CAPPRIS – JT2 – Conception de Systèmes respectueux de la vie privée

Benjamin Nguyen, INRIA Rocquencourt & U. de Versailles S^{t} Quentin
et al.

JT2- Conception de Systèmes Respectueux de la vie privée

- Constat:
  - La protection des données de l'utilisateur n'est pas au centre des applications de gestion de données à l'heure actuelle.
  - Certaines techniques (PETs) existent mais sont peu utilisées/génériques (*pourquoi*?).
  - Travail « *from scratch* » nécessaire pour toute application voulant prendre en compte la vie privée → De nombreux « bugs » peuvent se produire
- Objectifs :
  - Proposer un cadre (architecture de référence) permettant de développer des applications de type différent (OSN, LBS, EHR) où la protection des données sera centrale
  - Réutiliser les technologies déjà existantes

Axes de recherche: Conception de Systèmes Respectueux de la vie privée

1. Architecture « Privacy by Design »

2. Outils (composants) pour la réaliser (PETs)

Améliorer la protection des données de l'utilisateur

- Protéger les données à la source
  - Actuellement on perd le contrôle des données dès qu'elles sont « fournies »
- Échanger les données dans un environnement contrôlé
  - Permettre que l'accès et l'usage restent sous le contrôle de « l'utilisateur » (ou du « propriétaire ») : droits d'accès, droit d'usage (finalité), droit de destruction, etc.
- … et ce quelle que soit l'application !

Les « Privacy Enhancing Technologies »

Des outils pour protéger les utilisateurs existent déjà :

- « Anonymiseurs » d'IP en-ligne
- Communications anonymes (TOR)
- Projet Privacy Identity Management for Europe (PRIME)
- Platform for Privacy Preferences (P3P)
- Dossier Médico-Social Partagé
- …

Problème : Ils sont actuellement peu interopérables, ou très spécifiques à une application donnée. Difficulté d'utilisation dans un monde « ouvert », avec de nombreux acteurs.

→ Proposer une architecture et méthodologie de conception d'applications « Privacy by Design », exploitant les PETs existants, et développant de nouveaux si nécessaire.

Méthodologie de travail :
Canevas d'une architecture "Core"

- Basé sur une abstraction simple(iste) des scénarios les mieux (moins mal) maîtrisés
- Identifier les similitudes
- Proposer un premier niveau d'architecture (Boîtes + API + workflow) de haut niveau
    1. Fixer les hypothèses qui peuvent l'être
    2. Boîtes pouvant être implémentées différemment suivant les contextes
    3. Pas d'obligation de faire cohabiter tous les composants dans une même plate-forme
    4. Une 'famille' de solutions suivant un même canevas
- Valider cette archi avec les 'vrais' scénarios
- La compléter pour répondre à des scénarios plus complexes (dynamicité, contrôle utilisateur …)

Use case : Partage de Photos (Documents)

- OSN version « light »
- Un utilisateur publie des photos
- Il peut décider qui a accès aux photos (et leur retirer les droits)
- Il veut pouvoir contrôler la « dissémination » de ses photos
- Hypothèse de confiance dans le logiciel (ex. certifié, open source)

- Questions pour aller plus loin :
  - Qui peut exercer un contrôle sur ces photos ? (personnes *dans* les photos)

