- **La solution Livo Technologies**
- **Interopérabilité avec Windows CardSpace**

JM Livowsky
Pierre Couzy

Observatoire de la Sécurité des Systèmes d'Information et des Réseaux

Livo Technologies SAS - 38 rue de Berri 75008 Paris – www.livo.com
06 13 42 38 98 - engel@livo.com

Livo Technologies en 1 slide ☺

- **L'équipe**

Frédéric Engel,
President
Dir Marketing EMEA
ActivIdentity

Jean-Michel Livowsky
Inventeur Génonyme
Fondateur
Albert SA

Danielle Krivine
Recherche
Agrégée Mathématique
Professeur

Pascal Pérard
Développement
Président
Axinoe

- **La société**
  - **SAS, 2006, Paris**
- **L'IP**
  - **WO/2005/086569**
  - **Howrey & Simon**
- **Critères**
  - **Confort, Coût, Confiance**
- **Stratégie**
  - **OEM / Logiciel embarqué**
  - **Usages grand public**
- **Validations**
  - **Dr. Rouillié / INRIA**
  - **Dr. Daudé / FT R&D**
  - **Prix**
    - **IE Club 2005**
    - **Concours Nat. 2005**
    - **Assises Sécurité 2007**

Agenda

1. Historique
2. Equipe
3. Marché
4. Vision
5. Mission
6. Innovation
7. Validations
8. Produit
9. Avantages
10. Prototype
11. Objectif
12. Stratégie
13. CardSpace
14. Opportunité

Historique

- **2003-04**
  - **Pré-requis de grands opérateurs de e-commerce français**
    - L'authentification forte des utilisateurs, une fonction obligatoire des services web
    - Pré-requis: enfouir l'authentification forte dans les produits portables usuels
  - **Création of Livo Technologies SA, une société de R&D Suisse**
    - Dépôt d'un brevet (obtenu en 2007) : un « nouveau système d'authentification »
    - Les fondateurs et des Business Angels financent les premiers développements

- **2005-06**
  - Validations techniques (FT R&D, INRIA, experts independants)
  - Création de Livo Technologies SAS en France / Bourse R&D Min Recherche

- **2007**
  - **Prototype** : fédération de facteurs d'ID génère un identifiant unique et fort
  - **Prix de l'Innovation** / Assises de la Sécurité et des Systèmes d'Information
  - **Première intéropérabilité:** / Microsoft CardSpace

Equipe

Frédéric Engel
President
Marketing ActivIdentity

Jean-Michel Livowsky
Inventeur
Founder Albert SA
(IA, R&D)

Danielle Krivine
Recherche
PhD, Mathematics

Pascal Pérard
Developpement
Axinoe, SSII

Marché

Le fait

- **Le vol d'identité menace la croissance de services**
  - Perte de $50Milliards aux USA
  - Tous les secteurs économiques sont concernés
  - L'authentification faible: 95% des app., 15 MdP / internaute

Le problème

- **Inadéquation des technologies existantes**
  - Faible pénétration du marché (3%) des OTP et certificats
  - Un niveau de sécurité supplémentaire « bon à avoir »
  - Création de la demande par les applications grand public

La solution

- **Demande d'authentification forte et transverse**
  - Vers la fédération des identités : OATH, LAP, OpenID, MSFT…
  - La banque est motrice aux USA (FDIC) et en Europe (CAP)
  - Obj: une assurance facile, économique et proportionnée

Vision

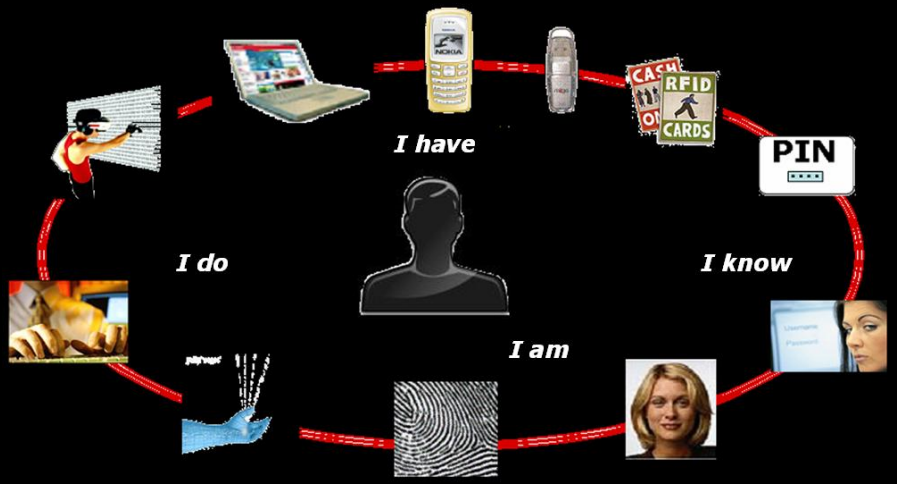
Le renforcement de la confiance dans l'Internet passe par l'intégration, transversale et durable, de l'authentification forte

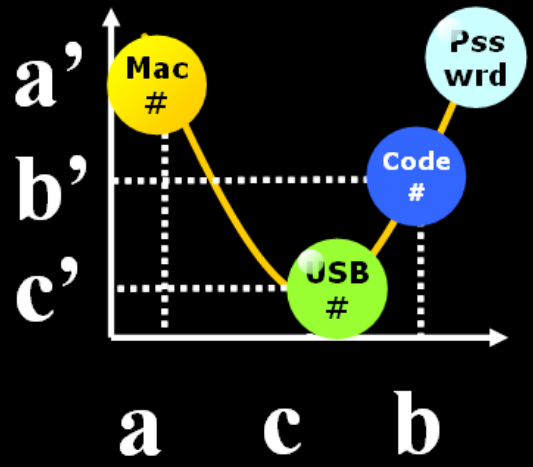
Mission

Renforcer la confiance dans l'Internet en simplifiant l'authentification forte des internautes

L'innovation

Livo fédère des informations d'identification usuelles et génère un identifiant fort, unique et facile à utiliser





L'identifiant fort et unique rassure l'utilisateur et l'opérateur

L'identifiant est un hash des coefficients du polynome généré par les 3 facteurs

Il est impossible à un tiers d'usurper les identités de l'utilisateur et de l'opérateur

Validations

HOWREY LLP

Brevet WO/2005/086569

IE-Club
Le club des acteurs de la ITech-Economie

Mention Spéciale du Jury

INRIA

Dr. F. Rouillié

concours national 2005
CRÉATION D'ENTREPRISES DE TECHNOLOGIES INNOVANTES
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

R&D grant of 375K euros

orange™ france telecom

Dr. F. Daudé

CNIL

Positive opinion

Prix de l'Innovation des Assises 07
L'Événement Européen de la Sécurité et des Systèmes d'Information

Communiqué de **Presse**

Contact : AL'X Communication - Véronique Loquet
vloquet@alx-communication.com
Tel: 06 68 42 79 68

La société LIVO Technologies remporte le Prix de l'Innovation des Assises 2007

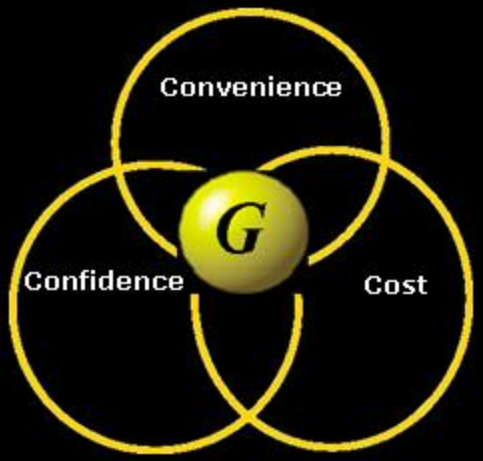
Prix de l'Innovation des Assises

Produit

Un middleware d'authentification forte embarqué dans les architectures client / serveur du marché.

