Contrôles d'accès préservant la vie privée

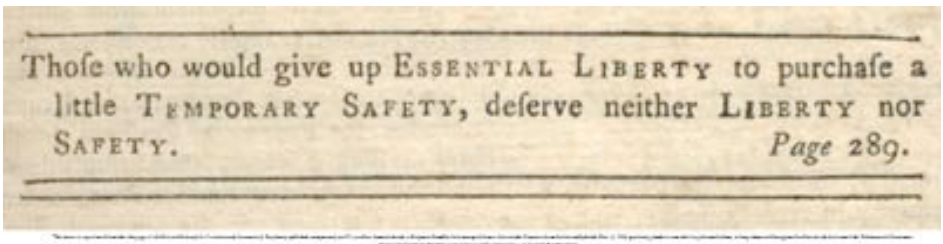
Yves Deswarte
deswarte@laas.fr

LAAS-CNRS

Toulouse, France

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.*

Sommaire

- Définitions
- Principes de base
- Contrôles d'accès
  - Identité et authentification
  - Contrôle d'accès et autorisation
    - Exemple : carte d'identité blanche
- Gestion des données personnelles
    - Exemple : projet PRIME

Privacy

Pri•va•cy |ˈprīvəsē|
noun
the state or condition of being free from being observed or disturbed by other people *: she returned to the privacy of her own home.*

- the state of being free from public attention *: a law to restrict newspapers' freedom to invade people's privacy.*

"Privacy" : définitions

- Intimité (contraire = promiscuité), respect/protection de la vie privée (PVP)
- Critères Communs (ISO 15408) : une classe de fonctionnalité, 4 propriétés :
  - Anonymat : garantit qu'un utilisateur peut utiliser une ressource ou un service sans révéler son identité d'utilisateur
  - "Pseudonymat" : idem, sauf que l'utilisateur peut quand même avoir à répondre de cette utilisation
  - "Non-chaînabilité" : garantit qu'un utilisateur peut utiliser plusieurs fois des ressources ou des services sans que d'autres soient capables d'établir un lien entre ces utilisations
  - Non-observabilité : garantit qu'un utilisateur peut utiliser une ressource ou un service sans que d'autres, en particulier des tierces parties, soient capables d'observer que la ressource ou le service est en cours d'utilisation

Pseudonymat < anonymat < non-chaînabilité < non-observabilité

1er Principe pour protéger la vie privée :

- "Souveraineté" : garder le contrôle sur ses 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.

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 : 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 …

Technologies de sécurité & PVP

- Identité et authentification
- Contrôle d'accès et autorisation
- Communications et anonymat
- Gestion des données personnelles

--> PETs: Privacy-Enhancing Technologies

Sécurité / Protection de la vie privée

- Protection de la vie privée (PVP) = confidentialité d'informations personnelles
- Confidentialité : une des propriétés de la sécurité informatique (CID)
- La sécurité fournit les moyens de la PVP :
  - Authentification, Autorisation, …
- Mais…

… "*the devil is in the details*"

- Certains moyens de sécurité
  - Audit
  - Traçabilité
  - Authentification forte, …

… sont des menaces pour la vie privée

  - Déséquilibre : les citoyens honnêtes sont plus observés que les criminels
  - Autocensure --> réduction de la liberté

Identité et authentification

- 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 est responsable de ses actes
- … mais atteinte à la "souveraineté" et à la "minimisation"
  - 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 individu ou d'une entreprise

Gestion d'identités multiples

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

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…)

