Technologies de Protection de la vie privée sur Internet

Yves Deswarte
deswarte@laas.fr
LAAS-CNRS, Toulouse

PETs : Privacy Enhancing Technologies

- Principe : "besoin d'en connaître" ("need-to-know")
  ne transmettre une information qu'à ceux qui en ont besoin pour réaliser la tâche qu'on leur confie
  -> Minimisation des données personnelles
  puis destruction/oubli

- … sur Internet comme dans le monde réel

- …avec des limites : certaines informations personnelles doivent pouvoir être fournies aux autorités judiciaires en cas de litige ou d'enquête (lutte contre le blanchiment d'argent sale, par exemple) : "pseudonymat" plutôt qu'anonymat total

3 types de PETs

- Protéger les adresses IP
- Autorisation respectant la vie privée
- Gestion des données / accès aux données

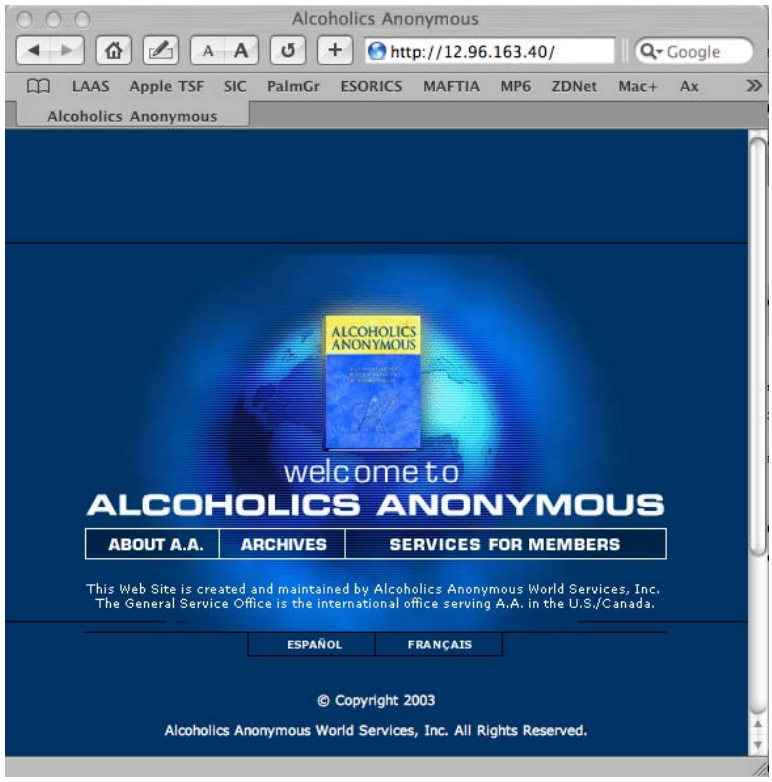
Adresse IP= "donnée nominative"

Exemple :

```
Return-Path: <Yves.Deswarte@laas.fr>
Received: from laas.laas.fr (140.93.0.15) by mail.libertysurf.net
(6.5.026)
      id 3D518DEF00116A4D for yves.deswarte@libertysurf.fr; Tue, 13 Aug
2002 13:44:40 +0200
Received: from [140.93.21.6] (tsfyd [140.93.21.6])
    by laas.laas.fr (8.12.5/8.12.5) with ESMTP id g7DBid1D001531
    for <yves.deswarte@libertysurf.fr>; Tue, 13 Aug 2002 13:44:39 +0200
(CEST)
User-Agent: Microsoft-Entourage/10.1.0.2006
Date: Tue, 13 Aug 2002 13:44:38 +0200
Subject: test
From: Yves Deswarte <Yves.Deswarte@laas.fr>
To: <yves.deswarte@libertysurf.fr>
Message-ID: <B97EBDC6.2052%Yves.Deswarte@laas.fr>
Mime-version: 1.0
Content-type: text/plain; charset="US-ASCII"
Content-transfer-encoding: 7bit
```

