
Remplaçabilité privée des services web

Nawal Guermouche
nawal.guermouche@loria.fr



Introduction: Contexte(1)

Les services web

- Les services web:
 - Composants logiciels.
 - Interopérabilité et Intégration d'applications.

- Utiliser des standards:
 - UDDI: Annuaire de publication des services web.
 - SOAP: Convention d'encodage des messages.
 - XML: Format des messages.

Introduction: Contexte(2)


Les protocoles de conversations

- Description des services web:
 - WSDL: description de l'interface des services web (insuffisante).
 - BPEL: processus métier interne d'un service web (insuffisant).
 - Protocoles de conversations (Business Protocols)
 - Modéliser le comportement externe des services web (Les échanges de messages avec les entités externes).

Introduction: Contexte(2)

Les protocoles de conversations

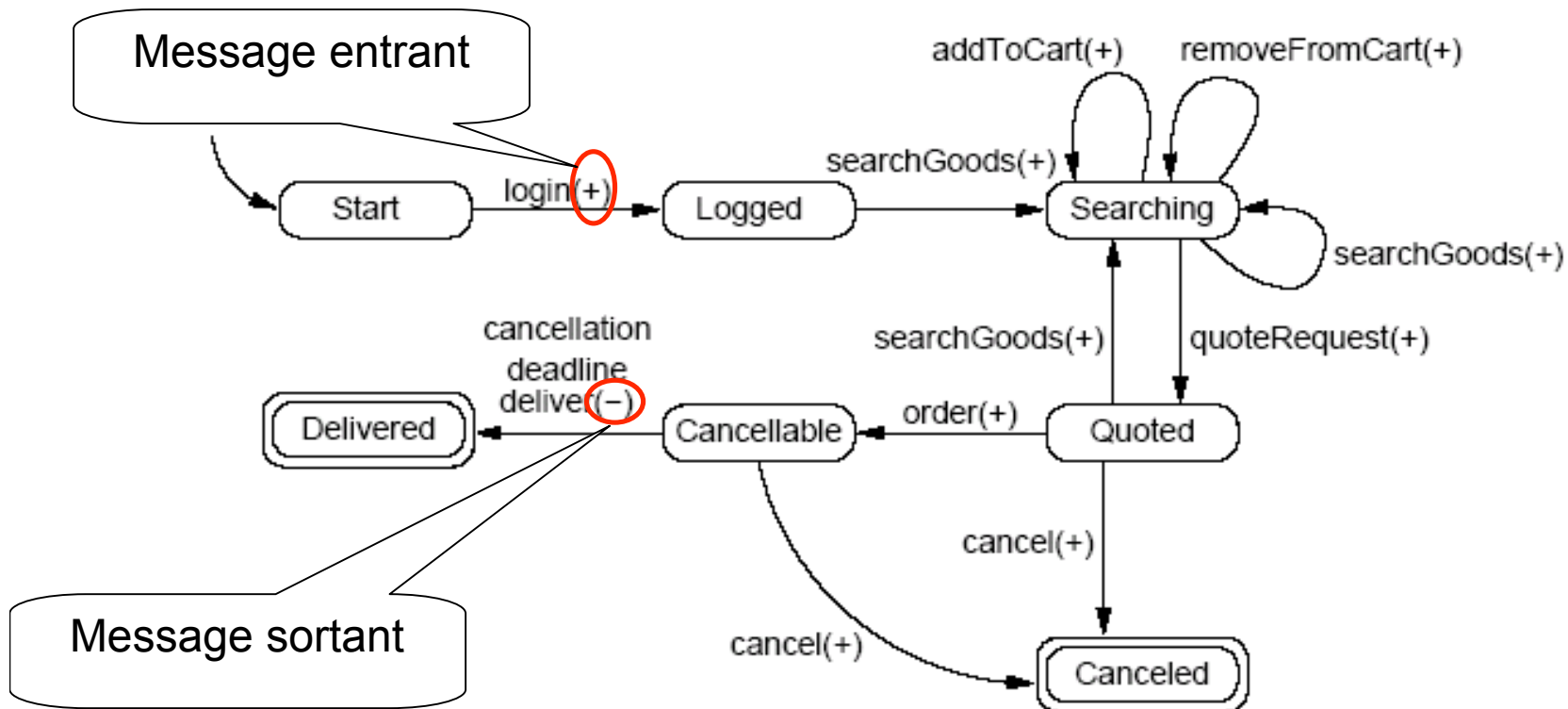
- Les protocoles de conversations permettent:
 - Savoir si un service client peut interagir avec un service fournisseur.
 - Savoir comment un client peut interagir avec un service fournisseur.

