UNIVERSITÉ DE NANTES

U.S.T.T-B

Interopérabilité et sécurité des systèmes d'information

Soutenance de thèse de Mr. Abdramane BAH

08 Octobre 2020

Jury

Directeur de thèse: **Christian ATTIOGBÉ**, *Professeur*, Université de Nantes

Co-encadrant: **Pascal ANDRÉ**, *Maitre de conférences*, Université de Nantes

Co-encadrant: **Jacqueline KONATE**, *Maitre de conférences*, USTTB, Mali

Rapporteurs: **Florence SEDES**, *Professeure*, Université de Toulouse III

Philippe ANIORTE, *Professeur*, Université de Pau

Examinateurs: **Jean-Paul BODEVEIX**, *Professeur*, Université de Toulouse III

Interopérabilité et sécurité des systèmes d'information

- Concerne les problèmes de sécurité (contrôle d'accès) dans le contexte de l'interopérabilité des SI appartenant à des organisations distinctes

Nous avons étudié

- les problèmes d'interopérabilité des modèles et mécanismes de sécurité
- et les problèmes d'interopérabilité des services en termes de sécurité

Nous avons proposé trois contributions

- deux (02) contributions à l'interopérabilité des modèles de sécurité
- une (01) contribution à l'interopérabilité des services

Sommaire

1. Contexte
2. Problématique
3. Contributions
   1. Propositions
   2. Mise en œuvre
   3. Expérimentations
4. Bilan et perspectives

Interopérabilité inter-domaine des systèmes d'information (SI)

Un besoin concret:

l'échange d'informations critiques dans une situation de catastrophe

Hôpitaux

Centres de transfusion sanguine

Direction de la police

- le nombre blessés,
- l'emplacement des blessés,
- l'état des routes,
- les lits hôpitaux disponibles,
- les types de sang disponible
- la quantité de sang disponible
- les menaces à la sécurité

Organisations d'intervention

Pompiers

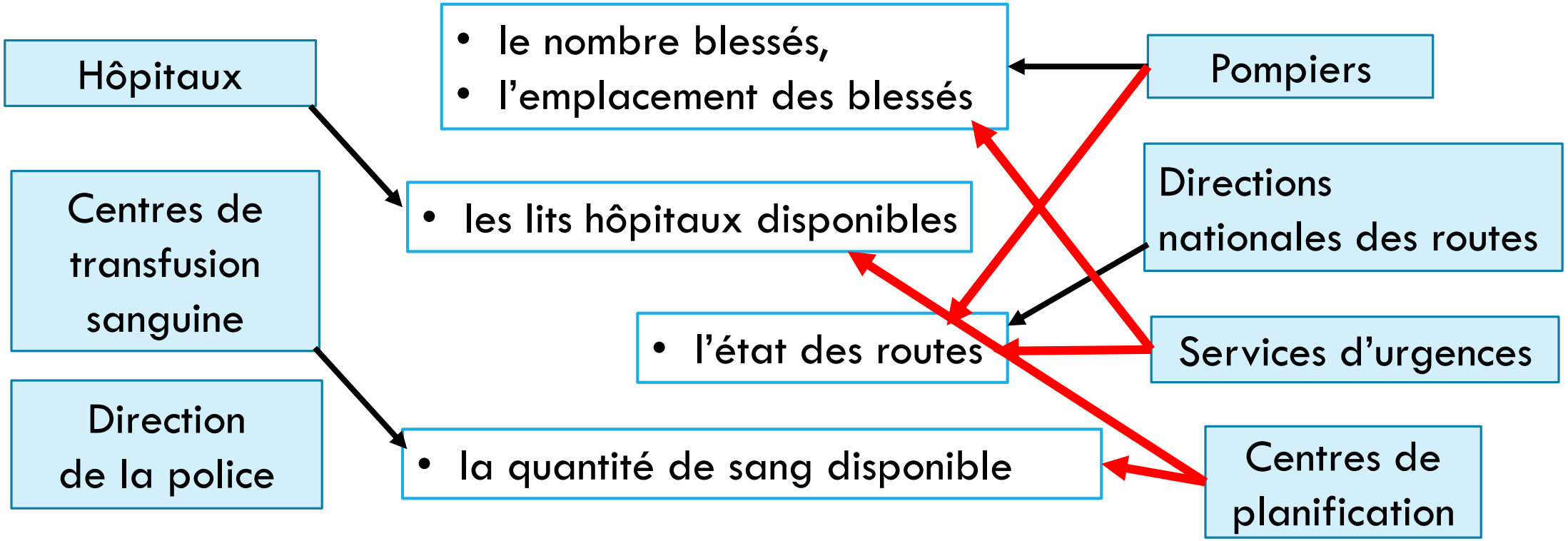
Directions nationales des routes

Services d'urgences

Centres de planification

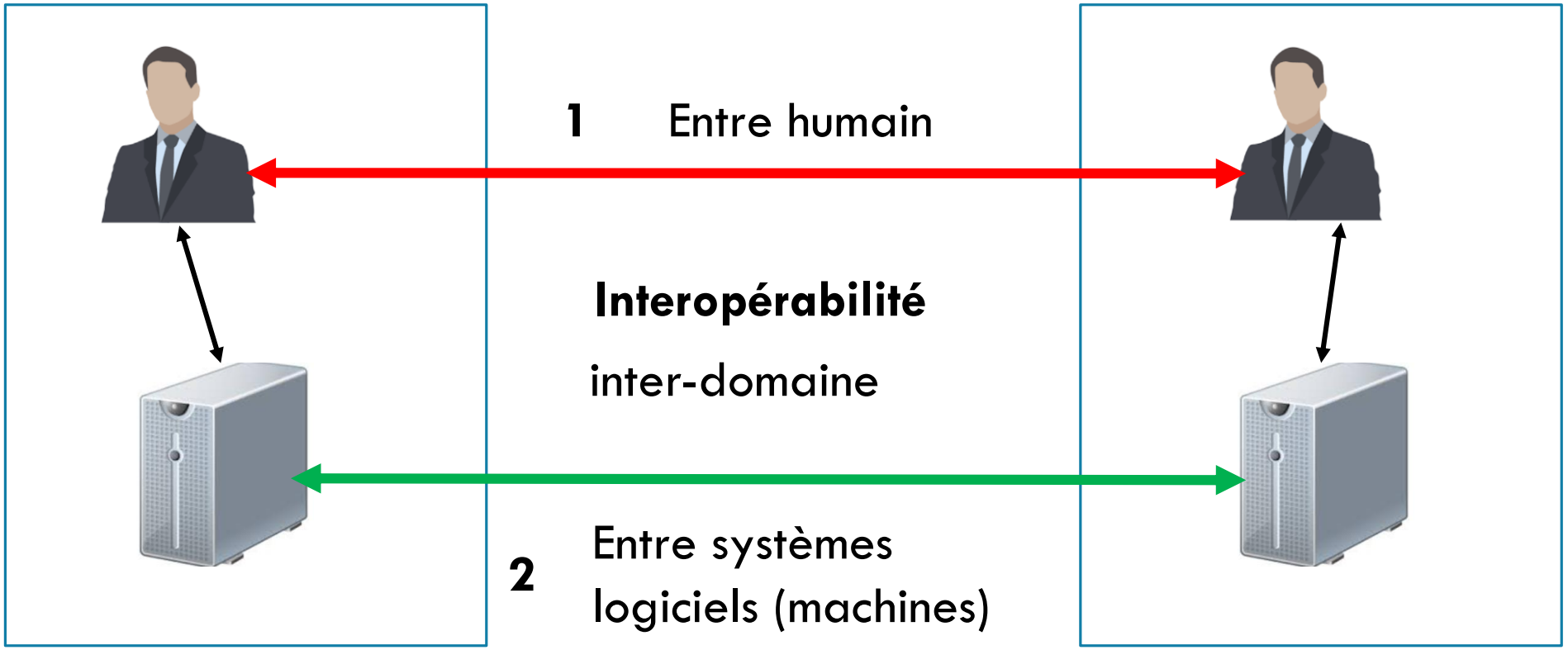
Interopérabilité inter-domaine des SI

Chaque organisation recueille et offre une catégorie d'informations



Interopérabilité inter-domaine des SI

Ce partage d'informations peut être effectué de deux façons



Interopérabilité inter-domaine des SI

Définition: Interopérabilité des systèmes d'information

> Capacité de communiquer et d'échanger des informations, de comprendre et d'agir à partir de ces informations et d'accéder aux fonctionnalités les uns des autres, [DUAN, 2009]

Définition: Domaine de sécurité (ou domaine)

> Est une unité unique d'administration de sécurité composée d'un ensemble d'utilisateurs, d'applications et de services.
>
> Il est séparé des autres domaines par des frontières de sécurité. [DUAN, 2009]

[DUAN, 2009] Duan, N.: Design Principles of a Federated Service-oriented Architecture Model for NetcentricData Sharing. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 6(4) (October 2009) 165–176

Interopérabilité inter-domaine des SI

Il existe plusieurs solutions:

1. **Solution techniques**
   - Enterprise service bus (ESB)
   - Services web, etc...

2. **Solutions architecturales**
   - Architecture-orientée services (**SOA**)
   - Systèmes multi-agents, etc...

Application
Langage: JAVA
Plateforme:WINDOWS

Domaine A

Progiciel intégré
Langage: Ruby
Plateforme: Linux

Domaine B

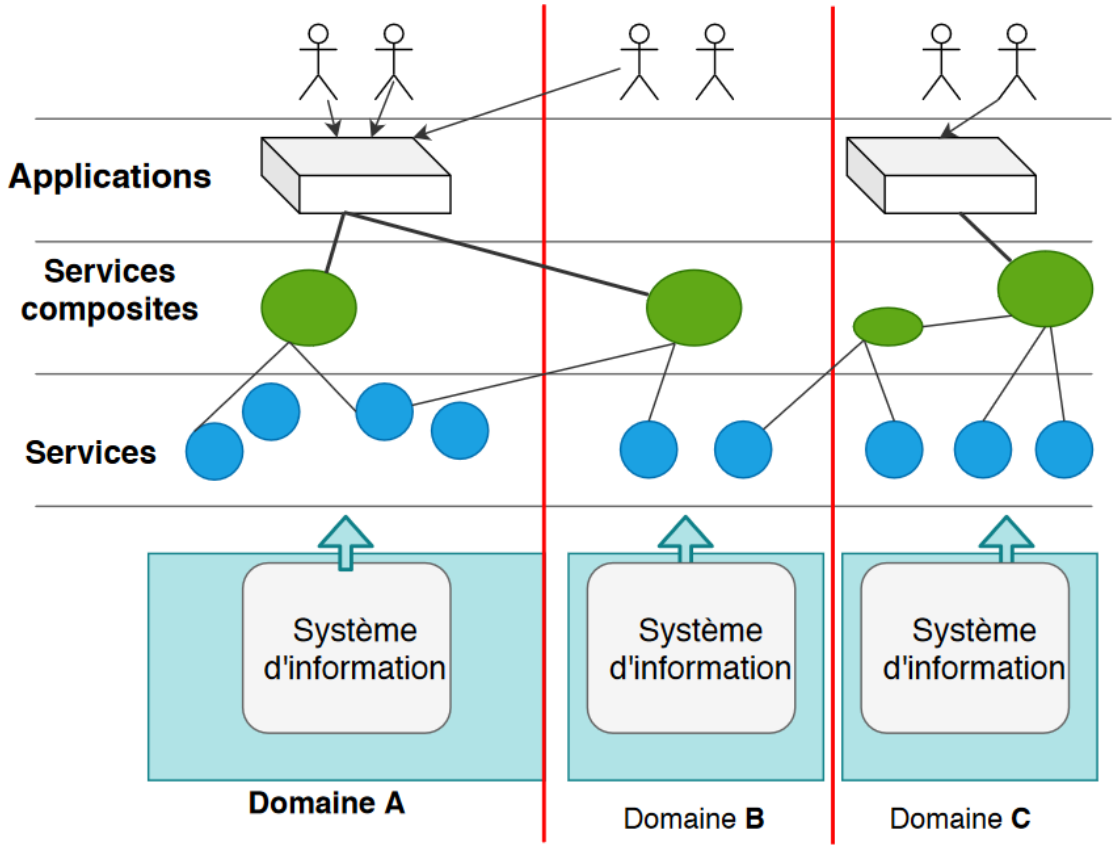
Interopérabilité inter-domaine des SI

Architecture-Orientée Services (SOA)

Les informations et les systèmes sont partagés sous forme de **services** autonomes, découvrables, faiblement couplés, composables.

