Technologies pour la Protection de la vie privée

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse

La sécurité des réseaux s'améliore

- Législation (mars 2000) sur les signatures électroniques -> IGC (PKI)
- IP-Sec -> IPv6
- Progrès de la détection d'intrusions

… mais croissance des menaces

- DDoS
- Fraude dans l'e-Commerce
- Criminalité transfrontière
- … et les failles sont nombreuses!

… d'où encore plus de sécurité

- Filtrage à la source
- "Traçabilité"
  - FAI
  - Serveurs
- Danger pour la vie privée

Sommaire

- "Privacy" :
  - Définition
  - Législation
- PETs : Privacy Enhancing Technologies
  - Gestion d'identités multiples
  - Protéger les adresses IP
  - Protéger la localisation
  - Accès anonyme à des services
  - Autorisation respectant la vie privée
  - Gestion des données personnelles
- Projet Prime

"Privacy" : définitions

- Intimité, protection de la vie privée, du domaine privé
- Critères Communs (ISO 15408) :
  une classe fonctionnelle, 4 propriétés :
  - Anonymat : impossibilité (pour d'autres utilisateurs) de déterminer le véritable nom de l'utilisateur associé à un sujet, une opération, un objet
  - "Pseudonymat" : idem, sauf que l'utilisateur peut être tenu responsable de ses actes
  - Non-"chaînabilité" : impossibilité (pour d'autres utilisateurs) d'établir un lien entre différentes opérations faites par un même utilisateur
  - Non-observabilité : impossibilité (pour d'autres utilisateurs) de déterminer si une opération est en cours

Législation

- Guides pour l'utilisation de données personnelles informatisées et leurs transmissions internationales : OCDE en septembre 1980, Assemblée Générale de l'ONU, en décembre 1990.
- Protection des données à caractère personnel : Convention 108 du Conseil de l'Europe (26/01/81), directives 95/46/EC (libre mouvement) et 2002/58/CE (communications électroniques) (remplaçant la directive 97/66/CE)
- Protection des données nominatives -> à caractère personnel : loi "Informatique et Libertés" du 06/01/78, révisée par loi du 6 août 2004 + loi 94-548 (recherche médicale) http://www.cnil.fr/
- Secret professionnel (N^{eau} Code Pénal, art. 226-13) et secret des correspondances (NCP art. 226-15) + code des postes et télécommunications (secret des correspondances + art. L-32-3-1, inséré par la "Loi relative à la sécurité quotidienne" du 15/11/2001, révisé par la "Loi pour la sécurité intérieure" du 18/03/2003, et la "Loi sur l'économie numérique" du 21/06/2004)

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

Exemple : commerce électronique (1)

- Parties impliquées :
  un client, un marchand, un service de livraison, des banques, un émetteur de carte de crédit, un fournisseur d'accès Internet, …
- Le marchand n'a pas besoin (en général) de l'identité du client, mais doit être sûr de la validité du moyen de paiement.
- La société de livraison n'a pas besoin de connaître l'identité de l'acheteur, ni ce qui a été acheté (sauf les caractéristiques physiques), mais doit connaître l'identité et l'adresse du destinataire.

Exemple : commerce électronique (2)

- La banque du client ne doit pas connaître le marchand ni ce qui est acheté, seulement la référence du compte à créditer, le montant …
- La banque du marchand ne doit pas connaître le client…
- Le f.a.i. ne doit rien connaître de la transaction, sinon les caractéristiques techniques de la connexion …

6 types de PETs

- Gestion d'identités multiples
- Protéger les adresses IP
- Protéger la localisation
- Accès anonyme à des services
- Autorisation respectant la vie privée
- Gestion des données personnelles

1° PET : gestion d'identités multiples

- Réduire les liens entre une personne et les données la concernant (*chaînabilité*)
  - Communications et accès anonymes
- Mais : accès personnalisés
  - Préférences (ex: météo)
  - "Rôles" différents -> pseudonymes différents
    - Ex: contribuable et électeur
  - Authentification adaptée

