societies

Self Orchestrating Community
ambiEnT IntelligEnce Spaces

Soutenance - Stage de fin d'étude

Gestion de données personnelles dans un réseau social

le cnam

TRIALOG

ensiie
école nationale supérieure d'informatique pour l'industrie et l'entreprise

Olivier Maridat, 29 septembre 2011

Plan

- Contexte du stage

1. Vie privée
2. Authentification anonyme
3. Obscurcissement de données personnelles

- Bilan

Partie 1

CONTEXTE DU STAGE

Trialog

- Conseil, étude et ingénierie
- Etude et développement
  - l'électronique automobile et grand public (voitures communicantes Renault),
  - les télécommunications,
  - la domotique (EHS, MonAMI),
  - et la distribution d'énergie (projet Linky compteurs intelligents EDF)
- Projets industriels / Projets européens

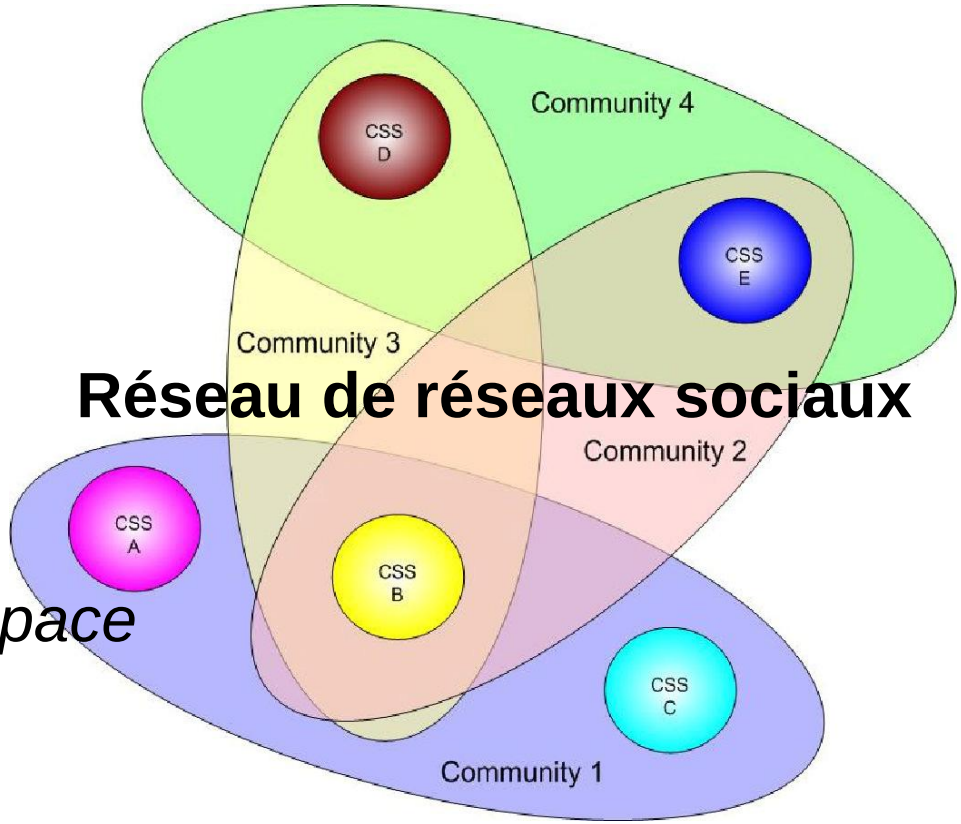
SOCIETIES

- Projet européen sur 4 ans
- Débuté en octobre 2010 (bientôt 1 an)
- Plusieurs sociétés et établissements académiques y participent
  - Intel
  - IBM
  - NEC
  - Telecom Sud Paris
  - Herriot Watt University
  - …
  - et bien sûr Trialog

SOCIETIES – en bref

- *Self Orchestrating Community amblEnT intelllgEnce Spaces*

- *Expérimentations*
  - *Scénario Université*
  - *Scénario Cataclysme*
  - *Scénario Entreprise*