SOA peut être implémenté par:

1. Services web REST
2. Services Web SOAP: Normes de sécurité



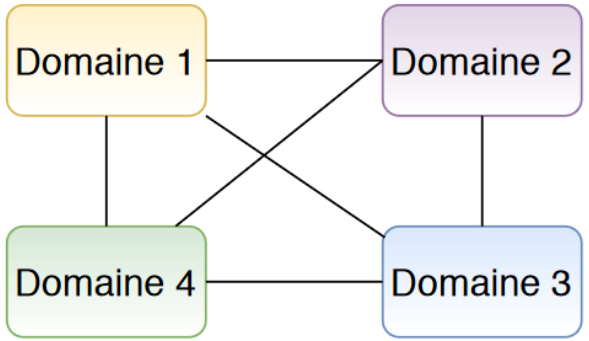
Interopérabilité inter-domaine et sécurité

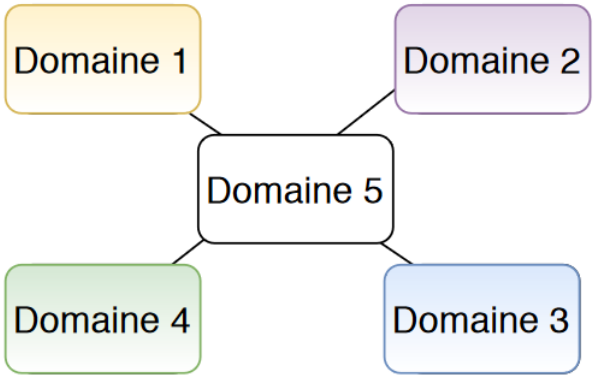
Besoin de sécurité:

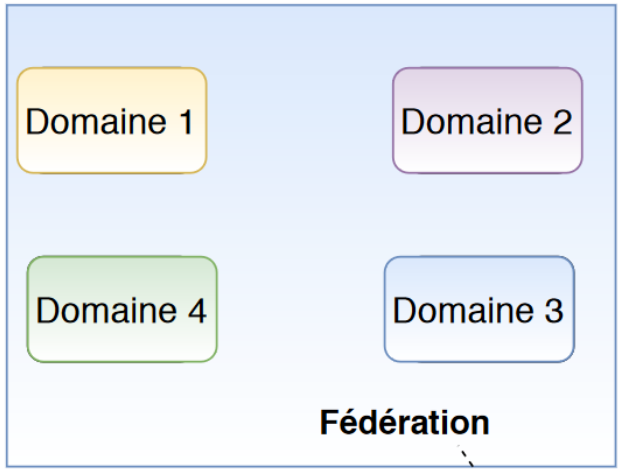
1. Avoir une relation de collaboration entre domaines
2. Garantir l'intégrité des informations, la sécurité des accès et la sécurité mutuelle des systèmes d'information des domaines

Interopérabilité inter-domaine et sécurité

Relation de collaboration entre domaines : trois modèles







Modèle point-à-point

- Complexe, mise à l'échelle difficile

Modèle étoile

- point unique de défaillance, perte d'autonomie

Modèle fédération

- Dynamique, autonomie des domaines, mise à l'échelle facile

Fédération de domaines (ou fédération)

Définition:

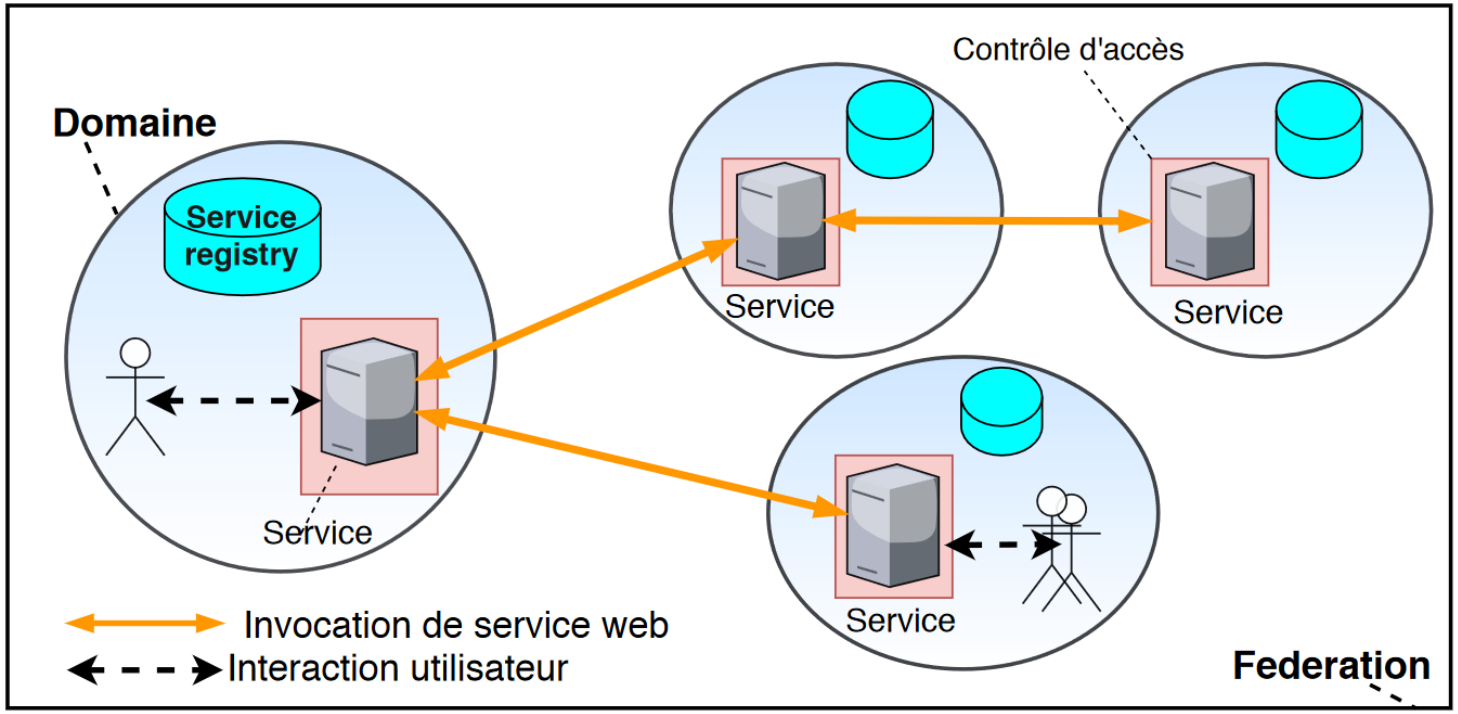
> Un fédération est une collection de domaines représentant ses membres. Chaque domaine est auto-organisé et peut fonctionner de manière autonome. Un domaine peut rejoindre ou quitter la fédération en suivant les protocoles standards.
>
> [DUAN et al, 2009]

Notre définition:

> Une fédération est un environnement de confiance où les domaines collaborent en partageant des informations et des services tout en conservant leur autonomie individuelle et leur auto-gouvernance.

Fédération de services (ou fédération SOA)

Lorsque les services sont partagés et composés entre les domaines, on parle de fédération de services ou SOA fédéré ou encore de fédération SOA.



Fédération de services et sécurité

Besoin de sécurité:

1. Avoir une relation de collaboration entre domaines : Fédération
2. Garantir l'intégrité des informations, la sécurité des accès et la sécurité mutuelle des systèmes d'information des domaines
   - Assuré par le contrôle d'accès

Contrôle d'accès: identification et authentification, autorisation

- Quel utilisateur peut accéder à quel service et dans quelles conditions
- Seuls les utilisateurs autorisés ont accès aux informations et aux services

Sommaire

1. Contexte
2. **Problématique**
3. Contributions
   1. Propositions
   2. Mise en œuvre
   3. Expérimentations
4. Bilan et perspectives

Fédération de services et sécurité

Deux problématiques de sécurité

(P1) Autorisation des utilisateurs

octroi et définition des permissions d'accès

(P2) Contrôle d'accès aux services

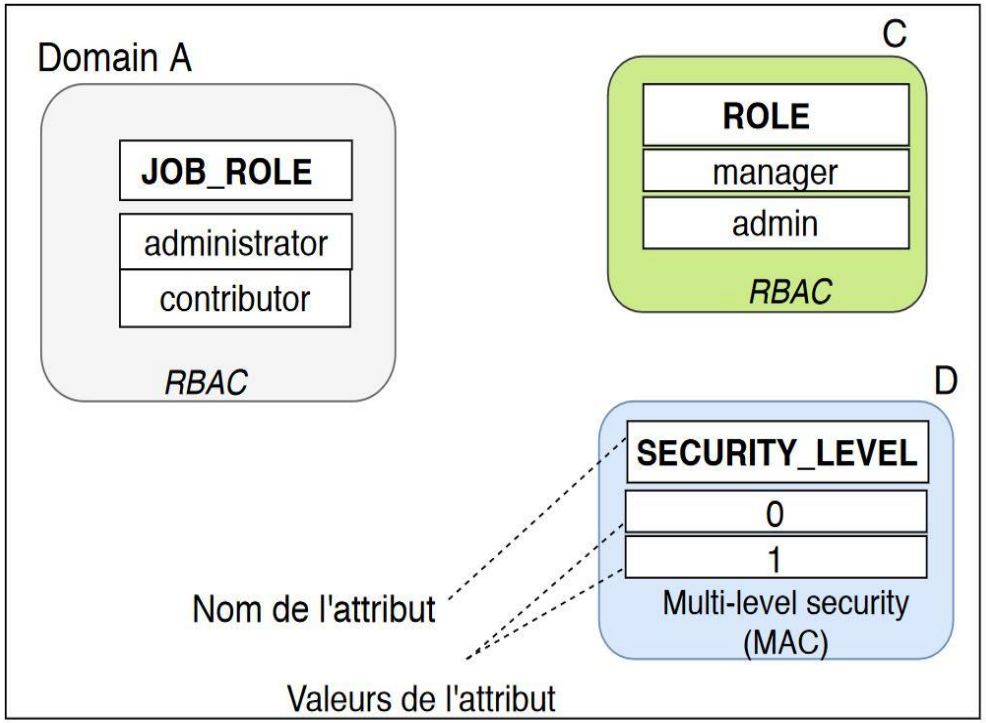
authentification et vérification des permissions d'accès

Fédération de services et sécurité

(P1) Autorisation des utilisateurs

1. Hétérogénéité des modèles d'autorisation
   - RBAC (Role-Based Access Control)
   - ABAC (*Attribute-Based Access Control*)
   - MAC (Mandatory Access Control), etc...

