mobilegov

L’ADN du Numérique

L’entreprise

Le contexte

Notre vision

Historique

- Création de Mobilegov SARL en mai 2004, transformation en SA en août 2006

- Siège social à Sophia Antipolis
- 15 personnes
- Statut JEI, Eligible FCPI

- 1er brevet en décembre 2004
- 2ème brevet en cours
- Partenariat technologique avec le CNRS. Accompagnée par INRIA-Transfert

A propos de MobileGov

Spin-off du projet Européen eJustice (Prochaine génération de documents d'identité biométriques)

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 >

Nous sommes

- Partenaire dans plusieurs projets européens (DG INFSO)
- et avec I3S/CNRS sur la sécurité des systèmes distribués
- En démo chez Unisys Belgique, Accenture, Thales, BKA, Europol
- Distribués par IPvista, SPIE, NextiraOne, Prossi, Quadria-Euralliance's (France), Infomanage (Suisse), Logica Plc (UK), DNP Global (Inde), Nexway (Internet)…
- Utilisés par des clients discrets

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

Une partie de l'équipe dans ses locaux :
des gens compétents, motivés, qui y croient.

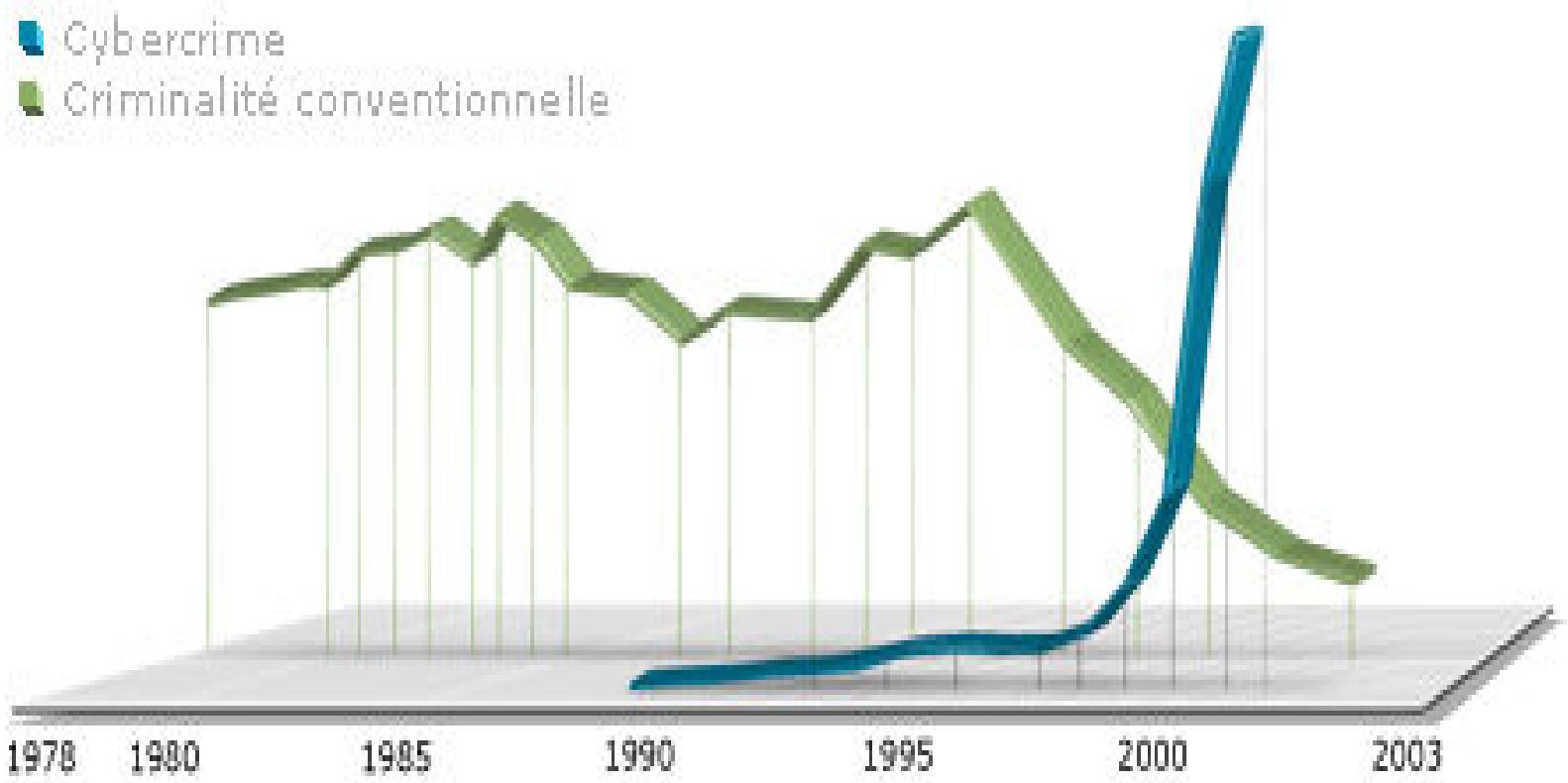
mobilegov

L’entreprise

Le contexte

Notre vision

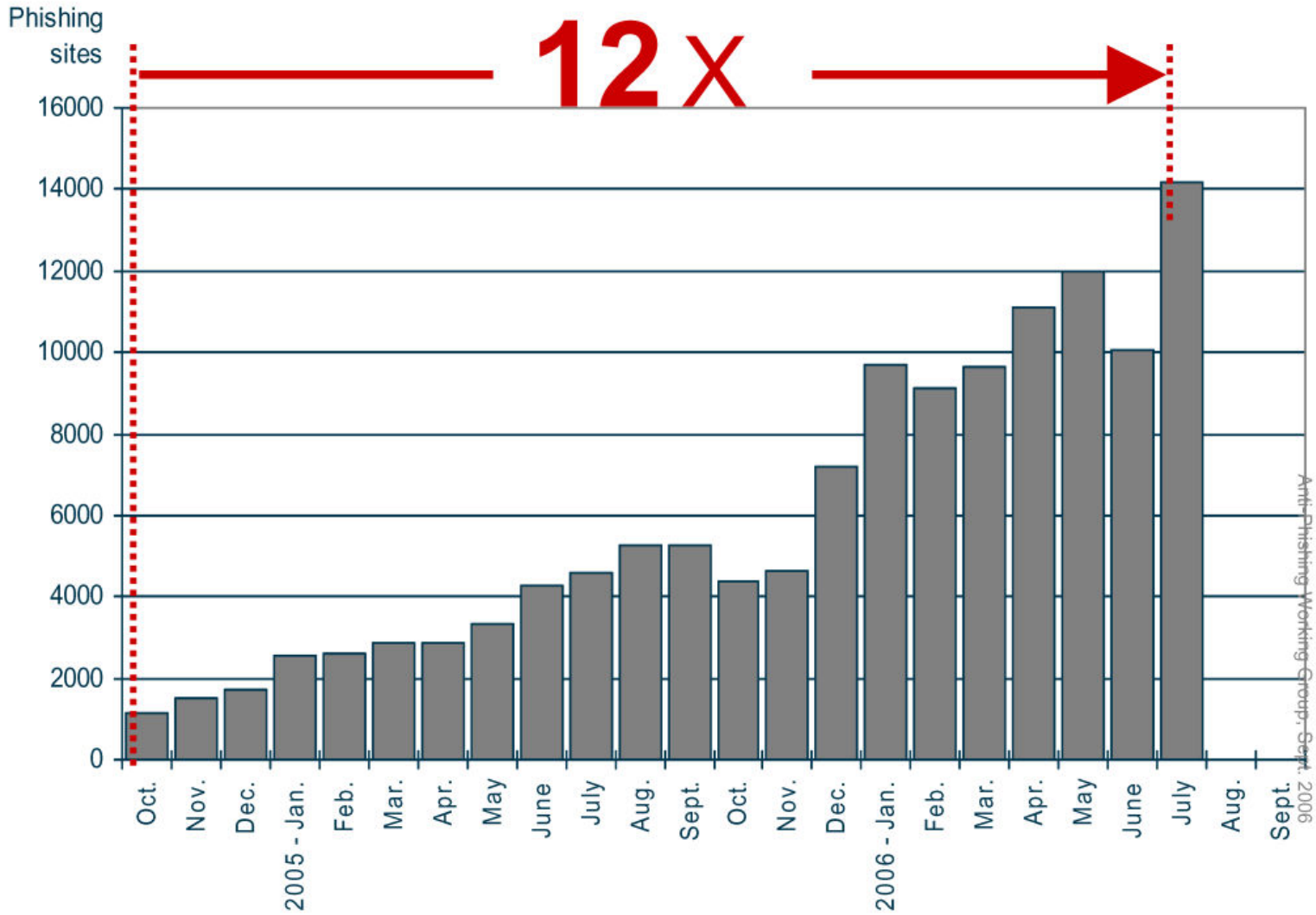
Cybercriminalité – long terme



Source: IBM

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

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

Le contexte