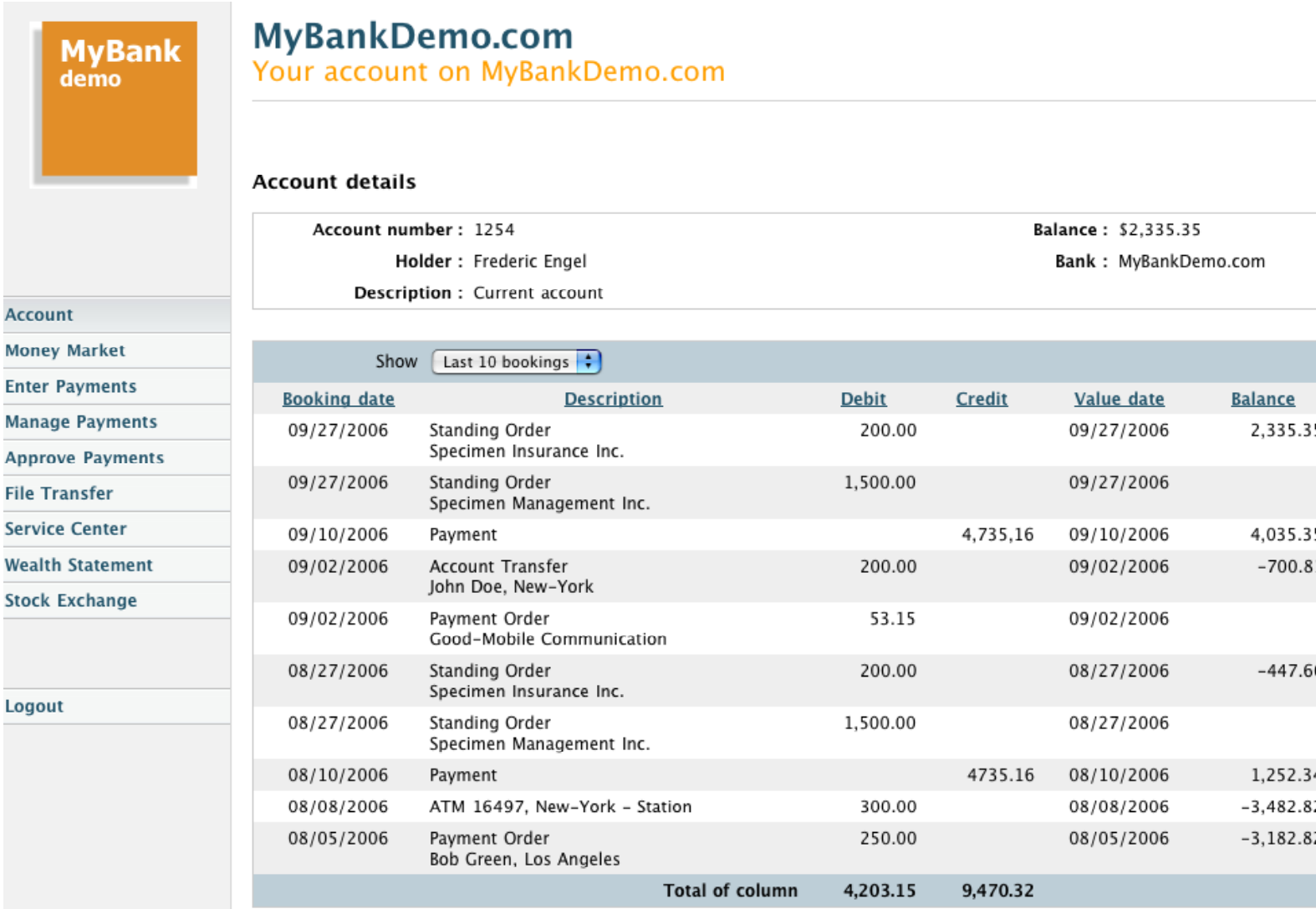
- **Client**
  - Fonction: collecter et hacher des informations d'identification
  - Embarqué dans des produits de stockage et de communication de données
  - Pré-initialisé ou téléchargé via Internet
- **Serveur**
  - Fonction: générer, valider, gérer l'authentifiant fort et unique
  - Inter opère avec les serveurs IdM du marché
  - 1er POC avec Microsoft CardSpace
- **Démo en ligne**
  - Gère toutes les phases du cycle de vie de l'authentifiant
  - Authentifie l'utilisateur d'une application web grand public

Avantages



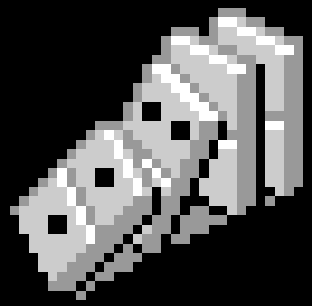
- **Confort d'usage**
  - Transforme les produits des internautes en token
  - L'expérience des utilisateurs ne change pas
  - L'agent embarqué automatise l'authentification forte
- **Coûts réduits**
  - Les fournisseurs ciblent des équipements existants
  - Evite la fourniture de produits dédiés, couteux
  - Les utilisateurs gèrent eux-mêmes leurs facteurs d'ID
- **Confiance accrue**
  - L'authentifiant est généré par au moins 3 facteurs
  - conforme à des normes de sécurité, évolutif
  - Réduit les risques d'hameçonnage, de rejeu (si https), de MITM

Prototype



Objectif

Devenir le leader des logiciels d'authentification forte embarquée



Livo → IdM → IdP → SP → Final buyer

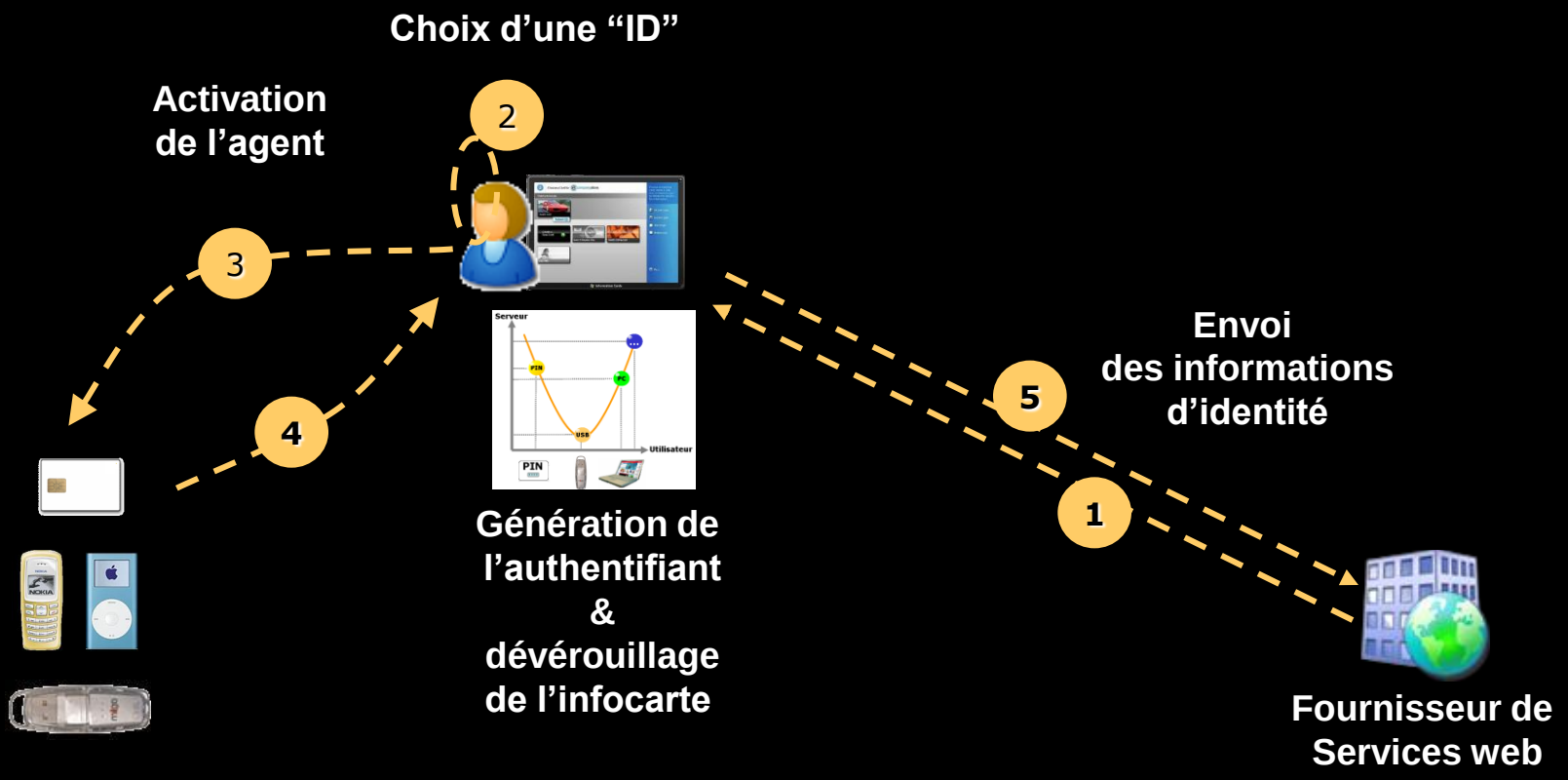
Stratégie

- **Développer un middleware d'authentification forte ouvert, normalisé et évolutif**
- **Embarquer le middleware au cœur de l'offre des éditeurs de solutions « IdM » et des fournisseurs d'identité « IdP »**
- **Cibler les applications de convergence et centrées sur l'utilisateur**
- **Un prix-levier transparent pour des millions d'utilisateurs**
- **Think big, start small!**

