



# Protection des données

6 janvier 2004



Crackage des mots de passe  
Mai 2003

# La protection des données

- **Protection des données d'entreprise, patrimoine informationnel d'une société**
  - Identification de l'information à valeur ajoutée
  - Un patrimoine d'information à protéger impérativement
  - Traitement des données nominatives
  - éclairage juridique
    - Exemples d'infractions pénales
- **Protection des données personnelles des systèmes ouverts - sites Web**
  - Le contexte marchand
  - Définition
  - Politique de protection des données personnelles
  - Les initiatives de protection associées
  - Eclairage juridique
    - rôle de la CNIL
    - responsabilités pénales de l'administrateur et du chef d'entreprise
- **Protection des données au format numérique**
  - Démonstration
  - Questions - Réponses
- **Intervenants**
  - Eric Jaillet
  - Raphaël Peuchot
  - Christophe Briguet
  - Christophe Jaskolski
- **Problématiques annexes**
  - Les données personnelles dans le cadre de l'administration électronique

## Qu 'entend-on par données personnelles ?

- « **Les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou par une personne morale** » \*
- **Exemples**
  - Données fiscales
  - Informations médicales
  - Etat civil
  - Casier judiciaire
- **Selon l'article 2 de la Convention européenne du 28 janvier 1981, les données à caractère personnel sont définies comme « toute information concernant la personne physique identifiée ou identifiable »**

\* Extrait de l'article 4 de la loi 1978

## Qu 'entend-on par données personnelles ?

- **Obtention du consentement**
- **Respect de la finalité de traitement**
- **Equité de traitement**
- **Durée de conservation vs droit à l'oubli**
- **Traçabilité des preuves**
- **Respect de la confidentialité**
- **Droit d'accès et de rectification**
- **Périmètre d'échange des données personnelles**
  - flux transfrontières en Europe
  - flux hors Union Européenne
- **Assurer la transparence au client ou à l'utilisateur quant à l'exploitation de ses données personnelles au cours du cycle**
  - la collecte
  - l'enregistrement
  - l'élaboration
  - la modification
  - la conservation
  - et la destruction des données

## Les principes

- **« Toute personne a droit au respect**
  - de sa vie privée et familiale,
  - de son domicile
  - et de sa correspondance »
  - D 'après la convention européenne de sauvegarde des droits de l 'homme et des libertés fondamentales
- **Qui est concerné ?**
  - Chacun d 'entre nous dès lors que
    - on se porte candidat pour un travail
    - on utilise une carte bancaire
    - on navigue sur Internet

D 'où la notion de maître de fichiers :

## Les règles

- les données doivent être traitées loyalement et légalement;
- elles doivent être collectées à des fins explicites et légitimes et utilisées en conséquence;
- les données doivent être pertinentes et non excessives par rapport à l'usage auquel elles sont destinées;
- les données doivent être précises et, le cas échéant, tenues à jour;
- les maîtres de fichiers sont tenus de prévoir des dispositifs raisonnables permettant aux personnes concernées de rectifier, d'effacer ou de verrouiller les données incorrectes les concernant;
- les données identifiant des personnes ne doivent pas être conservées plus longtemps qu'il est nécessaire;
- la directive stipule que chaque État membre doit prévoir une ou plusieurs autorités de surveillance de manière à assurer le suivi de l'application de la directive. Une responsabilité de l'autorité de surveillance consiste à tenir un registre public à jour de façon que le grand public ait accès aux noms de tous les maîtres de fichiers et aux types de traitements que ceux-ci effectuent;
- en principe, tous les maîtres de fichiers doivent aviser les autorités de surveillance lorsqu'ils traitent des données. Les États membres peuvent prévoir une simplification ou une exemption de notification pour des types spécifiques de traitement n'impliquant pas de risques particuliers. Les procédures d'exception et de simplification peuvent également être autorisées, lorsque, en conformité avec la législation nationale, un responsable indépendant en charge de la protection des données a été désigné par le maître de fichiers. Les États membres peuvent exiger une vérification préalable, à conduire par l'autorité de surveillance, avant que ne soient entreprises des opérations de traitement impliquant des risques particuliers. Il appartient aux États membres de déterminer quels types d'opérations de traitement impliquent des risques particuliers.