- Des chaînes de confiance de plus en plus complexes: convergence informatique-telecom-multimédia
- Des composants distribués, hétérogènes, discrets, puissants, peu maîtrisés
- Opérations par téléphone portable
  - Intérêt à déterminer le modèle de téléphone (iPhone)
- Services basés sur la localisation
  - Et si le GPS était modifié?
- Services à des communautés d'usagers
  - Login/pwd remplacé par biométrie et match on card
  - Et si le lecteur biométrique était attaqué?
- Des logiciels de mieux en mieux sécurisés
- Le maillon faible: les composants matériels

La menace en milieu professionnel

- Le vol de données comme l'injection de programmes malveillants (virus, espions) constituent une menace permanente pour l'entreprise, qui dépend de son informatique.
- Des solutions sont en place: sécurité physique, sécurité réseau, contrôle d'accès logiciel, pare-feu, anti-virus, cryptage…
- La prolifération des équipements mobiles (USB, BlueTooth, WiFi…), de plus en plus puissants, invisibles de l'administrateur réseau, rendent ces solutions insuffisantes.
- Nouveaux problèmes liés à cette prolifération :
  - La gestion de leur nombre (personnels et professionnels)
  - La supervision des informations échangées avec le réseau
  - La pertes ou le vol des équipements hors de l'entreprise

Le risque

- Le risque est 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