CardSpace (1/4)

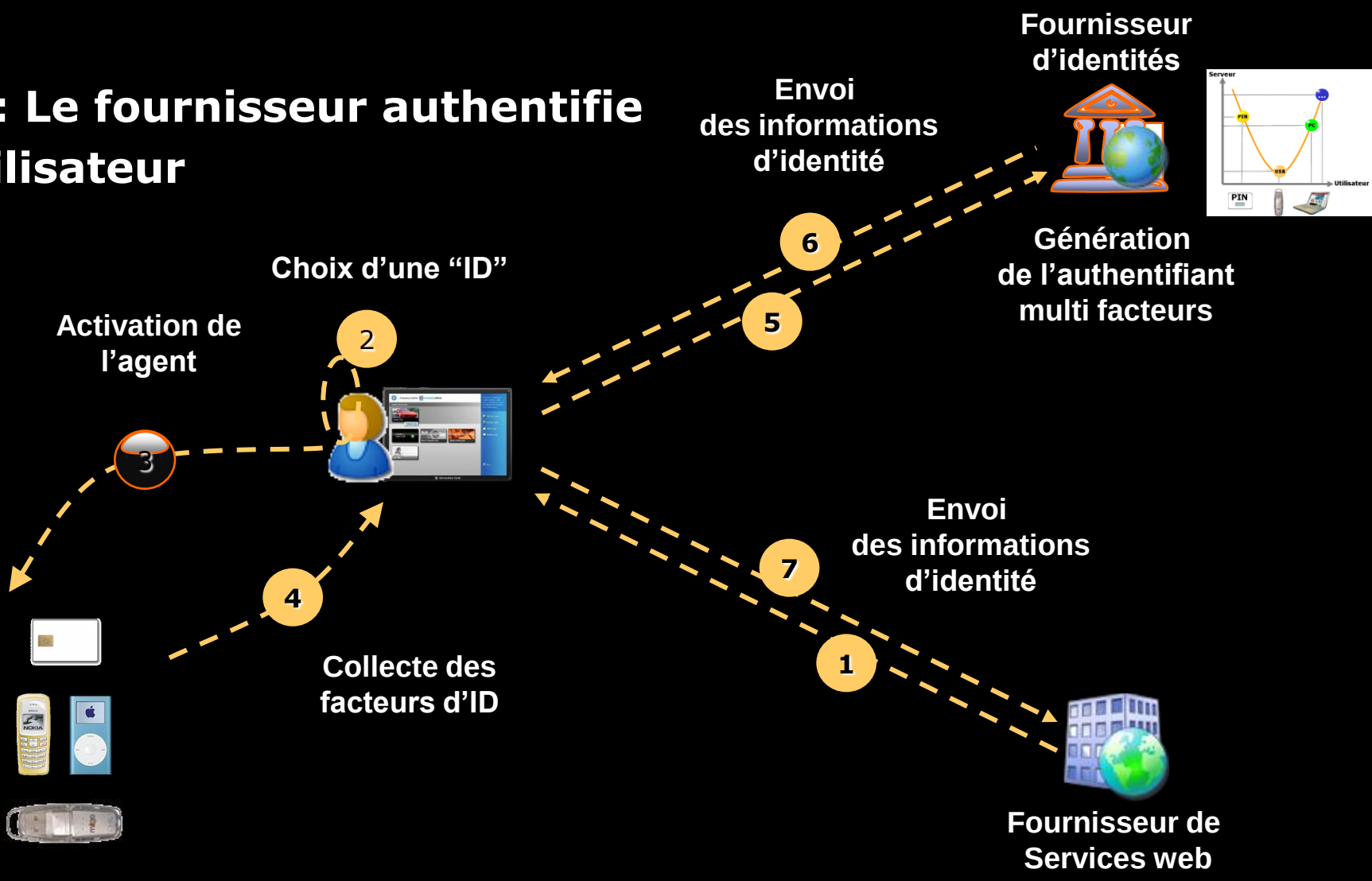
CardSpace (2/4)

#1 : L'utilisateur s'authentifie localement



CardSpace (3/4)

#2 : Le fournisseur authentifie l'utilisateur



CardSpace (4/4)

L'opportunité

- **Technologique**
  - Livo 'embrasse et étend' la gestion de facteurs d'ID existants
  - La propriété intellectuelle est bevetée, la technologie est validée
  - Le système est prototypé; 1er POC avec MSFT CardSpace

- **Commerciale**
  - Le model OEM est adapté aux déploiements à grande échelle
  - Un enjeu pour tous les acteurs : IdM, IdP, SP et utilisateurs finaux
  - Plusieurs acteurs du marché prêts à valoriser Livo

- **Financière**
  - Des partenaires et des investisseurs pour construire et financer
    - Le développement d'un serveur industrialisé et des API
    - Nos premiers accords OEM avec un éditeur IdM et/ou un IdP/MSSP
    - Le lancement du produit Genonym

Merci de votre attention

Frédéric Engel - 06 13 42 38 98
engel@livo.com - www.livo.com

Mission

#1 Renforcer et simplifier l'authentification forte des internautes avec leurs facteurs d'identité usuels (j'ai, je sais, je suis, je fais… comme d'habitude)

#2 Créer un 'Identifiant d'Utilisateur Unique' (UUID) qui soit assez facile, économique et sûr pour être adopté par le plus grand nombre

L'innovation – les détails

- **Le UUID est généré par 3 facteurs d'identité communs, existants**
  - 3 facteurs qui sont des choses que 'je sais', le possède', je suis, 'je fais'
  - Ex: 2 HW (PC + USB) + 1 SW (code PIN), ou 1 HW + 2 SW, ou 3 HW, etc
  - Le nombre et la nature des facteurs déterminent x niveaux d'assurance
- **Les 3 facteurs génèrent un authentifiant fort et unique**
  - Côté client, un 'agent' collecte, hache et envoie 3 facteurs à un serveur
  - Côté serveur, les 3 facteurs génèrent un polynôme
  - L'authentifiant unique qui en résulte est le haché des coefficients du polynôme
  - Un 4ème facteur enregistré permet le remplacement d'un facteur volé ou perdu
- **Les avantages pour l'utilisateur et le fournisseur de services**
  - Le vol des 3 facteurs n'assure plus personne contre l'usurpation
  - L'autogestion du remplacement des facteurs réduit les coûts d'administration
  - L'authentifiant est généré de façon automatique et transparente, facilement

Les validations

Avis de David Naccache

- « Le schéma de partage de secrets de Shamir, la technique cryptographique qui fonde le produit de Livo Technologies, est inconditionnellement sûr. (…) La valeur ajoutée de Livo Technologies est de permettre une intégration souple de ce schéma de partage de secrets dans les serveurs d'authentification communs du marché, qu'ils soient basés sur LDAP, RADIUS ou TACACS. »

Rapport de Fabrice Rouillier

- « Le procédé est facile à implanter efficacement et complémente les systèmes usuels d'authentification / identification. Si l'état de l'art en cryptologie assure la robustesse de certaines fonctions de base, alors le système est inviolable modulo quelques précautions simples de mise en œuvre et assure une plus grande souplesse dans la gestion de perte d'identifiants. »

Analyse de France Télécom R&D

- L'analyse confirme que le système valide l'identité d'un utilisateur à partir de plusieurs facteurs d'identité dont le renouvellement s'effectue par l'utilisateur, sans qu'il ait à recourir à une tierce partie. L'analyse recommande l'usage du système lorsque le recours à une tierce partie de confiance pour renouveler l'identité d'un utilisateur s'avère prohibitive en termes de coût. Le rapport valorise enfin l'anonymisation des fonctions d'identification de l'utilisateur

Avis de la Commission Nationale Informatique et Liberté

- la CNIL a émis un avis qui indique que la solution d'identification et d'anonymisation développée par Livo Technologies ne soulève pas de difficulté au regard des dispositions de la loi « informatique et libertés » du 6 janvier 1978 modifiée en août 2004. La CNIL informe Livo Technologies qu'une procédure de labellisation du logiciel « Génonyme » par la CNIL pourra être envisagée lorsque les modalités d'une telle procédure seront définies dans un décret d'application à paraître.