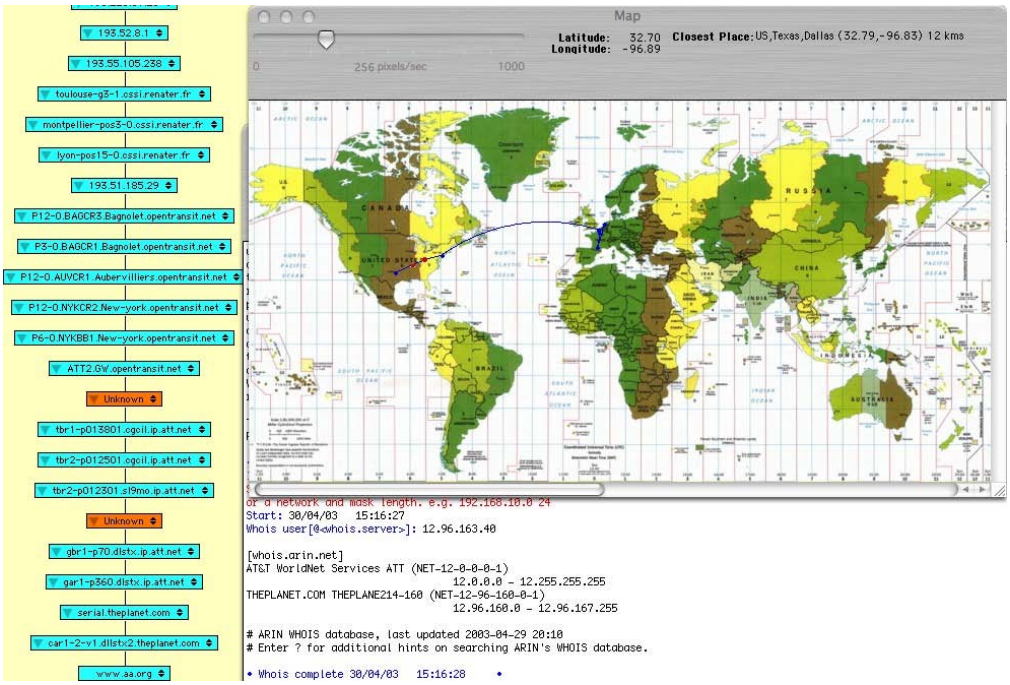
Adresse IP= "info sensible"

Exemple :



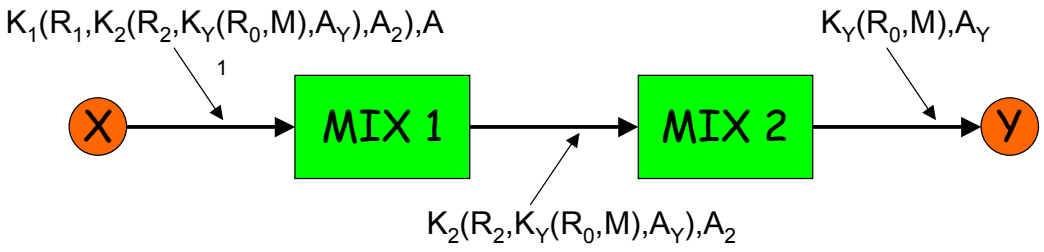
Adresse IP= localisation

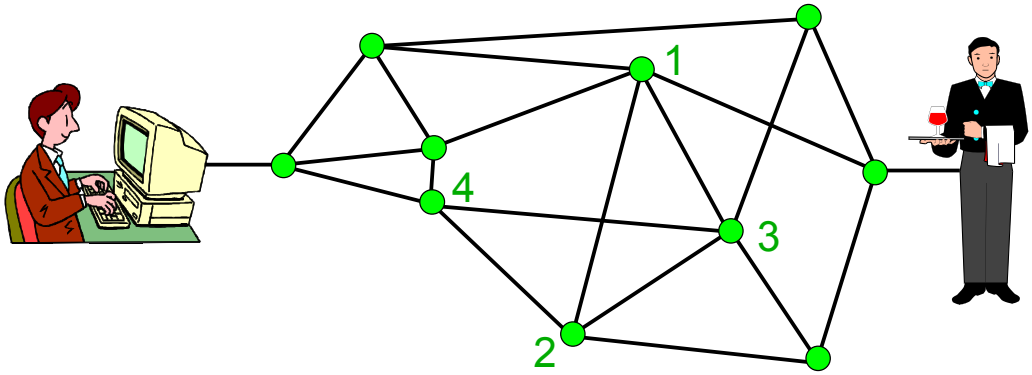
Exemple :



1° PET : Protéger les adresses IP

Relais de communication IP : MIX





2° PET: Autorisation sur Internet

- Aujourd'hui : client-serveur
  le serveur accorde ou refuse des privilèges au client en fonction de son identité déclarée (éventuellement vérifiée par des mécanismes d'authentification)
- Le serveur doit enregistrer des données personnelles : preuves en cas de litige
- Ces données peuvent être utilisées à d'autres fins (profilage des clients, marketing direct, revente de fichiers clients, chantage…)
- Action P3P (W3C) : *Platform for Privacy Preferences Project*
  vérification de la compatibilité des politiques de sécurité/privacy "déclarées"