Ce schéma est dépassé

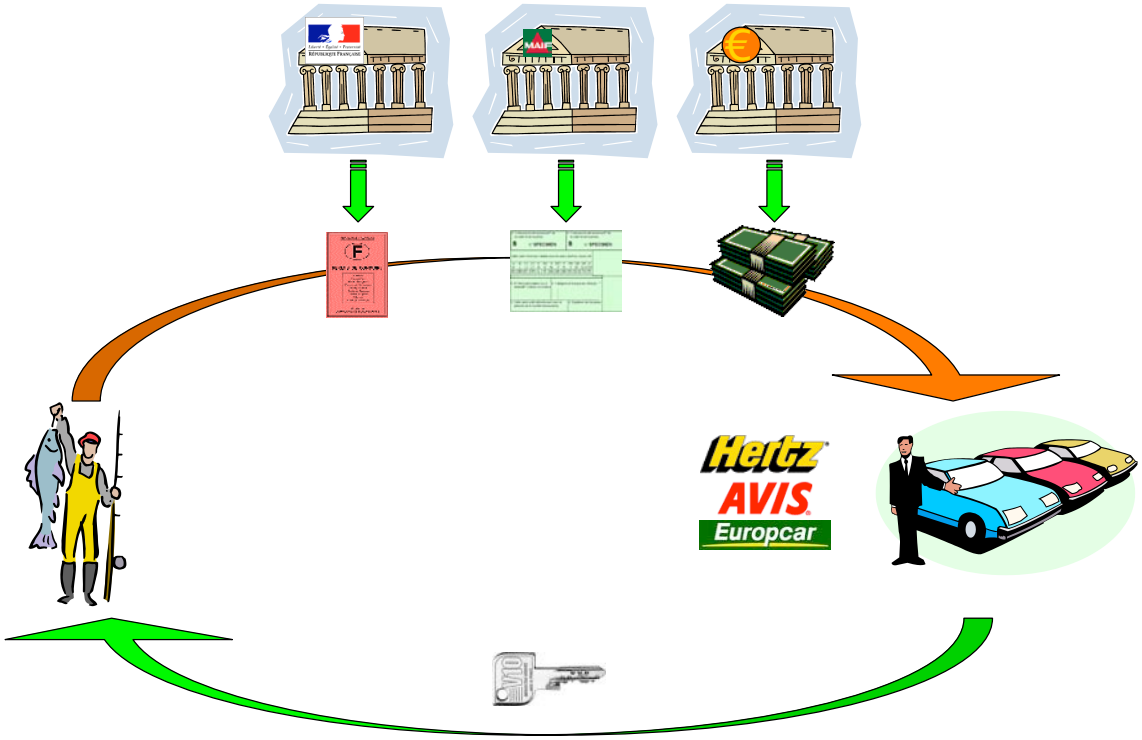
- Les transactions sur Internet mettent en jeu généralement plus de deux parties
  (ex : commerce électronique)
- Ces parties ont des intérêts différents (voire opposés) : suspicion mutuelle
- Nocif pour la vie privée :
  opposé au "besoin d'en connaître"

Preuves d'autorisation: credentials

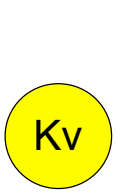
- *Credential* = garantie, accréditation
- Exemples :
  - cartes d'abonnement, de membre d'association, …
  - permis de conduire, carte d'identité, d'électeur, …
- Certificats multiples :

  ex: SPKI : certificats d'attributs/d'autorisation
- Certificats restreints :
  - *"Partial Revelation of Certified Identity"*
    Fabrice Boudot, CARDIS 2000

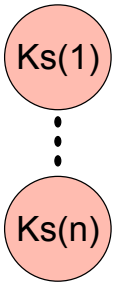
"Anonymous Credentials" (Idemix)



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

À quoi sert une carte d'identité ?

- Prouver qu'on est français
  ex. quand on rentre en France (ou dans un pays des accords Schengen)
- Prouver la validité d'un document pour une personne
  ex. vérification de chèque, de carte d'embarquement, réservation, …
- Prouver des droits
  ex. carte vermeil, accès à une déchetterie, piscine…
- Prouver son identité pour une inscription « sensible » (responsabilité, imputabilité)
  ex. compte en banque, URSSAF, bibliothèque, …
- Prouver qu'on n'est pas sur une liste de personnes recherchées
  ex. contrôle de police, …
- … et beaucoup d'usages abusifs :
  ex. surveillance, traçage, croisement d'informations, marketing, …

Risques des cartes actuelles

- Sécurité insuffisante :
  - Toutes les informations sont lisibles
    - Vol de carte --> usurpation d'identité
      - Facile si la photo est plus ou moins ressemblante
      - Sinon : falsification de la carte
    - Fabrication de faux (copie identique ou non)
  - Difficulté en cas de vol ou perte, ou de faux !!!
- Intrusion dans la vie privée
  - Toutes les informations sont lisibles, quelque soit l'utilisation

Carte d'identité électronique

- Meilleure sécurité (puce sécurisée) …
  - Falsification plus difficile
  - Usurpation d'identité plus difficile si authentification biométrique (ex. empreinte digitale)
- … mais intrusive pour la vie privée
  - Les informations d'identité sont lisibles
  - Risque de généralisation de la preuve d'identité ex. e-administration, commerce en ligne, …

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

Utilisations à distance

- Il faut analyser chaque cas :
  - E-gouvernement
  - Preuve d'identité :
    - Réduire la force d'authentification :
      ex. réservation de vol, d'hôtel, *frequent flyer*
    - Limites de la biométrie non supervisée ?

