. Il faut ensuite définir les mesures à prendre si le périphérique est connecté à un environnement imprévu : rendre le périphérique illisible, transmettre discrètement des informations sur l'environnement, détruire les données ou demander une autorisation d'usage temporaire.

Principales fonctionnalités :

▶▶ Définition dynamique des environnements : sélection des paramètres d'identification d'une machine hôte à partir d'une liste préétablie (CPU/ OS/ cartes mère/ etc.).

▶▶ Gestion des machines hôtes : enregistrement direct sur une machine non identifiée et gestion des listes de machines autorisées.

▶▶ Enregistrement des modifications sur la clé et gestion transparente et sécurisée (mot de passe généré inconnu de l'utilisateur) d'une partition chiffrée et cachée.

▶▶ Options de backup et de restauration des clés

▶▶ Edition Personnelle (grand public) et Entreprise (administration de groupes de clés Linker, des remontées d'alertes, …).

▶▶ Peut s'utiliser conjointement avec Device Authenticator® (voir http://deviceauthenticator.com), les clés Device Linker pouvant ainsi être intégrés à la logique de sécurité réseau.

Principaux matériels compatibles :

Certifié U3, Device Linker® reconnaît les matériels informatiques USB U3

mobilegov
2000, Route des Lucioles
Les Algorithmes
06901 Sophia Antipolis, France
Tel: +33.492.944.894
Fax: +33.492.944.895
mail: info@mobilegov.com
Sandgate House 102 Quayside
Newcastle upon Tyne NE1 3DX
United Kingdom

mobilegov

mobilegov

L'ADN du Numérique

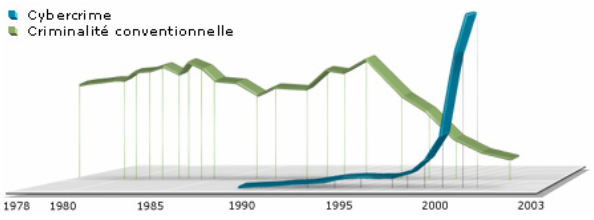
mobilegov

Le contexte

L'entreprise

mobilegov

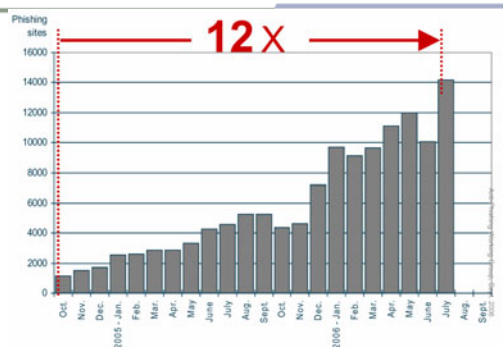
Cybercriminalité – long terme



Source: IBM
http://www-03.ibm.com/ondemand/ca/fr/pointofview/cybercrime/jul18/ibm_future_crime.html

mobilegov

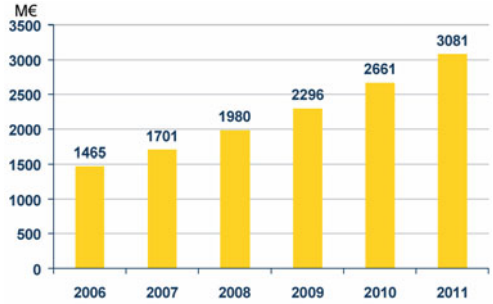
Bank of Canada – tendance 24 mois



Source: National Bank of Canada, Cybercrime & Identity theft, 5 mars 2007
http://www.pwgsc.gc.ca/recgen/colloquium2007/pdf/panel-discussion-jose-navarro-e.pdf

mobilegov

Marché français – sécurité informatique



Dépenses des entreprises françaises en sécurité (logiciels, appliances et services)
Source: Etude IDC « Le marché français des solutions de sécurité informatique, 2007

mobilegov

Les risques

- Cybercrime organisé: injection de malware, usurpation d'identité, intrusion physique, vol de données, fraude bancaire…
- Risque aggravé par le facteur humain: 70% du vol de données se fait avec la complicité (volontaire ou non) du personnel, contre 20% via le réseau
- Les solutions sophistiquées (biométrie, cryptage) sont alors inopérantes

Risques juridiques

Conséquences pénales du non respect de la législation :

Article 226-17 du Code Pénal :

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6 janvier 1978 (protection des fichiers de données à caractère personnel) est puni de 5 ans d'emprisonnement et de 300 000 Euros d'amende.