Inadéquation de l'offre à la demande

- **Les tokens d'authentification dédiés sont coûteux et mono applicatif**

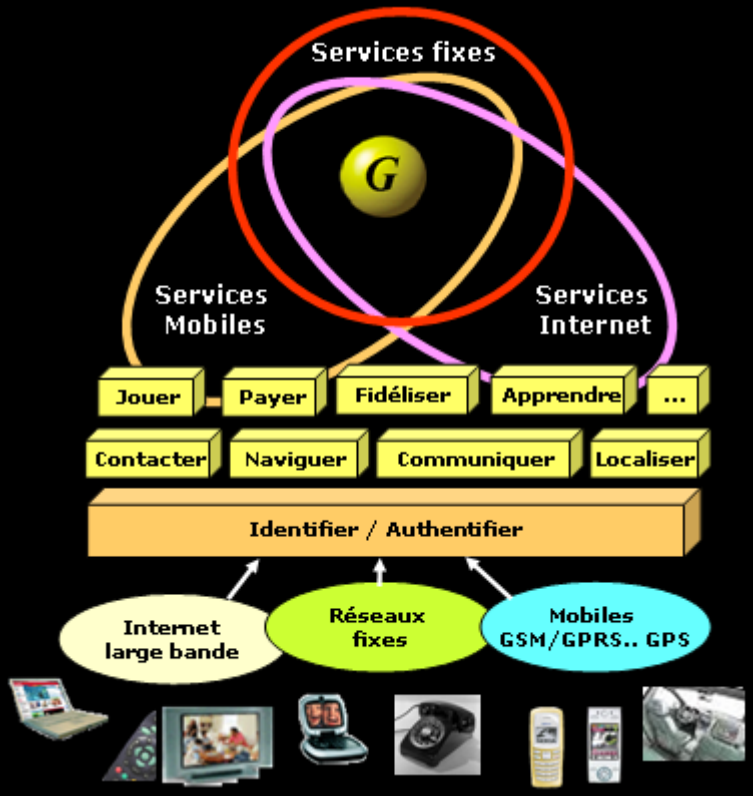
- **L'authentification à 2 facteurs (2FA)**
  - **Qui va la payer?**
  - **Quelle est son application à venir?**
  - **Combien de temps durera-t-elle?**
  - **Qui va détenir et gérer le secret partagé?**
  - **Comment migrer les secrets partagés?**

- **L'expérience utilisateur**
  - **Je ne veux pas transporter un nouveau token…**
  - **Je ne veux pas transporter plusieurs token…**
  - **J'ai oublié mon token à la maison…**

Coûts de distribution

- **Coûts du token, gestion de l'inventaire…**
- **Coûts de la distribution, de l'approvisionnement**
- **Coût de modification d'une application…**
- **Éducation du consommateur, support clientèle…**

Les besoins d'authentification forte



La convergence, vecteur de croissance

Les risques d'usurpation d'identité

Need for Stronger Authentication

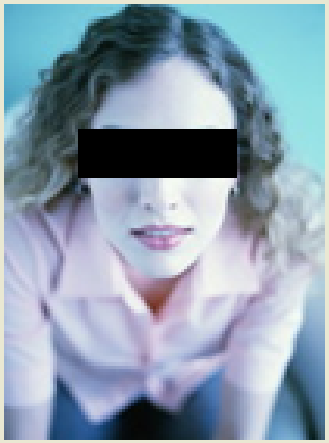
ID Theft costs users $500 and 30 hours per incident (US FTC, 2003)

70% of users would trade their password for chocolate

Demonize-T Trojan Horse forwards password keystrokes to hacker websites

Identity Theft

Password Sniffers



Wireless LAN's and VPN's eliminate the security perimeter

On-line Commerce fastest growing method and twice the cost of in-person payment

Remote Workers

On-line Commerce

$3B in remote payment fraud

Phishing

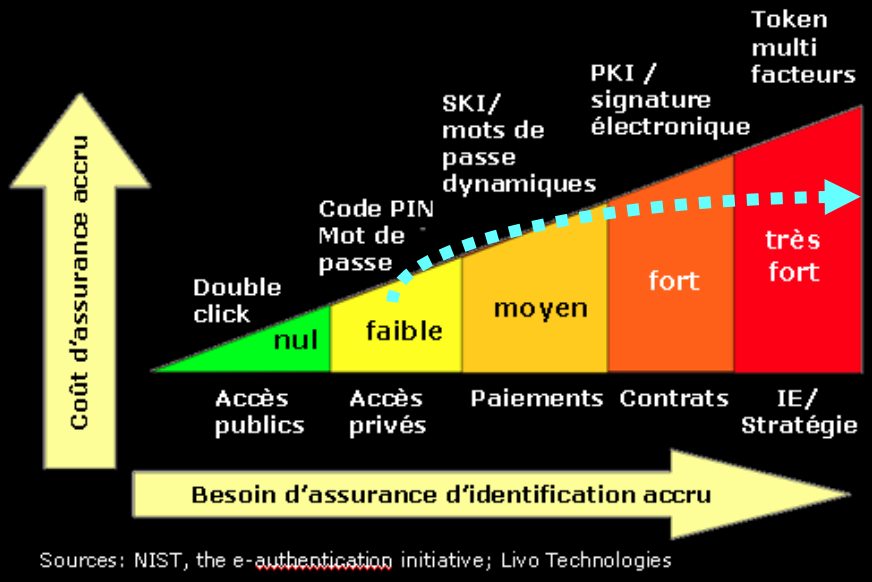
Crack once, spoof everywhere (my bank password is also my Yahoo! Mail password)

In 2005, liability can be shifted to issuing banks… how will they pass-on the losses?

Phishing successful 5-10% of the time

As we begin to rely on shared credentials, the need for strong authentication will become even more important

Les problèmes de l'authentification forte



Sources: NIST, the e-authentication initiative; Livo Technologies

La croissance des coûts

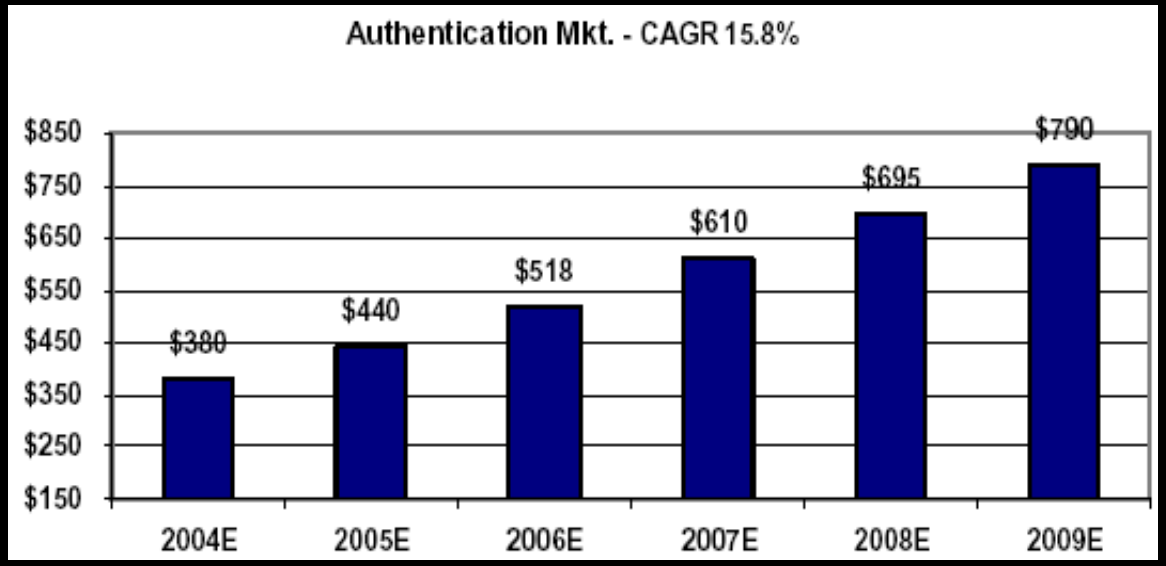
What is Wrong with Strong?