Et en plus…

- En cas de perte ou vol :
  - Inutilisable par d'autres (biométrie)
  - Ne fournit aucune information personnelle
  - Rien à révoquer
  - … mais reconstruire rapidement ?
- Sauvegarde périodique du contenu
  - Sur un serveur distant, chiffré (mot de passe utilisateur + clé publique de l'autorité)
- Recréation de la carte par l'autorité
  - Avec le consentement de la personne (mot de passe)
  - Et la clé privée de l'autorité

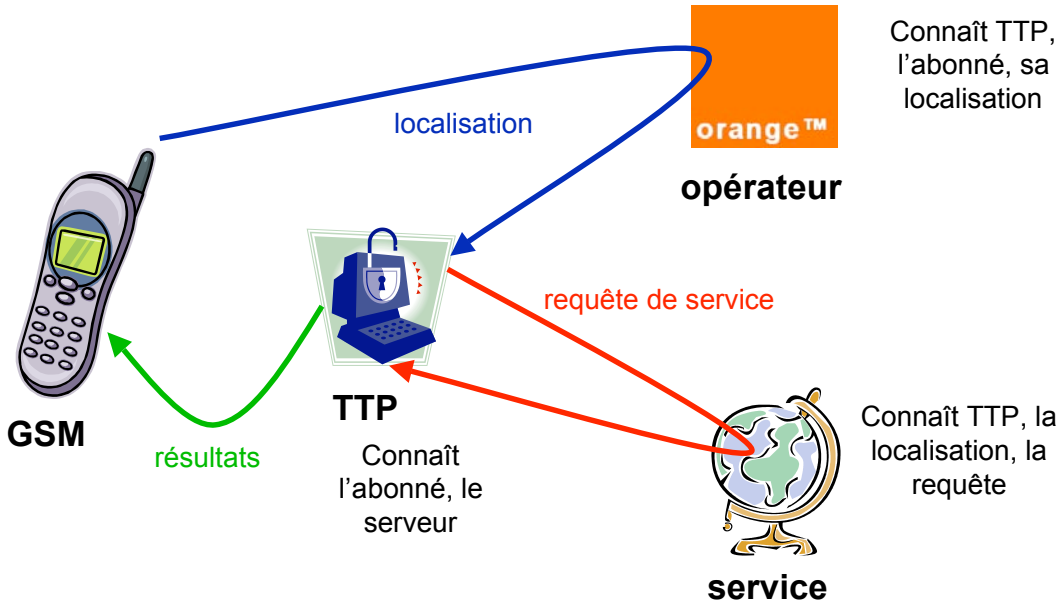
Gestion des données personnelles

- Négociation entre l'individu et l'entreprise
  "consentement éclairé"
  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)

Service basé sur la localisation

- Ex: PRIME : pharmacie la + proche



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 »)

  http://vimeo.com/5280042
- Ces données peuvent être très sensibles : 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 (TCG)
  - Support matériel : TPM
  - Bootstrap sûr
  - Vérification sceau S/W au chargement
  - Vérifiable à distance, sans dévoiler d'identité (DAA)

PRIME (03/2004 - 05/2008)

