Intelligence ambiante et protection de la vie privée

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, Toulouse

Intelligence ambiante

- Développement de nouvelles technologies, utiles et/ou pratiques
- Marché créé/développé par des fournisseurs de technologie (matériels, réseaux, services, …)
- … mais généralement sans souci de respecter la vie privée des utilisateurs

Ex. RFID

- Identifiant unique pour chaque objet, lecture sans visibilité
- Meilleure gestion des approvisionnements, des stocks, traçabilité des contenants/contenus, sécurité alimentaire, service après-vente, …
- Mais possibilité de traçage des acheteurs
- … danger pour la vie privée !!!

Sommaire

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

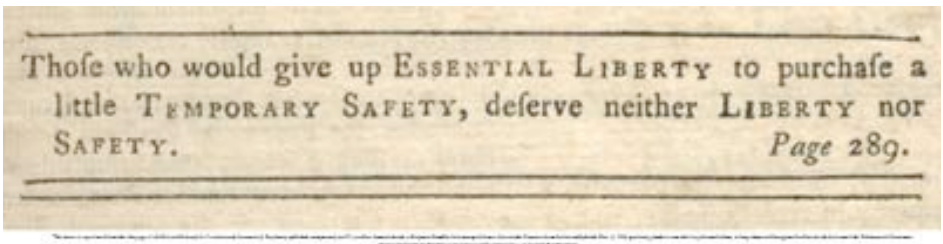
"Privacy" : définitions

- Intimité, protection de la vie privée, du domaine privé
- Critères Communs (ISO 15408) :
  une classe de fonctionnalité, 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

Pseudonymat < anonymat < non-chaînabilité < non-observabilité

Sécurité et respect de la vie privée

- Deux droits fondamentaux
  - Déclaration universelle des droits de l'homme, ONU, 1948 :
    - Art. 3 : Tout individu a droit à la vie, à la liberté et à la sûreté de sa personne.
    - Art. 12 : Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.


Thoſe who would give up ESSENTIAL LIBERTY to purchaſe a little TEMPORARY SAFETY, deſerve neither LIBERTY nor SAFETY. *Page* 289.

1er Principe pour protéger la vie privée :

- "Souveraineté" : garder le contrôle sur ses [méta-]données personnelles

  -> stockage sur un dispositif personnel (carte à puce, PDA, PC…)

  -> si ces données sont divulguées à un tiers, imposer des **obligations** sur leur usage

  - Date de péremption
  - Notification en cas de transfert ou d'usage non prévu
  - etc.

- Application aux réseaux de capteurs : ne transmettre les informations qu'à des dispositifs personnels

2ème Principe pour protéger la vie privée :

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

- … dans le "cyber-espace" 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

- Liens : minimisation <--> proportionnalité et finalités légitimes

- Exemple : quelles informations peut transmettre un RFID ?

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 …

PET : Privacy-Enhancing Technology

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

Identité et authentification

Vision de la sécurité informatique :

- Identité = représentation d'une personne dans un système d'information
- Authentification = vérification de l'identité (contre l'usurpation d'identité)
  - Autorisation : vérifier les droits d'accès
  - Imputabilité : chacun doit être responsable de ses actes
- … mais risque d'atteinte à la vie privée
  - S'il faut présenter son identité pour exercer ses droits --> divulgation de données personnelles
  - Imputabilité vis-à-vis de la Société, pas vis-à-vis d'un marchand ou d'une entreprise

1° PET : gestion d'identités multiples

- Identité = représentation d'une personne physique
- Réduire/contrôler les liens entre une personne et les données (et méta-données) la concernant (contrôler la *chaînabilité*)
  - on présuppose la non-chaînabilité des communications et des accès
- Mais : accès personnalisés / privilégiés : pseudonymes
  - Préférences (ex: météo)
  - "Rôles" différents -> pseudonymes différents
    - Ex: contribuable et électeur
  - Authentification adaptée au risque d'usurpation d'identité (et à la responsabilité)
  - Durée de vie liée aux besoins de chaînabilité -> pseudonymes "jetables"
- Identités virtuelles multiples vs. "single-sign-on"
  Liberty Alliance <http://www.projectliberty.org>
  vs. Microsoft Passport

Adresse IP= "donnée identifiante"

Exemple :