Article 226-22 du Code Pénal :

La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 € d'amende. La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 € d'amende.

Quelques affaires

- Journal du Net 6/02/2007 : Un disque dur externe a disparu dans un centre médical d'Alabama pour anciens combattants. Il contenait notamment des informations personnelles concernant 48.000 anciens combattants américains.
- Network World 7/03/2007 : Fidelity National Information Services, un fournisseur de solutions pour le secteur financier, a reconnu le vol d'informations personnelles concernant 2,3 millions de personnes enregistrées sur sa base de données. Cette violation est survenue à travers le société Certegy Check Services, qui supervise la gestion des chèques et des cartes de crédit.
- Boursier.com 18/05/2007 : Alcatel-Lucent : un disque de données salariés a disparu pendant sa livraison par UPS.

La situation est grave, mais pas désespérée

- Le Monde Informatique 19/11/2007 : Les DSI dépassés par l'essor des périphériques mobiles personnels
- Réseaux-Télécom 24/09/2007 : Deloitte Touche Tomatsu « 2007 Global Security Survey »: les employés et les clients restent le plus grand facteur de risque d'une institution financière
- 80 millions d'identité volées en 2004-2007
- Et ça ne fait que commencer…
  Mobilegov apporte une vision nouvelle!

Notre vision de la sécurité

- 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
- Elle doit évoluer vers des solutions proactives
- Ces solutions seront génériques, applicables dans tous les domaines touchés par la « convergence »

L'ADN du numérique

- Avec la convergence et l'explosion des objets communicants, la sécurité doit être intégrée aux objets.
- Il faut redéfinir l'intérieur de l'entreprise (sûr) par rapport à l'extérieur,
  - par la reconnaissance mutuelle des objets
  - rendue possible par leur ADN numérique.

Mobilegov, un savoir faire unique

- L'ADN du numérique est une telle solution: nous savons authentifier tout composant numérique (processeur, carte mémoire, clé USB, téléphone, caméra, PC…)
- Solution opérationnelle exploitée dans nos premiers produits de sécurité pour PC,
  - applicable à tout environnement numérique,
  - vendable dans le monde entier,
  - adaptable à un large éventail d'applications présentes et futures.

Le contexte

L'entreprise

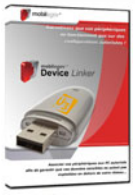
- Un brevet « process » en 2 temps:
  1. Définition des politiques de sécurité: un composant (ou une famille) peut être interdit, obligatoire ou indifférent
  2. Vérification de l'intégrité: à toute connexion d'un composant, on vérifie sa conformité à la politique.
- Une implémentation légère et portable (PC, PDA, microcontrôleur, clé USB, carte à puce…)
  - Méthodologie CMMI, développement OOM
  - Noyau dur en C/C++
  - Interfaces .net, Java (JNI), XML…

Deux familles de produits qui veillent sur les composants amovibles:

mobilegov Device Authenticator

Autorise seulement la connexion de composants de confiance aux machines d'un réseau

mobilegov Device Linker



Autorise seulement la connexion d'un composant sur des machines de confiance

- Ils souhaitent rester discrets, de façon à garder l'effet de surprise
- Ce sont des industriels, des administrations publiques, des labos de recherche, des PME
- En France, au Royaume-Uni, ailleurs en Europe