## Cas légitimes de traitement des données (recueillies et exploitées)

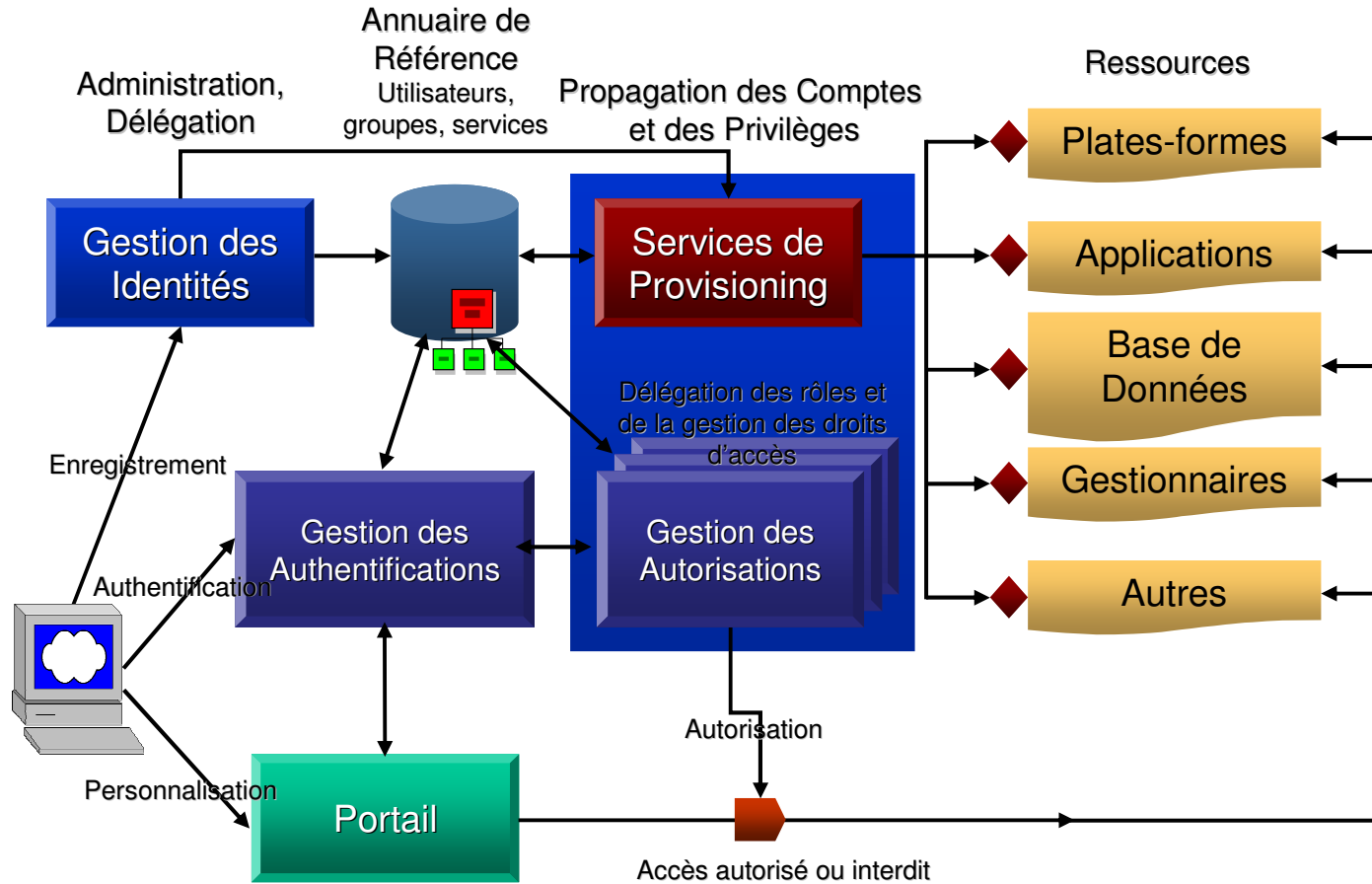
- la personne concernée a sans ambiguïté marqué son accord, à savoir a librement et spécifiquement consenti après avoir été dûment informée;
- le traitement des données est nécessaire à l'exécution d'un contrat ou pour souscrire un contrat sollicité par la personne concernée, à savoir traitement des données à des fins de facturation ou traitement des données relatives à un candidat à un emploi ou à l'octroi d'un prêt;
- le traitement est exigé par la loi;
- le traitement des données est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée. Un exemple est celui d'un accident d'automobile à la suite duquel la personne concernée se trouve dans un état d'inconscience: des auxiliaires médicaux d'urgence sont autorisés à communiquer les résultats de tests sanguins, si ceux-ci sont jugés essentiels pour sauver la vie de la personne;
- le traitement est nécessaire pour effectuer des missions d'intérêt public ou des missions effectuées par des instances officielles (telles que le gouvernement, les administrations fiscales, la police, etc.);
- enfin, les données peuvent être traitées à chaque fois que le maître de fichiers ou un tiers a un intérêt légitime à le faire. Cependant, cet intérêt ne peut outrepasser l'intérêt de protection ou les droits et libertés fondamentaux de la personne concernée, et notamment de son droit à la vie privée. Cette disposition établit la nécessité de trouver dans la pratique un équilibre raisonnable entre l'intérêt commercial des maîtres de fichiers et la vie privée des personnes concernées. Cet équilibre est d'abord évalué par les maîtres de fichiers sous le contrôle des autorités en charge de la protection des données, bien que la décision finale appartienne le cas échéant aux tribunaux.