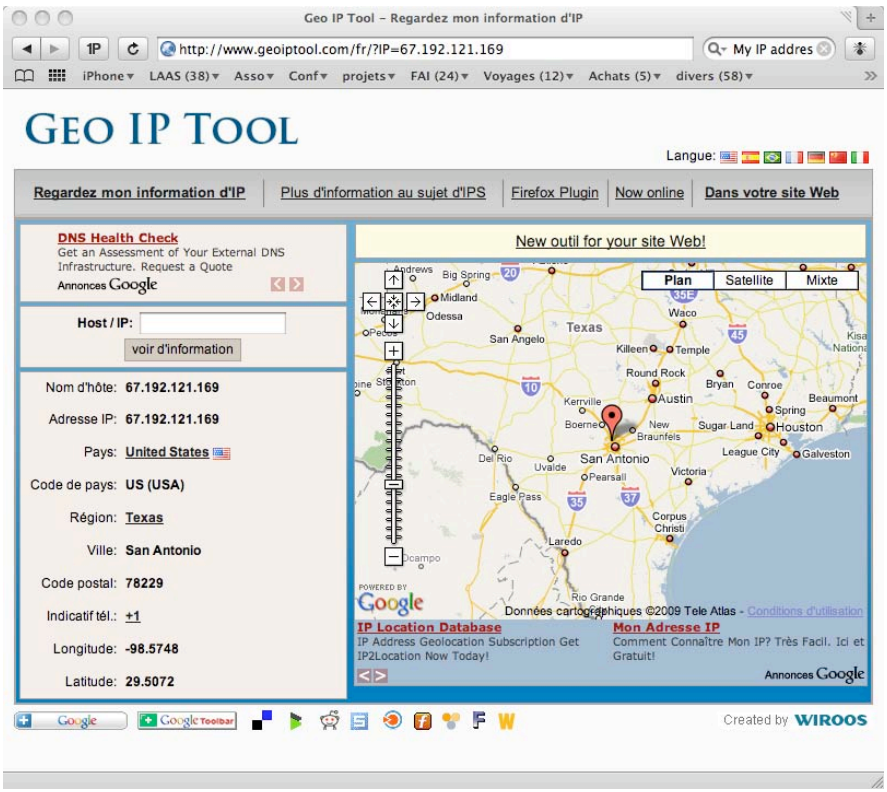
```
Return-Path: <Yves.Deswarte@laas.fr>
Received: from laas.laas.fr (140.93.0.15) by mail.libertysurf.net
(6.5.026)
      id 3D518DEF00116A4D for yves.deswarte@libertysurf.fr; Tue, 13 Aug
2002 13:44:40 +0200
Received: from [140.93.21.6] (tsfyd [140.93.21.6])
    by laas.laas.fr (8.12.5/8.12.5) with 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 :



IP-address.com - IP Tracer and IP Locator. What is my IP address? IP Tracer and IP Locator.

Home | IP Tracing | Reverse IP | My IP | Hide IP | Email Trace | Speedtest | IP Distance | IP FAQ | Proxy Checker | IP Whols | Sitemap | My IP is: 140.93.65.222

IP Tracing and IP Tracking (140.93.21.6)

With our IP address locator you can trace any IP address, host or website. We use a professional, accurate IP address to location database. Try it yourself.

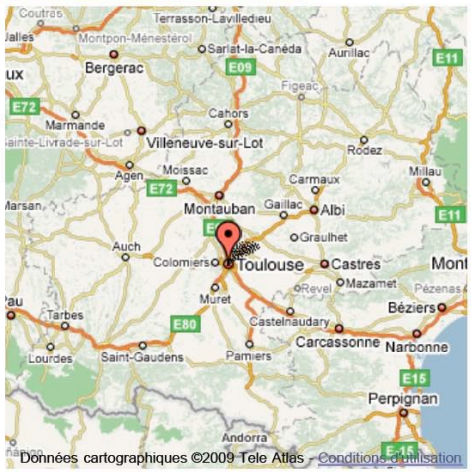
140.93.21.6 [Track IP, host or website]

Examples: 213.86.83.116 (IP address) or google.com (Website)

You should hide your IP address

More IP Tools:

- Trace Email Senders
- Big IP address satellite image (Google Maps)
- Enhanced System and my IP information (Popular)
- Test your Internet Speed
- Calculate Distance between IP addresses
- Whois IP and Domain Whois
- Reverse IP lookup



140.93.65.222 IP address location & more:

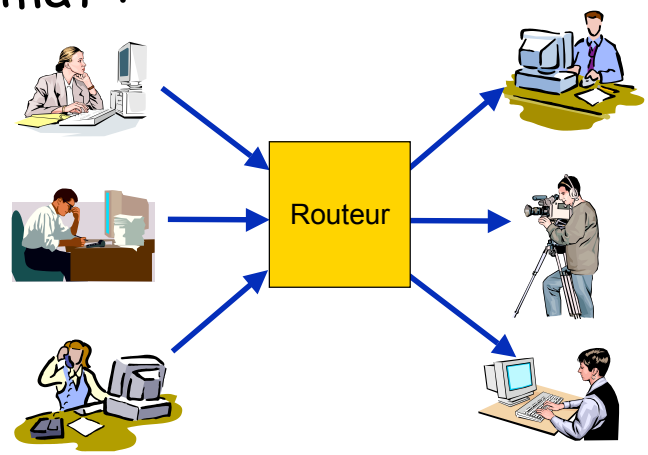
My IP address [?]:	**140.93.21.6** [Whois] [Reverse IP]
My IP country code:	FR
My IP address country:	France
My IP address state:	Midi-Pyrenees
My IP address city:	Toulouse
My IP address latitude:	43.6000
My IP address longitude:	1.4333
My ISP [?]:	Laboratoire d'Automatique et d'Analyse des Systeme
My Proxy:	None / Highly Anonymous [Proxychecker]
Organization:	Laboratoire d'Automatique et d'Analyse des Systeme
Host of my IP: [?]:	tsfyd.laas.fr [Whois] [Trace]