2. Hétérogénéité des ***attributs d'autorisation***
   a. Hétérogénéité de définition
   b. Hétérogénéité sémantique

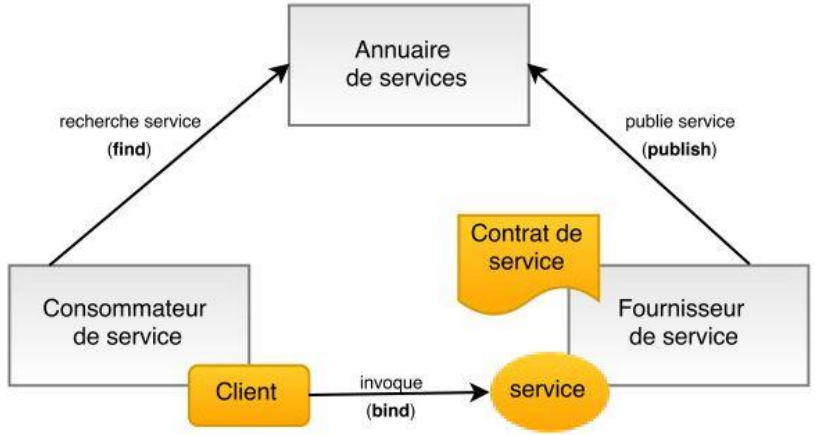


Fédération de services et sécurité

(P1) Autorisation des utilisateurs

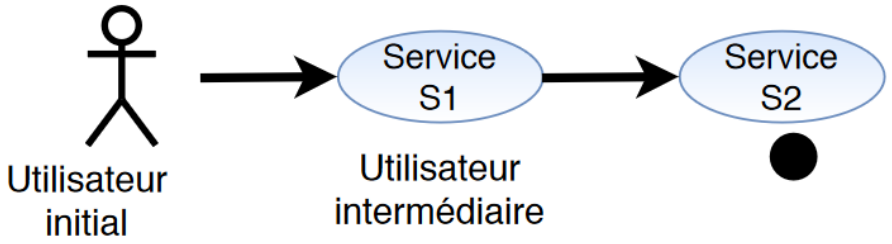
3. Couplage faible des services

- Les utilisateurs ne sont pas connus à l'avance



4. Composition de services

- Les utilisateurs intermédiaires doivent aussi être autorisés



Fédération de services et sécurité

(P1) Autorisation des utilisateurs: synthèse

Obstacles

- Hétérogénéité des modèles et attributs d'autorisation des domaines
- Autonomie des domaines : ne peuvent **abandonner** leurs modèles existants

Contraintes: les domaines ne sont pas en mesure d'accorder des permissions d'accès aux utilisateurs des autres domaines

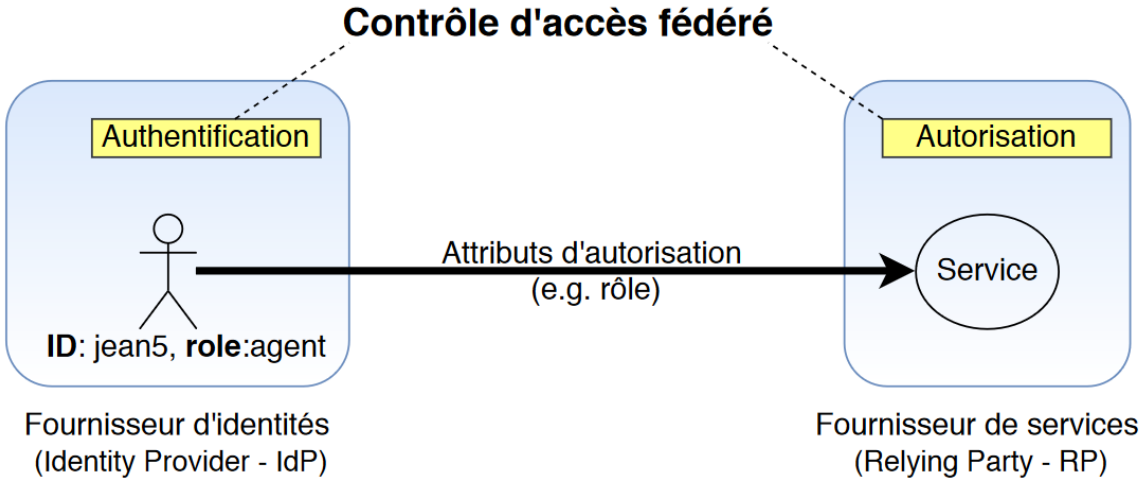
Question de recherche (Q1): Comment assurer l'interopérabilité entre les modèles et les attributs d'autorisation des domaines?

Fédération de services et sécurité

(P2) Contrôle d'accès aux services

Délégation de l'authentification?

1. Hétérogénéité des attributs d'autorisation
   - Absence d'attributs communs aux domaines

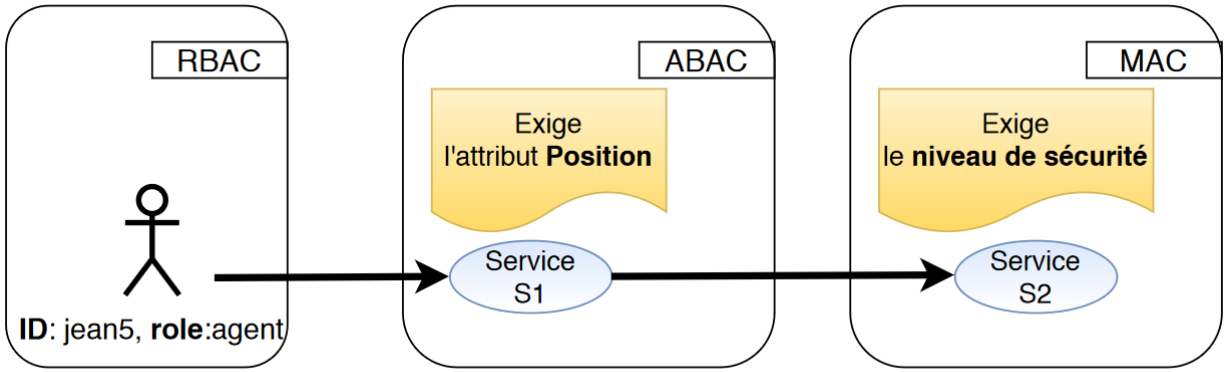


Fédération de services et sécurité

(P2) Contrôle d'accès aux services

Délégation de l'authentification?

2. Hétérogénéité des services
   - des exigences de contrôle d'accès des services



Fédération de services et sécurité

(P2) Contrôle d'accès aux services: synthèse

Obstacles

- Hétérogénéité des attributs d'autorisation (autonomie des domaines)
  Hétérogénéité des exigences de contrôle d'accès des services

Contraintes

- L'authentification des utilisateurs ne peut être déléguée à leurs domaines
- Les services ne sont pas interopérables au niveau de la fédération

Question de recherche (Q2): Comment assurer l'interopérabilité entre les services en termes de contrôle d'accès sans compromettre leurs consommateurs existants?

SOMMAIRE

1. Contexte
2. Problématique
3. **Contributions**
   1. Propositions
   2. Mise en œuvre
   3. Expérimentations
4. Bilan et perspectives

Solutions existantes et insuffisances

1. Interopérabilité des modèles d'autorisation: **ABAC**
2. Interopérabilité des attributs d'autorisation: **Mapping d'attributs**
   - ~~aucunes de méthodes satisfaisantes pour une fédération SOA~~
   - **Une méthode de mapping d'attributs pour SOA (Q1) (Q2)**
3. Contrôle d'accès des services web: **normes et services de sécurité**
   - ~~ne supporte pas le mapping d'attributs~~
   - **Un mécanisme de contrôle d'accès fédéré basé sur le mapping (Q1)**
4. Interopérabilité des services en termes de contrôle d'accès: ~~**Aucune solution**~~
   - Une nouvelle approche: **la promotion de services (Q2)**

Contributions

Interopérabilité de contrôle d'accès

1. **Notre méthode de mapping d'attributs**

2. Notre mécanisme de contrôle d'accès fédéré basé sur le mapping

Interopérabilité des services en termes de contrôle d'accès

3. Notre nouvelle approche: **la promotion de services**

3.1. Notre méthode de mapping d'attributs

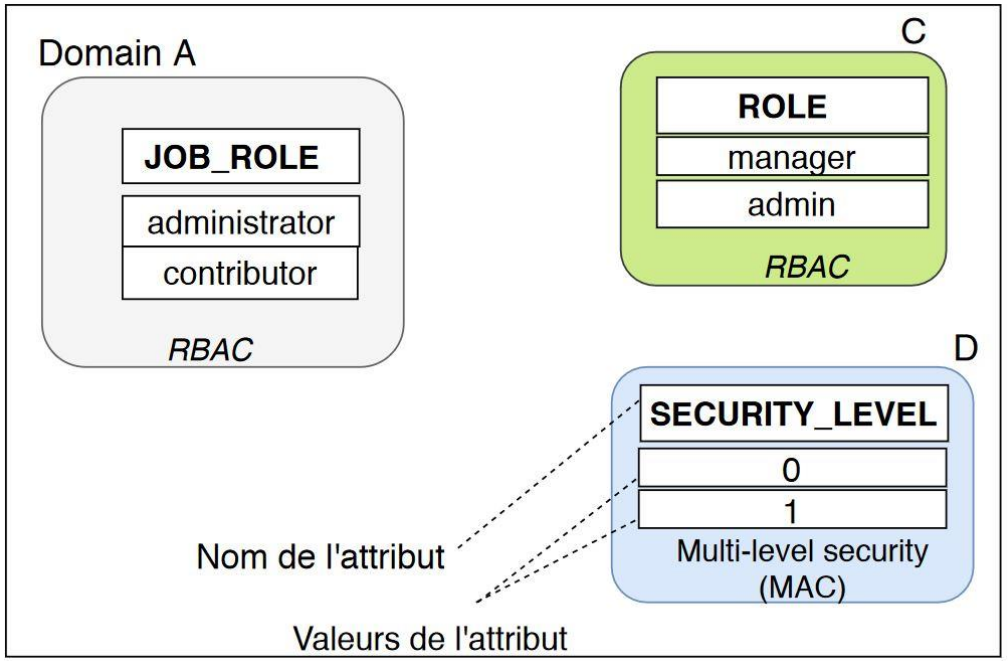
Mapping d'attributs: concepts

- définir les correspondances (ou mapping) entre les attributs d'autorisation des domaines