□ □  Inclure le protocole de conversations dans la description des services web.

Introduction: Contexte(2)

Les protocoles de conversations

- Exemple: Service d'achat d'articles sur internet:



Problématique

- L'échange de messages entre les services web:
 - Contenir des données privées (Données sensibles).

⇒ Définir et intégrer les règles de gestion de l'utilisation des données privées aux services web.

Remplaçabilité des services web.

Problématique

- Un service web endommagé:
 - Remplacement dynamique en assurant:
 - Les mêmes fonctionnalités.
 - Cohérence des règles de gestion de l'utilisation des données privées.

□ □  Un mécanisme d'**analyse de remplaçabilité** en présence des règles privées.

Plan

- ***Introduction:***

- Contexte
- Problématique

- ***Travaux existants***

- Modélisation des règles privées
- Remplaçabilité des services web

- ***Remplaçabilité privée des services web***

- Modélisation des règles privées
- Intégration des règles privées aux services web
- Classes de remplaçabilité
- Remplaçabilité voisine

- ***Conclusion et perspectives***

Travaux existants:

Modélisation des règles privés

I. Modèles de règles privées:

- P3P « Platform for Privacy Preferences » pour les sites web:
 - Définit deux types de règles:
 - ✓ Politiques: règles spécifiées par les fournisseurs
 - ✓ Préférences: règles spécifiées par les clients
 - ✓ Les Politiques/Préférences sont composées de:
 - ✓ *Purpose*: but
 - ✓ *Recipient*: utilisateurs
 - ✓ *Retention*: durée de sauvegarde des données

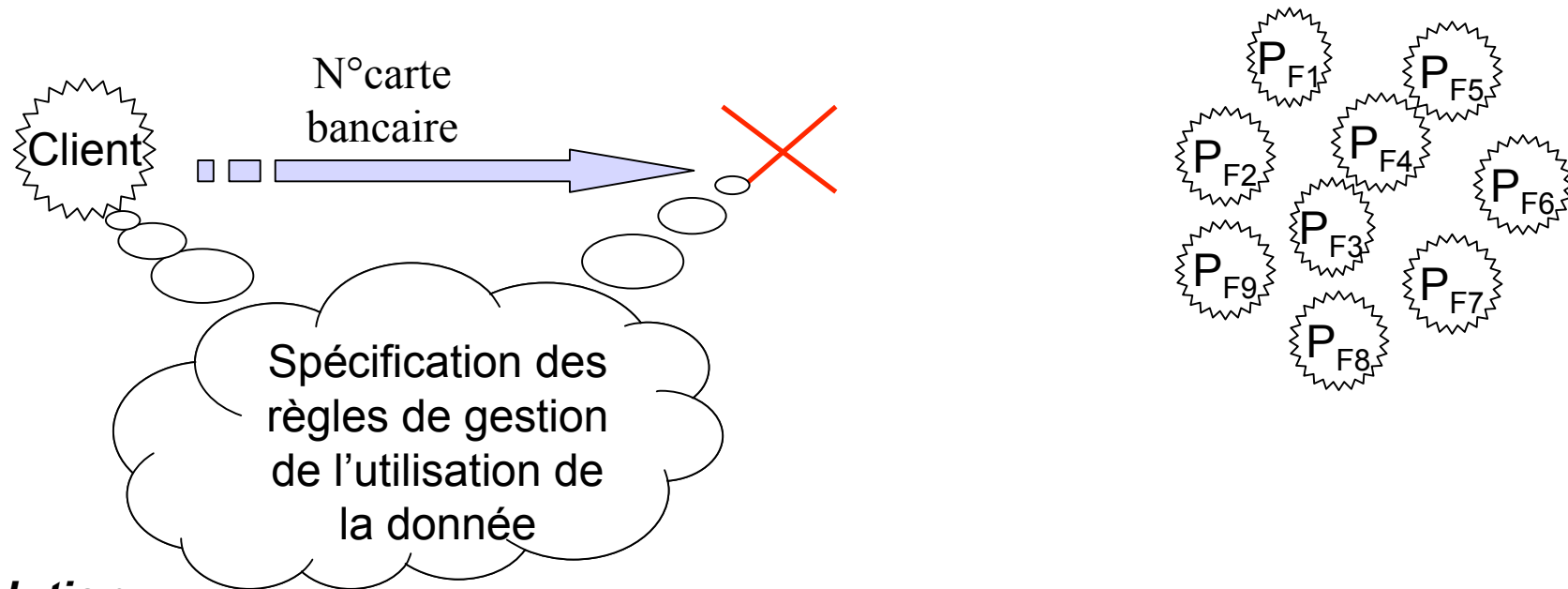
Travaux existants:

Remplaçabilité des services web

B.Benatallah, F. Casati, and F.Toumani. *Analysis and management of web service protocols*.
2004

- II. Analyse de la remplaçabilité des services web
 - Se reposer sur les protocoles de conversations: Proposition d'une algèbre.
 - Mais seulement du point de vue **fonctionnel**.

Remplaçabilité privée des services web



Solution:

1. **Modéliser** et **Intégrer** les règles privées dans les services web.
2. **Remplacer** le service par un autre service ayant:
 - Les mêmes fonctionnalités.
 - Des règles de gestion des données privées cohérentes.
 - Sinon, celui ayant des règles privées voisines.

Modélisation des règles privées dans les services web

I. Définir deux types de règles:

- Politiques privées: explicitant la manière avec laquelle le **fournisseur** utilisera les données privées de ses clients.
- Préférences privées: explicitant la manière avec laquelle le **client** souhaite que ses données privées soient utilisées.
- Les règles privées sont des propriétés **non fonctionnelles** des services web.

Modélisation des règles privées

- Une politique définit l'ensemble des termes d'utilisation des données privées (TUD)

$Plcy(TUD)$

- Chaque *tud* spécifie le but (*Purpose*) pour lequel une donnée a été collectée.

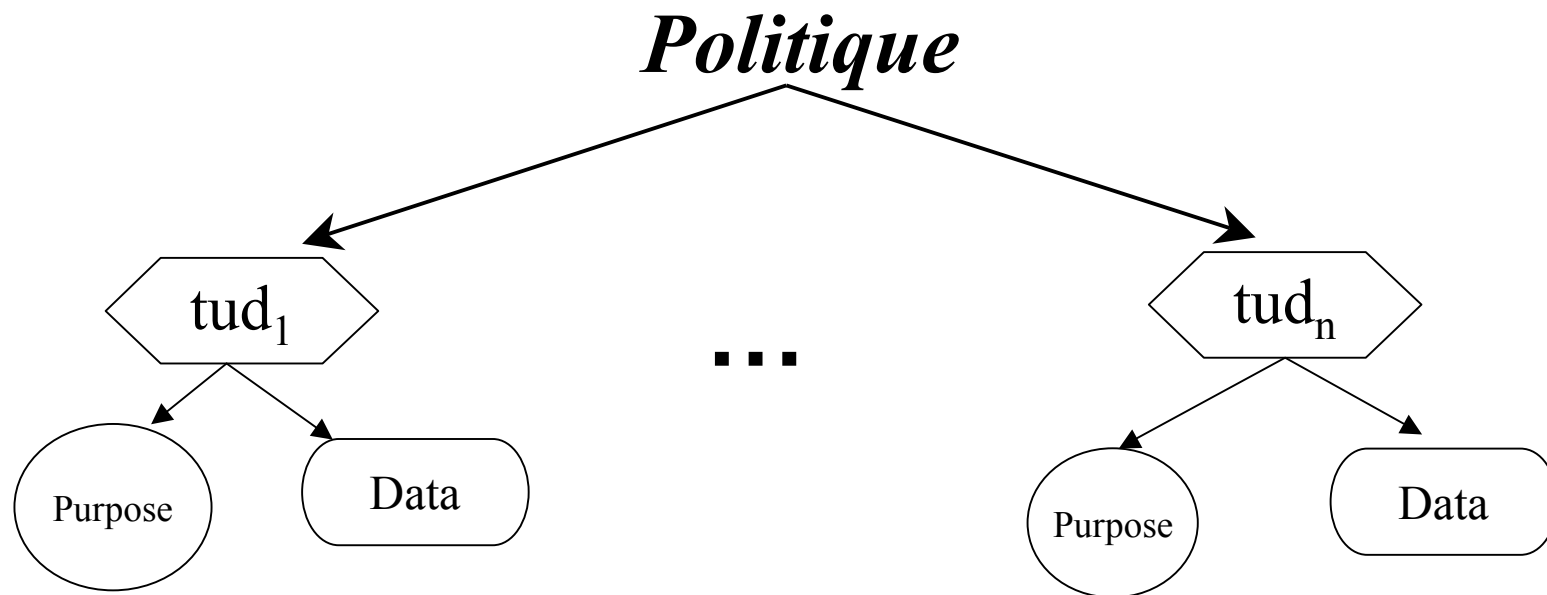
$\forall tud \in TUD, tud(d,p)$



- Un but déclenche :

