

5. Gestion des données et vie privée du citoyen urbain

- Architectures de gestion de données face au respect de la vie privée
- **Gestion de la vie privée dans les réseaux sociaux mobiles**
- Privacy-by-design: gestion de données confinée (puces et capteurs)
- Gestion de la vie privée dans les applications mobiles participatives
- Traitements de données globaux respectueux de la vie privée

Les réseaux sociaux mobiles

- Villes intelligentes = citoyens connectés par téléphones mobiles
- Citoyens = vie sociale
- Applications web pour réseaux sociaux, mais aussi...
- Les réseaux “mobile first” -> WhatsApp, SnapChat, Tinder

**Assurer la vie privée est
un enjeu majeur !**

La vie privée dans les réseaux sociaux mobiles

- Les téléphones stockent beaucoup d'informations personnelles
 - Nom
 - Adresse
 - Position actuelle
 - Photos
 - Lieux visités
 - Liste des “amis”

**Il faut contrôler qui peut
accéder à quelle information**

Un contrôle d'accès idéal

- **Expressif**

- “Tout le monde peut lire l'adresse email de Bob
- “Les amis de Bob peuvent lire l'adresse email et postale de Bob”

Un contrôle d'accès idéal

- Expressif
 - **Flexible**
-
- Les préférences pour le contrôle d'accès sont très subjectives :
 - ✓ “Les amis d’Alice peuvent accéder aux données de Bob”

Un contrôle d'accès idéal

- Expressif
- Flexible
- **Un modèle sensible aux liens sociaux**
 - Défini en terme de concepts sociaux
 - ✓ Distingue les amis et les collègues de Bob
 - ✓ Peut s'adapter à l'évolution de l'environnement social

Un contrôle d'accès idéal

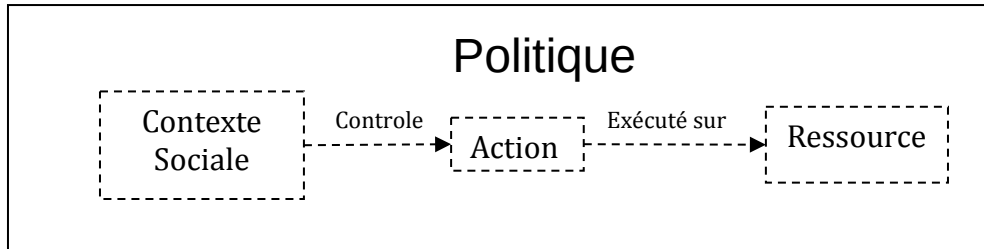
- Expressif
- Flexible
- Un modèle sensible aux liens sociaux
- **Capable de fonctionner sur différentes plateformes**
 - Smart Phone
 - PC Portable
 - Appli "Cloud"...

Un contrôle d'accès idéal

- Expressif
- Flexible
- Un modèle sensible aux liens sociaux
- Capable de fonctionner sur différentes plateformes
- **Intuitif et facile à utiliser**
 - Pas difficile de s'exprimer
 - Même pour les non-informaticiens !

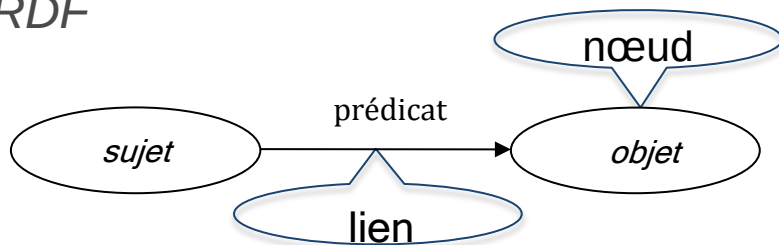
Modèle de Politique

- 3 composants
 - Ressource : Objet à accéder
 - Contexte Social : conditions qui contrôlent l'accès aux ressources, liées à la condition sociale de l'objet
 - Action : l'action à exécuter sur une ressource



1. Ressources

- *Les ressources sont les données sociales de chaque utilisateur*
- *Nous utilisons le modèle défini dans [TONINELLI2010]*
- *Les données sociales sont représentées en « Resource Description Framework » (RDF) :*
- *Phrases RDF:*
 - *< sujet, prédicat, objet >*
- *Triplets RDF liés ensemble...*
 - *dans un graphe RDF*



2. Actions et 3. Contexte Social

- 3 types d'actions :
 - Read : lecture de triplet(s)
 - Add : ajout de triplet(s)
 - Remove : suppression de triplet(s)
- Contexte Social : l'information sociale qui permet de contrôler l'accès à une ressource.
 - "Les amis de Bob"
 - "Les collègues de Bob"
 - "Les sujets qui intéressent Bob"

Représentation Formelle de Politiques (1)

- Politiques définies comme des requêtes sur des données RDF
 - Langage de requête SPARQL:

```
CONSTRUCT {%subject% %predicate% %object%.}
```

```
WHERE{?req rdf:type ns:requestor.
```