Local time in France:	2009-04-30 16:31

More about my IP and my system:

My Speed:	Unknown [Speedtest]
My Browser [?]:	Safari 4.0
My Operating System [?]:	MacOSX
Referer:	Unknown

2° PET : Protéger les adresses IP

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



IP V6, réseaux ad hoc, …

- Demain : IP partout (*pervasive/ubiquitous computing, intelligence ambiante, sensor networks, RFID, convergence 4G …*)
- chaque "machin" aura une adresse IP implicite *unique et permanente* (basée sur un numéro de fabrication)
- 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.

Connexion IP nomade anonymisée

Roaming : PC portable, PDA, téléphone …

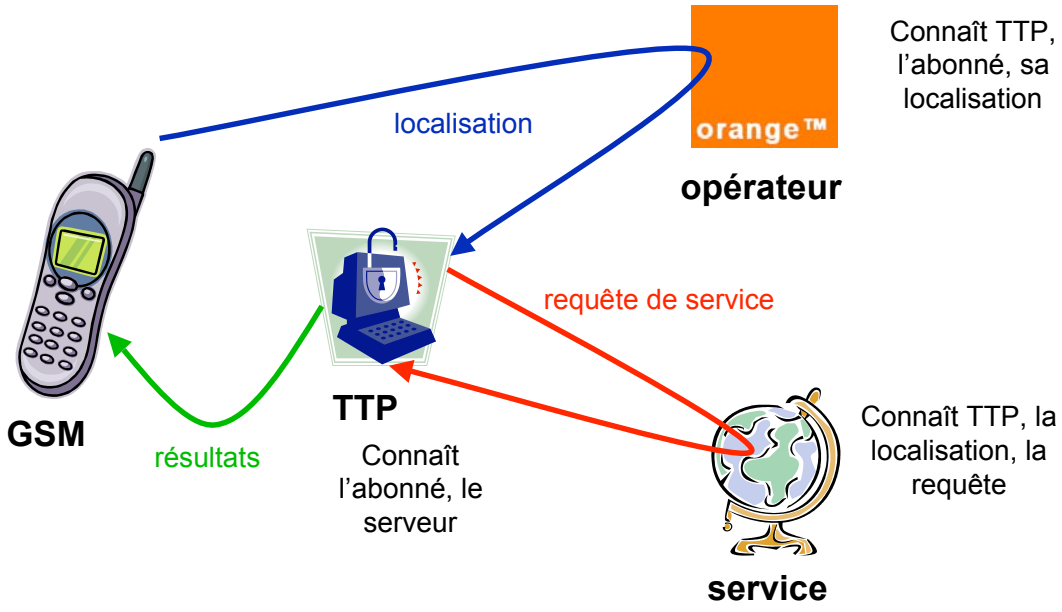
1. Génération d'1 @MAC aléatoire
2. Obtention d'1 @IP temporaire
3. Tunnel vers un TTP de roaming
4. Génération d'une autre @IP
5. Authentification sur FAI

3° PET: Accès anonyme à des services

- Relais d'anonymat (*anonymity proxy*) : unidirectionnels (ou bidirectionnels?)
  - e-mail, news (Usenet)
    - anon.penet.fi (700 000 utilisateurs en 1996 !)
    - Cypherpunks
  - ftp
  - Web : ex: proxify.com
  - ...
- Serveur de pseudonymes :
  - e-mail
  - Identités multiples fournies par des f.a.i. (adresses mél)

Service basé sur la localisation

- Ex: PRIME : pharmacie la + proche



4° PET: Autorisation

- Aujourd'hui sur Internet : 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"

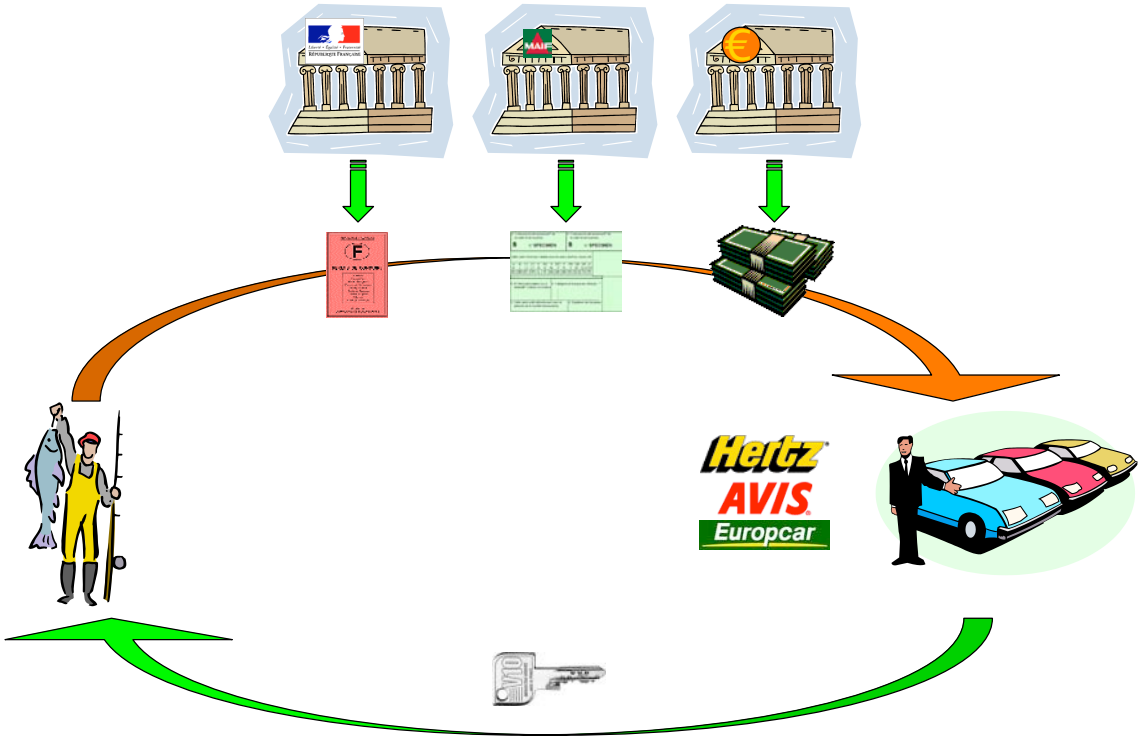
Preuves d'autorisation: credentials

- *Credential* = garantie, accréditation
- Exemples :
  - cartes d'abonnement, de membre d'association, …
  - permis de conduire, carte d'identité, d'électeur, …
- Certificats multiples :

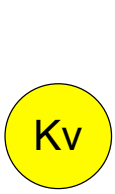
  ex: SPKI : certificats d'attributs/d'autorisation

  pb : *linkability* : 1 certificat => 1 clé publique
- Certificats restreints :