Les mappings sont définies en fonction de:

- du sens (sémantique) des attributs
- de la décision des administrateurs de sécurité

Il peut ne pas y avoir de correspondances



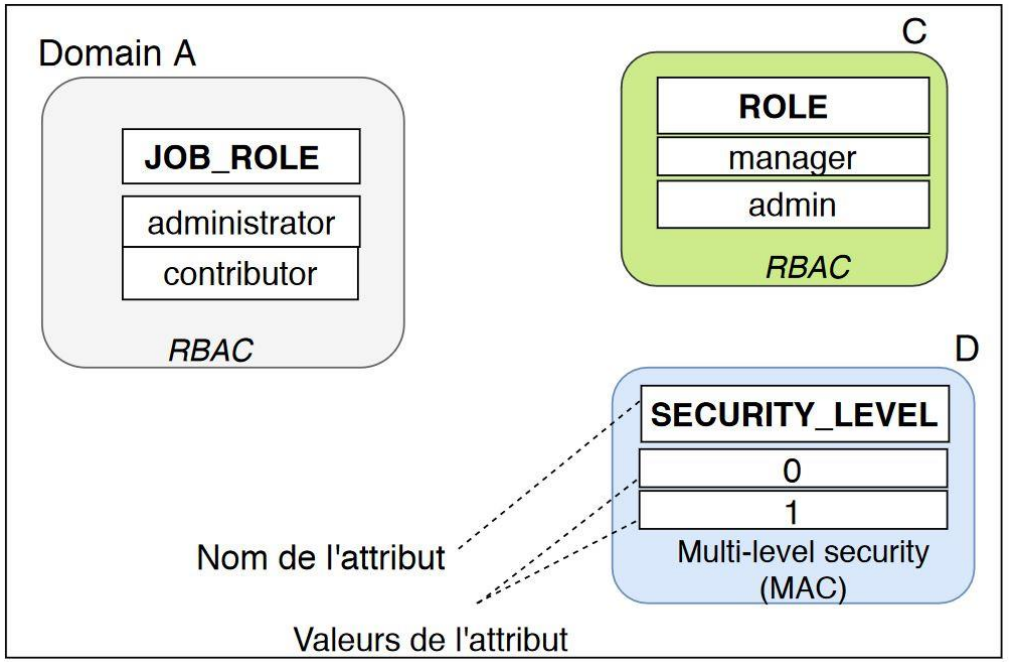
3.1. Notre méthode de mapping d'attributs

Concepts: techniques de définition des correspondances

1. **Ontologie:** inférence automatique

2. Règles logiques: politiques de mapping

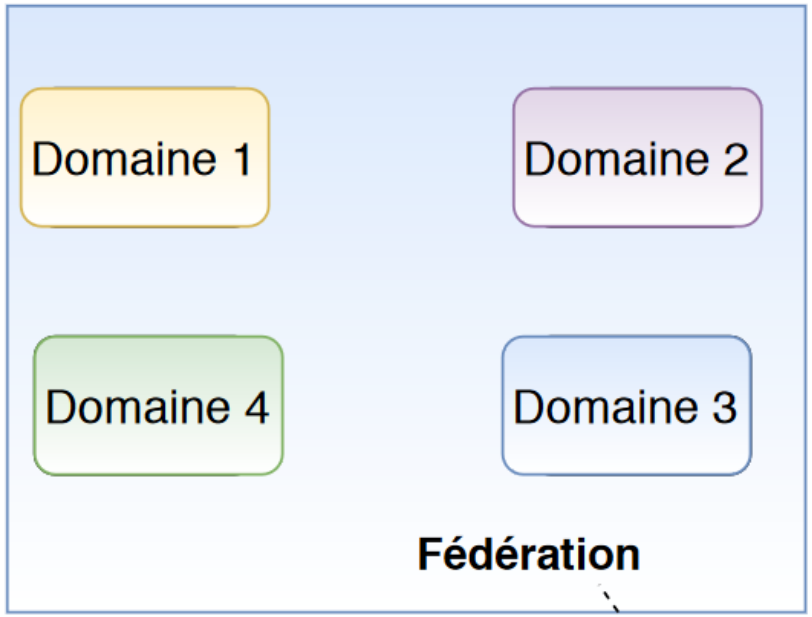
SI
l'attribut ***role*** = « admin » dans $\mathbf{D_C}$
Alors
l'atribut ***niveau-securite*** = « 1 » dans $\mathbf{D_D}$



3.1. Notre méthode de mapping d'attributs

Mapping d'attributs dans SOA: exigences

1. Autonomie des domaines pour l'autorisation
2. Simplicité de définition des politiques de mapping
3. Flexibilité des politiques de mapping
4. Adaptation dynamique des politiques de mapping
5. Confidentialité des attributs d'autorisation

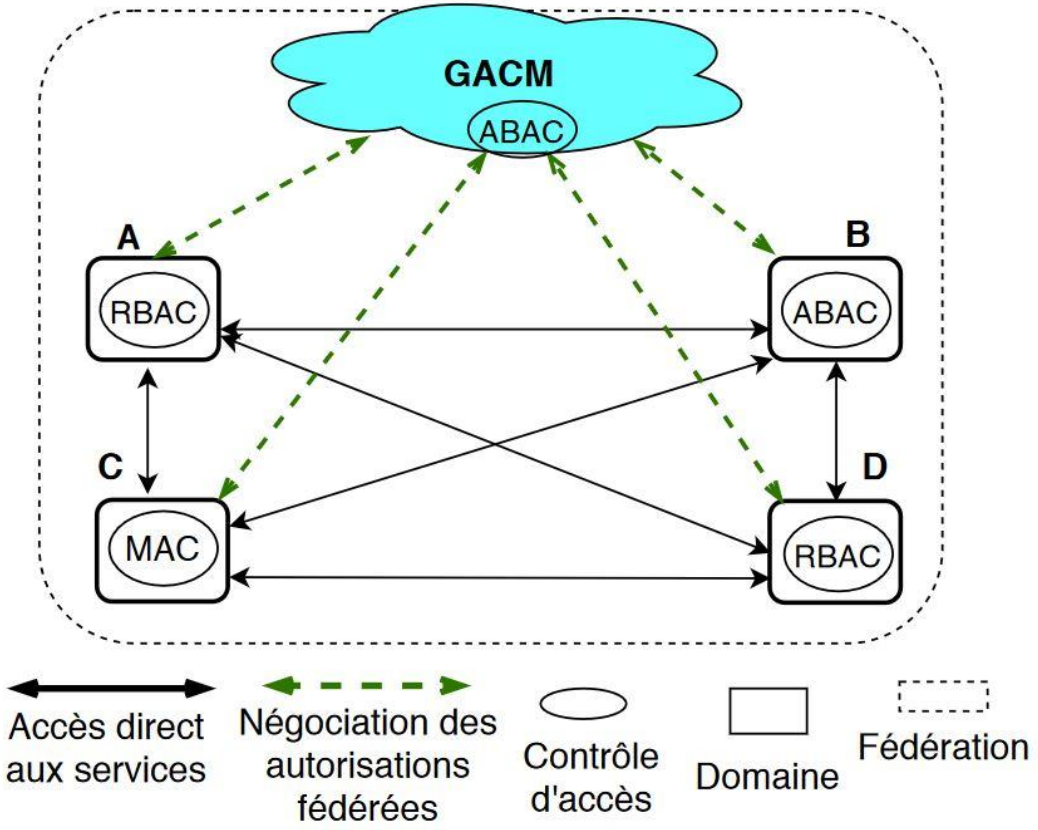


3.1. Notre méthode de mapping d'attributs

Nous proposons d'abord une **nouvelle architecture de fédération**

Global Access Control Mediator - **GACM**
médiateur d'interopérabilité

- GACM est un domaine
- GACM représente l'autorité de la fédération

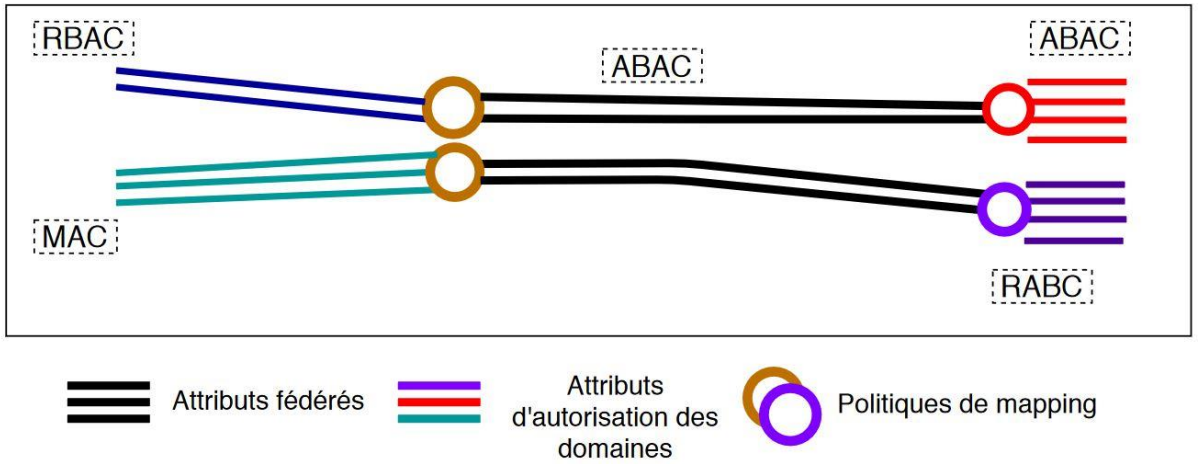


3.1. Notre méthode de mapping d'attributs: principes

Deux principes:

1. **Mapping à deux niveaux:**
   - deux types de politique de mapping

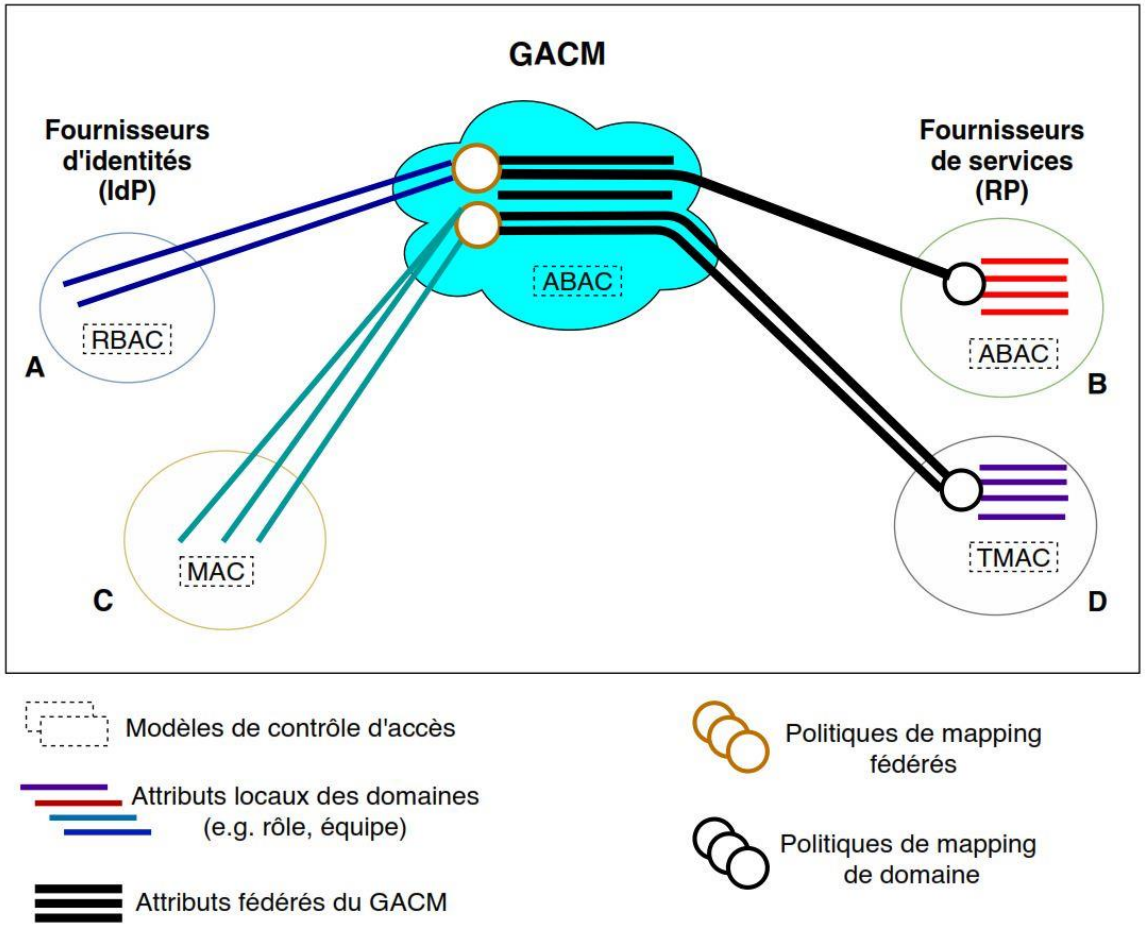
2. **Attributs fédérés**
   - Attributs d'autorisation communs
   - Définis par le **GACM**



3.1. Notre méthode de mapping d'attributs: principes

Architecture de médiation

1. **Au niveau du GACM:**
   - politiques de mapping fédérés (PMF)
   - une copie du PMF est gardé au niveau des domaines
2. **Au niveau des domaines:**
   - Une politique de mapping de domaine (PMD)



3.1. Notre méthode de mapping d'attributs: principes

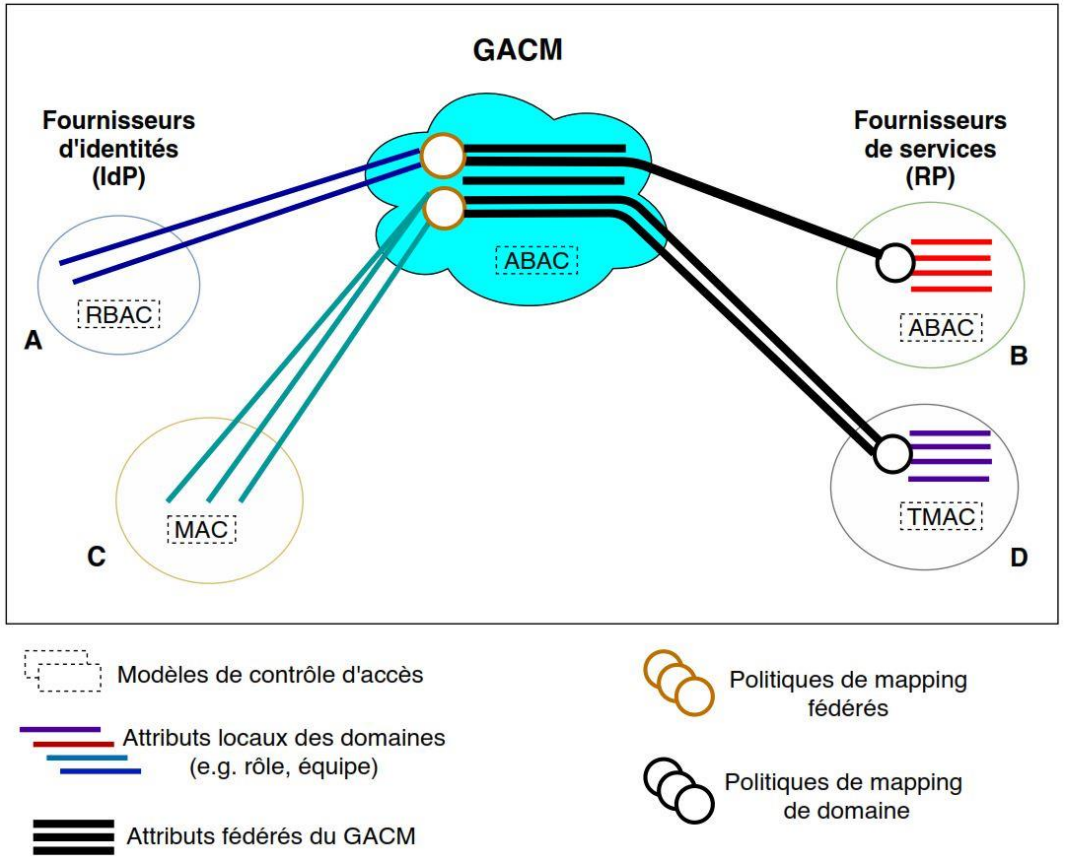
Architecture de médiation

Principaux intérêts du GACM

1. Sécurité
   - divulgation contrôlée des attributs;
   - Fiabilité des autorisations

2. Stabilité et flexibilité des politiques de mapping

3. Dynamisme des politiques de mapping face à l'évolution de la fédération



Contributions

Pour l'interopérabilité de contrôle d'accès

1. **Une méthode de mapping d'attributs**

2. **Un mécanisme de contrôle d'accès fédéré basé sur le mapping**

Pour l'interopérabilité des services en termes de contrôle d'accès

3. Une nouvelle approche: **la promotion de services**

3.2. Contrôle d'accès fédéré basé sur le mapping

Contrôle d'accès des services web : basé sur

1. **Normes de sécurité:**
   - WS-Security, WS-Federation, WS-Trust, SAML, XACML, etc...

2. **Orienté services:** services de sécurité

consiste à intégrer les fonctions de la sécurité dans un service dédié

- Service d'authentification, service d'autorisation, Etc...

3.2. Contrôle d'accès fédéré basé sur le mapping

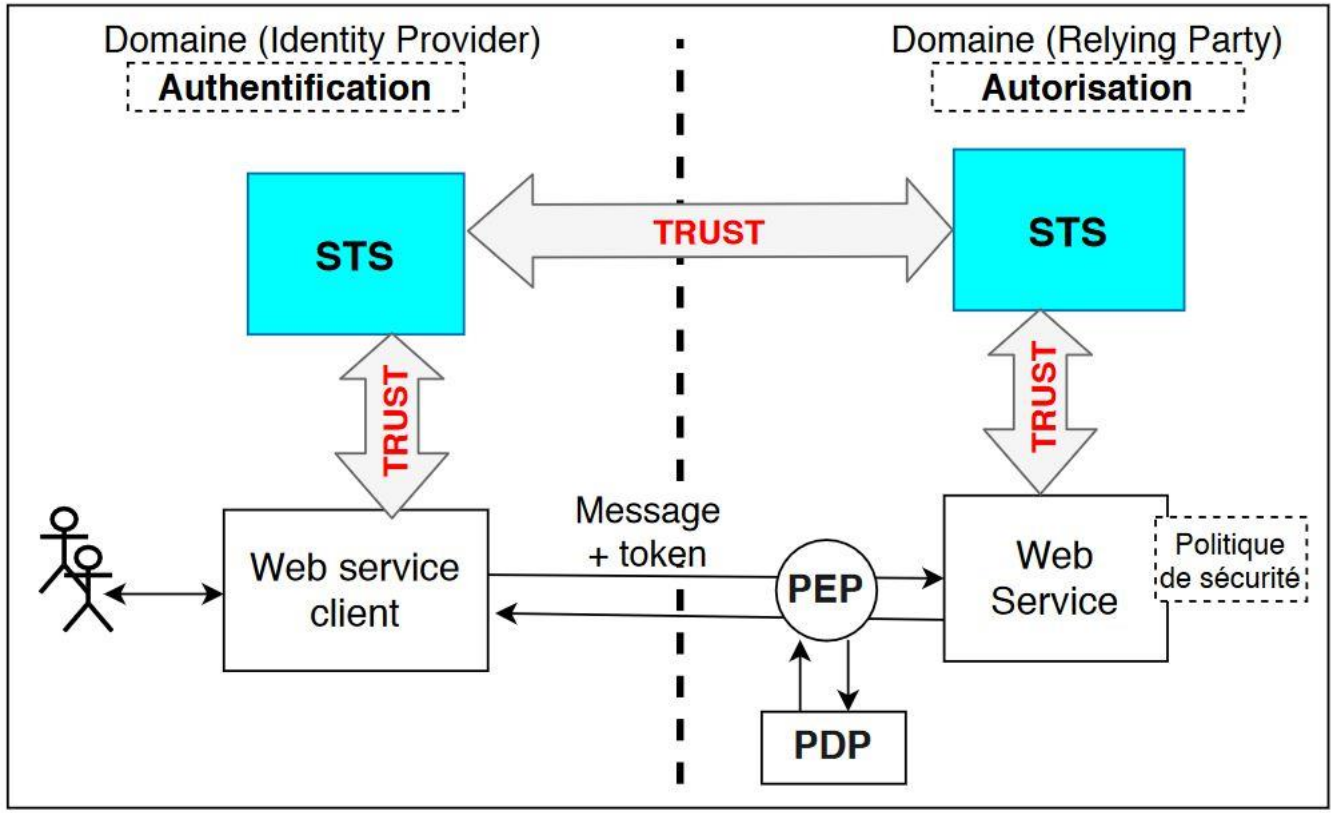
Architecture de contrôle d'accès fédéré (WS-Federation)