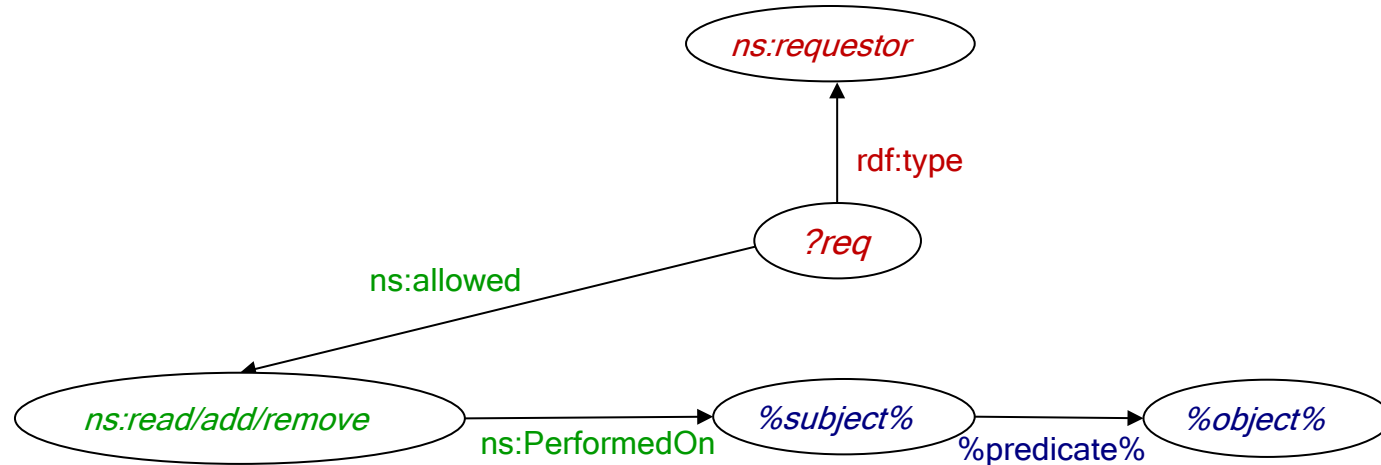
```
    ?req ns:allowed ns:(read/add/remove).
```

```
    ns:(read/add/delete) ns:PerformedOn subject%.
```

```
%subject% %predicate% %object%.}
```

Représentation Formelle de Politiques (2)

- Représentation graphique d'une politique

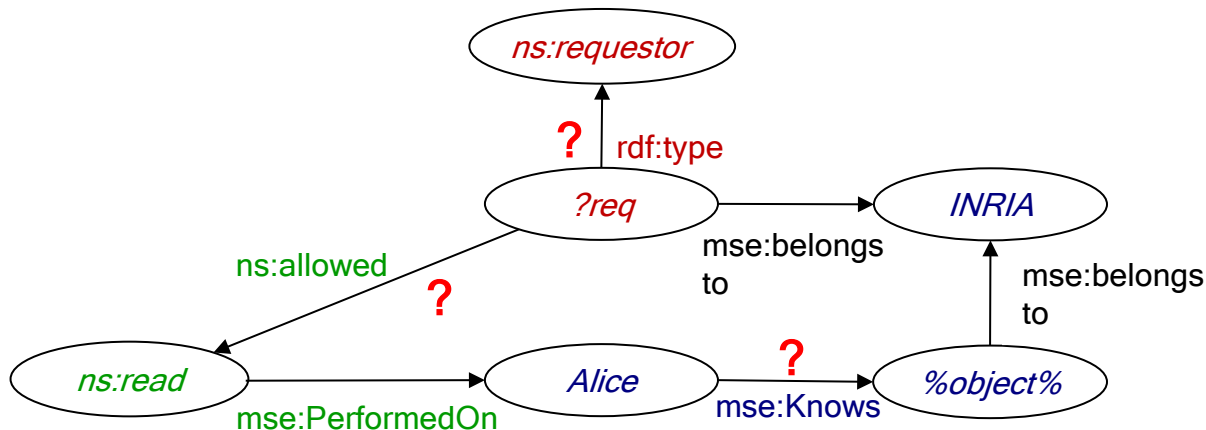


Exemple : Lecture de triplets

- Requête
 - « Bob veut lire la liste des amis d'Alice qui sont membres d'Inria »
- Requête « Read »
 - Envoyée comme un pattern SPARQL
<Alice mse:knows ?obj.>
- Politique
 - Chaque membre d'Inria peut lire la liste des amis d'Alice qui sont aussi membres d'Inria

Exemple : Lecture de triplets

Chaque membre d'Inria peut lire la liste des amis d'Alice qui sont aussi membres d'Inria.