  - *"Partial Revelation of Certified Identity"*
    Fabrice Boudot, CARDIS 2000

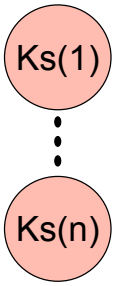
"Anonymous Credentials" (Idemix)



Signature de groupe



1 clé publique de vérification



n clés secrètes de signature

$[\ \Sigma\ ]_{Kv}$ = ? = Défi

Défi = nb aléatoire

$\Sigma = \{Défi\}_{Ks(i)}$

Carte nationale d'identité blanche

- Principe : prouver des droits, sans divulguer d'information personnelle :
  - l'utilisateur est authentifié par biométrie
  - le lecteur de carte pose une question, la carte répond oui ou non

Fonctionnement de la carte blanche

- La puce contient les informations d'état-civil + preuves de droits + …
- Carte émise par une autorité (ex. préfecture)
  puce supposée inviolable (confidentialité, intégrité)
- Carte à contact (consentement du détenteur,
  détection de déconnexion)
- Authentification mutuelle de la puce ① et du lecteur ② (certifié)
- Authentification du porteur par biométrie ③
  - Capteur sur la carte (*fingerprint*) ou lecteur (*fingerprint*, iris, voix, …)
  - Références biométriques maintenues/vérifiées dans la puce
- Principe de base :
  - Les informations stockées ne quittent jamais la puce
  - On peut poser des questions à la puce ④ (selon habilitation du lecteur), les réponses sont toujours binaires : oui ou non ⑤

Utilisations de la carte d'identité

- Preuve de nationalité (ex. police des frontières) :
  - Réponse = OUI (dès vérification de la biométrie ③)
- Vérification d'identité (ex. carte d'embarquement, chèque…) :
  - Question : nom et prénom = "Dupont, Marcel" ?
  - Réponse : oui ou non
- Vérification de domicile : commune, département, région, …
  (ex. réduction à la piscine)
  - Question : commune = "Asnières" ?
  - Réponse : oui ou non
- Vérification de majorité, de carte vermeil, …