- La sécurité centralisée doit descendre au niveau du poste de travail pour lutter contre
  - Actions internes : Erreurs humaines, mauvais comportement de l'utilisateur, actes de malveillance
  - Actions externes : Vol du terminal, attaque pirate du terminal mobile, espionnage des échanges de données

Le coût du risque

- Le signal d'alarme est tiré (Notes du SGDN, du CLUSIF, du MEDEF…)
- Les enquêtes confirment l'augmentation des coûts
  - L'objectif des virus est désormais financier
  - Le coût du cybercrime est de 24 k$ par an par entreprise (JDN Solutions du 24 janvier 2006 – enquête sur 2000 sociétés US)
  - Sondage national US 2006 (sur plus de 1000 entreprises):

Incidents informatiques	2004	**2005**
Pertes générées par accès non autorisé	51 545 $	**303 234 $**
Pertes générées par vol de données	16 859 $	**355 552 $**

- Les attaques connues représentent le sommet de l'iceberg
- Le marché du logiciel malveillant dépasse les 26Md$ du marché de la sécurité en 2005

Banalisation du risque

- 175 millions de clés USB en circulation
- 81% des PDA stockent des contacts professionnels
- 59% des PDA stockent des agendas professionnels et 27% des données d'entreprises.
- 60% des vols de données proviennent d'un appareil volé, trafiqué ou perdu contre seulement 25% pour une intrusion de réseau.*
- 89% des terminaux ne sont protégés que par l'éternel duo « login-password ».