STS: Security Token Service

PEP: Policy Enforcement Point

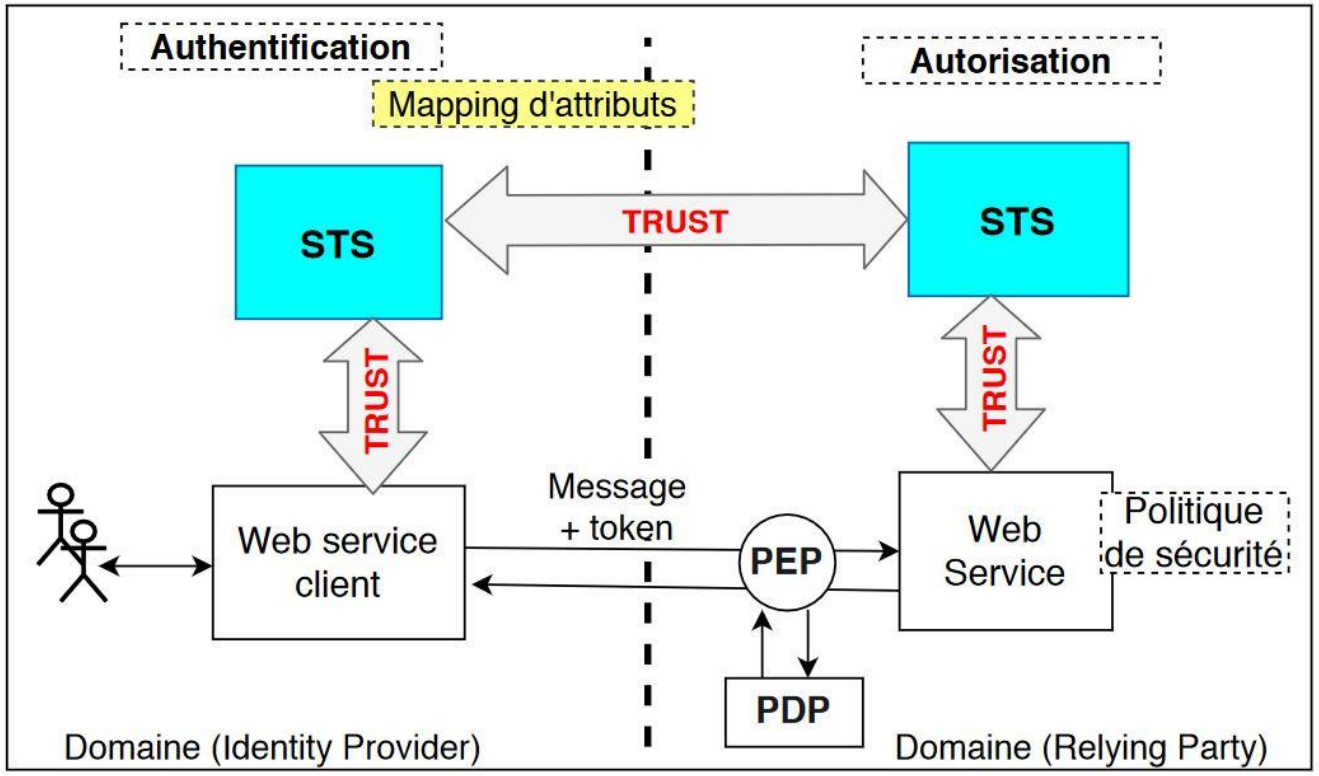
PDP: Policy Decision Point

STS (WS-Trust), PEP, PDP (XACML)



3.2. Contrôle d'accès fédéré basé sur le mapping

Nous proposons d'évaluer les politiques de mapping lors de **l'authentification** par les services de jetons de sécurité (STS)

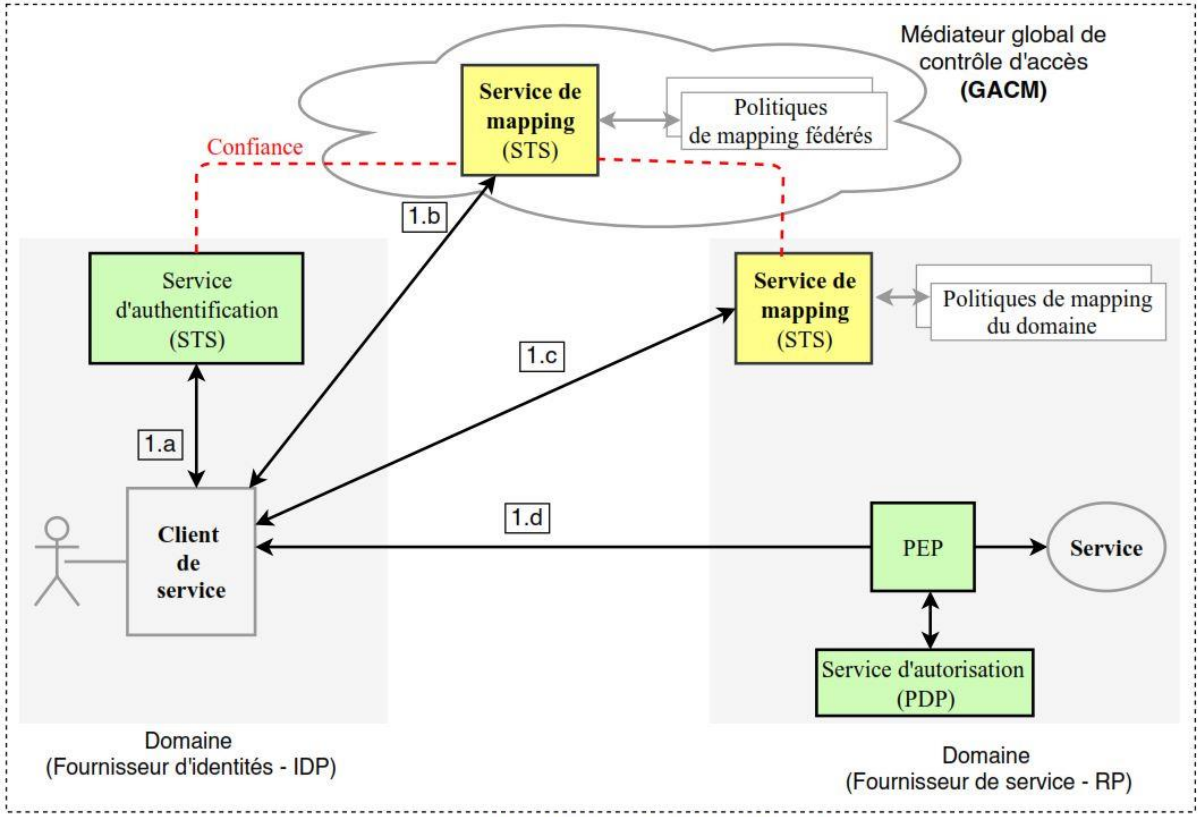


3.2. Contrôle d'accès fédéré basé sur le mapping

Nous proposons un nouveau type de service de jetons (STS) : le **service de mapping**

Fonctions d'un service de mapping

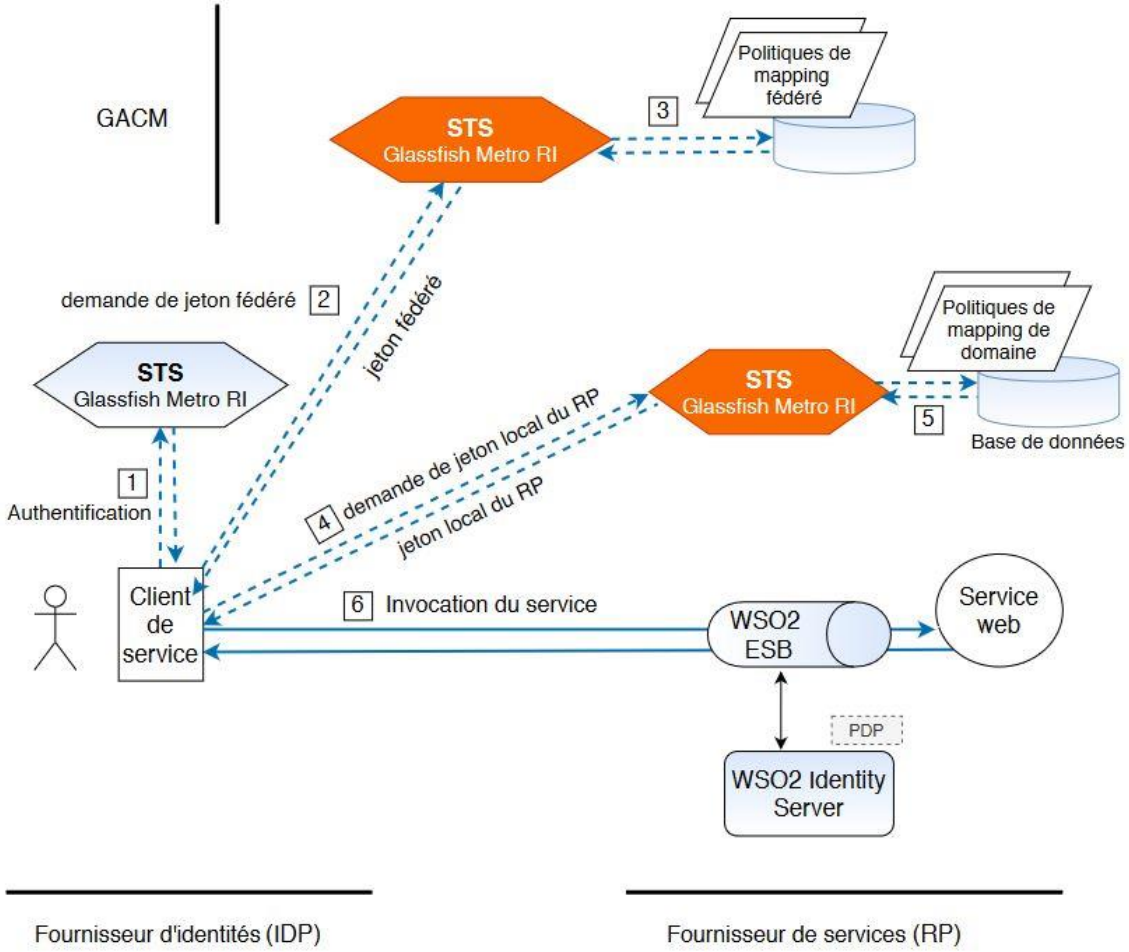
- émission, validation, conversion (**type** et contenu de jeton SAML), renouvellement et résiliation



3.2. Contrôle d'accès fédéré basé sur le mapping

Implémentation du contrôle d'accès

- **Services de sécurité:** implémenté par le STS de Glassfish Metro RI
- **Metro RI:** Une pile de services web, open source et extensible qui fait partie de GlassFish