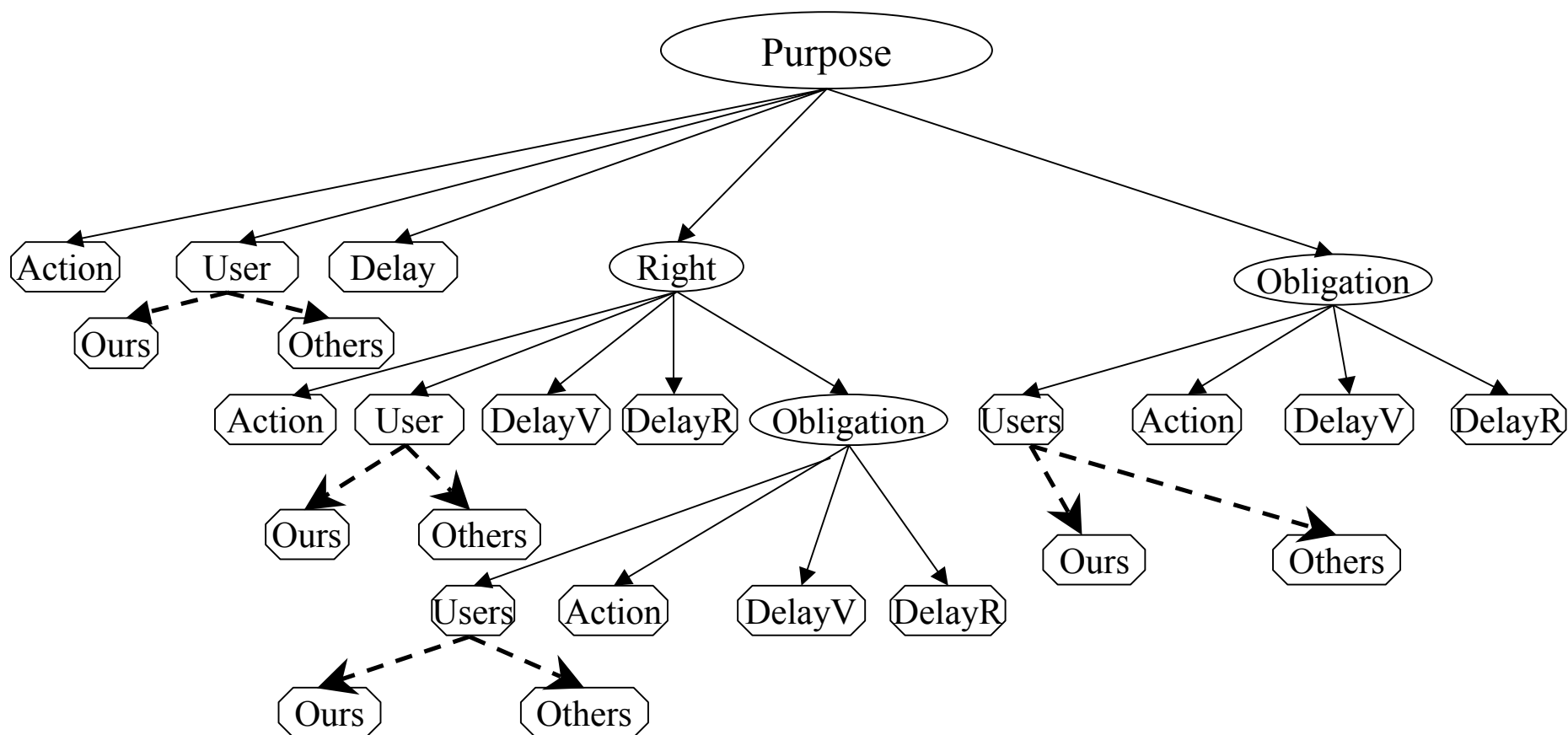
- Droit (*Right*): Les actions que le fournisseur à le choix de faire ou de ne pas faire. Un droit peut aussi déclencher une obligation.
- Obligation (*Obligation*): Les actions que le fournisseur doit réaliser afin d'assurer la sécurité des données collectées.