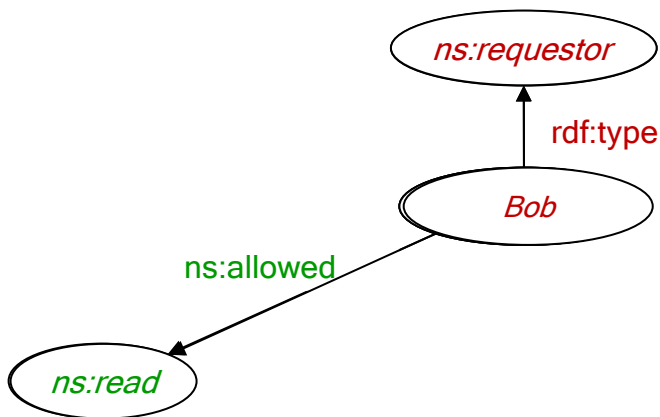


Triplet demandé

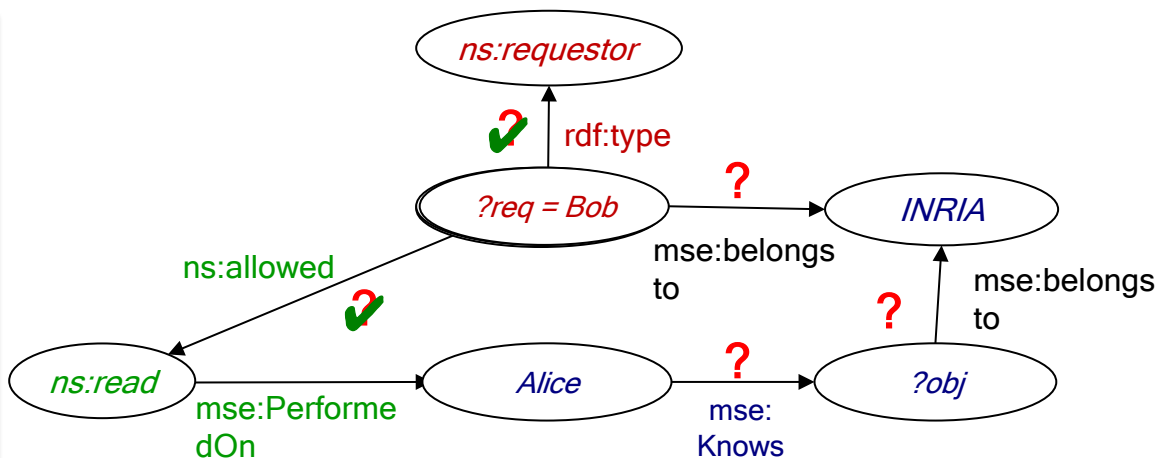


Exemple de lecture : Requête et politique (1)

« Bob veut lire la liste des amis d'Alice qui sont membres d'Inria »



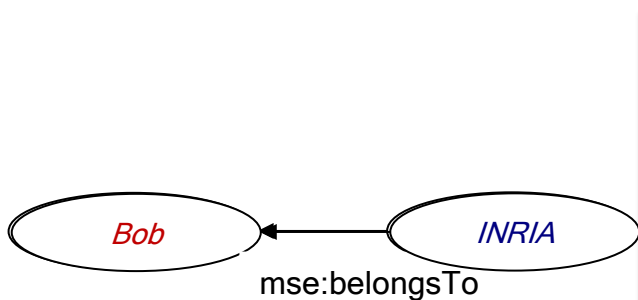
Triplets trouvés



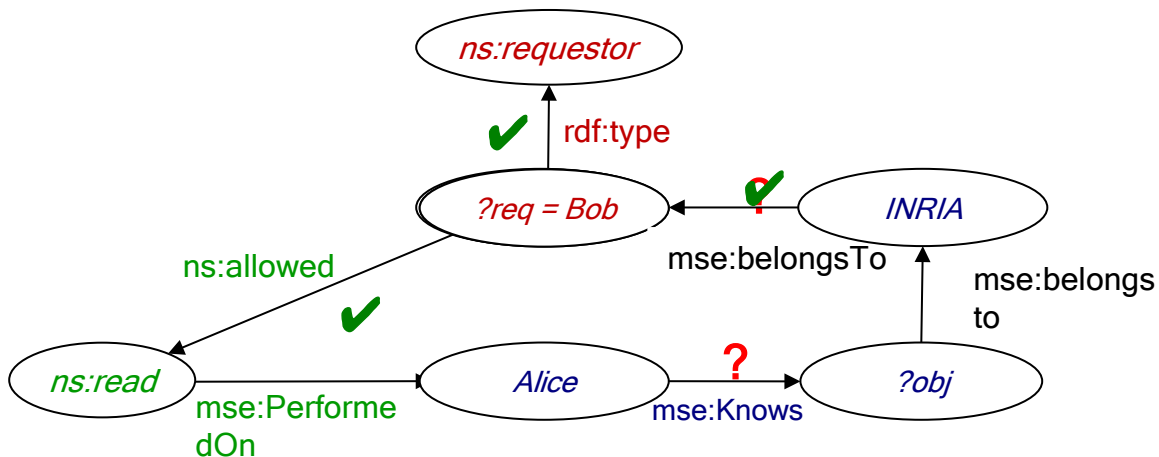
Politique après
substitution

Exemple de lecture : Requête et politique (2)

- « Bob veut lire la liste des amis d'Alice qui sont membres d'Inria »
- Condition : le demandeur doit être membre d'Inria