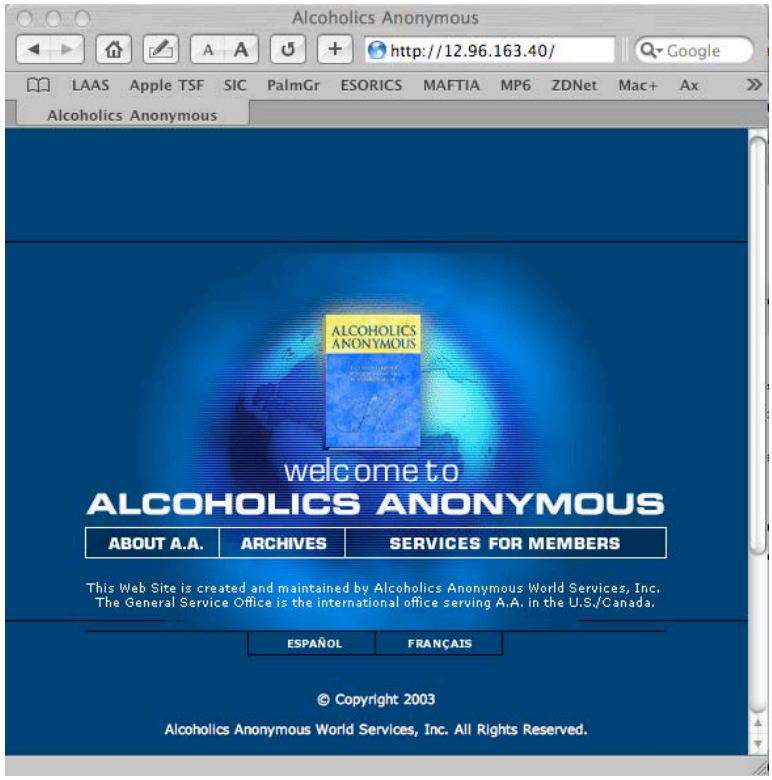
Adresse IP= "donnée nominative"