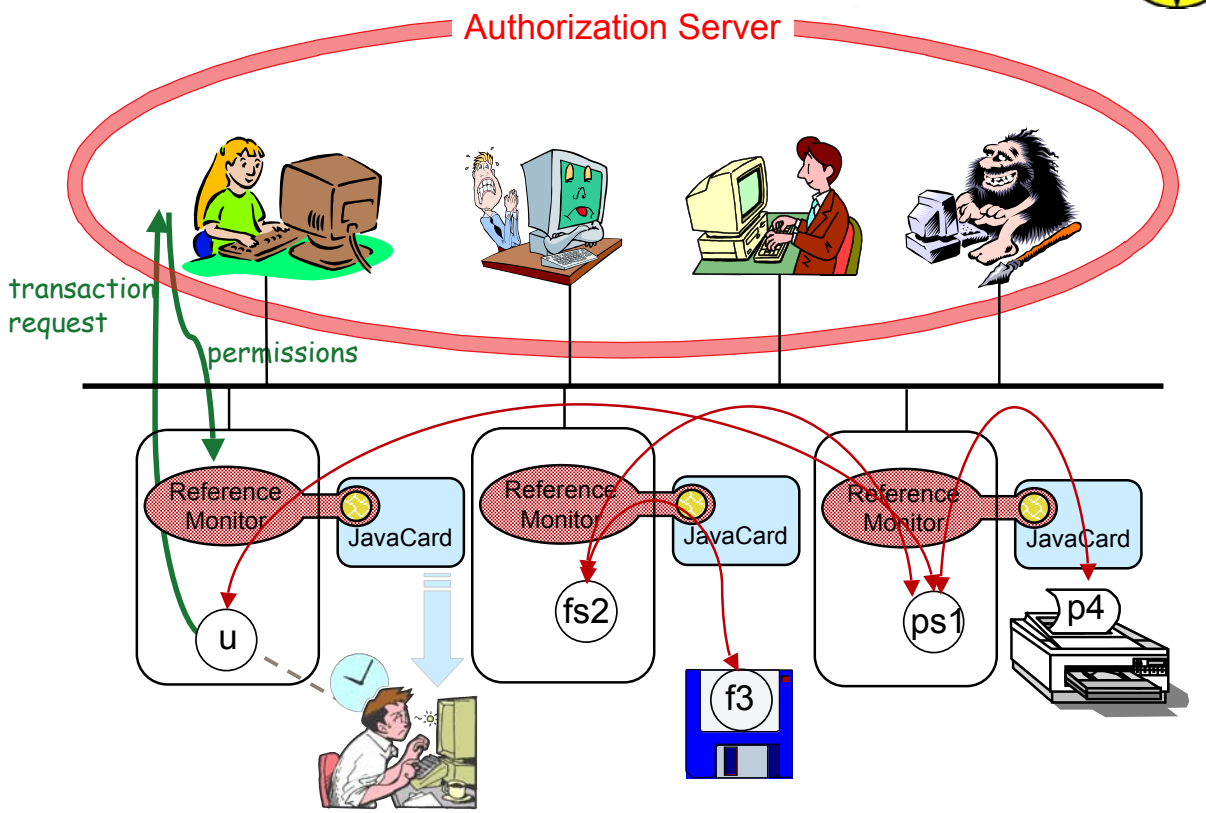
Ce schéma est dépassé

- Les transactions sur Internet mettent en jeu généralement plus de deux parties (ex : commerce électronique)
- Ces parties ont des intérêts différents (voire opposés) : suspicion mutuelle
- Nocif pour la vie privée : opposé au "besoin d'en connaître"