CSS = *Cooperating Smart Space*
Représente une personne
ou une organisation

Partie 2

VIE PRIVÉE

Etat de l'art : vie privée

- En France : loi Informatique et Libertés
- En Europe : Data Protection Directive
- Processus de développement : Privacy-By-Design (Antonio Kung)
  - **Data Minimization**
    - réduction des données personnelles collectées et utilisées
  - **Enforcement**
    - mise en application, vérification
  - **Transparency**
    - explications claires et simples des données collectées et de la finalité de cette collecte
    - vérification et audit du respect des engagements

Objectifs de ma recherche

- Dans Societies : protection de la vie privée
- **Comment minimiser l'utilisation de données personnelles dans des réseaux sociaux ?**
- Deux possibilités, deux études :
  - En amont : architecture
    - Authentification anonyme
  - En aval : obscurcissement de données
    - Obscurcissement de la géolocalisation

Partie 3

AUTHENTIFICATION ANONYME

Authentification – Problème

- Un utilisateur est membre d'une communauté
- Il souhaite s'authentifier
  - Prouver qu'il est le membre qu'il prétend être
  - Pour utiliser des services de la communauté
- Si les services proposés par la communauté n'utilisent pas l'identité du membre
  - L'identité n'a pas à être transmise durant la phase d'authentification !
  - Nécessité d'une **authentification anonyme**

Authentification anonyme - Exigences

- S’assurer que l’utilisateur est membre de la communauté
- Ne rien savoir d’autre au sujet de cet utilisateur (~~identité~~, ~~code d’accès~~, …)
- Impossibilité de tracer les authentifications successives d’un membre

Quelle architecture choisir ?

- Etude des différents moyens d'authentification
- Classables en 3 catégories

1. Code d'accès partagé par tous les membres de la communauté
2. Stockage des codes d'accès séparément des identités
3. Passeport certifiant l'appartenance à une communauté

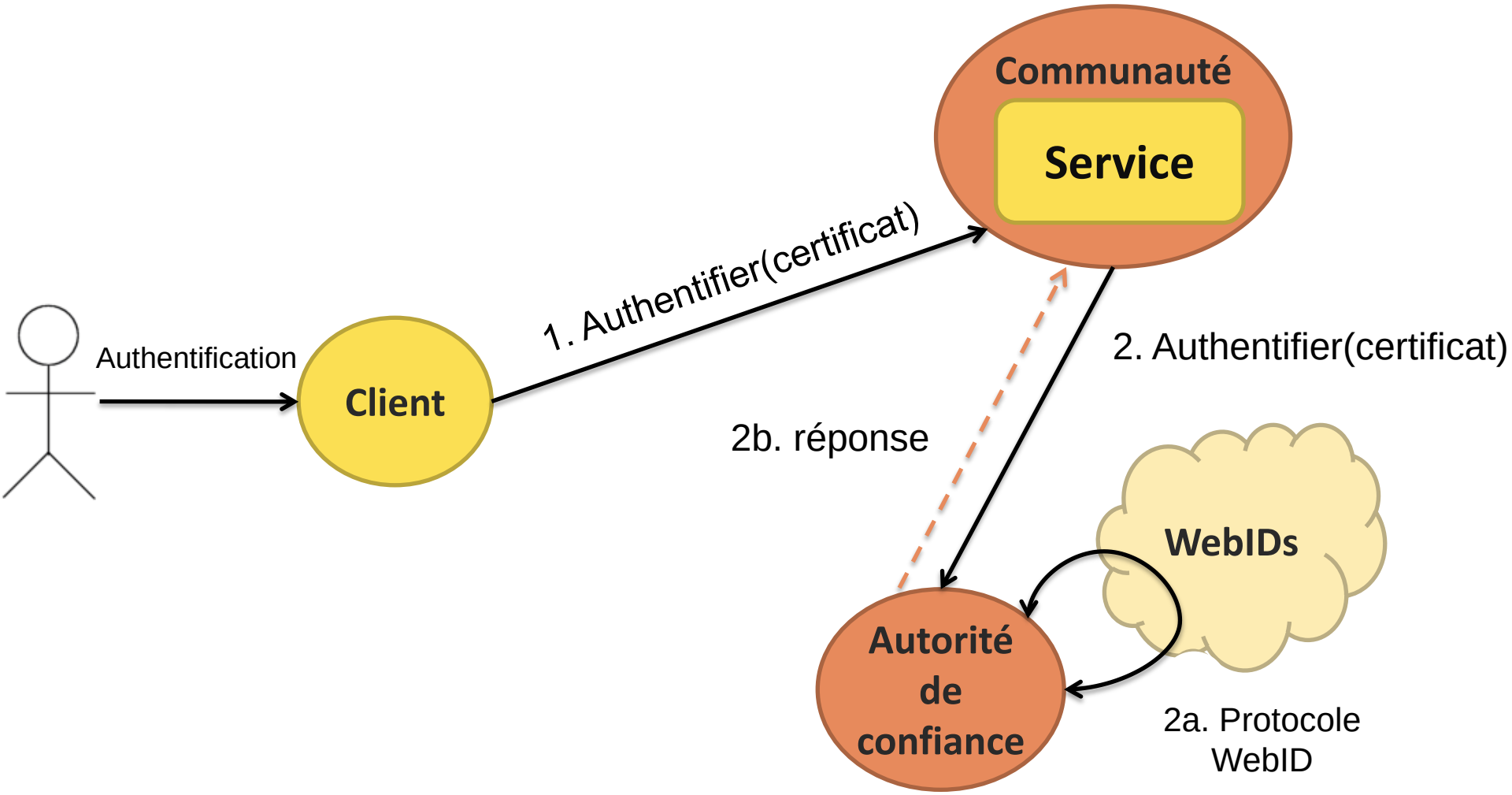
Quelle architecture choisir ?