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
```

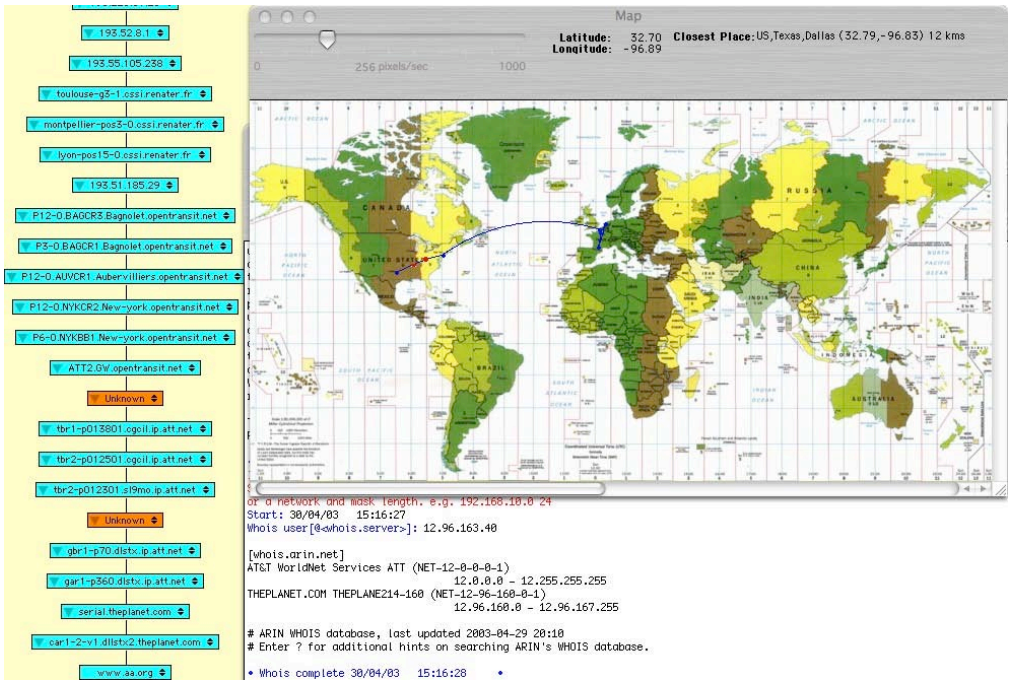
Adresse IP= "info sensible"

Exemple :



Adresse IP= localisation

Exemple :

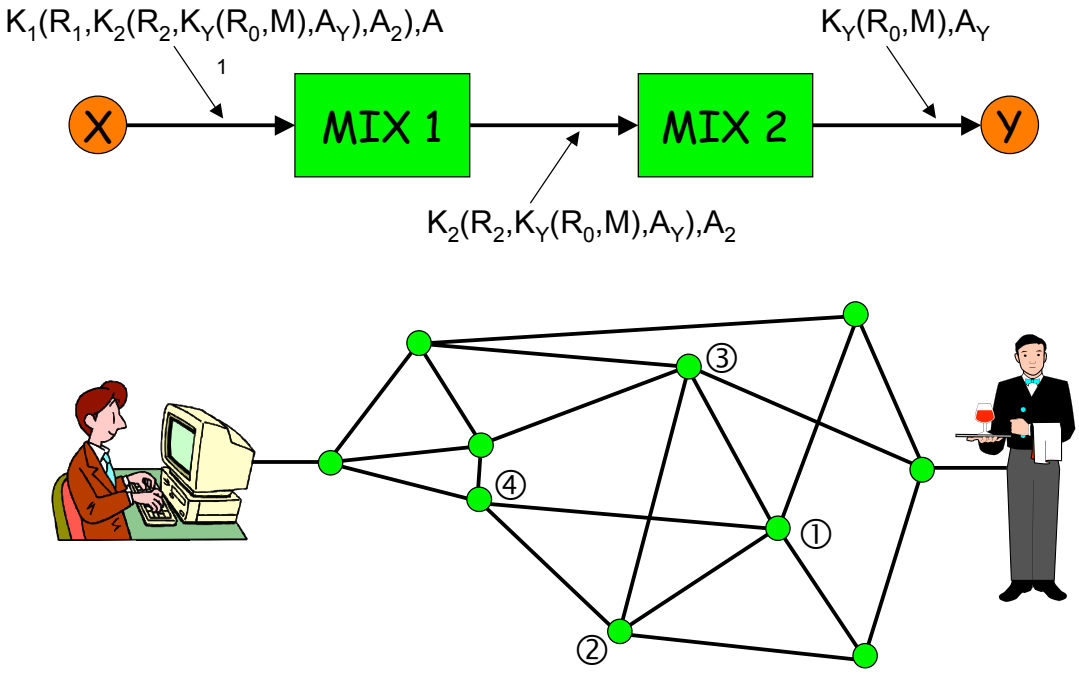


2° PET : Protéger les adresses IP

- PET : affectation dynamique des adresses IP (DHCP, PPP, NAT, …)
- Routeurs d'anonymat :
  - MIX
  - Onion Routing
  - Crowds

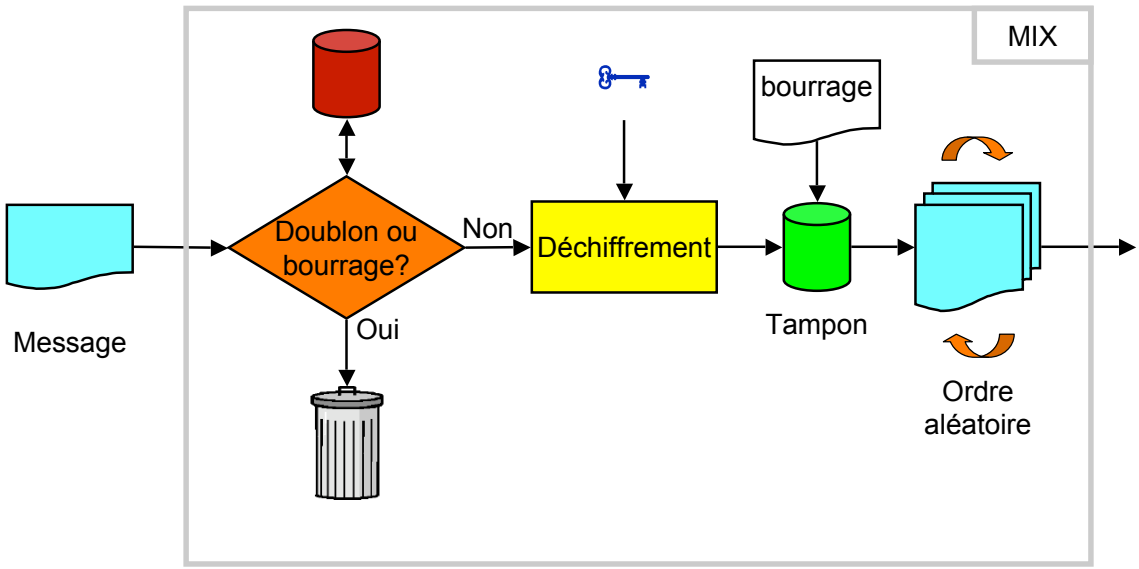
MIX / Onion Routing / Crowds

http://www.vote.caltech.edu/wote01/pdfs/juels2-wote.ppt



MIX : comment ça marche ?

http://www.inf.tu-dresden.de/



2° PET : Protéger la localisation

- Aujourd'hui : une @ IP <-> localisation (pcq: routage)
- De nombreux services connaissent la localisation de leurs clients
  - Aujourd'hui : fournisseurs d'accès Internet, GSM, …
  - En cours de déploiement :
    gestion de flotte, navigation, surveillance (anti-kidnapping), …