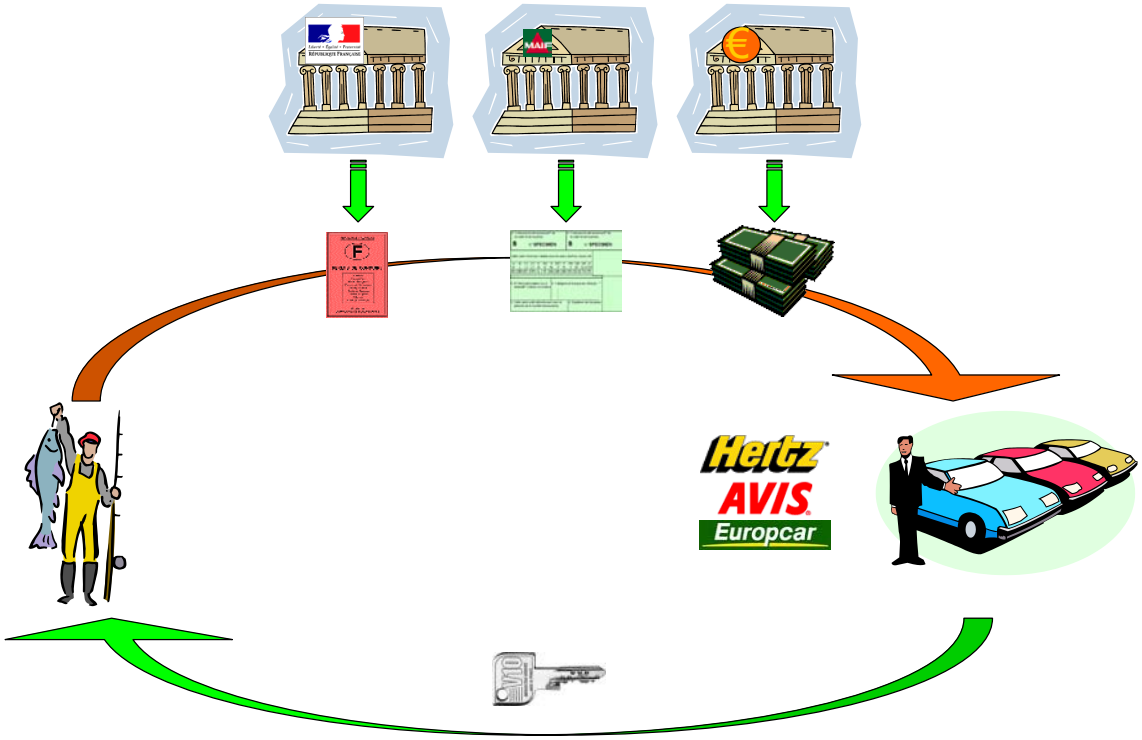
Preuves d'autorisation

- Certificats multiples : "credentials"
  ex: SPKI : certificats d'attributs/d'autorisation
  - cartes d'abonnement, de membre d'association, …
  - permis de conduire, carte d'électeur…
- Certificats restreints :
  - "Partial Revelation of Certified Identity" Fabrice Boudot, CARDIS 2000
- Problèmes: "chaînabilité" (une seule clé publique pour plusieurs certificats?), gestion des certificats/clés, authentification (biométrie?), préservation des preuves, révocation, …

Autorisation dans MAFTIA



"Anonymous Credentials" (Idemix)



3° PET : Gestion des données

- Minimisation des données personnelles
  -> répartition : séparation des pouvoirs, fragmentation des données
  -> anonymisation + appauvrissement
  ex: remplacer le code postal par l'identifiant de la région
- Auto-détermination : celui qui fournit des informations sur lui-même doit pouvoir contraindre l'usage qui pourrait en être fait
  ex: à effacer dans 48 h.
- Négociation entre l'individu et l'entreprise
  ex: coupons de réduction en échange d'une publicité ciblée

3° PET-bis : Accès aux données

- Principe du moindre privilège : un individu ne doit avoir que les droits minimaux nécessaires à sa tâche
- Politique de sécurité et mécanismes de protection : le détenteur d'une information en est responsable
- Ces données peuvent être très critiques :
  ex: dossiers médicaux
  - Disponibilité : temps de réponse (urgence), pérennité
  - Intégrité : nécessaire à la confiance, éléments de preuve
  - Confidentialité : vie privée <-> intérêts économiques
- Privacy = contrôle d'accès + obligations

PRIME (03/2004 - 02/2008)