		1	2			3	
Libellé	Poids	Clé partagée	SRP	FFS	Hashage	WebID	OpenID
Mode anonyme possible	5	1	0	1	1	1	0,5
Mode identifié possible	3	0	1	1	1	1	1
Protéger contre le pistage externe	3	1	1	1	0,5	1	0,5
Protéger contre le pistage interne	2	1	0	0	0	1	0
Permet la double authentification	0,5	1	1	0	0	0	0
Algorithme sécurisé	2	0	1	1	1	1	1
Code d'accès sécurisé	1	0	1	1	1	1	1
Partage clef de session	0,5	0	1	0	0	1	0
Autorité de confiance non nécessaire	1	1	1	1	1	0	0
Calcul faisable par un ordinateur	3	1	0,8	0,5	0,3	1	1
Calcul faisable par un *smartphone*	3	1	0,1	1	1	1	1
Login + code d'accès	1	0	1	0	1	0	1
Aucun stockage chez le client	1	0	1	0	1	0	1
Implémentation existante	2	0	1	1	1	0,5	1
Facilité d'implémentation (de 1 à 3)	0,5	3	2	2	3	1	1
Total pondéré		**19,0**	**18,7**	**22,5**	**23,5**	**24,0**	**20,5**

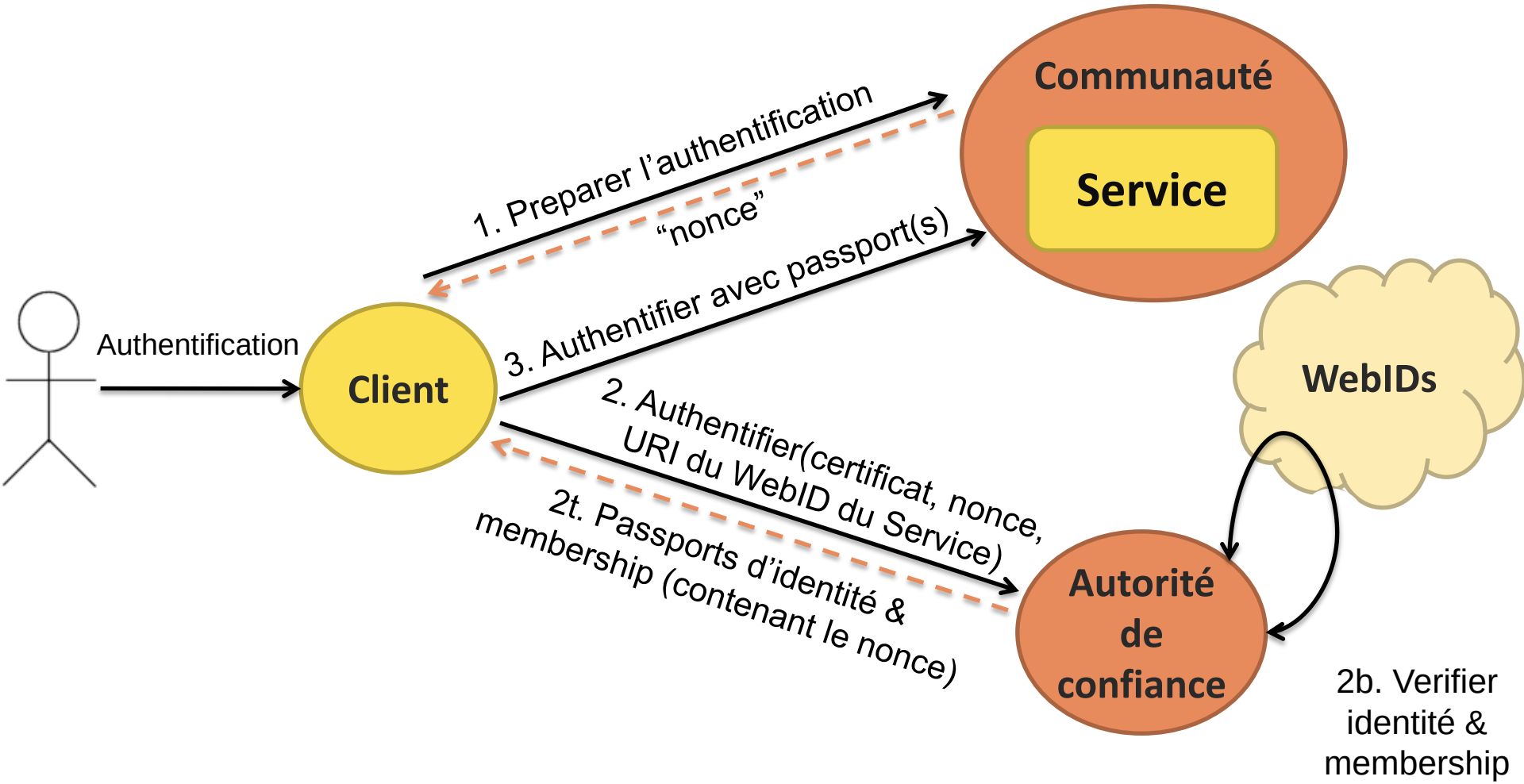
Choix d'une architecture

- Passeport certifiant l'appartenance à une communauté **3**
  - \+ Authentification anonyme de qualité
  - \+ Un unique moyen pour s'authentifier partout (Single-Sign-On)
  - \- Nécessité d'une autorité de confiance
- Technologie : WebID
  - \+ Proposée dans Societies
  - \+ Aucun login / mot de passe à retenir
  - \+ Lien avec la notion de « Web of Trust », « Web Sémantique »
  - ± W3C : en cours de standardisation