- Demain : IP partout (*pervasive computing, intelligence ambiante…*) : chaque "machin" aura une adresse IP *permanente* (nomade), chaque personne aura plusieurs machins, qui se connecteront aux machins proches (réseaux ad-hoc), qui s'identifieront, routeront leurs communications, fourniront des infos contextuelles, etc.
- Il faudra développer des PETs pour protéger la localisation.

3° PET: Accès anonyme à des services

- Relais d'anonymat (*anonymity proxy*) :
  unidirectionnels (ou bidirectionnels?)
  - Web
  - ftp
  - e-mail
  - …
- Serveur de pseudonymes :
  - e-mail
  - Identités multiples fournies par des f.a.i. (adresses mél)
  - Identités virtuelles multiples vs. "single-sign-on"
    Liberty Alliance <http://www.projectliberty.org>
    vs. Microsoft Passport

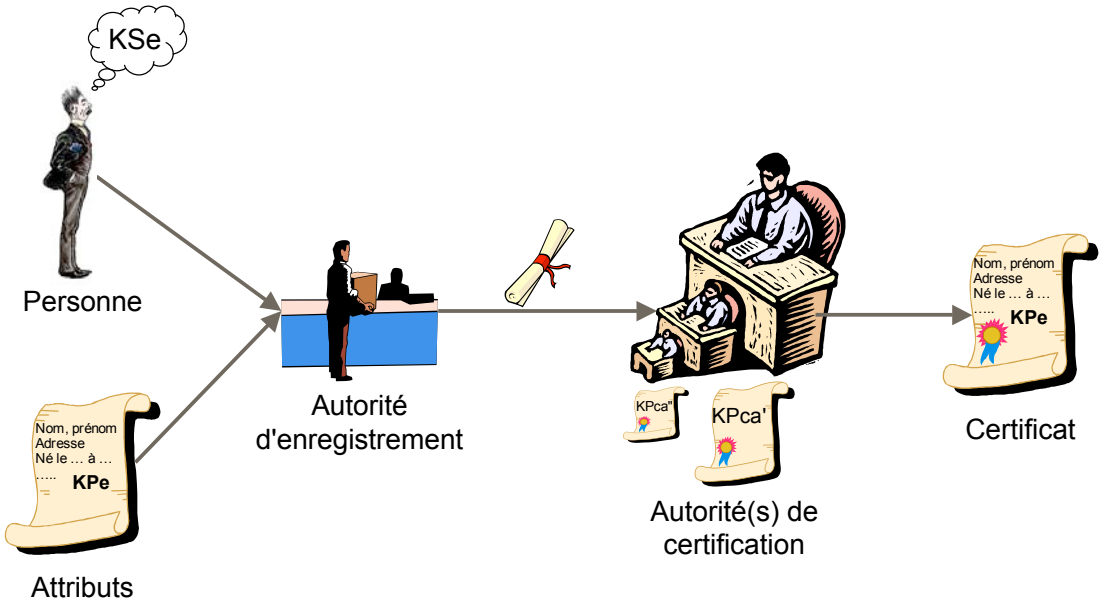
4° PET: Autorisation sur Internet