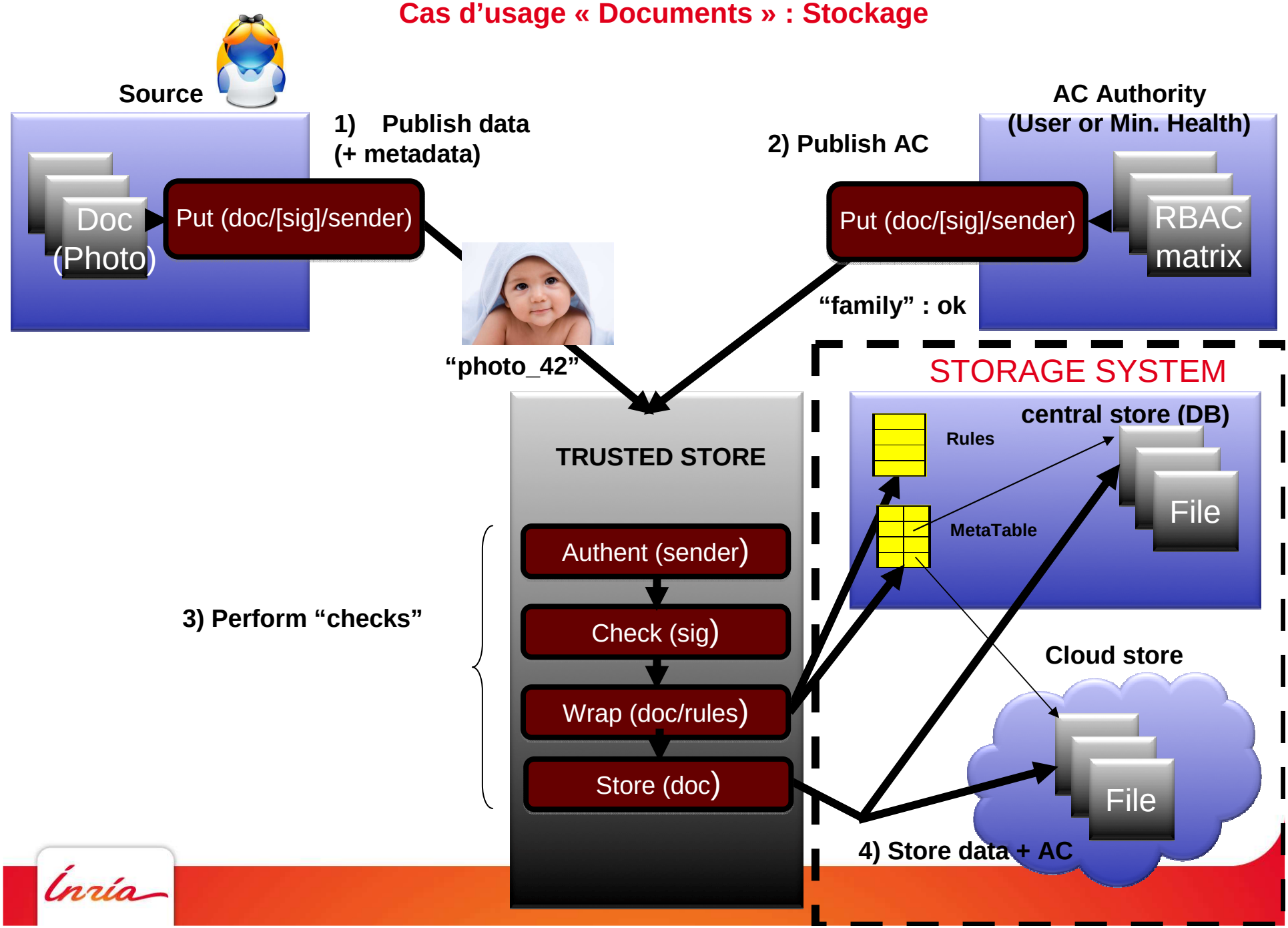
Use case : Partage de documents médicaux

Hyp simplificatrice ‘monde structuré’

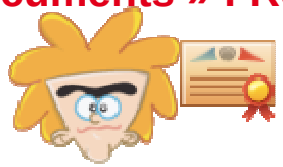
- Matrice “Role Based Access Control” (RBAC) publiée par une autorité
- Acteurs authentifiés par certificat (ex. Médecin, infirmière)
- Types de doc. connus (ex. Prescription, compte rendu hospitalier)
- Utilisation en déconnecté et avec du matériel « sécurisé » (donc de confiance)

- Exemple: DMP
  - User $\in$ Role ➔ accès à certains types de doc
  - Meta-données simpliste (type)
    Metatable = 1 table
    Query = KVS
- Principe de Privacy traité ici : contrôle d’accès (AC)

Cas d'usage « Documents » : Stockage



Cas d'usage « Documents » : Requêtes



« bob » : alice's brother

Q: « Photo_42 »

Put (query/sig/sender)

Get (data)

STORAGE SYSTEM

TRUSTED STORE

Logique RBAC
Q compatible avec {F} ?

colonne RBAC:
S a droit à {F}

Select fileId
From MetaTable
Where cond

SQL-KVS

Authent (S)

Opt-in

Check (sig)

Compute (Q/S)

Get AC Constraints

Get Data

central store

Rules

MetaTable

File

Cloud store

File

Approche

- Lister / Définir des principes de protection de la vie privée qui doivent être garantis par un système (ex. stockage, droit d'accès)

- Identifier des « boites » (primitives de protection de la vie privée) réalisant la protection au niveau atomique, et sur un flux de données d'un certain type

- Étant donné une combinaison de « boites », prouver quels principes sont garantis sur l'ensemble du système; *ou bien* étant donné des principes à garantir, quelle combinaison de « boites » utiliser

Organisation JT 2

Phase 1 (M1-M18) : Analyse

- Identification de scénarios pour les applications LBS, Santé et OSN
- Caractérisation des données, acteurs, rôles, PETs, flux d'information dans ces scénarios
- Classification de PETs existants

Responsable: B. Nguyen

Participants: P.Pucheral, D. Le Metayer, B. Nguyen, G. Piolle, R. Molva, Y. Deswartes, M-O. Killijian, +1 Thésard

Organisation JT 2

Phase 2 (M18-M32) : Conception et Réalisation

- Cahier des charges de l'architecture
- Réalisation de l'architecture de référence « PbD »

Responsable: P.Pucheral / D. Le Metayer

Participants: P.Pucheral, D. Le Metayer, B. Nguyen, G. Piolle, R. Molva, Y. Deswartes, M-O. Killijian, +1 Thésard

Organisation JT 2

Phase 3 (M32-M48) : Validation

- Instanciation de l'architecture sur (quelques) scenarios considérés durant la phase 1
- Etude de généricité de déploiement sur différentes architectures physiques

Responsable: B. Nguyen

Participants: P.Pucheral, D. Le Metayer, B. Nguyen, G. Piolle, R. Molva, Y. Deswartes, M-O. Killijian, +1 Thésard