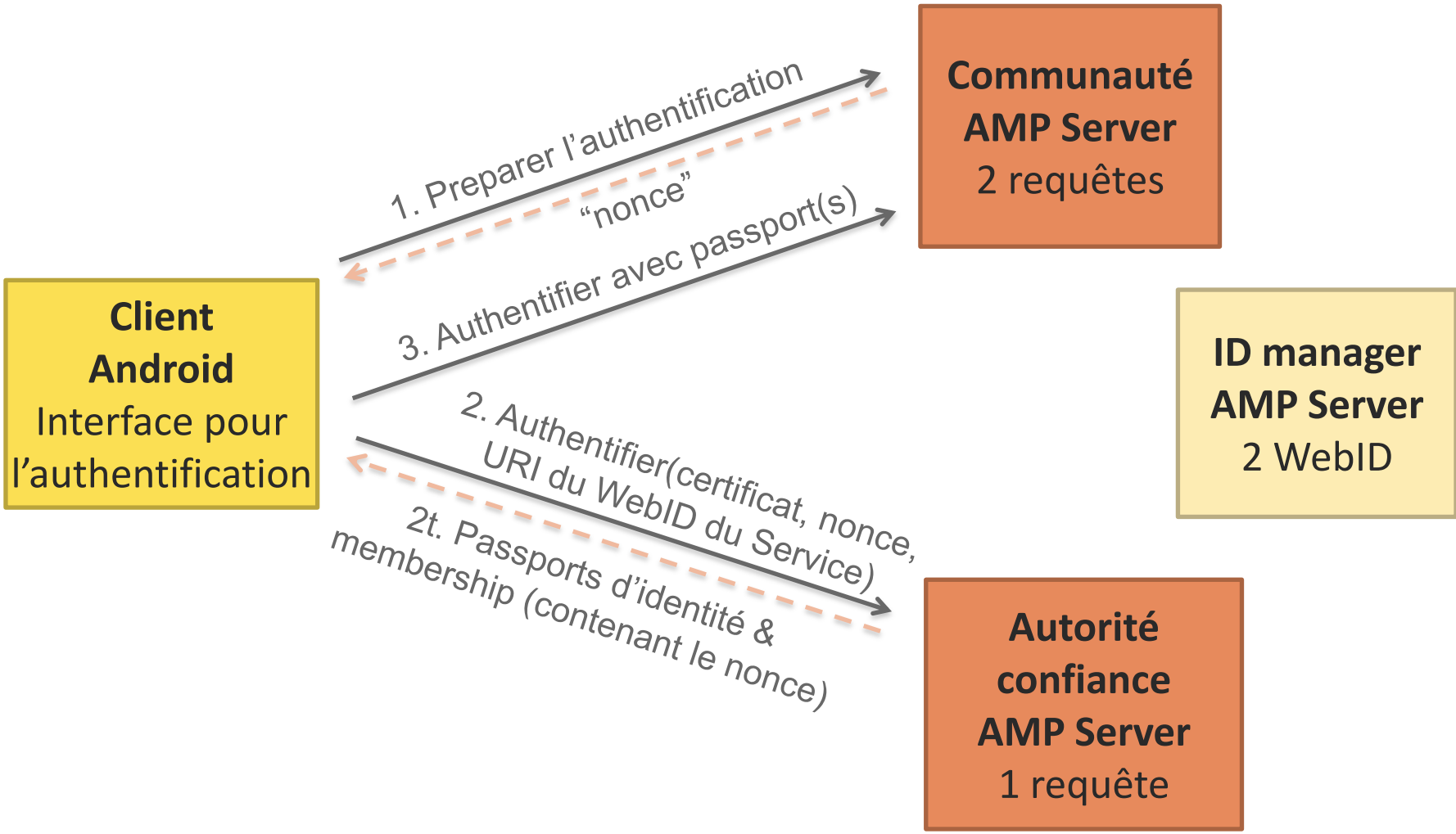
Authentification identifiée via WebID



Authentification anonyme via WebID



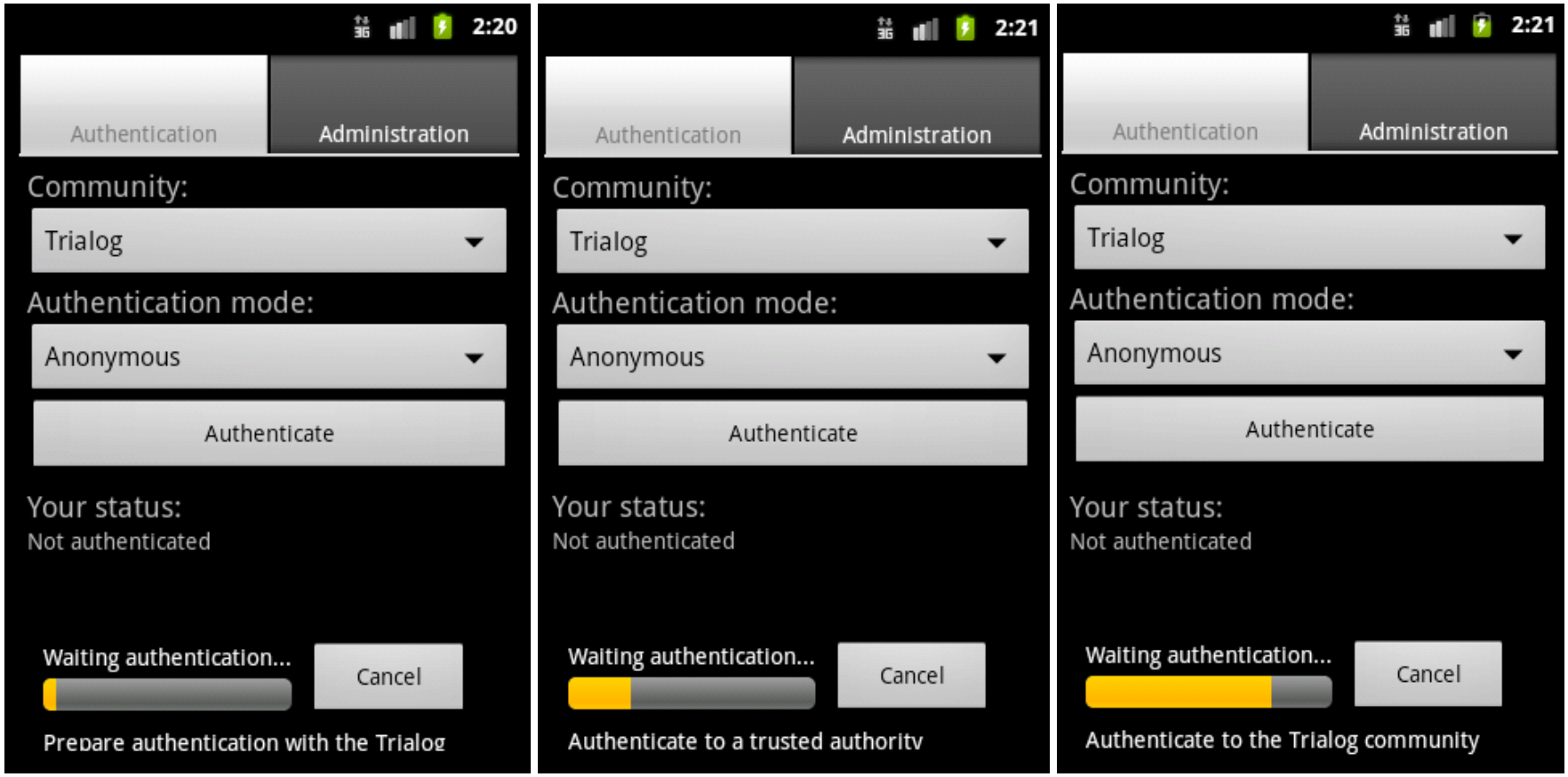
Implémentation du prototype



societies

Démonstration >>>

Précisions sur la démo



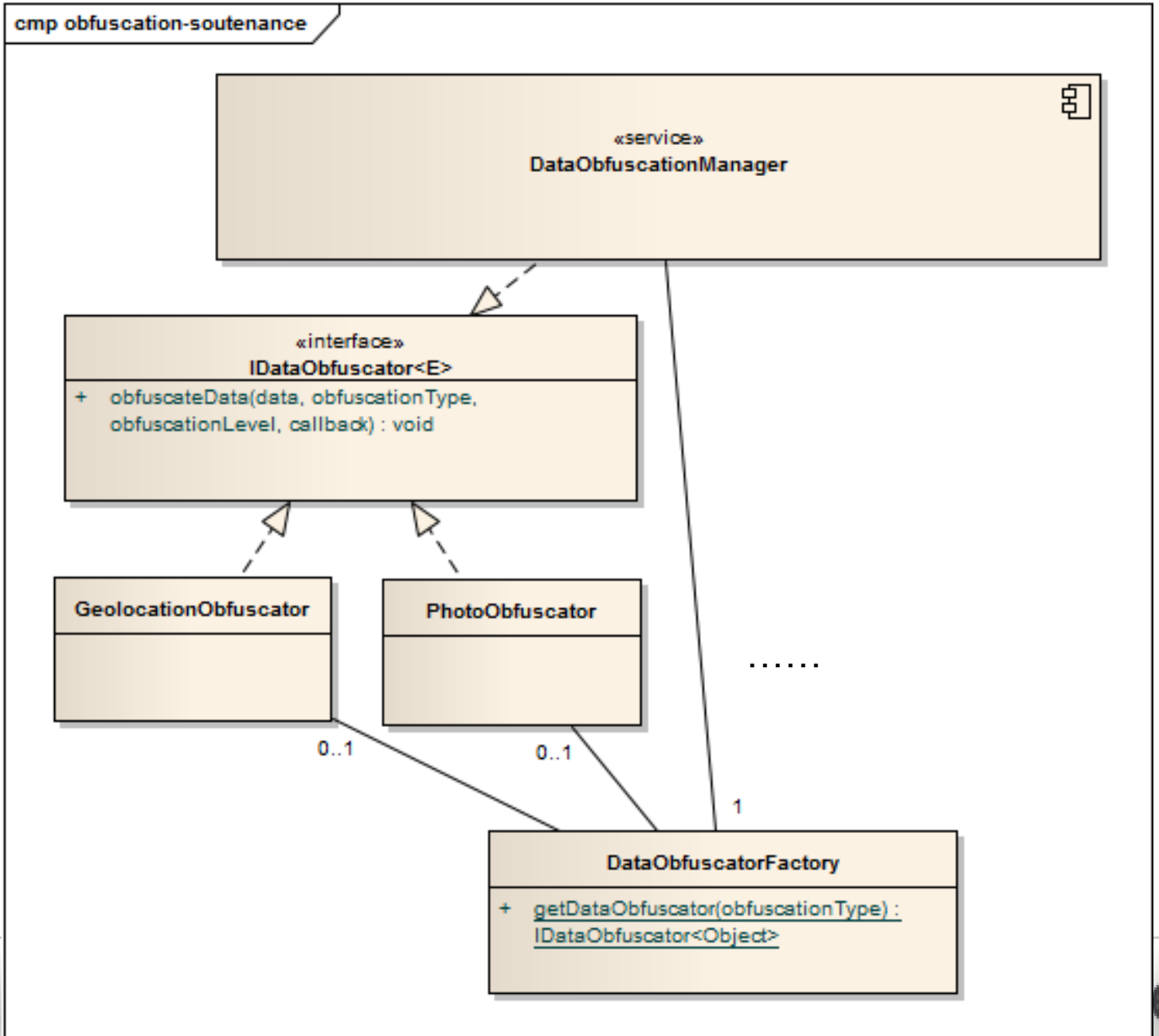
Partie 4

OBSCURCISSEMENT DE DONNÉES PERSONNELLES

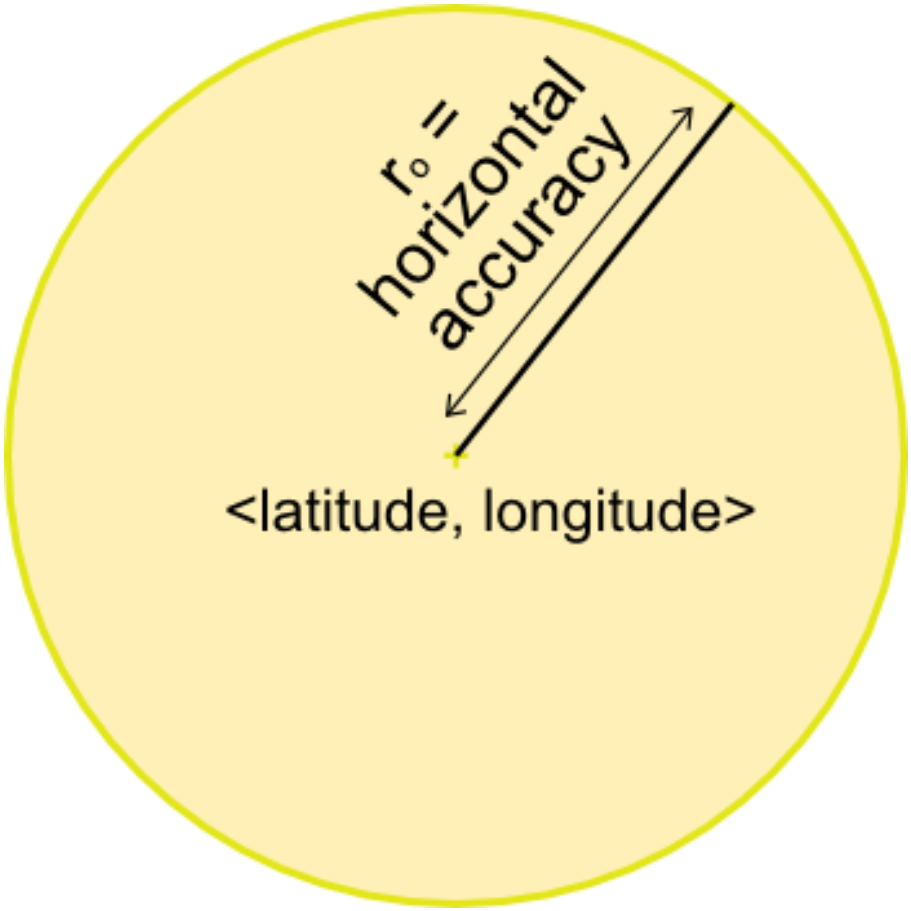
Obscurcissement des données

- Réduire la teneur en informations personnelles
  - Ex : 48, rue des Lilas, 75008 Paris, FRANCE
  - Niveau d'obscurcissement