*Source: Yankee Group, Gartner, Clusif, Infosecurity 2006

Le patrimoine de l'entreprise

- Informations à protéger
  - Informations stratégiques d'entreprises
  - Données à caractère personnel
- Conséquences pour l'entreprise des pertes de données
  - Economiques : perte d'opportunités de marchés, de client, d'image, non respect des procédures « qualité »
  - Juridiques : non respect de la législation en vigueur, non respect des normes en vigueur
  - Industrielles : indisposition de l'outil de production, divulgation d'informations stratégiques aux concurrents

Quelques titres d'articles

- **Valéo :** équipementier automobile
  Intrusion dans le système, copie de données de RD
- **« Vol du fichier des anciens combattants US » :**
  Vol d'un ordinateur portable contenant des fichiers de données à caractère personnel
- **« Vol de secrets de fabrique portant sur concept d'interrupteurs et de produits émetteurs-récepteurs»**
- **Réseaux sans fil :** Un cadre part avec les secrets de fabrication de son employeur et crée sa propre entreprise
- **Opérateur Telecom** : Sécurité des données médicales sur les terminaux mobiles» : Très faible protection des données de santé chez les professionnels du secteur médical

Contexte juridique

- Responsabilité des dirigeants (PDG, DSI…)
  - Responsabilité réglementaire et juridique
  - Responsabilité économique et industrielle
- Qualification des infractions
  - Accès frauduleux, abus de confiance, vol d'informations, Atteinte au secret d'un information économique à caractère protégé…
- Réglementation
  - Nouvelle loi « Informatique et libertés »

  Relative à la protection de données à caractère personnel, transpose la Directive 95/46/CE
  - Décret relatif à l'hébergement des données de santé à caractère personnel
  - Loi de sécurité financière (LSF)

  Assure la sincérité et la qualité des informations financières aux actionnaires des sociétés

Contexte juridique 2

- **Principaux textes de loi**

  - Articles 34 de la Loi n°78-17 du 6 janvier 1978 modifié par Loi n°2004-801 du 6 août 2004 art. 5 (JORF 7 août 2004) : Le responsable du traitement des fichiers est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées (= obligation d'intégrité des données), ou que des tiers non autorisés y aient accès.

  - Décret n° 2006-6 du 4 janvier 2006 Relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique

- **Normalisation**
  - Norme ISO 27001 – (BS7799) : Définit l'ensemble des tests et contrôles à effectuer pour s'assurer du bon respect d'ISO/CEI 17799.
  - Norme ISO 17799 : Bonnes pratiques en matière de sécurité d'information

Contexte juridique 3

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 oeuvre 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.

mobilegov

L’entreprise
Le contexte
Notre vision

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, de façon à être bien comprises et applicables dans tous les domaines touchés par la « convergence »
- L'ADN du numérique est une telle solution
- Nous l'exploitons déjà dans nos premiers produits

Nous savons

- Reconnaître les composants matériels (et logiciels) : processeur, carte mémoire, clé USB, téléphone, PC, OS…, via leur « **ADN numérique** ».
- Utiliser notre techno brevetée pour étendre la sécurité réseau aux composants amovibles d'un système, filaires ou non,
- redonner aux professionnels des conditions de travail performantes: il n'est pas raisonnable de bloquer les ports USB parce que les clés U3 sont dangereuses,
- proposer des développements spécifiques (SOCA, DST).
- Distribuer à travers un réseau constitué deux familles de produits:

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

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

Nos produits

Deux familles de produits qui veillent sur les composants amovibles:

mobilegov® Device Linker

Device Authenticator

Parce que l'ajout, la suppression ou le changement d'un composant dans votre environnement informatique constitue un risque:

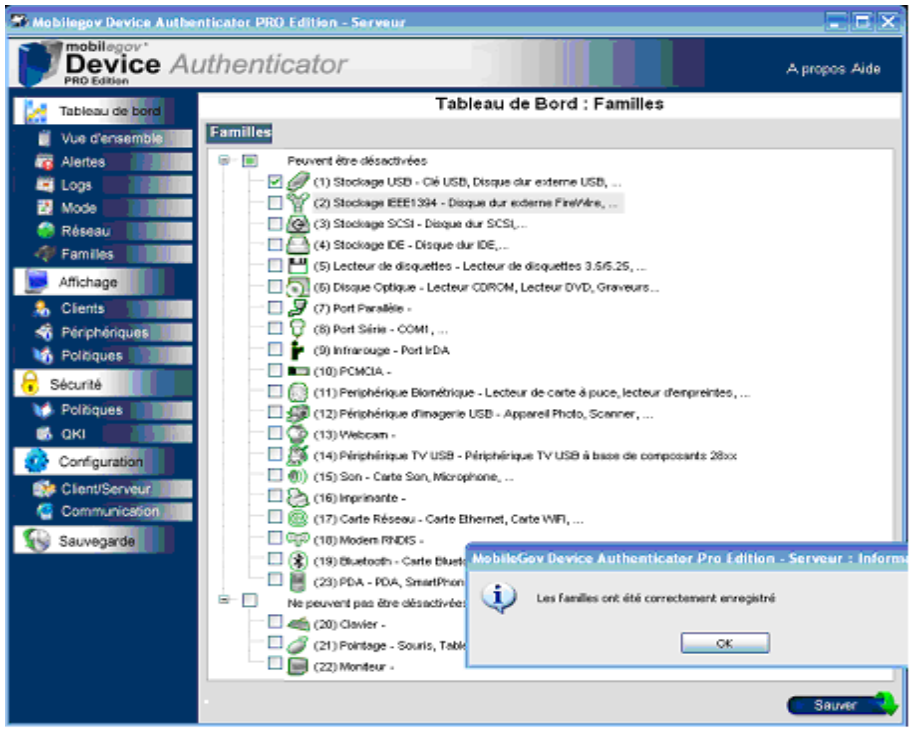
- Sécurise les réseaux face aux périphériques externes (clés USB, iPod, composants WiFi, BlueTooth, etc..) et internes (disque dur, carte réseau, etc.)
- Sécurise les réseaux face aux équipements mobiles de type PDA et Smartphone
- Mémorise les configurations matérielles et logicielles

Avantages produit

- Gère des politiques de sécurité au niveau de l'entreprise
- Détecte les changements de configuration du poste client
- Associe un utilisateur à ses périphériques et gère ses droits
- Gère les périphériques au niveau de sa famille, du type et du n° de série
- Supporte Windows, extensible à Linux, MacOS, Symbian, etc.
- Choix « à la carte » de l'action à prendre en cas de détection d'un changement de configuration
- Suivi des alertes en temps réel sur la console d'administration
- Rapports statistiques et logs détaillés (par utilisateur, par périphérique, par période, etc.)
- Fonctionne de façon sécurisée (certificats X509, cryptage RSA)
- Débrayable sous conditions pour autoriser temporairement un périphérique non autorisé
- Évolutif : supporte déjà des périphériques futurs, mise à jour en ligne

Configuration

- Conçu pour un grand nombre de postes clients :
  - Facile à installer et à intégrer à l'existant
  - Facile à utiliser, invisible sur le poste client
  - Paramétrage souple des politiques de sécurité
  - Personnalisation des actions à prendre en cas de détection



Device Linker

- Une clé USB protégée par Device Linker ne peut être lue que sur des PC préalablement autorisés.
- Le « mot de passe » est le PC: moins de risque qu'avec le cryptage ou la biométrie
- Fonctionne sous Windows.
- Produit vendu pré-installé sur des clé USB à notre marque, et en téléchargement sur Internet (FNAC, Darty…) et sur CD-Rom (pour gérer une flotte de clés)