- 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 automatique de 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"

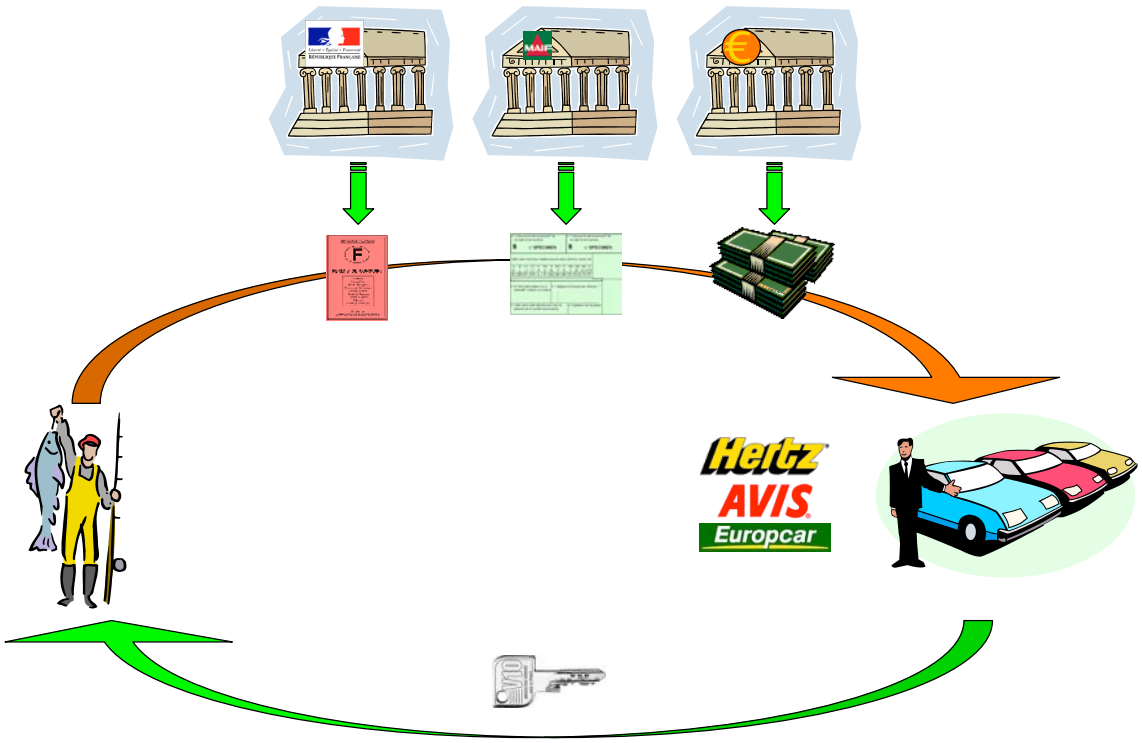
Certificats (ex: X509)



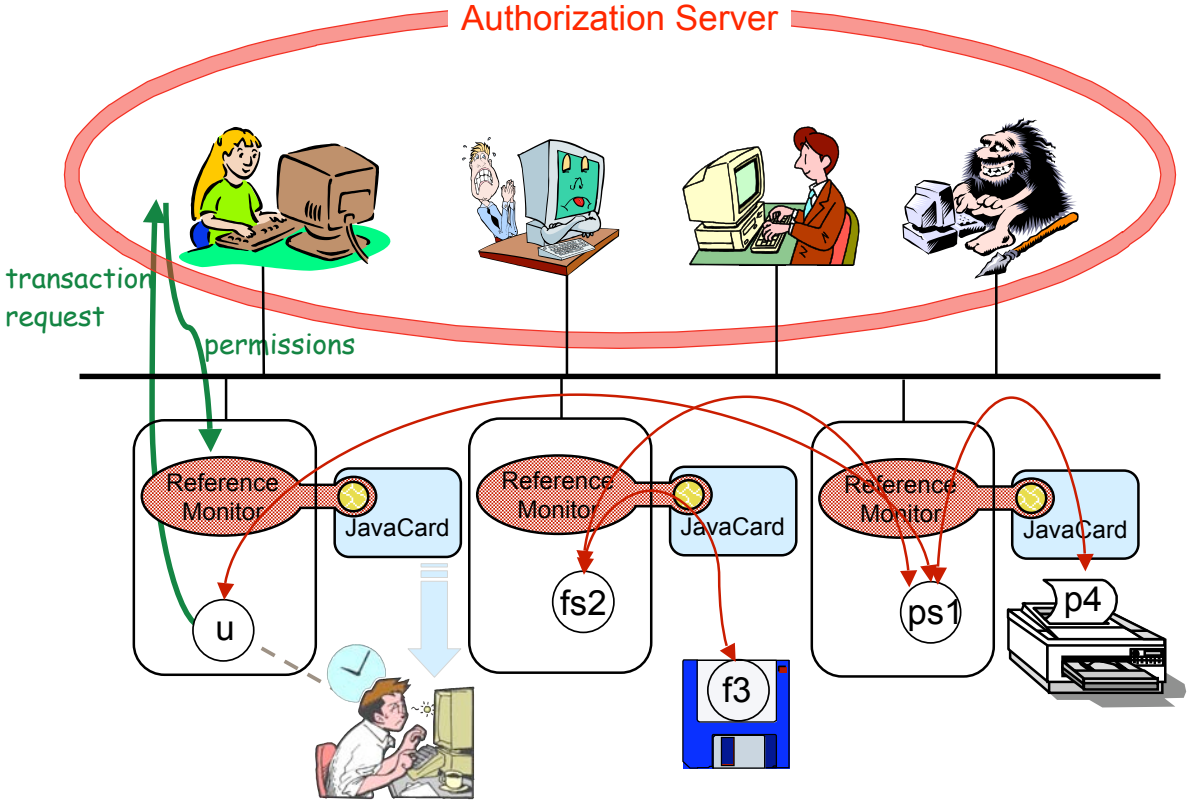
Preuves d'autorisation: credentials

- Certificats multiples :
  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, préservation des preuves, révocation, …

"Anonymous Credentials" (Idemix)



Autorisation dans MAFTIA



5° PET : gestion des données personnelles

- Minimisation des données personnelles
  -> répartition : séparation des pouvoirs, fragmentation des données
  -> anonymisation + appauvrissement
  ex: remplacer le code postal par l'identifiant de la région
  -> Private Information Retrieval (PIR)
- 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

5° 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 (art 34 de la loi « informatique et libertés »)