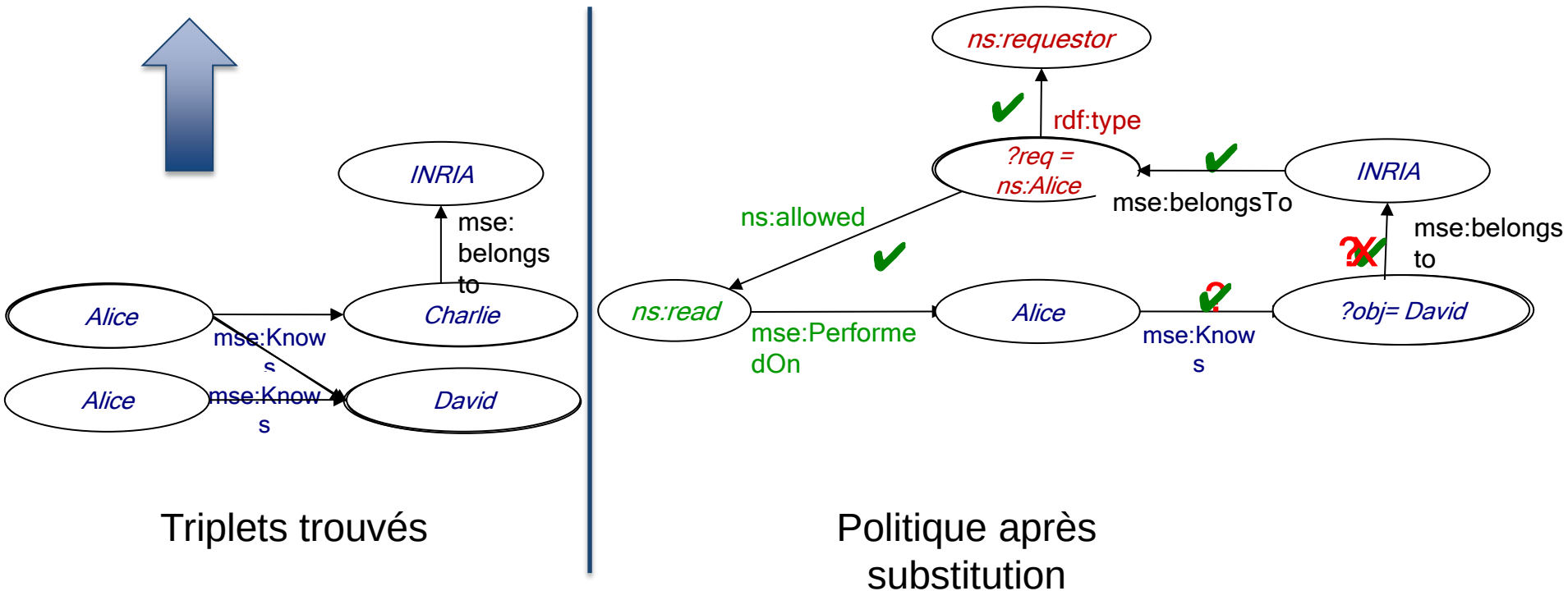
Triplets trouvés



Politique après
substitution

Exemple de lecture : Exécution de la requête

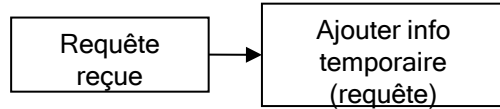
- « Bob veut lire la liste des amis d'Alice qui sont membres d'Inria »



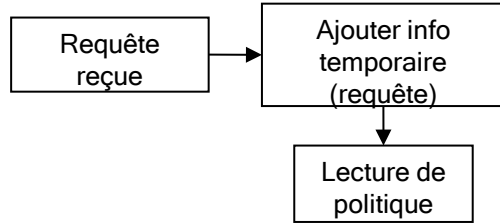
Vue d'ensemble de la vérification des Politiques

Requête
reçue

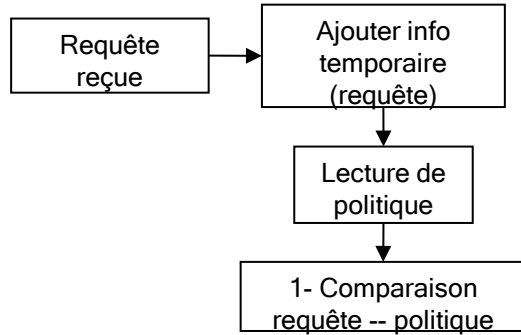
Vue d'ensemble de la vérification des Politiques



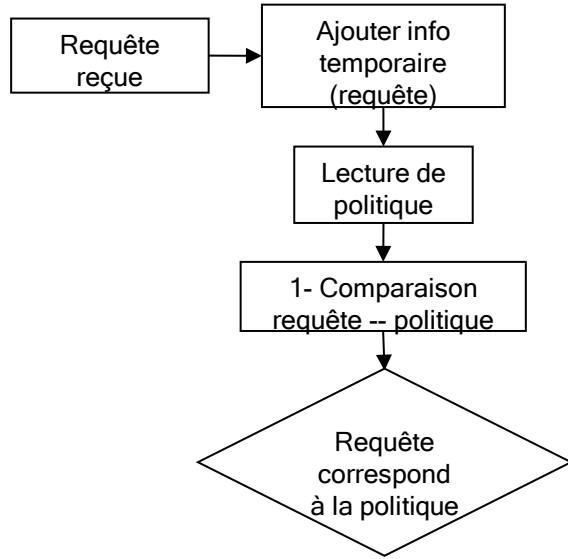
Vue d'ensemble de la vérification des Politiques