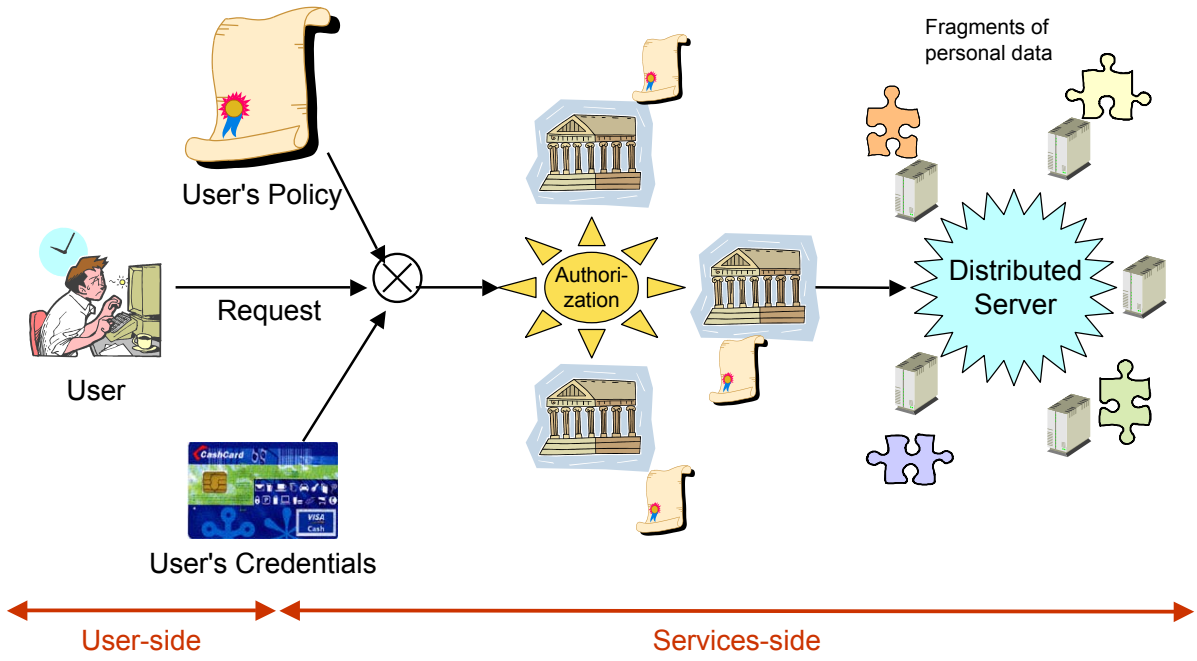
http://www.prime-project.eu.org/

- Privacy and Identity Management for Europe
  - Aspects juridico-socio-économiques
  - Côté utilisateur (dévelopt, utilisabilité)
  - Côté système, réseau, serveur
  - Applications réelles
- 20 Partenaires, subvention (CE+CH) : ~11,3 M€
  - Fournisseurs (IBM, HP, …)
  - Labos (KUL, U. Dresde, U. Milan, Eurécom, LAAS…)
  - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)

PRIME Principe :

- Identités différentes selon les besoins

Exemple d'architecture



Bibliographie

- Simone Fischer-Hübner, *IT-Security & Privacy*, LNCS 1958, 2001.
- Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.
- Fabrice Bodot, "Partial Revelation of Certified Identity", *4th IFIP WG8.8 Working Conference on Smart Card and Advanced Applications* (CARDIS-2000),Sept. 2000, Bristol (UK), Kluwer (Eds: J. Domingo-Ferrer, D. Chan, A. Watson), pp.257-269.
- J. Camenisch and A. Lysyanskaya, "Efficient non-transferable anonymous multishow credential system with optional anonymity revocation", *Advances in Cryptology - EUROCRYPT 2001*, LNCS 2045 (B. Pfitzmann, editor), pp.93 - 118, Springer, 2001.
- Jan Camenisch, Els Van Herreweghen, "Design and Implementation of the Idemix Anonymous Credential System", *proc. of the 9th ACM Computer and Communication Security (CCS-2002)*, nov. 2002, Washington DC, pp. 21-30
- David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Communications of the ACM*, 24/2 (1981) 84-88.
- David Chaum, "Showing credentials without identification: Transferring signatures between unconditionally unlinkable pseudonyms", *Auscrypt'90*, LNCS 453, Springer-Verlag, Berlin 1990, pp.246 - 264.
- M. K. Reiter and A. D. Rubin. "Crowds: Anonymity for web transactions", *ACM Transactions on Information and System Security*, 1(1):66-92, November 1998.
- Yves Deswarte, Noreddine Abghour, Vincent Nicomette, David Powell, "An Internet Authorization Scheme using Smartcard-based Security Kernels", in *Smart Card Programming and Security*, Proc. e-Smart 2001, Cannes (France), 19-22 septembre 2001, Springer, LNCS 2140, pp.71-82.
- MAFTIA Delivrable D6 <http://www.research.ec.org/maftia/deliverables/index.html>
- Anas Abou El Kalam, Yves Deswarte, Gilles Trouessin, Emmanuel Cordonnier, "Gestion des données médicales anonymisées : problèmes et solutions", 2ème Conférence Francophone en Gestion et Ingenierie des Systèmes Hospitaliers (GISEH 2004), Mons (Belgique), 9-11 septembre 2004.