- 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

Donner confiance aux utilisateurs…

… que leur vie privée est protégée?

- Certification & labellisation
- Approche Trusted Computing Group
  - Support matériel : TPM
  - Bootstrap sûr
  - Vérification sceau S/W avant chargement
  - Vérifiable à distance

PRIME (03/2004 - 02/2008)

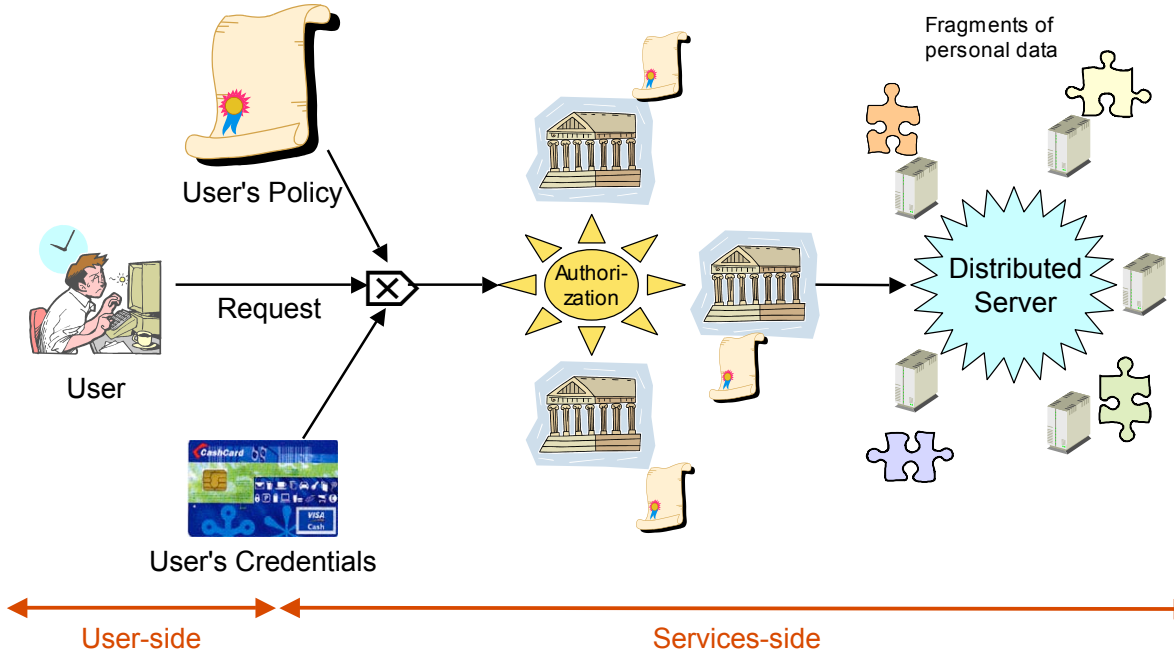
http://www.prime-project.eu.org/

- Privacy and Identity Management for Europe
  - Aspects juridico-socio-économiques
  - PET Côté utilisateur (dévelopt, utilisabilité)
  - PET Côté système, réseau, serveur
  - Applications réelles
- 20 Partenaires, 16 M€, subvention : ~10 M€
  - Fournisseurs (IBM, HP, …)
  - Labos (KUL, U. Dresde, U. Milan, Eurécom, LAAS…)
  - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)

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.