- Tokens are difficult to use and are usually only good for one application (VPN, etc.)
- Users demand convenience to readily adopt a technology… this means:
  - Better integration with apps
  - Fewer, multiple-use devices
  - Security balanced with utility of usage (what else can I do with the device?)
  - Existing user behavior needs modification
- Costs are a key driver to deploying at enterprise and external/consumer-facing apps
  - Token
  - Provisioning
  - Lifecycle
  - Transactional

La difficulté d'usage

Croissance

- **Rapide …**



- **… gros potentiel**

Market	Potential Users	Current Penetration Rate	Strong Authentication Users
Remote Access	85M	20%	17,0M
Corporate Banking	10M	20%	2,0M
Retail Banking	130M	8%	10,4M
Enterprise Security	350M	3%	10,5M
On-Line Consumers	900M	0,30%	2,3M

Source: Solving the World's Identity Crisis, Jeanney Montgomery Scott, LLC. November 2005

Notre compétitivité / généralités

Génonyme		Au quotidien		Concurrents	
Automatique 3 à 5 secondes		Durée de l'authentification		Manuel 20 sec à 2 minutes	
non		Mot de passe exigé		oui	S1
non		Je n'ai aucune donnée à recopier, donc aucun risque d'erreur		risque réel	S2
non		Les données sont chiffrée sur le réseau		oui	S3

S1: Il est toujours possible d'observer un utilisateur en train de taper son mot de passe, ou d'intercepter ce mot de passe avec un keylogger.

S2: L'erreur humaine est la première cause d'appels dans les Hotlines, et donc l'une des principales causes de coûts pour les prestataires de services.

S3: On peut imaginer que si l'on chiffre, c'est que l'on a quelque chose à cacher. Le génonyme ne transmet que des nombres publics, qui ne contiennent en eux-même aucune information exploitable : aucun chiffrement n'est donc nécessaire.

Notre compétitivité / usage

	Utilisation du service au quotidien	Genonyme	Concurrents
Sécurité	La Sécurité de la transaction est parfaite		
	Je ne saisis aucune donnée confidentielle		
	Ma sécurité est assurée par un Agent Logiciel Spécialisé		
Compatibilité	Le système est compatible avec les standards SSL/ RSA/ HTTPS / X509		
Terminal utilisateur	Je choisis librement mon Token parmi mes périphériques usuels		
	Mon Token est gratuit		
	Mon Token assure d'autres fonctions (disque dur, musique, téléphone…)		
Convivialité	Je n'ai aucune donnée à recopier, donc aucun risque d'erreur		
	Je n'ai aucun mot de passe à mémoriser		
	Je suis reconnu et authentifié en moins de trois secondes		
Notoriété	J'utilise un système reconnu et éprouvé par le marché		

Notre compétitivité / usage

Génonyme		Utilisation du service au quotidien		Concurrents
Automatique		J'ai oublié mon mot de passe, ou je pense qu'il est corrompu		Hotline
Automatique		On m'a volé mon ordinateur (perte de la SKI)		Hotline + répudiation+ ré-émission clef
Automatique		On m'a volé mon Token, ou je l'ai perdu		Hotline + répudiation+ ré-émission Token
5 minutes		Mon service est interrompu :		de une à trois semaines
gratuit		Coût de l'opération:		de 100 à 300 euros

Notre compétitivité / vol d'ID

Génonyme		On vient de me voler mon Token		Concurrents
33 %		Je suis en danger		50 %
En ligne		Je déclare le vol		Hotline
Localement		Je m'authentifie par password secret		Hotline
Automatique un autre de mes périphériques		Je remplace mon Token		Hotline + répudiation + ré-émission Token
2 à 5 minutes		Durée de l'opération		de une à trois semaines
gratuit		Coût de l'opération		de 100 à 300 euros
En ligne		Régénération de mes droits		UPS ou FEDEX
C'est vrai...		Si je perd mon Token, je perd aussi mon téléphone...		C'est vrai...
oui		Mais je m'en rends compte plus facilement, et donc j'agis plus vite.		l'utilisateur s'en rend compte moins vite
oui		Je peux changer de Token à tout moment pour les raisons qui me regardent		non

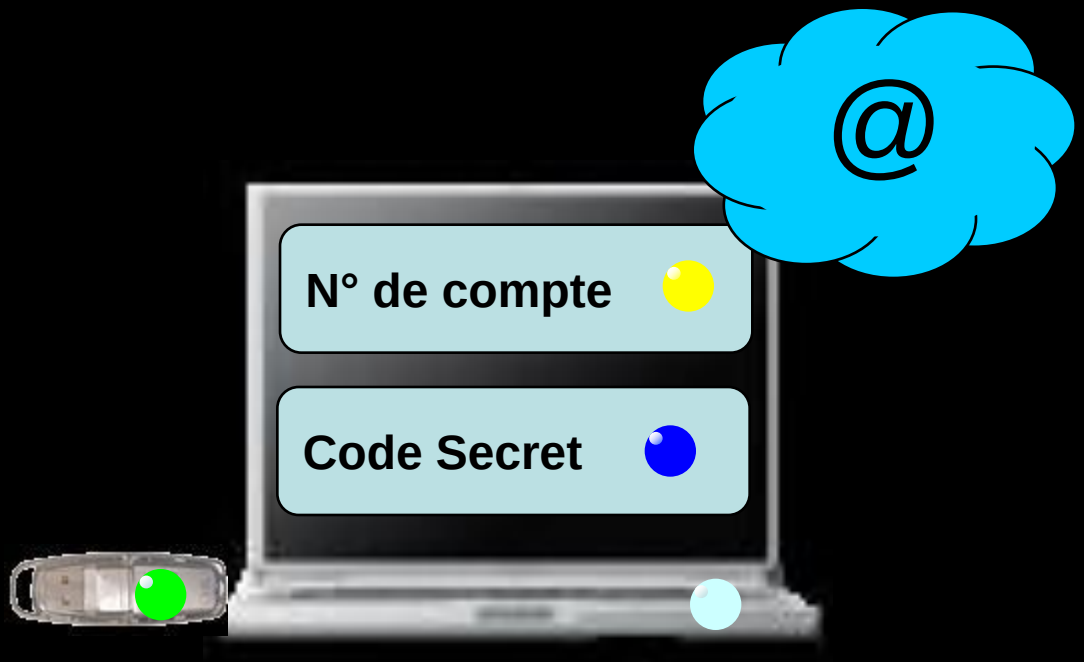
Notre compétitivité / remplacement d'ID

Génonyme		Token		Concurrents
J'en ai déjà un		Je veux obtenir un Token		Hotline
Gratuit		Prix du Token		80 à 150 euros
Immédiat		Durée de l'opération		de une à trois semaines
non		J'ai un dossier à remplir (coordonnées, passe secret pour Hotline, conditions diverses, autorisations de débit)		oui
non		Quelqu'un d'autre que moi connaît mon mot de passe secret		oui (Hotline) S1
gratuit		Coût de l'opération		de 100 à 300 euros

S1: La présence d'une information exploitable dans le serveur de la Hotline est une faille de sécurité très largement répandue et exploitée par le piratage interne.

Démonstration

J’ai 4 facteurs d’identité.
Par exemple:



2 choses que j’ai

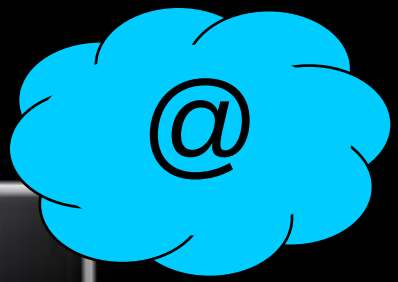
- Mon terminal
- Ma clé usb

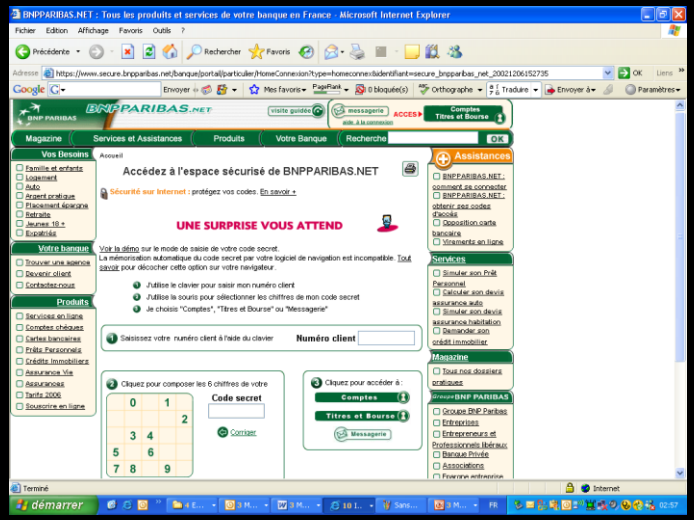
2 choses que je sais

- Mon n° de compte
- Mon code secret

Connexion

Je me connecte à ma banque comme d'habitude

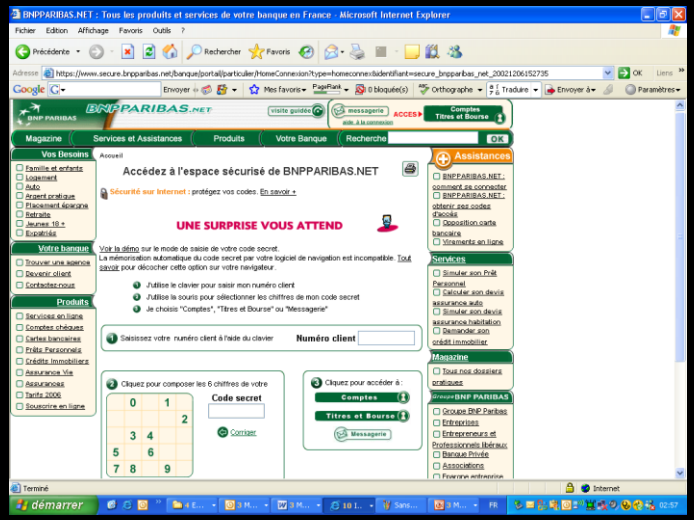


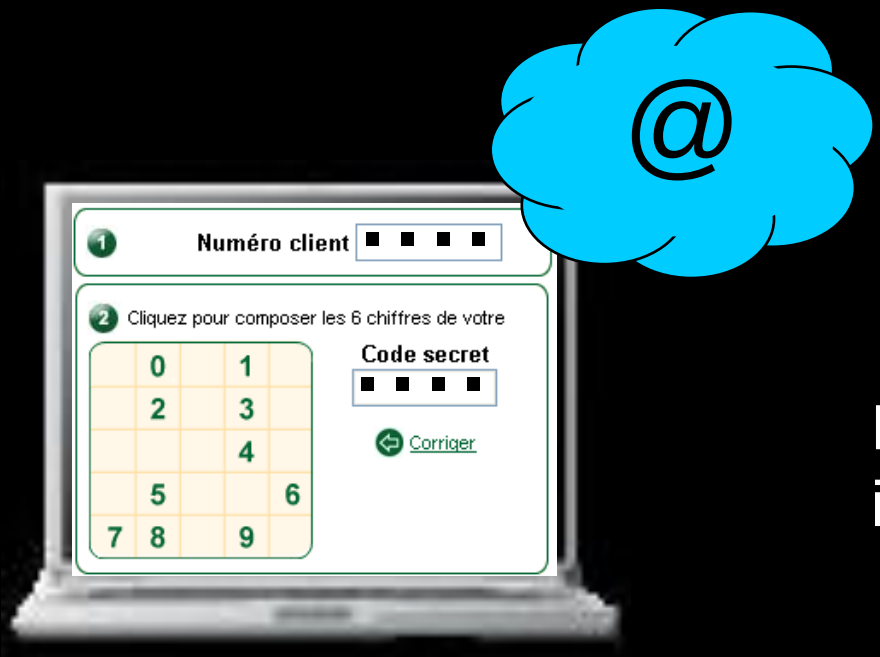


La seule chose dont j'ai besoin est d'un compte déjà ouvert.

Authentification usuelle

Je m'authentifie avec mes identifiants / authentifiants habituels





Ma banque valide mon identité

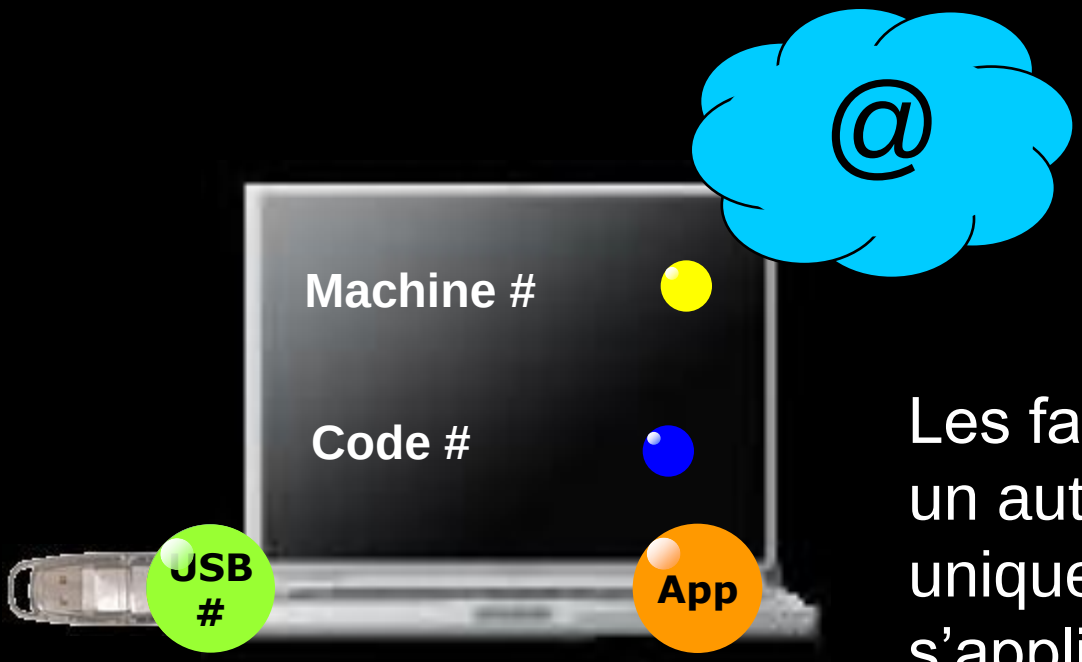
Acquisition d'un agent

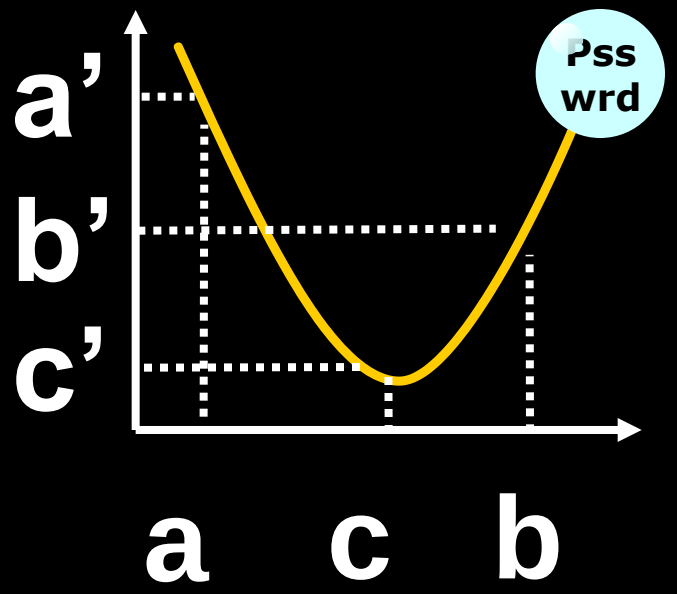
L'agent d'authentification peut être téléchargé ou m'être remis en main propre

- Cas de téléchargement:
Je choisis un produit portable
- Cas de remise en main propre
Ma banque me remet une clé, par exemple.

Création de l'authentifiant

L'agent d'authentification est dans mon produit portable.
Il collecte, croise et hache 3 facteurs d'identité.





Les facteurs d'Identité génèrent un authentifiant multi-facteurs, unique et non cassable. Il ne s'applique qu'à ma banque

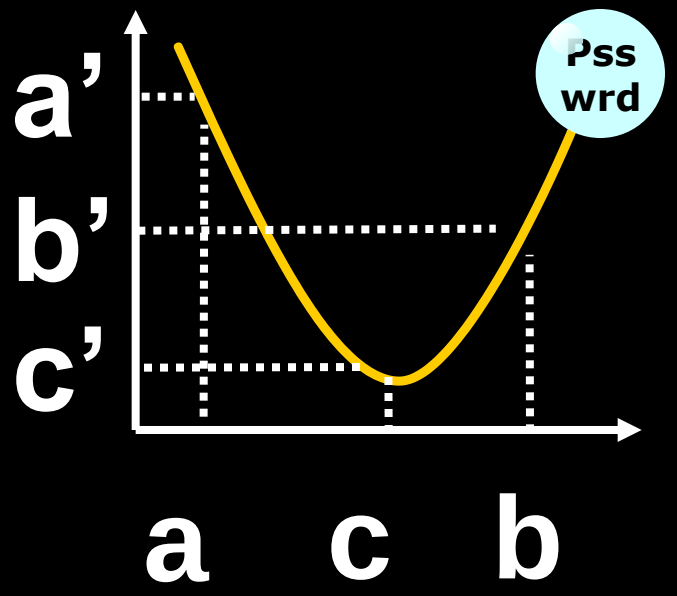
Usages

A chaque connexion, l'agent re-collecte mes facteurs d'identité et régénère mon authentifiant unique de façon dynamique.