- But
  - Éviter « tout ou rien »
  - Accéder à des services utiles en protégeant sa vie privée
- Moyen d'y parvenir
  - À chaque type de données son algorithme et son niveau d'obscurcissement
- SOCIETIES : système distribué

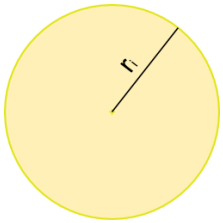
Conception de l'obscurcissement



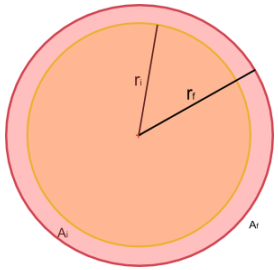
Géolocalisation



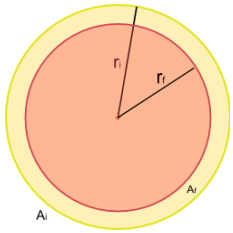
Obscurcir une géolocalisation



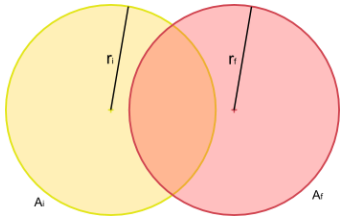
Géolocalisation mesurée



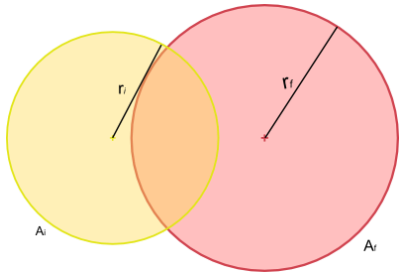
Augmentation du rayon



Réduction du rayon



Déplacement du centre



Combinaison

Niveau d'obscurcissement L :
Le cercle final :

- formera L% du cercle initial, OU
- contiendra L% du cercle initial

Démonstration >>>

Partie finale

BILAN

Bilan

- Définir, spécifier et concevoir le concept d'authentification anonyme et l'obscurcissement de données
- Implémentation de deux prototypes
- Cerner de mieux en mieux le projet Societies
  - Le projet dans son ensemble
  - Aspect « Vie privée »
- Approfondissement et découverte de nouvelles technologies
- Améliorer mon anglais !
- Entre bien dans le prolongement des enseignements
  - Du CNAM : contraintes de l'embarqué, Android, réseaux mobiles, sécurité
  - De l'ENSIIE : architecture n-tiers, base de données, méthode de conception

Pour conclure

- Obscurcissement
  - Optimisation des algorithmes
  - Création d'autres algorithmes
- Transparence
  - Ergonomie !
  - Ergonomie aussi pour les développeurs

Merci de votre écoute !

DES QUESTIONS ? DES REMARQUES ?