- Antivol du futur : prévient à la fois le vol des données et le vol des équipements
  - Un composant n'est utilisable que dans son contexte: la maison, le bureau, la voiture, le bateau…
  - Par exemple Disk Linker : Imaginez un disque dur qui ne fonctionne qu'avec des machines préalablement identifiées
  - Etudes avec ST Microelectronics, Gemalto, LaCie
  - Travaux de normalisation avec le CNRS
- Téléphonie :
  - Services d'identification des éléments matériels à l'usage des clients professionnels
  - Etudes avec ORANGE R&D et Trustmission
- Défense/Sécurité/Douanes/Justice
  - Futur marché lié aux cartes d'identité électroniques
  - Etudes avec Gemalto, Accenture, Logica PLC

- Systèmes bancaires, banque et paiements en ligne: sécurité à base de mot de passe à améliorer d'urgence
- Service de tiers de confiance, ventes/enchères en ligne, etc.
- Media, vidéo à la demande, set top box, TV interactive...
- Jeux, consoles de jeux vidéo, jeux en réseau, bourse en ligne
- Automobile (chronotachygraphes, EEPROM, GPS...)
- Energie, compteurs électriques, compteurs de gaz, etc.

La Société MobileGov

Spin-off du projet Européen eJustice : 15 ans d'expérience internationale sécurité/Défense/crime organisé

Brevet et produit validés par le DCSSI, le SGDN, la DST, les RG et accord avec le Ministère de l'Intérieur, Haut Fonctionnariat d'État aux Nouvelles Technologies pour « garder » l'innovation en France.

Qualifiée « Entreprise Innovante » au titre des FCPI par OSEO-ANVAR et JEI par la DGI

Membre du CLUSIF. Membre associé du Pôle SCS. Partenaire Pacte PME.

Elu « Best Innovation 2005 », Capital-IT Paris
Prix de la Start-up Innovante, Cap Innovation 2007.

Partenaires

< Récompenses et Validation >

< Industriels >

< Technologiques / Stratégiques >

< Grossistes / Distributeurs >

Equipe 1/2

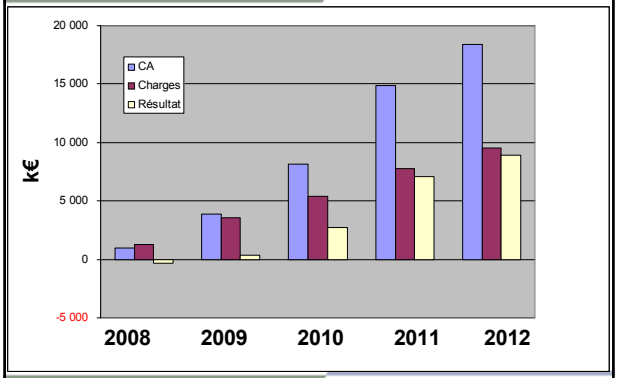
- Fondateurs

- Michel Frenkiel, Président, Ingénieur Arts et Métiers, Master of Science, IST Consultants, Thales, Lectra Systèmes, IBM
- François Le Page, DG, MBA CERAM et Phoenix-Arizona, créateur de Promorepublic SA
- Eric Mathieu, Directeur Technique, Ingénieur des Mines, Eurocopter, SEMA, Amadeus

Equipe 2/2

Aujourd'hui 15 personnes compétentes et motivées

Prévisions de croissance



Pourquoi nous entrons en bourse

- Pour bénéficier de la notoriété et être reconnus par nos partenaires technologiques et commerciaux
- Pour pouvoir satisfaire tout de suite la demande du marché en Europe, aux Etats-Unis, en Asie
- Pour conserver notre avance technologique, développer un standard de sécurité et prendre le leadership sur ce marché.

Pourquoi vous investirez chez nous

Pour faire un investissement gagnant:

- Technologie innovante mais prouvée
- Marché nouveau mais en forte croissance et en forte demande d'innovation
- Equipe exceptionnelle: expérience, complémentarité, réseaux
- Produits uniques, futurs produits incontournables
- Marché mondial, mode de commercialisation au point, effet de levier important

La sécurité de demain dès aujourd'hui

MobileGov France S.A.

2000 route des Lucioles
06901 Sophia Antipolis
France

Contact:
Michel FRENKIEL
michel.frenkiel@mobilegov.com
+33 662 012 851

+33 492 944 894
+33 492 944 895
info@mobilegov.com

www.mobilegov.com