Modélisation des règles privées



Modélisation des règles privées

- Purpose (But)



Modélisation des règles privées

■ Politique Plcy1

tud(NCB,p1) tel que:

 p1 (rechargerCompte, Ours:SFinancier,Delay:[0h,2h],r1,o1), tel que:

 r1 (VerifierValidité,Others:banque,DelayV:[0h,2h],DelayR:[0h,1h],o2)

 o1 (Suppression,Ours:SFinancier,DelayV:[2h,4h], DelayR:[0h,0h])

 o2(Crypter,Others:banque,DelayV[1h,3h],DelayR: [0h,0h])

Modélisation des règles privées

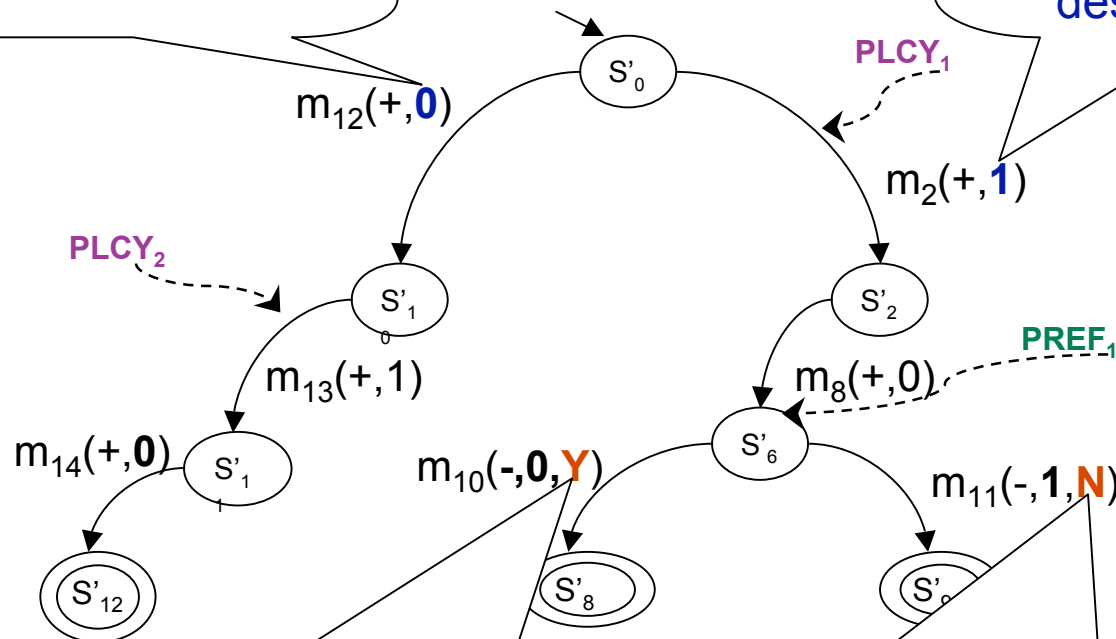
- Préférence:
 - Préférences locales: Propres données du service.
 - Préférences externes: Les données privées des clients.
 - Constituées d'un ensemble de TUD.
 - On ne distingue pas entre les utilisateurs internes et externes.

Intégration des règles privées aux services

web

+: Un message entrant
0: Pas de données
privées des clients

+: Un message entrant
1: Le message contient
les données privées
des clients



-: Un message sortant
Y: Le message transmet
les propres données privées
du service

-: Un message sortant
N: Le message ne transmet pas
les propres données privées
du service