  - Question : aujourd'hui = 27/04/2009; âge ≥ 18 ?
  - Réponse : oui ou non
- Contrôle de police (ex. individus recherchés)
  - Question : nom et prénom = "Ben Laden, Oussama" ?
  - Réponse : non

5° PET : gestion des données personnelles

- Négociation entre l'individu et l'entreprise
  ex: coupons de réduction en échange d'une publicité ciblée
- Souveraineté : celui qui fournit des informations sur lui-même doit pouvoir contraindre l'usage qui pourrait en être fait --> Obligations
  ex: à effacer dans 48 h.
- 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)

5°-bis PET : 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

Contrôle d'accès aux données

- Séparation entre décision de contrôle d'accès et mise en œuvre
  - Décision : à un niveau élevé (ex. transaction)
    - Cohérence de l'ensemble des opérations
    - Décision sur la « sémantique » de la transaction
    - Moindre privilège : le privilège d'exécuter la transaction est inférieur à celui d'exécuter les opérations élémentaires

    Si OK --> génération de preuves d'autorisation
  - Mise en œuvre : à chaque opération élémentaire : fournir ou bloquer l'accès en fonction de l'opération et de ses paramètres vs. les preuves d'autorisation

Exemple : virement bancaire

- Transaction : virer 2000 € du compte 184-948449 au compte 946448-658
  - Lire le solde du compte 184-948449
  - Tester si le solde est supérieur à 2000 €
  - Si oui :
    - solde := solde - 2000; écrire solde 184-948449
    - Lire le solde du compte 946448-658
    - solde := solde + 2000; écrire solde 946448-658
  - Si non : retourner « solde insuffisant ».

Donner confiance aux utilisateurs…

… que leur vie privée est protégée?

- Certification & labellisation
- Approche Trusted Computing Group (TCG)
  - Support matériel : TPM
  - Bootstrap sûr
  - Vérification sceau S/W avant chargement