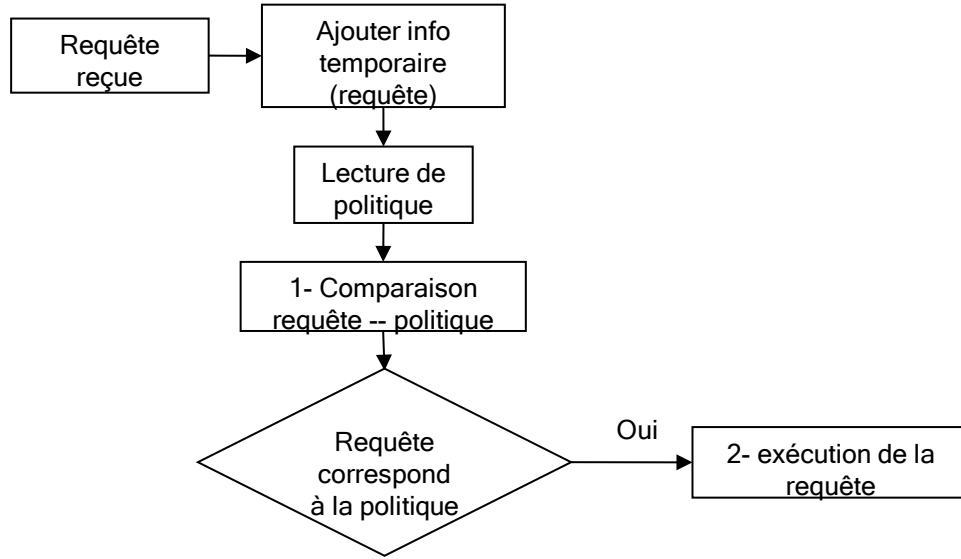
Vue d'ensemble de la vérification des Politiques



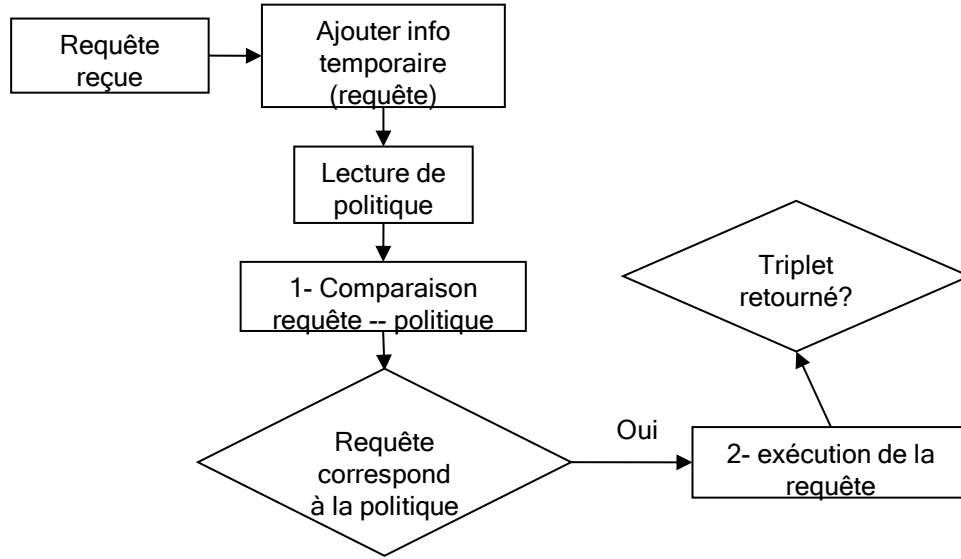
Vue d'ensemble de la vérification des Politiques



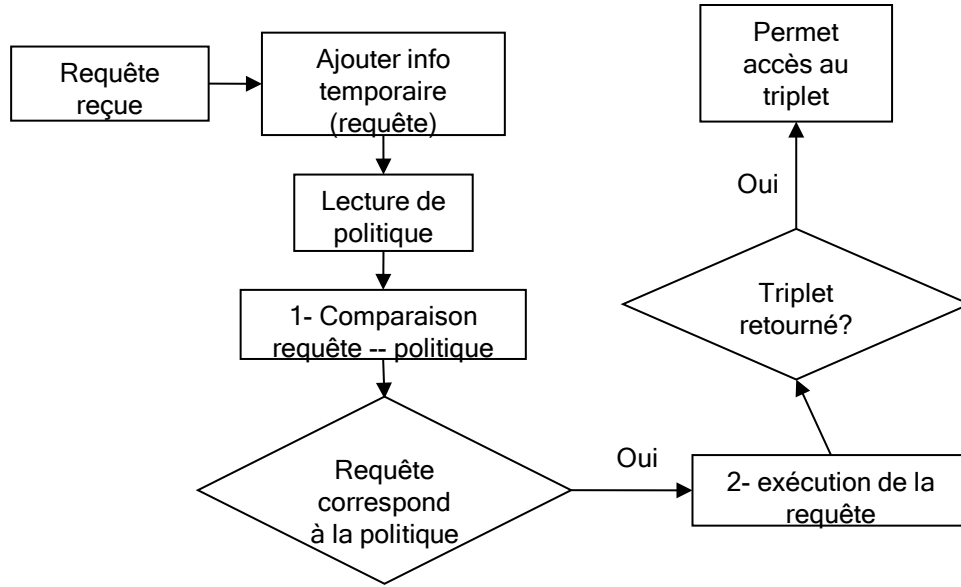
Vue d'ensemble de la vérification des Politiques