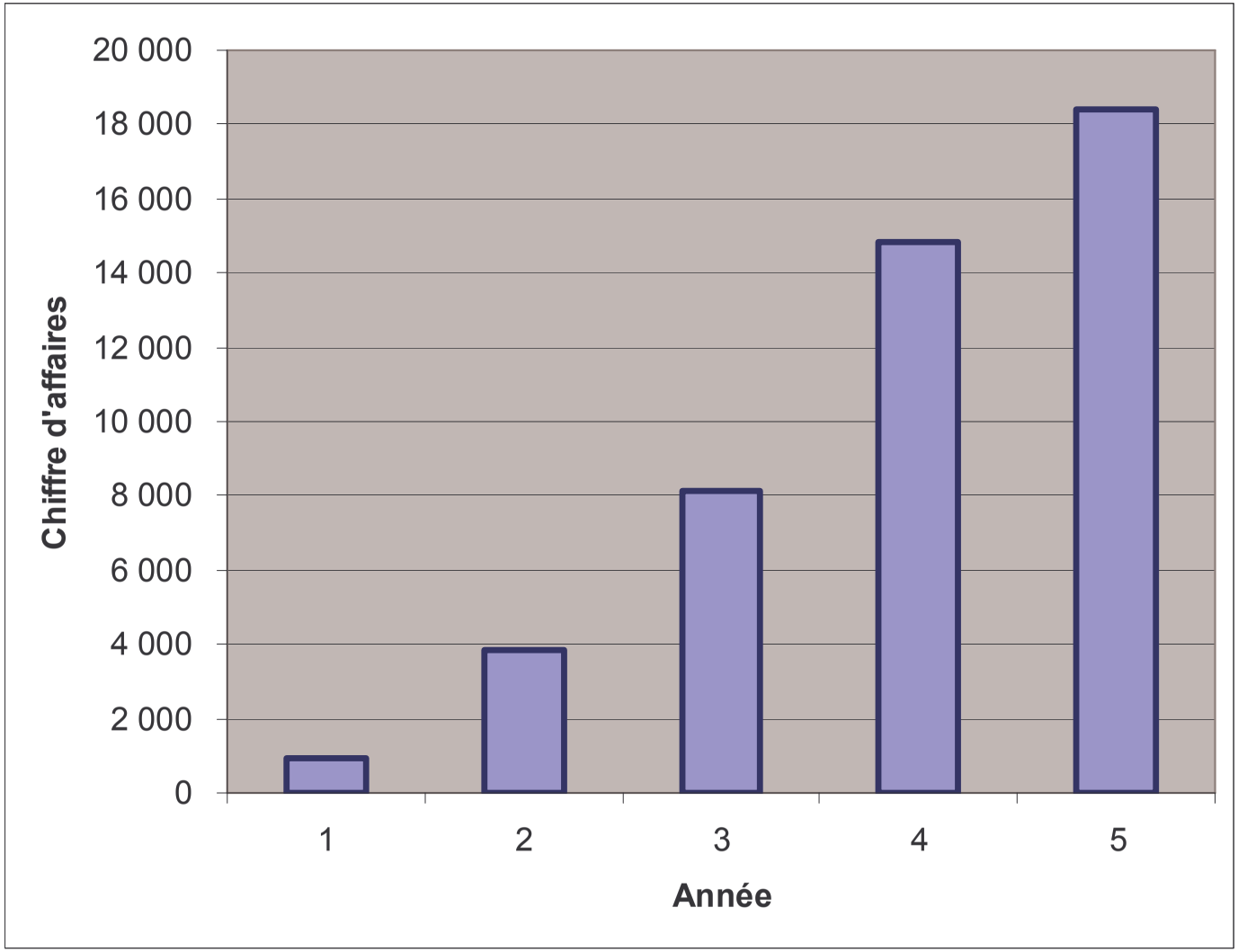
Produits futurs 1/2

- 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
  - Etude avec Gemalto

Produits futurs 2/2

- 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, GPS...)
- Energie, compteurs électriques, compteurs de gaz, etc.