  - Vérifiable à distance, sans dévoiler d'identité (DAA)
- PRIME : preuve d'obligation

PRIME (03/2004 - 07/2008)

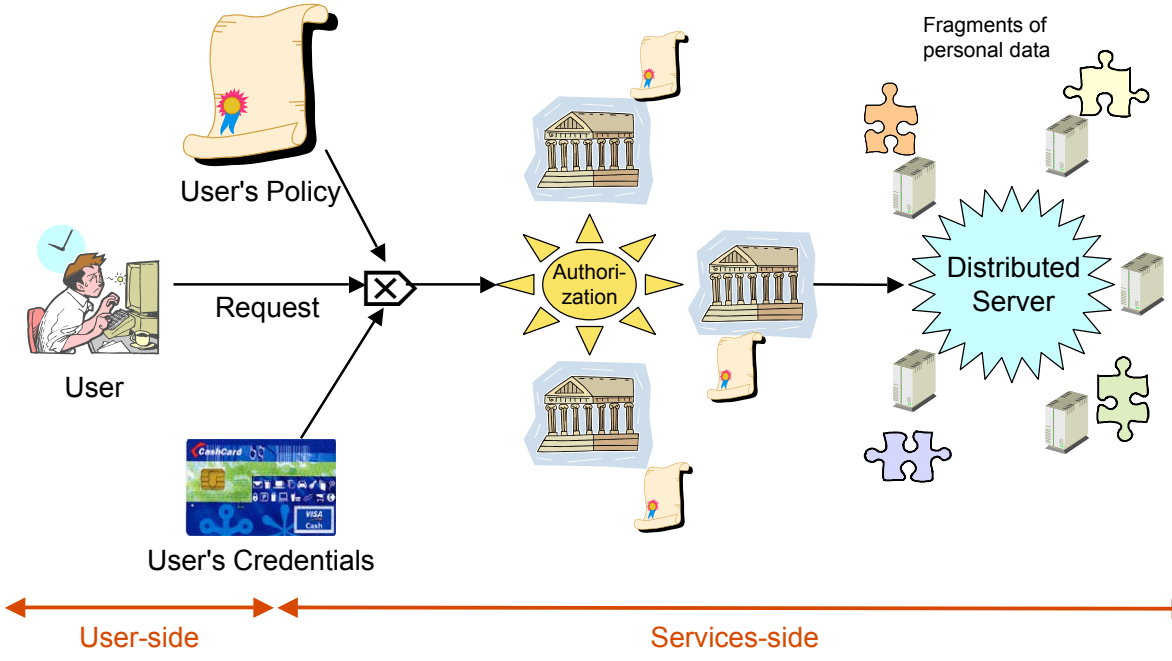
http://www.prime-project.eu.org/

- 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



Conclusion

- Analyser les impacts sur la vie privée dès la conception de nouvelles technologies
- Respecter les principes de souveraineté et de minimisation des données personnelles
- Développer des nouveaux objets personnels pour faciliter la protection de la vie privée :
  ex. stockage de données personnelles, gestion des identités, e-Cash, anonymous credentials …

Bibliographie <mailto: deswarte@laas.fr>

- *Sécurité des systèmes d'information,* V.2, dir. Ludovic Mé & Yves Deswarte, Traité IC2, série Réseaux et télécommunications, Hermès, ISBN 2-7462-1259-5, 390 pp., juin 2006.
- Simone Fischer-Hübner, *IT-Security & Privacy*, LNCS 1958, Springer, 2001.
- Stefan A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates*, MIT Press, 2000.
- Yves Deswarte, David Powell, Yves Roudier, « Sécurité, protection de la vie privée et disponibilité », chapitre XIII in *Informatique diffuse* (dir. V. Issarny), Arago 31, OFTA, Paris, mai 2007, ISBN 2-906028-17-7, pp. 301-344. <http://www.lavoisier.fr/notice/gb/not2.asp?id=36ONXOZ3SRLOFJ>
- Yves Deswarte, Carlos Aguilar-Melchor, "Current and Future Privacy Enhancing Technologies for the Internet", *Annales des Télécommunications*, vol.61, n°3-4, March/April 2006.
- Yves Deswarte, Carlos Aguilar-Melchor, Vincent Nicomette, Matthieu Roy, "Protection de la vie privée sur Internet", *Revue de l'Électricité et de l'Électronique* (*REE*), octobre 2006 (n°9), pp.65-74.
- Carlos Aguilar-Melchor, "Les communications anonymes à faible latence", Thèse de l'Institut National Polytechnique de Toulouse, 4 juillet 2006, LAAS n°06571.