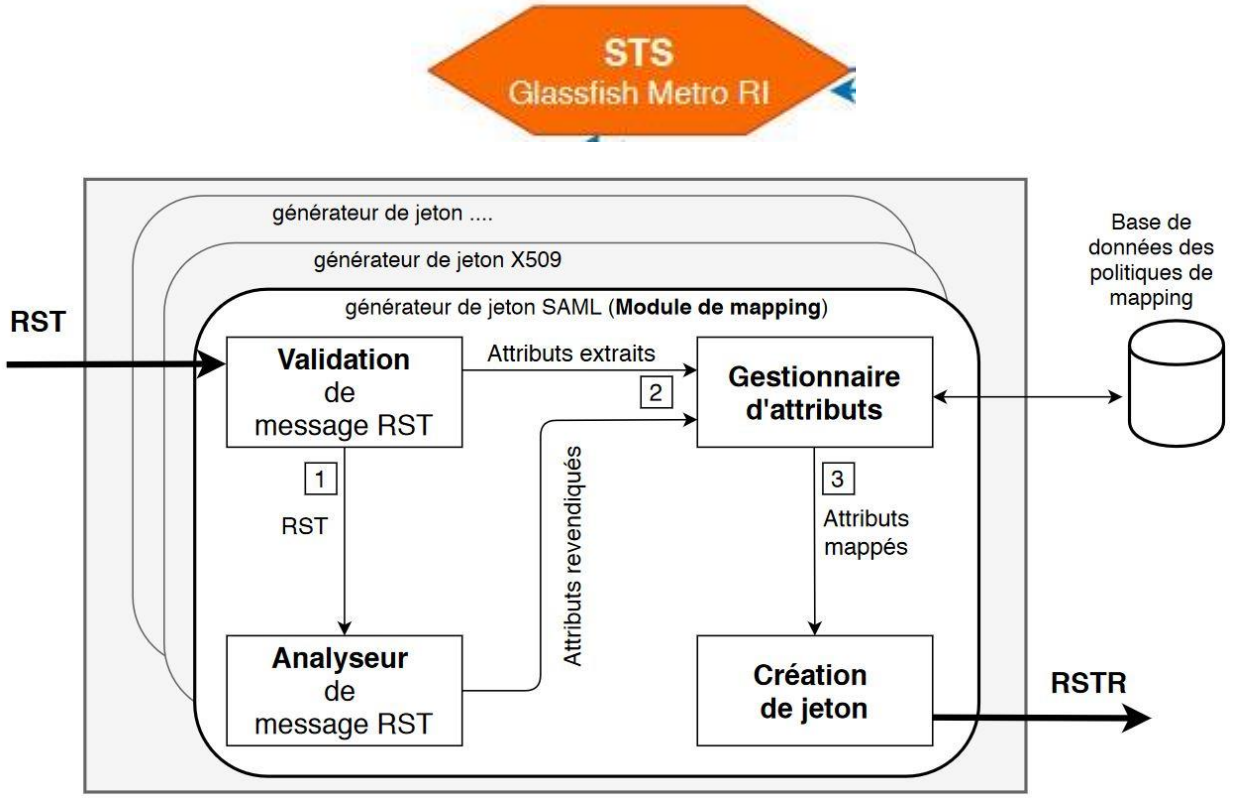
3.2. Contrôle d'accès fédéré basé sur le mapping

Implémentation du contrôle d'accès

Détails du service de mapping

- nous ajoutons un module de mapping

RST/RSTR (Request Security Token/ Request Security Token Response): protocole de demande de jeton de WS-Trust



3. Contributions

3.1. Notre méthode de mapping d'attributs
3.2. Contrôle d'accès fédéré basé sur le mapping

Ces deux contributions ont fait l'objet d'une **publication:**

- Federation of Services from Autonomous Domains with Heterogeneous Access Control Models- Abdramane Bah, Pascal André, J. Christian Attiogbé and Jacqueline Konaté-Information and Cyber Security - 18th International Conference (ISSA 2019) Springer, Communications in Computer and Information Science, Vol. 1166, pp. 83–98 2019,Johannesburg, South Africa

Contributions

Pour l'interopérabilité de contrôle d'accès

1. Une méthode de mapping d'attributs

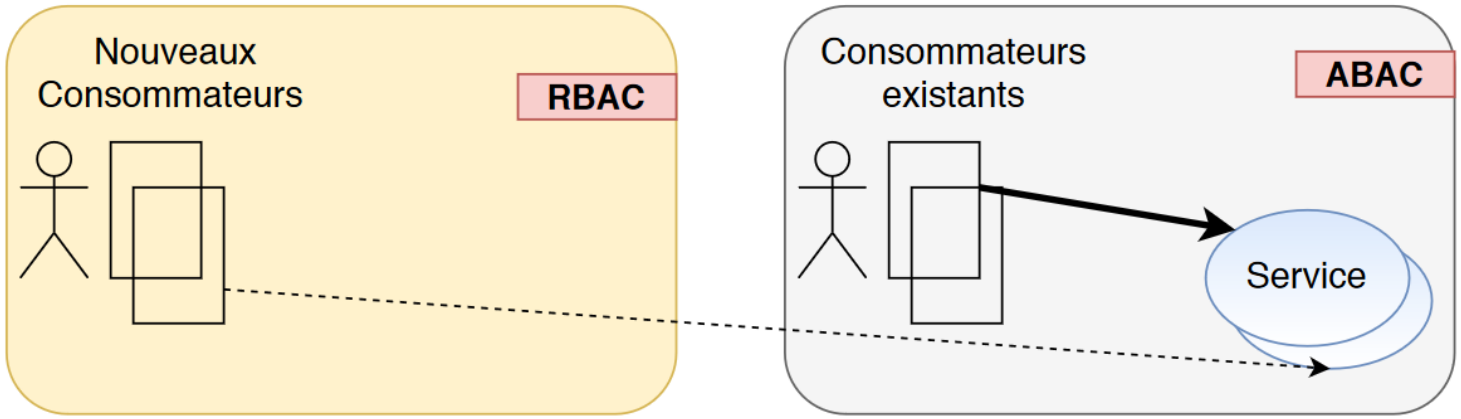
2. Un mécanisme de contrôle d'accès fédéré basé sur le mapping

Pour l'interopérabilité des services en termes de contrôle d'accès

3. Une nouvelle approche: **la promotion de services**

3.3. Promotion de services

Rappel: Comment assurer l'interopérabilité entre les services en termes de contrôle d'accès sans compromettre leurs consommateurs existants?



***RBAC**: Role-Based Access Control*

ABAC: Attribute-Based Access Control

3.3. Promotion de services

L'interopérabilité des services comporte trois aspects [DUAN et al, 2009]:

1. **Visibilité** : capacité de découvrir et localiser les services
2. **Accessibilité**: l'accès aux services basé sur les politiques prédéfinies
3. **Compréhension**: représentation et sémantique des données échangées

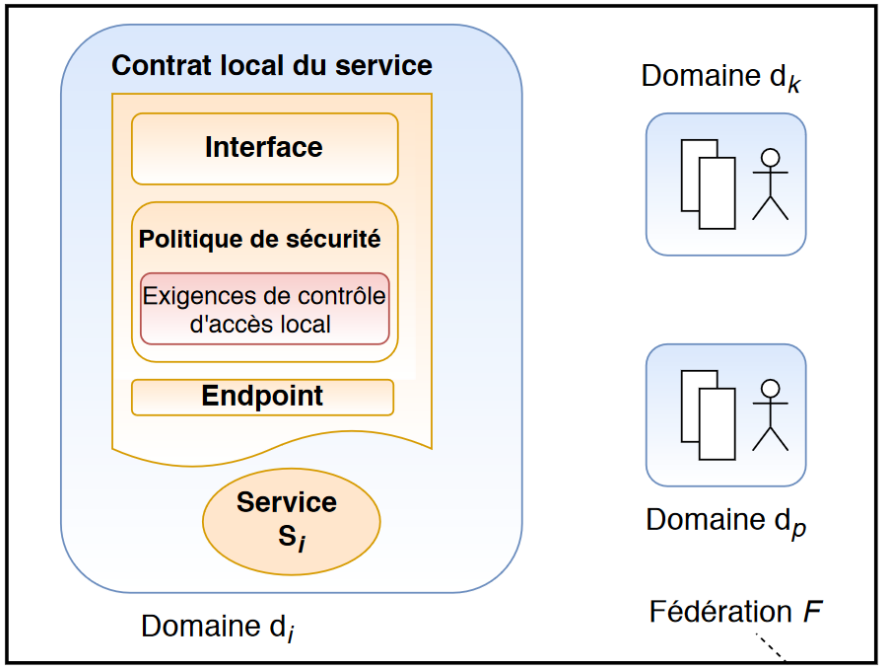
[DUAN, 2009] Duan, N.: Design Principles of a Federated Service-oriented Architecture Model for NetcentricData Sharing. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 6(4) (October 2009) 165–176

3.3. Promotion de services

Pour rendre les services interopérables dans la fédération:

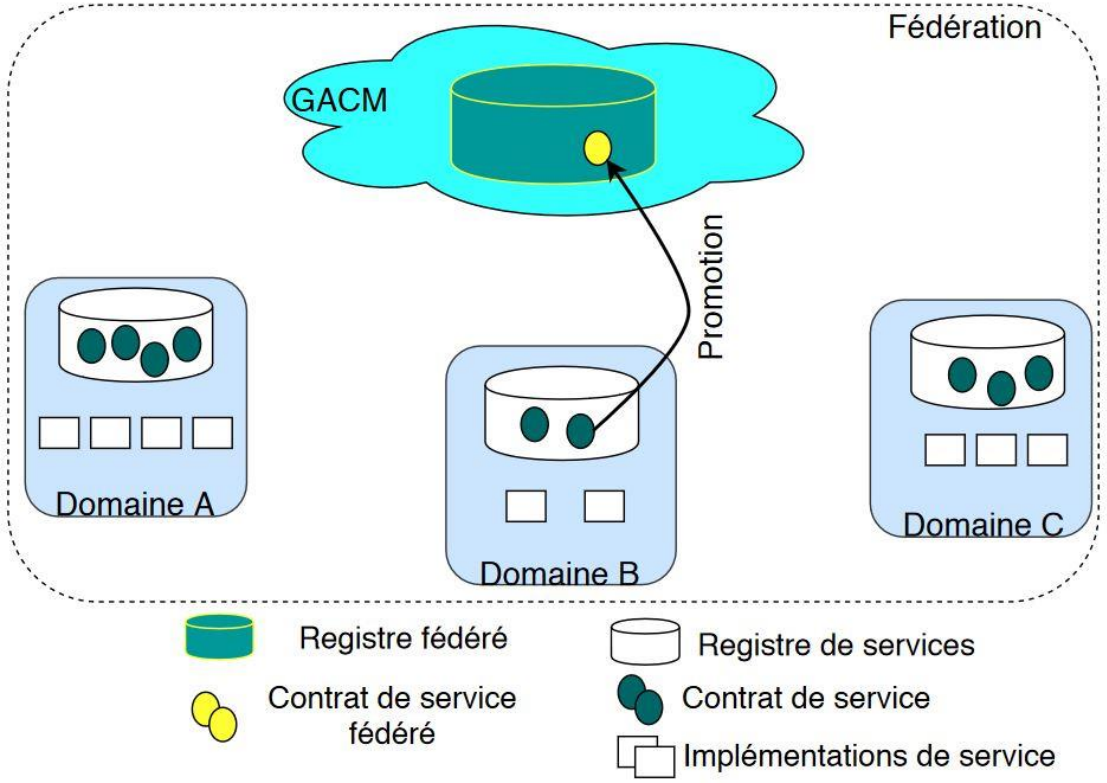
- nous proposons de redéfinir leurs exigences de contrôle d'accès (ACR) avec les **attributs fédérés** (AF)