## Données sensibles

- l'origine raciale ou ethnique,
- aux opinions politiques,
- aux croyances religieuses ou philosophiques,
- à l'appartenance syndicale,
- à la santé
- ou aux préférences sexuelles.
- En principe, les données de ce type ne peuvent être traitées. Des dérogations sont tolérées dans des circonstances très spécifiques.

Le développement du Marché unique et de la société de l'information augmente les flux de données à caractère personnel entre les Etats membres de l'UE. Afin de supprimer les obstacles potentiels à de tels flux, tout en assurant un niveau élevé de protection de la vie privée au sein de l'Union, la législation sur la protection des données a été harmonisée. La Commission européenne a également engagé un dialogue avec les pays non-membres de l'Union afin d'assurer un niveau élevé de protection lors de l'exportation des données à caractère personnel vers ces pays. La Commission poursuit également des études, au niveau européen et international, sur l'état actuel de la protection des données.

## Exemple d 'architecture ouverte



\* Extrait de l'article 4 de la loi 1978

# Un exemple de politique de données personnelles

The screenshot shows a Microsoft Internet Explorer browser window displaying the website of Groupe AFAQ. The address bar shows the URL <http://www.afaq.org/>. The page title is "Groupe AFAQ - Organisme Certificateur International". The browser's menu bar includes "Fichier", "Edition", "Affichage", "Favoris", and "Outils". The address bar also shows navigation buttons like "Précédente" and "Rechercher". The browser's toolbar includes various icons for search, home, and other functions. The website's navigation bar includes "GROUPE AFAQ", "NOS SERVICES", and "ACTUALITES". The main content area is titled "DONNÉES PERSONNELLES" and contains the following text:

Nous nous engageons à préserver la confidentialité des informations que vous fournissez en ligne et vous invitons à lire la charte qui suit afin de connaître l'usage fait des informations personnelles que vous nous communiquez en exploitant nos services d'informations en ligne. Nous nous réservons la possibilité de modifier la présente charte et vous incitons par conséquent à vous y reporter régulièrement.