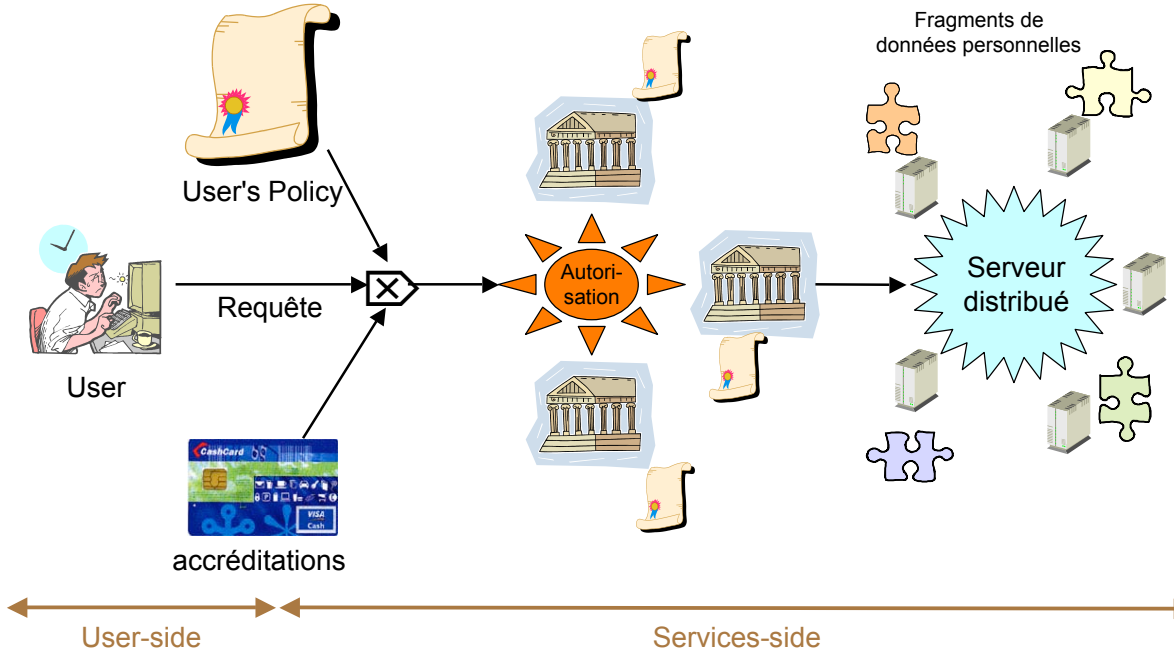
http://www.prime-project.eu/

- 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, LAAS…)
  - Utilisateurs (Lufthansa, T-Mobile, Swisscom, HSR)

Principe :

Différentes identités pour différents besoins

Architecture typique



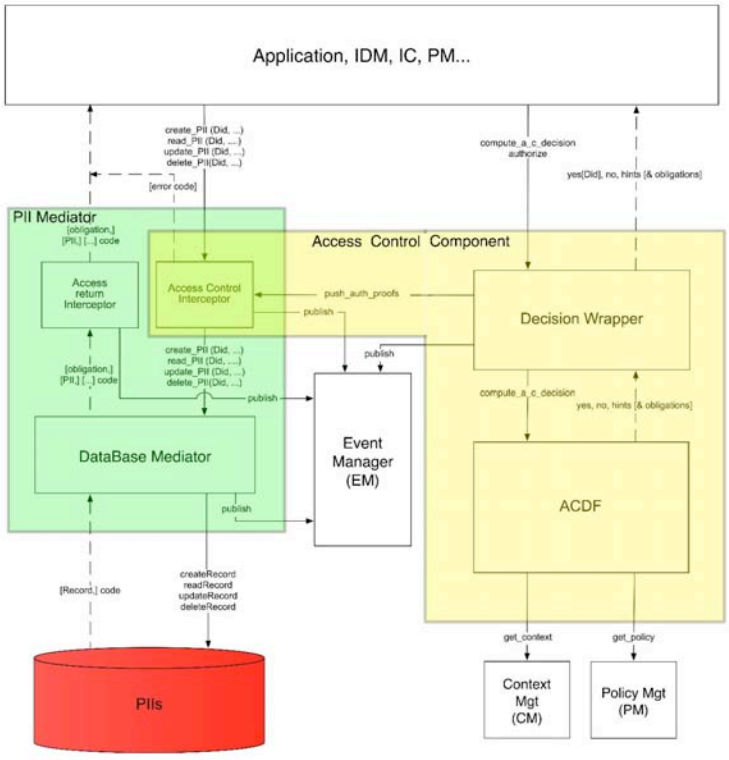
Décision et mise en vigueur : granularités

- Exemple:

  Transaction : transférer 2000 € du compte 184-948449 vers le compte 946448-658

  - Lire le montant actuel du compte 184-948449
  - Vérifier si > 2000 €
  - Si oui :
    - montant := montant - 2000; écrire montant dans 184-948449
    - lire montant actuel du compte 946448-658
    - montant := montant + 2000; écrire montant dans 946448-658
  - Si non : retourner "crédit insuffisant"

PRIME Access Control



Conclusion

- Il est possible de renforcer à la fois la sécurité et le respect de la vie privée
  - On peut prouver ses droits sans avoir à dévoiler son identité
- … mais est-ce l'intérêt des gouvernements (et des entreprises) ?

Recommandation

- 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, …
  Ex. carte d'identité blanche

Droits futurs ?

- Droit au mensonge : ex. contre les abus vis-à-vis de la minimisation des données
- Droit à l'oubli
- Droit à la répudiation --> authentification la plus faible possible