Classes de remplaçabilité privée

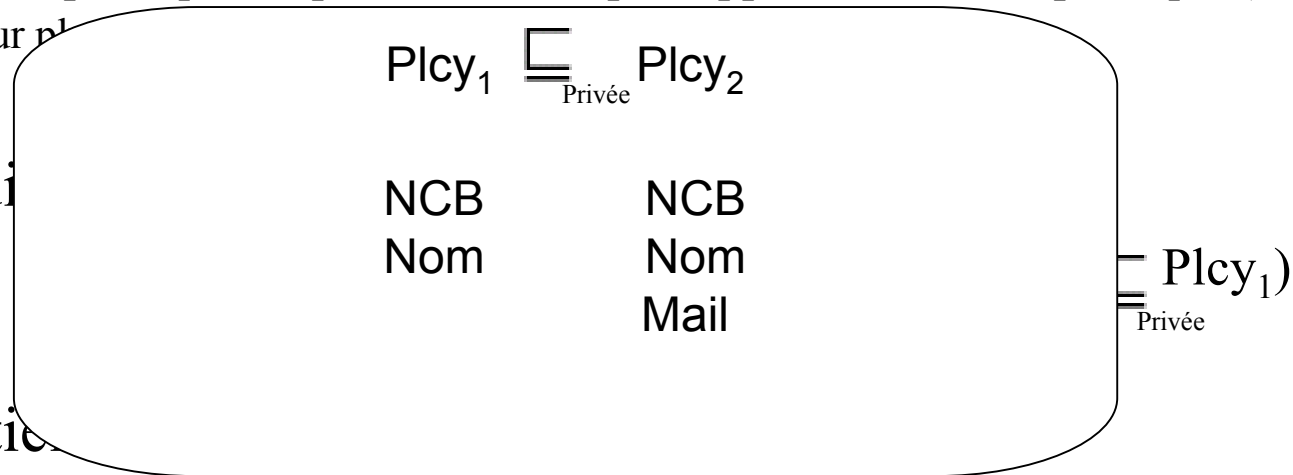
- Classes de remplaçabilité des politiques:

- Subsumption : $\sqsubseteq_{\text{Privée}}$

- Une politique est totalement cohérente avec une autre politique.
 - Une politique est plus restrictive par rapport à une autre politique (Des restrictions sur pl

- Équi

- Partie



Plcy₂ remplace partiellement Plcy₁ si $\neg(\text{Plcy}_1 \sqsubseteq_{\text{Privée}} \text{Plcy}_2)$

Classes de remplaçabilité privée

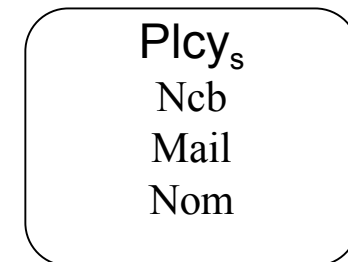
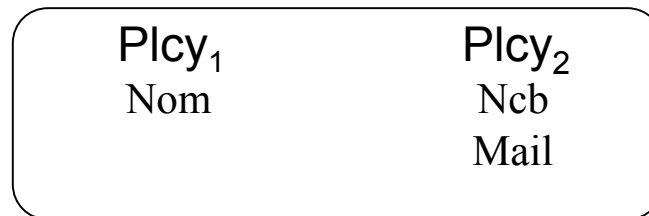
- Opérateur de différence privée $\downarrow^{privé}$: Calculer tous les éléments manquants dans la politique Plcy_2 pour qu'elle soit équivalente à Plcy_1 .
- Propositions:
 - Si $\text{Plcy}_1 \downarrow^{privé} \text{Plcy}_2 = \emptyset$ alors $\text{Plcy}_1 \sqsubseteq_{\text{Privée}} \text{Plcy}_2$
 - Si $\text{Plcy}_1 \downarrow^{privé} \text{Plcy}_2 = \emptyset$ et $\text{Plcy}_2 \downarrow^{privé} \text{Plcy}_1 = \emptyset$ alors $\text{Plcy}_1 \equiv_{\text{Privée}} \text{Plcy}_2$
 - Si $\text{Plcy}_1 \downarrow^{privé} \text{Plcy}_2 \neq \emptyset$ alors Plcy_2 remplace partiellement Plcy_1

Remplaçabilité voisine

- Absence d'une politique totalement cohérente.
- Chercher un service ayant une politique voisine suivant deux contextes:
Sécurité et Réalisation des buts

- *Sécurité*: Attribuer un ordre de priorité pour le choix des services:

- Data
- Obligation
- Purpose
- Right

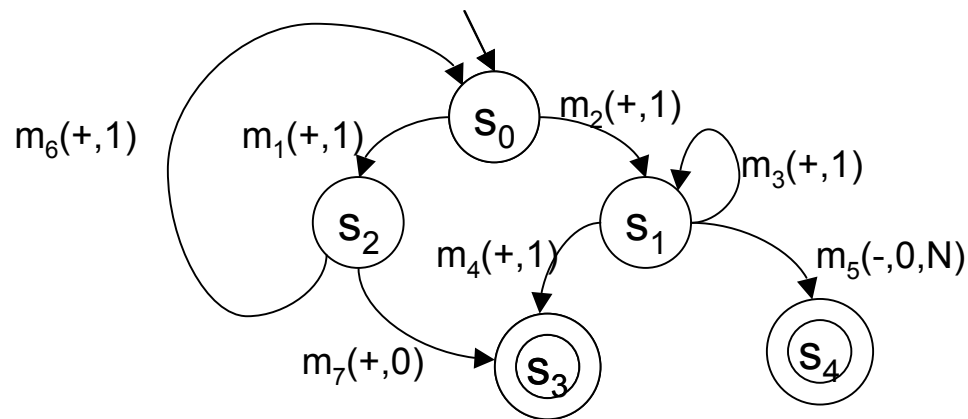


- *Réalisation des buts*: Attribuer un ordre de priorité pour le choix des services:

- Purpose
- Obligation
- Right

Remplaçabilité voisine

- Augmenter le niveau de remplaçabilité:
 - Éclatement du business protocole: Remplacer des *granularités* du protocole par un service.

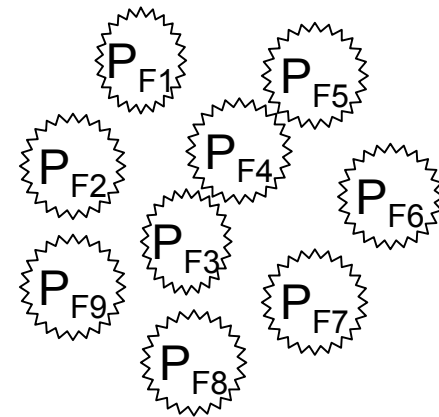
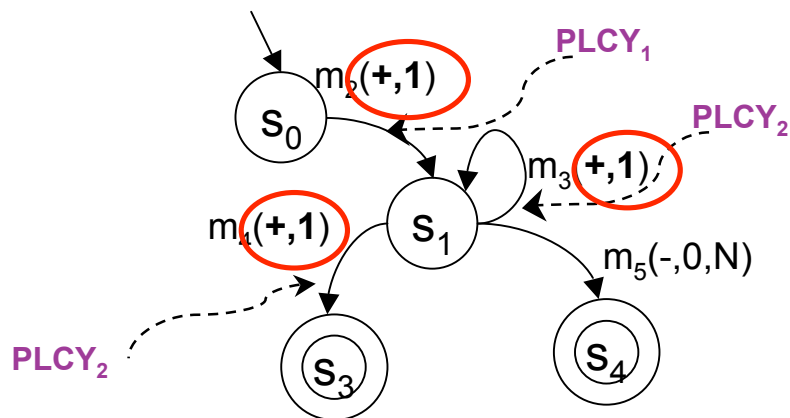


Sous protocole 1

Sous protocole 2

Remplaçabilité voisine

- Pour chaque sous protocoles P_{si} :
 1. Chercher les services qui le subsument fonctionnellement.
 2. Chercher un service voisin:
 1. Pour chaque transition contenant un message entrant privé.
 3. Sélectionner le service choisi souvent (nombre d'occurrence maximal).



Remplaçabilité voisine

Hypothèse: Plcy_2 remplace au moins partiellement Plcy_s , alors:

Théorème:

$$\text{Plcy}_2 \sqsubseteq_{\text{Privée}} \text{Plcy}_1 \implies \text{Plcy}_2 \lesssim_{\text{Plcy}_s} \text{Plcy}_1$$

$\| \text{TUD}_s \sqsubseteq_{\text{TUD}} \text{TUD}_1 \| \geq \| \text{TUD}_s \sqsubseteq_{\text{TUD}} \text{TUD}_2 \|$

Conclusion et perspectives

- ❑ Modélisation des règles de gestion de l'utilisation des données privées.
- ❑ Intégration de ces règles dans les protocoles de conversations des services web
- ❑ Définition de l'opérateur de différence privée:
 - Analyser la remplaçabilité des services web au vu de leurs règles privées.
- ❑ Définition de la méthode de remplaçabilité voisine

Conclusion et perspectives

- Implémentation de l'approche proposée
- Enrichir le modèle des règles privées:
 - Prohibitions
 - Pénalités
- Étendre l'approche proposée par les contraintes temporelles.

Merci de votre attention
Vos questions?