L'authentification est forte et Mutuelle. Si je perds ma clé, mon code PIN ou mon terminal, personne ne peut rien en faire.

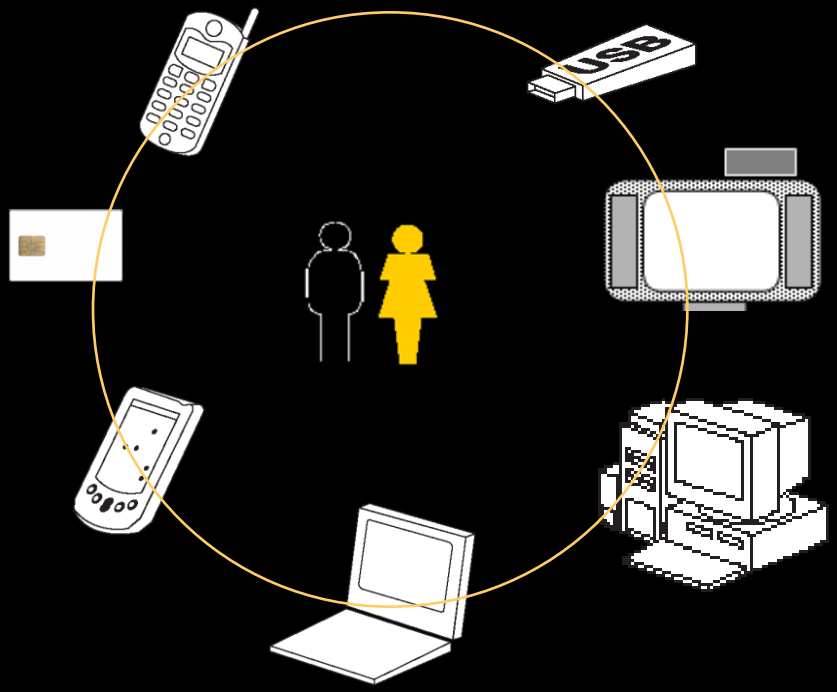
Administration

Je dois remplacer un facteur manquant. J'utilise un 4ème facteur d'ID enregistré au préalable

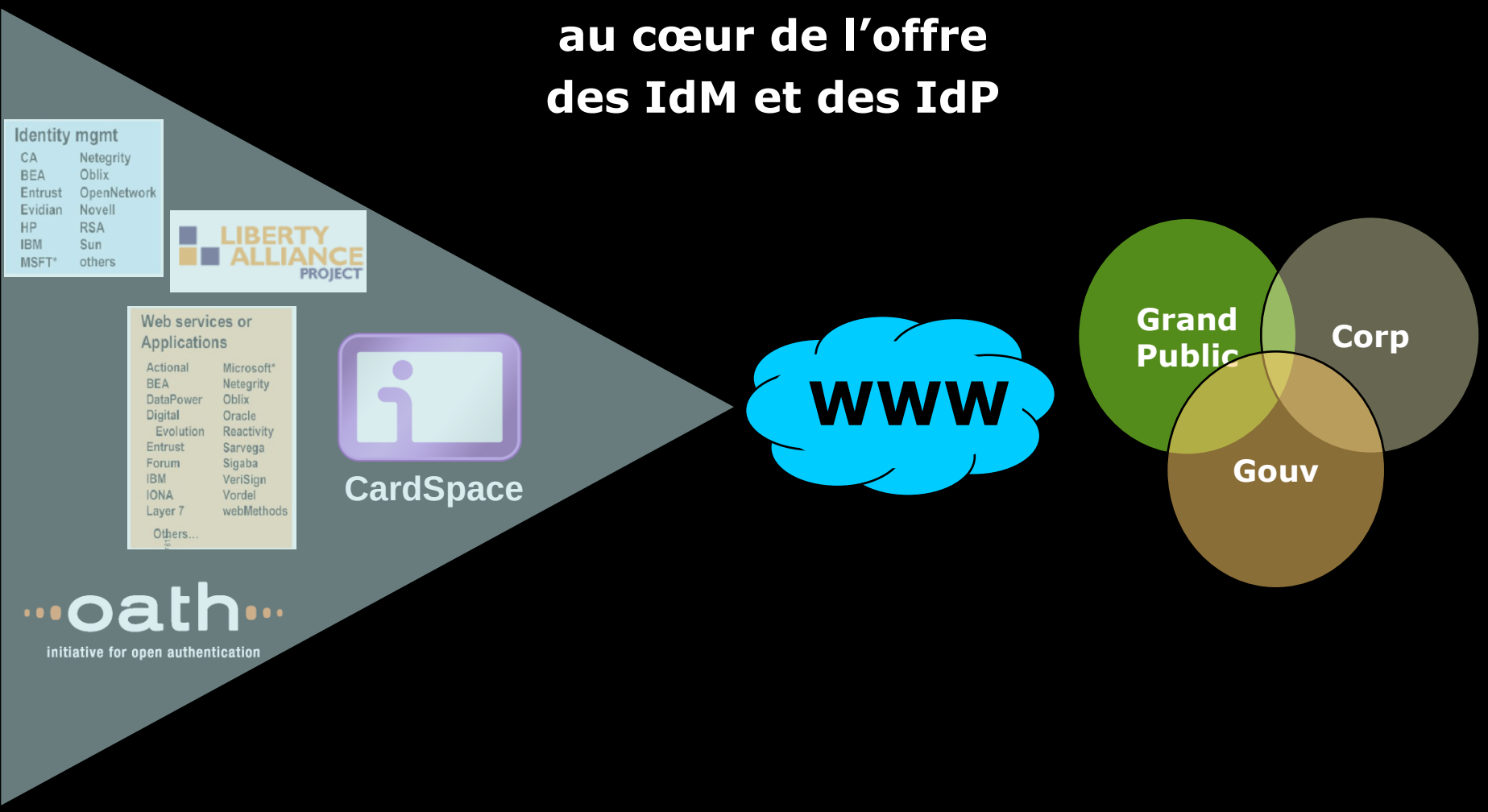


Ce 4ème facteur peut être
- un mot de passe
- un matériel
- un SMS...

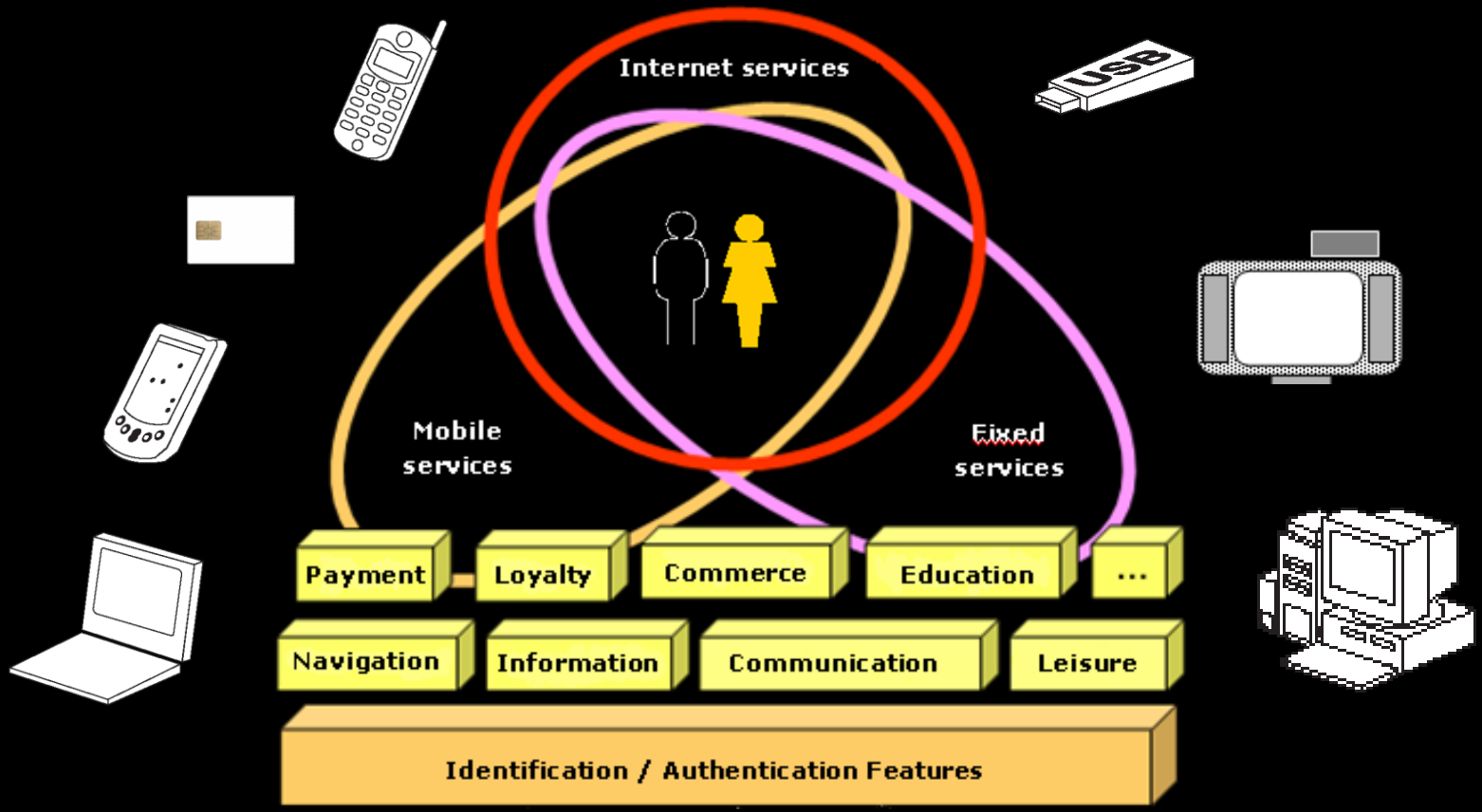
Développer un middleware d'authentification embarqué dans les produits de stockage et de communication de données