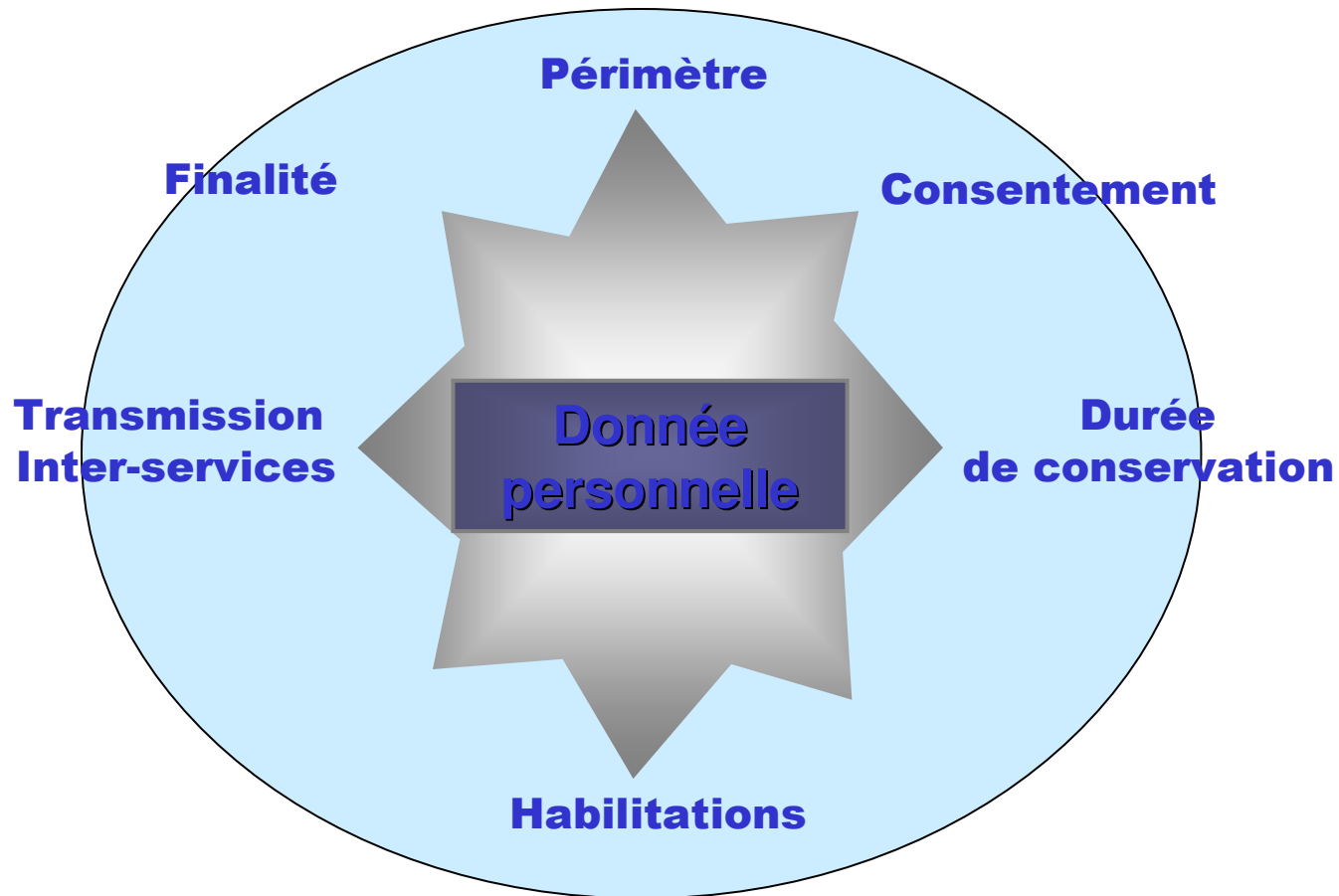
- > [Quelles informations personnelles le Groupe AFAQ recueille-t-il sur moi au travers de ce site ?](#)
- > [Comment mes informations personnelles sont-elles utilisées par le Groupe AFAQ ?](#)
- > [Qui a la possibilité de recueillir des informations me concernant ?](#)
- > [Comment puis-je accéder à mes informations personnelles, les mettre à jour ou les supprimer ?](#)
- > [Quelles sont les mesures de sécurité mises en place pour lutter contre la perte, l'utilisation frauduleuse ou la détérioration des informations me concernant ?](#)
- > [Que sont les cookies et comment les utilisons-nous ?](#)
- > [Quels sont les risques associés à l'utilisation des cookies ?](#)
- > [Comment afficher ou supprimer mes fichiers de cookies ?](#)

Below the list, there is a section titled "Quelles informations personnelles le Groupe AFAQ recueille-t-il sur moi au travers de ce site ?" which states: "Le Groupe AFAQ collecte plusieurs types d'informations à partir de n'importe lequel de ses sites web pays, lorsque vous ouvrez un compte web AFAQ dans la rubrique 'votre compte web AFAQ': votre nom, votre adresse, votre e-mail et autres informations vous concernant personnellement ou concernant votre entreprise. Plus vos

On the right side of the page, there is a section for "Vos commentaires ou questions à propos de cette charte du Groupe AFAQ" with the email address [webmaster@afaq.org](mailto:webmaster@afaq.org) and two buttons: "par email" and "Ajoutez à vos favoris".