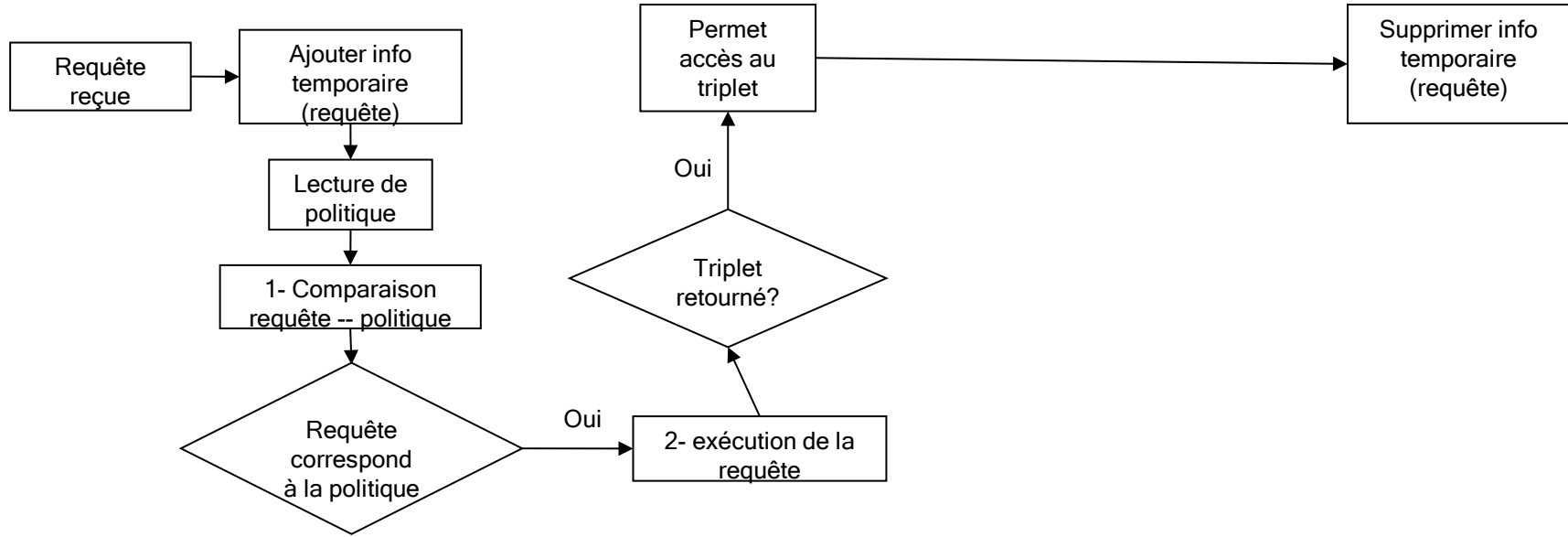
Vue d'ensemble de la vérification des Politiques



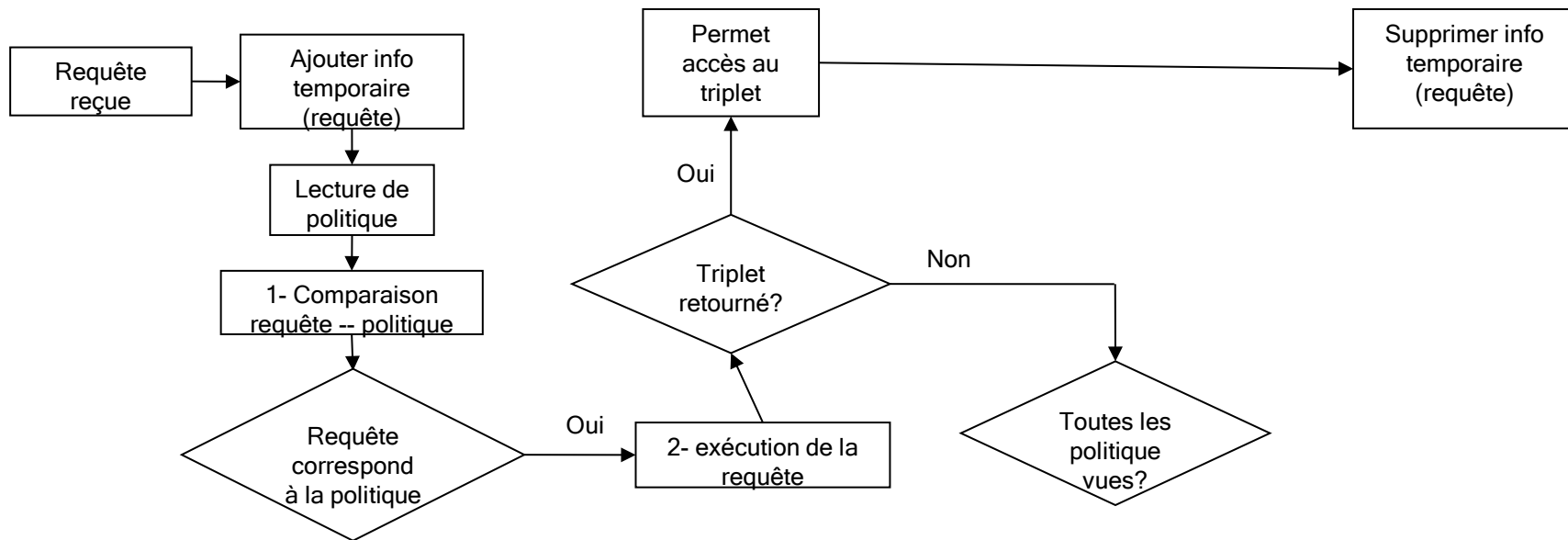
Vue d'ensemble de la vérification des Politiques