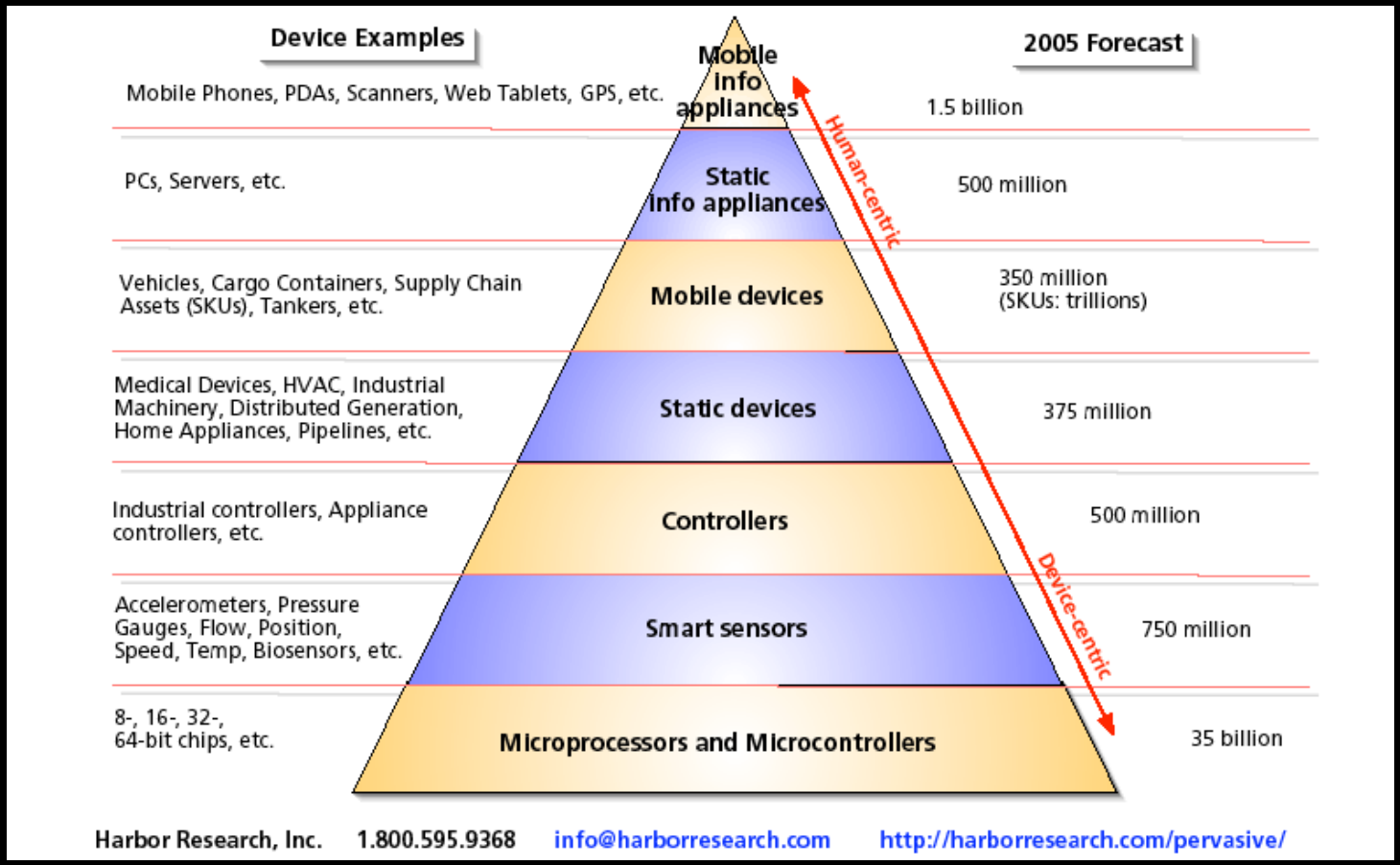
Embarquer le middleware au cœur de l'offre des IdM et des IdP



Cibler des applications centrées sur l'utilisateur et la convergence



Un prix-levier transparent pour des millions d'utilisateurs



Exemple

Estimations pour 10 000 utilisateurs sur 5 ans		Token OTP		Token USB		Carte à puce*		Produit usuel**	
Acquisition	Produit matériel	$360 000		$300 000		$532 750		100 000 €	
	Serveur matériel	$4 000		$4 000		$4 000		4 000 €	
	Serveur logiciel	$211 400		$211 400		$211 400		120 000 €	
	Client logiciel	- -	19%	$175 000	46%	$175 000	50%	80 000 €	60%
	Maintenance	$211 400		$386 400		$386 400		95 800 €	
	Coût total Système	$786 800		$1 076 800		$1 309 550		399 800 €	
	Coût Système / pers. / an	**$16**		**$22**		**$26**		**8 €**	
Déploiement	Installation - configuration	$9 000		$9 000		$9 000		9 000 €	
	Formation	$83 333		$125 000		$125 000		75 000 €	
	Distribution initiale	$133 333	5%	$180 000	13%	$186 667	13%	20 000 €	15%
	Coût total de Déploiement	$225 666		$314 000		$320 667		104 000 €	
	Coût Construction / pers. / an	**$5**		**$6**		**$6**		**2 €**	
Opérations	Distribution courante	$66 667		$90 000		$93 333		20 000 €	
	Administration Base de données	$125 000		$125 000		$125 000		125 000 €	
	Support à la clientèle	$250 000		$250 000		$250 000		25 000 €	
	Support Mot de passe	$2 000 000	76%	$500 000	41%	$500 000	37%	- -	25%
	Support Token re-sync	$750 000		- -		- -		- -	
	Coût total d'Opération	$3 191 667		$965 000		$968 333		170 000 €	
	Coût total Opération / pers. / an	**$64**		**$19**		**$19**		**3 €**	
Coût total Système + Construction + Opérations		$4 204 133	100%	$2 355 800	100%	$2 598 550	100%	673 800 €	100%
Coût total / pers. / an		**$85**		**$47**		**$52**		**13 €**	

* sans lecteur; ** le produit usuel ici considéré est une clé à mémoire USB dont le coût d'achat moyen est de 7€

Estimations pour 10 000 utilisateurs sur 5 ans	Token OTP		Token crypto USB		Crypto Carte à puce*		Clé USB Livo**	
Coût d'Acquisition du Système / personne / an	12 €	19%	17 €	46%	20 €	50%	8 €	60%
Coût de Déploiement du Système / personne / an	4 €	5%	5 €	13%	5 €	13%	2 €	15%
Coût d'Opération du Système / personne / an	49 €	76%	15 €	41%	15 €	37%	3 €	25%
Coût Total des Systèmes d'Authentification / personne / an	**65 €**	100%	**37 €**	100%	**40 €**	100%	**$13**	100%

* sans lecteur; ** le produit usuel ici considéré est une clé à mémoire USB dont le coût d'achat moyen est de 7€

Un état d'esprit

Think Big

Start Small