En pratique, l'internaute ne prend pas connaissance de ce type d'informations

## Modèle de données personnelles orienté objet



# La protection des données personnelles

- Définition, enjeux & besoins
- Les pratiques sur Internet autour des données personnelles
- Du client global au ... Citoyen
- Certification des acteurs et protection des données personnelles
- Architecture, les approches de gestion possibles
- Conclusion

## P3P : Platform for Privacy Preferences Project

- **Une politique de protection des données personnelles**
  - Notamment sur l'usage des informations générées par les cookies
  - N'accepte que des cookies en provenance de sites certifiés P3P
- **Créé en 1997 par le W3C : World Wide Web, consortium qui inclut notamment**
  - IBM
  - e-trade
  - Compaq
  - AT&T
- **Technologie de filtrage conçue pour favoriser la confidentialité et la confiance dans le cyberspace en permettant aux fournisseurs de contenu d'énoncer leurs pratiques d'utilisation des données personnelles et aux utilisateurs de contrôler les données concernant leur vie privée.**
- **Ce type d'usages est né du constat suivant**
  - Il est plus rapide de contrer l'existence d'un site non conforme aux lois en en bloquant l'accès par un mécanisme de blocage ou de filtrage que de le faire condamner par un tribunal traditionnel

## P3P : un succès mitigé ?

- « **seulement** » 17% des internautes l'utilisent \*
- **Limites**
  - Avec le ralentissement du secteur des nouvelles technologies, la protection des données personnelles n'est pas une priorité
  - P3P fournit
    - Un mécanisme de vérification de la charte
    - Et non un moyen de vérifier si la technique du site est en accord avec sa charte
  - Plutôt destiné aux sites américains, peu contraints par les dispositions légales
- **Nouvelle recommandation sur P3P V1.0**
  - Méthode grâce à laquelle un site peut décrire dans un fichier XML l'usage des données personnelles
  - Ce fichier est interprétable par un navigateur compatible P3P (IE et Netscape le sont)
  - Possibilité de traduire la politique de protection des données personnelles avec des outils comme
    - P3P Policy Editor d'IBM
    - YOUpowered de Consumer Trust
- **A suivre**
  - les prochaines versions de P3P devraient également proposer des mécanismes offrant
    - un choix de plusieurs politiques P3P aux visiteurs
    - ou leur permettant d'exprimer très clairement leur accord

\* D'après le journal du net - avril 2002

## Des initiatives concurrentes

- **Comparatif au niveau européen des possibilités offertes à l'utilisateur en matière de protection de données personnelles par les technologies suivantes**
  - Mozilla Password Manager,
  - authentification par proxy,
  - Microsoft Passport,
  - Liberty Alliance.
- **Microsoft Passport**
  - Système de collecte des données personnelles sur Internet
  - La CE évalue sa compatibilité
  - Les quinze clarifie leur position début 2003
- **Liberty Alliance**
  - Se positionne sur la protection des données personnelles comme plus « indépendante »
    - 130 compagnies & organisations de consommateurs
    - Conduite par Sun pour contrer Microsoft
    - Nouvelle spécification publiée en novembre

## Back-up

- Exemple de liens utiles
- [www.spamfree.org](http://www.spamfree.org)

## Back-up

•La dernière stratégie de Microsoft, .Net, lancée en juin 2000, s'illustre dans .Net My Services. L'objectif de cette stratégie est de transformer Internet en une vaste plate-forme d'échanges de données entre tous les terminaux (PC, PDA, téléphones mobiles) afin de relier au sein d'un même service divers éléments comme la messagerie, l'agenda électronique, le commerce ou la banque en ligne.

Le but est de permettre à un utilisateur de regrouper voire de partager ses informations personnelles, éparpillées entre différents terminaux, sur le web.

L'offre de .Net My Services s'appuie sur Passport, système d'authentification dont le principe est la saisie unique par l'internaute de ses informations personnelles, lui évitant ainsi de s'identifier à chaque connexion aux sites partenaires de Microsoft. Ce programme devrait voir le jour en 2002.

Il est cependant très controversé par les défenseurs de la vie privée et pose simultanément les questions de la confiance des consommateurs envers une société à laquelle ils confieraient leurs données personnelles et de l'usage qu'en ferait cette société. En outre, des difficultés liées à la sécurité du logiciel gérant les données confidentielles subsistent.