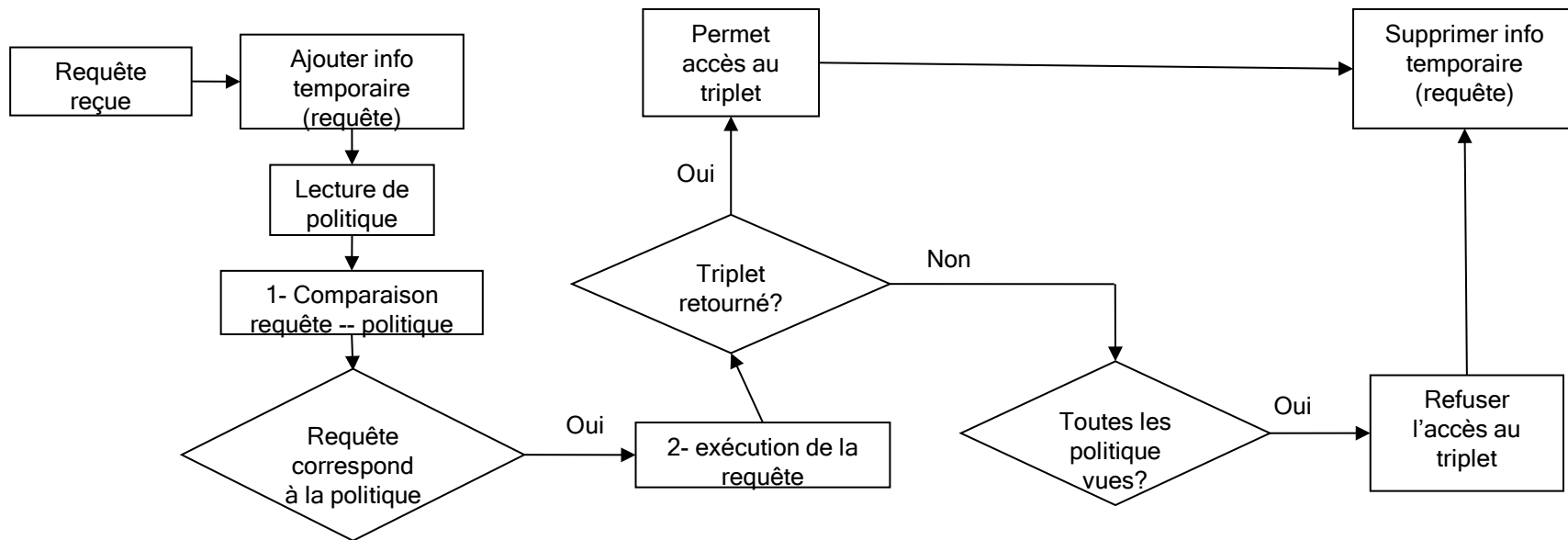
Vue d'ensemble de la vérification des Politiques



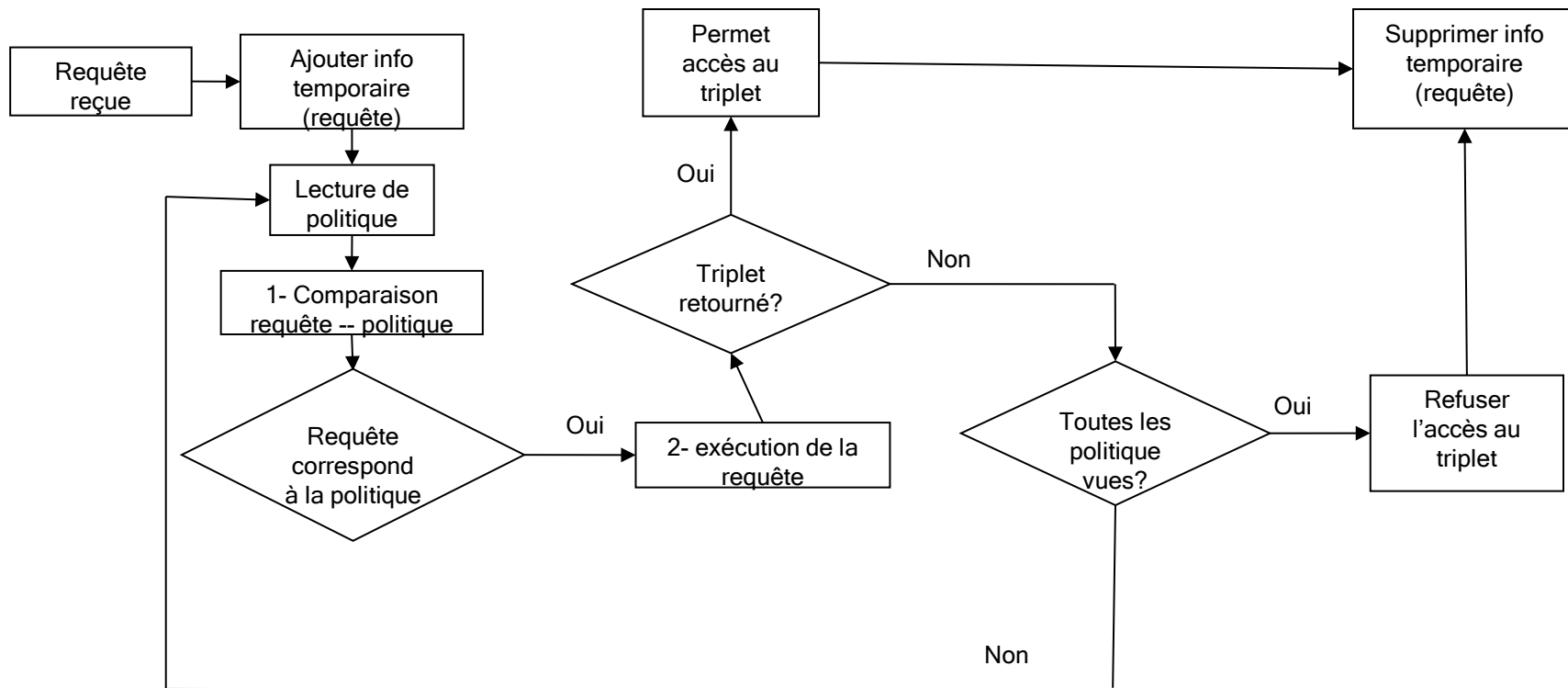
Vue d'ensemble de la vérification des Politiques