Prévisions de croissance



Prévisions de croissance

	2008	2009	2010	2111	2112
Chiffre d'Affaires					
Ventes de Licences (toutes licences confondues)	800,00	3 450,00	7 300,00	13 400,00	17 000,00
Support & Maintenance (10% des contrats)	80,00	345,00	730,00	1 340,00	1 275,00
Conseil (dont projets Européens)	30,00	30,00	30,00	30,00	30,00
Subventions d'exploitation	0,00	0,00	0,00	0,00	0,00
Autres produits (clés Linker)	29,00	44,00	58,00	73,00	100,00
Total des Produits (A)	**939,00**	**3 869,00**	**8 118,00**	**14 843,00**	**18 405,00**
Achats					
Achats de m/ses : Clés Linker	16,00	25,00	40,00	40,00	40,00
Fournitures diverses (petites fournitures)	0,80	0,80	1,80	1,80	1,80

Charges externes					
Commissions Distributeurs	220,00	1 138,50	2 409,00	4 422,00	5 482,50
Leasing	0,00	0,00	0,00	0,00	0,00
Loyer (FR + virtual office UK) + UK & USA	30,00	40,00	50,00	70,00	80,00
Assurances (Locaux + RC prof)	3,00	3,00	4,00	5,00	5,00
Charges locatives (y compris eau, edf, etc)	9,00	9,00	9,00	9,00	9,00
Sous-traitance	7,00	28,00	49,00	70,00	70,00
Intelligence économique & Veille	6,20	6,20	6,20	6,20	6,20
Entretien Brevets, Label FCPI, etc.	7,20	7,20	7,20	7,20	7,20
Honoraires (Comptable et juriste, enregistrement)	15,00	15,00	15,00	30,00	30,00
Publicité & Salons	20,00	100,00	200,00	250,00	250,00
Hebergement & ISP	1,50	1,50	1,50	1,50	15,00
Ordinateurs, logiciels et serveurs (location)	10,00	20,00	30,00	45,00	55,00
Frais de déplacement (missions, receptions)	52,80	171,60	171,60	184,80	240,00
Frais de poste, téléphone	5,00	6,00	8,00	10,00	10,00

Impôts & Taxes					
Taxe d'apprentissage	3,57	3,57	8,38	10,23	11,34
Formation continue	2,55	2,55	5,99	7,31	8,10
Taxe professionnelle	1,44	0,72	0,96	1,20	1,68

Charges de personnel					
Salaires bruts (salaires nets + parts salariales)	637,97	1 497,17	1 827,56	2 025,56	2 477,96
Charges sociales (part patronale)	190,76	453,80	519,88	579,28	709,36

Charges financières					
Intérêts sur emprunts	0,00	0,00	0,00	0,00	0,00
Agios bancaires	3,00	0,00	0,00	0,00	0,00
Dotations aux amortissements & provisions	16,00	15,00	14,00	14,00	14,00
Charges exceptionnelles	0,00	0,00	0,00	0,00	0,00
Total des Charges (B)	**1 258,79**	**3 544,61**	**5 379,08**	**7 790,09**	**9 524,15**
Resultat avant impôts (A) - (B)	-319,79	324,39	2 738,92	7 052,91	8 880,85
Pas d'Impôts sur les bénéfices puisque statut J.E.I	0,00	0,00	0,00	0,00	2 989,29
Resultat net comptable	**-319,79**	**324,39**	**2 738,92**	**7 052,91**	**5 891,56**

MobileGov France S.A.

2000 route des Lucioles
06901 Sophia Antipolis
France

+33 492 944 894
+33 492 944 895

info@mobilegov.com

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

www.mobilegov.com