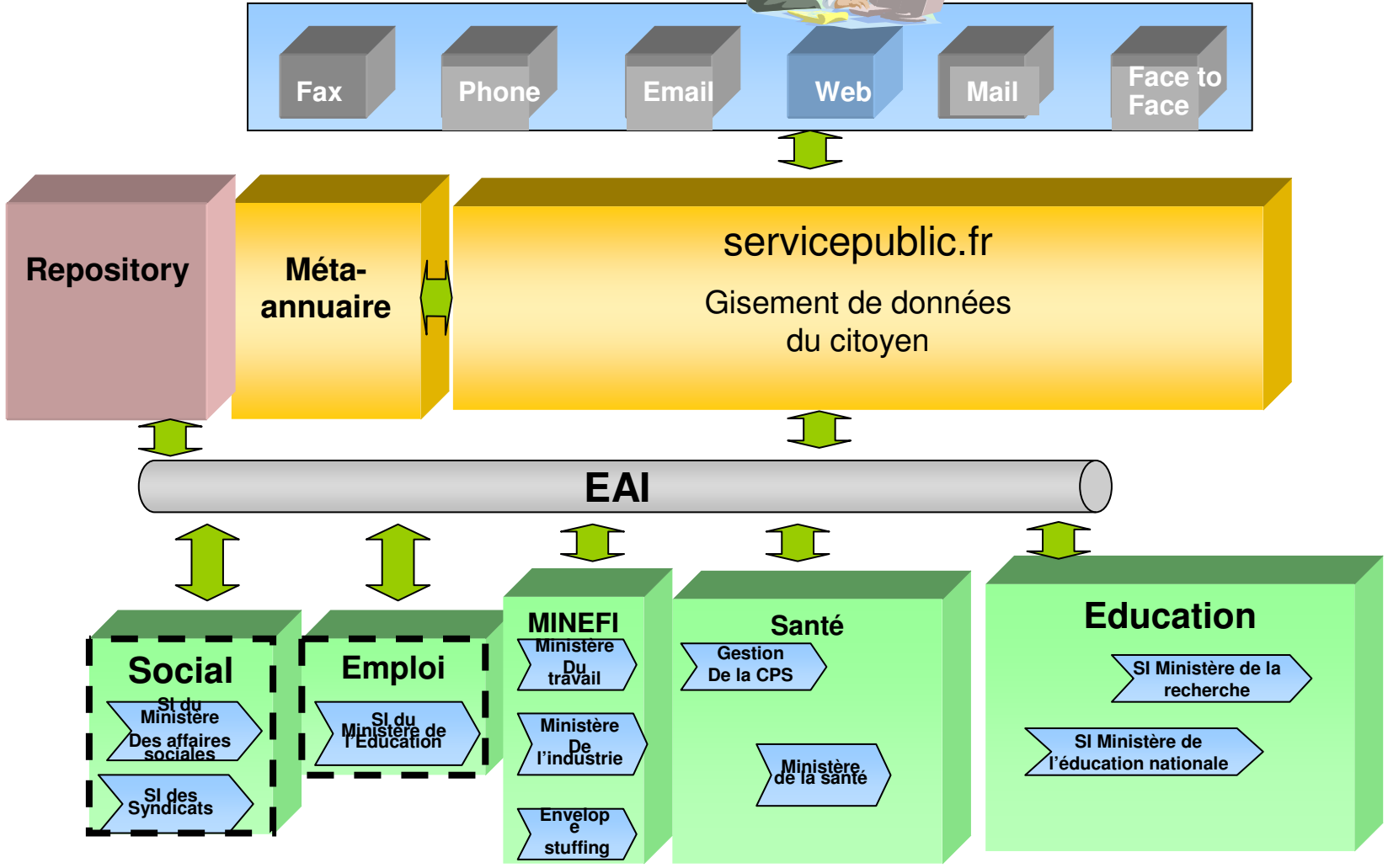
Enfin, cette nouvelle stratégie illustre à nouveau à la bataille entre Microsoft et ses concurrents AOL et Sun.

- Microsoft souhaite rendre universelle sa technique d'authentification des données sur Internet...
- ...soulevant une controverse relative à la collecte des données personnelles et la sécurité du système...
- ...et provoquant une riposte de ses principaux concurrents.