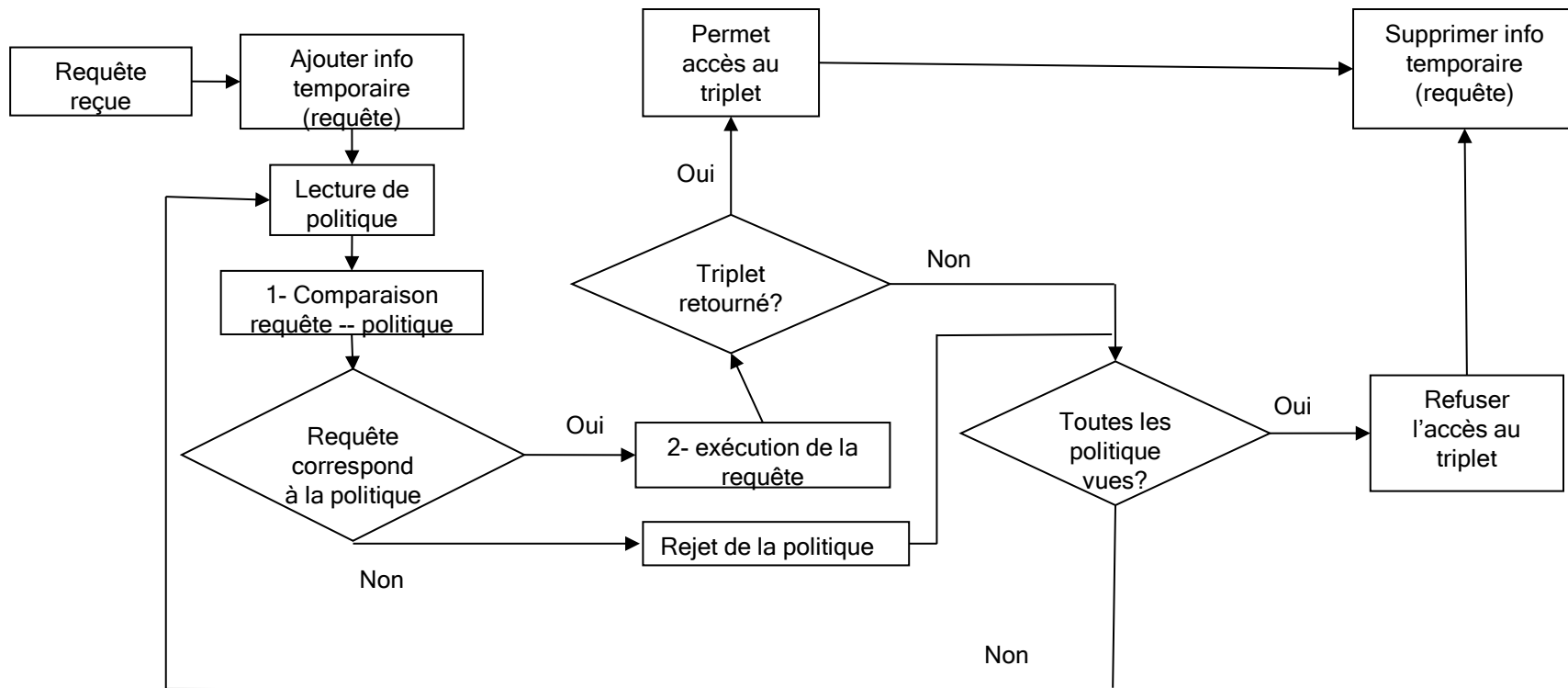
Vue d'ensemble de la vérification des Politiques



Vue d'ensemble de la vérification des Politiques



Vue d'ensemble de la vérification des Politiques



Conclusions

- La vie privée est extrêmement importante dans les réseaux sociaux mobiles
- Un système de contrôle d'accès idéal doit être :
 - expressif, flexible, et sensible aux aspects sociaux
 - facile à utiliser et exécutable sur les différentes plateformes
- Les techniques sémantiques constituent une base solide pour un système assurant le respect de la vie privée et le contrôle d'accès
- Il reste du travail, notamment en termes de performance et d'utilisation

Références

- [TONINELLI2010] Alessandra Toninelli, Animesh Pathak, Amir Seyedi, Roberto Speicys Cardoso, Valérie Issarny, “Middleware Support for Mobile Social Ecosystems”, 2010, Proceedings of the 2nd IEEE International Workshop on Middleware Engineering, to be held with COMPSAC 2010.
- Sara Hachem, Alessandra Toninelli, Animesh Pathak, Valérie Issarny. Policy-based Access contrôle in Mobile Social Ecosystems. *IEEE International Symposium on Policies for Distributed Systems and Networks*, Jun 2011, Pisa, Italy. IEEE computer society, 2011.
- RDF : www.w3.org/RDF/
- SPARQL : <http://www.w3.org/TR/rdf-sparql-query>