# La gestion des habilitations d'un service en ligne personnalisable : premier espace de liberté



# Un maître mot : l'interopérabilité...





# ***Protection des données***

## ***Sécurité des information au format numérique***

**CLUSIR**

**Rhône Alpes**



Sécurité des informations  
6 janvier 2004

**Auteurs: Christophe BRIGUET**

# Plan

---

- Problématique des données numériques
- Fuite d'information dans des documents
- Risques associés aux formats de fichiers
- Recommandation pour la protection des informations

# Problématique des informations numériques

---

- L'immatérialisation des données engendre:
  - La duplication sans limite (copie)
  - La reproduction (impression, capture d'écran, re-saisie)
  - La diffusion non contrôlée de l'information
  - La fuite d'informations non souhaitée

# Fuite d'informations personnelles

- Inclusion d'informations à l'insu de l'utilisateur
  - Informations personnelles
  - Informations "marketing"
  - Temps d'utilisation
  - Habitudes d'utilisation
  - Relations avec d'autres documents, applications, ressources réseau (y compris Internet)
- Contenu actif, pouvant modifier l'apparence des documents en fonction de l'environnement dans lequel ils sont ouverts
  - Problème de la signature de documents actifs

# Fuite d'informations dans les fichiers PDF

---

- Recadrage d'un document scanné, permet de faire apparaître des parties supplémentaires du document qui auraient dû être éliminées
  - Dans Document/Recadrer des pages, cliquer sur Remettre à zéro
- Suppression de masques en surimpression
  - Permet de révéler des informations masquées volontairement

# Fuite d'informations dans les fichiers Word (1/2)

---

- Propriétés du document
  - Informations lisibles directement:
    - Nom de l'auteur
    - Entreprise de l'auteur
    - Date et heure de création
    - Temps passé à l'édition
    - Heure d'impression
    - Etc ...
- Suivie des modifications (cf fichier Alcatel  
[http://web.morons.org/external/CPE\\_statement.doc](http://web.morons.org/external/CPE_statement.doc))

# Fuite d'informations dans les fichiers Word (2/2)

- Ouverture d'un document dans un éditeur hexa décimal (chemin d'accès successif, enregistrement différentiel, imprimante, adresse MAC (après \_PID\_GUID))
- Permettent à l'auteur de recueillir de l'information sur les lecteurs des documents (processus inverse)
  - Moment de la lecture
  - Lieu de la lecture (adresse IP)
  - Informations diverses sur l'identité et sur l'environnement du lecteur (logiciel utilisé, langue, etc...) et sur son type de connexion Internet

# Risques associés formats de fichiers

Liste non exhaustive ...

<b>Format</b>	<b>Extensions</b>	<b>Risques</b>	<b>Conteneur</b>	<b>Type</b>
Word	doc, dot, wbk, dohtml	Élevé	oui	binaire
Excel	Xls, xl?, wbk, xlhtml	Élevé	oui	binaire
Powerpoint	Ppt, pot, pps, ppa, pwz, ppthtml, pothtml	Élevé	oui	binaire
RTF	rtf	Très élevé	oui	texte
HTML	Html, htm ...	Faible	non	texte
Adobe Acrobat	pdf	Faible	oui	texte

# Recommandations (1/4)

---

- Ne pas diffuser un document ayant été retouché (très contraignant)
- Recréer les documents avant diffusion publique
- Opter pour un traitement de texte libre et compatible avec les leaders du marché StarOffice ou OpenOffice
- Utiliser un firewall personnel pour interdire certaines applications d'accéder à Internet

# Recommandations (2/4)

---

- Dans MS Word
  - Désactiver l'enregistrement rapide
  - Désactiver le suivi des modifications
  - Désactiver toutes les macros (y compris signées)
  - Configurer les fichiers modèles (.dot) en read-only
- Depuis Office XP/2002 (option / sécurité)
  - Cocher « Supprimer les informations personnelles de ce document lors de la sauvegarde »
  - Cocher « Avertir avant d'imprimer, de sauvegarder ou d'envoyer un fichier qui contient du suivi de modifications ou des commentaires»

# Recommandations (3/4)

---

- Utiliser des outils spécialisés
- AirZIP ([www.airzip.com](http://www.airzip.com))
  - Protection contre la duplication / diffusion
  - Trace l'utilisation
  - Restreinte dans le temps
- Microsoft IRM (Information Rights Management ([www.microsoft.com/RM](http://www.microsoft.com/RM)))

# Recommandations (4/4)

---

- Toute organisation doit donc considérer la gestion des documents propriétaires en fonction du degré de confidentialité de ses informations
- Il est recommandé d'inclure cette problématique dans les politiques de sécurité
- Il est indispensable de sensibiliser des utilisateurs (avec démonstration)