Les (ACR) des services sont prédéfinies avec les **attributs d'autorisation** (AT) de leur domaines



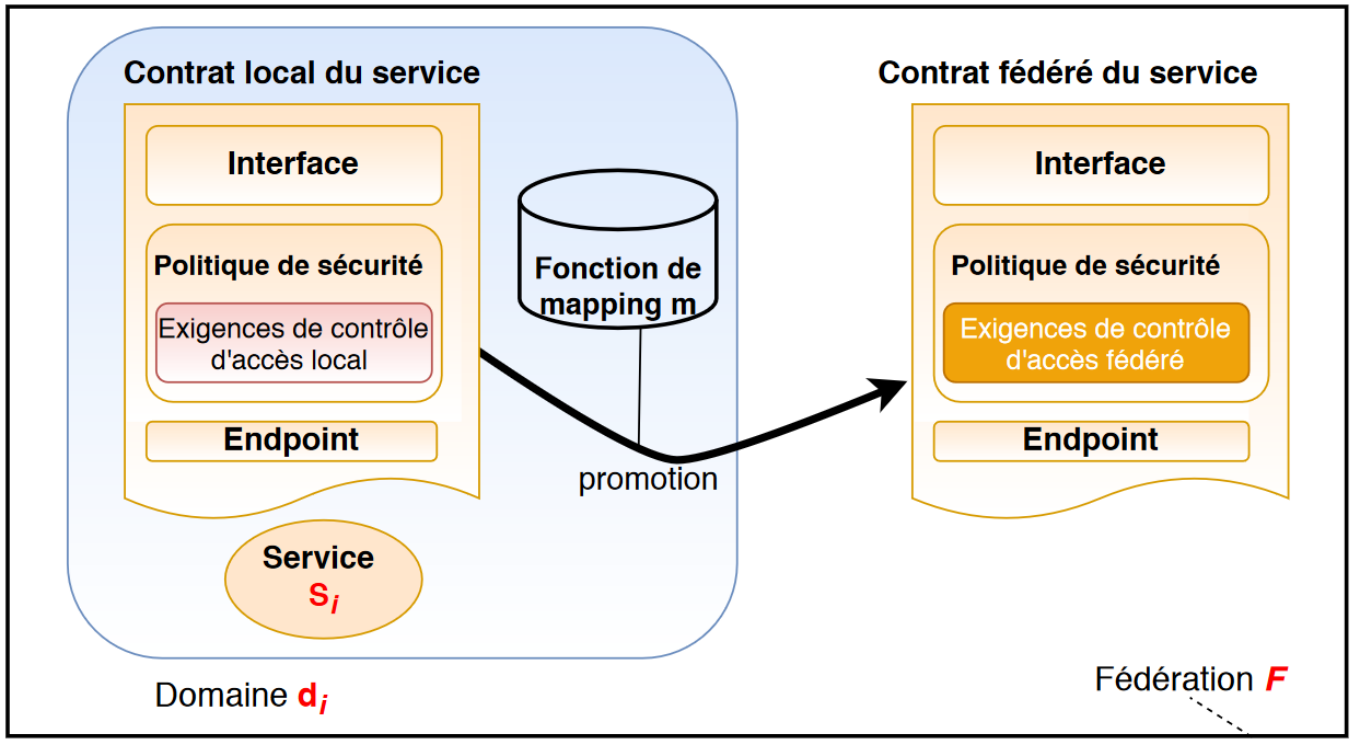
3.3. Promotion de services

- Chaque service partagé est à la fois dans le registre de services de son domaine et dans le registre fédéré
- Les services partagés ont deux contrats : local et fédéré



3.3. Promotion de services: les principes

Promouvoir un service s_i d'un domaine d_i dans la fédération F



Nous redéfinissons les exigences de contrôle d'accès local (ACR) avec les attributs fédérés (AF) pour créer les ACR fédérés.

Cette redéfinition est basée sur les politiques de mapping fédérés entre les attributs d'autorisation (AT) du domaine d_i et les attributs fédérés (AF) de **F**

3.3. Promotion de services: Formalisation

Principes de formalisation: définition formelle des services, des domaines, des conditions et contraintes d'accès etc...

- avec les règles de la **sémantique opérationnelle**
- afin de garantir l'accès sécurisé aux services promus

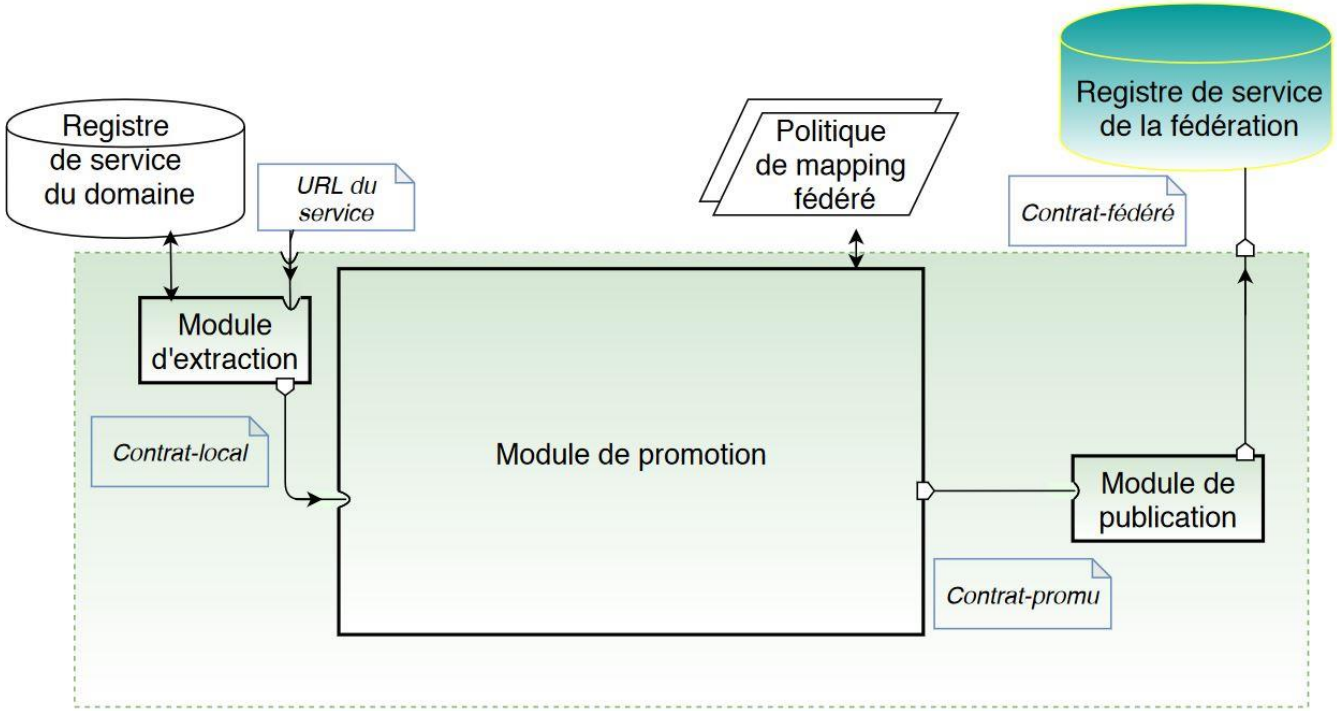
Cette formalisation a fait l'objet d'une **publication**

- qui sera présentée à la conférence CARI'2020: African Conference on Research in Computer Science - Colloque Africain sur la Recherche en Informatique (CARI 2020) October 2020, Thiès, Senegal, www.cari-info.org

3.3. Promotion de services: implémentation

Pour valider les principes de promotion, nous proposons:

- Un mécanisme de promotion de service avec trois modules logiciels en Java

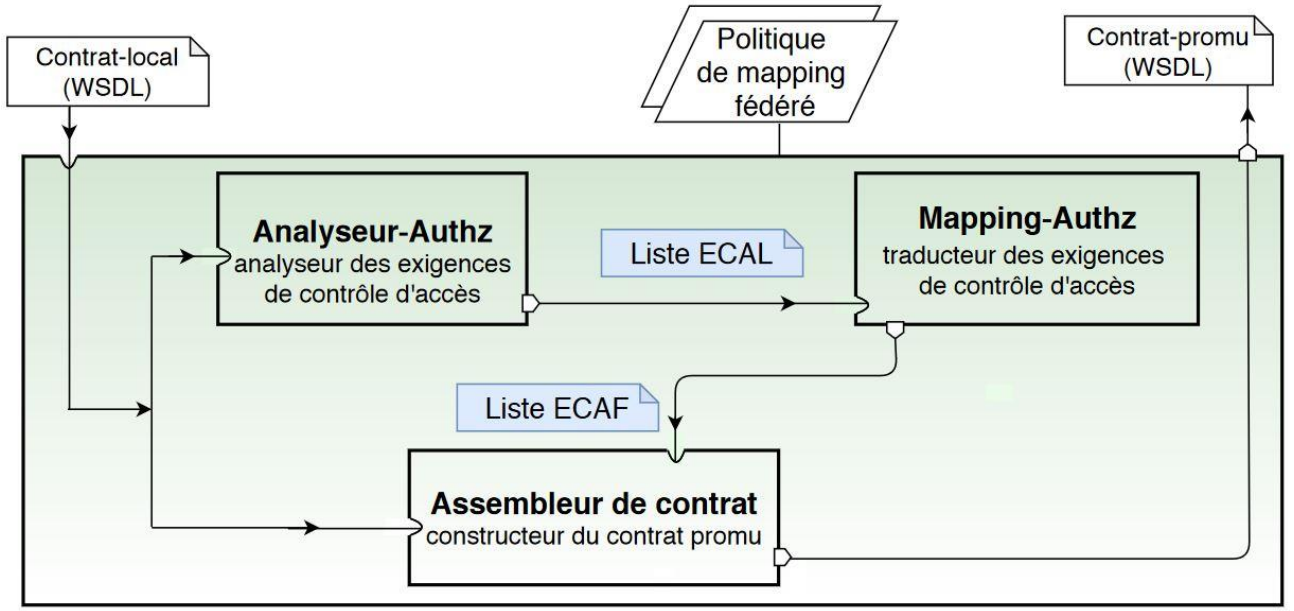


3.3. Promotion de services: implémentation

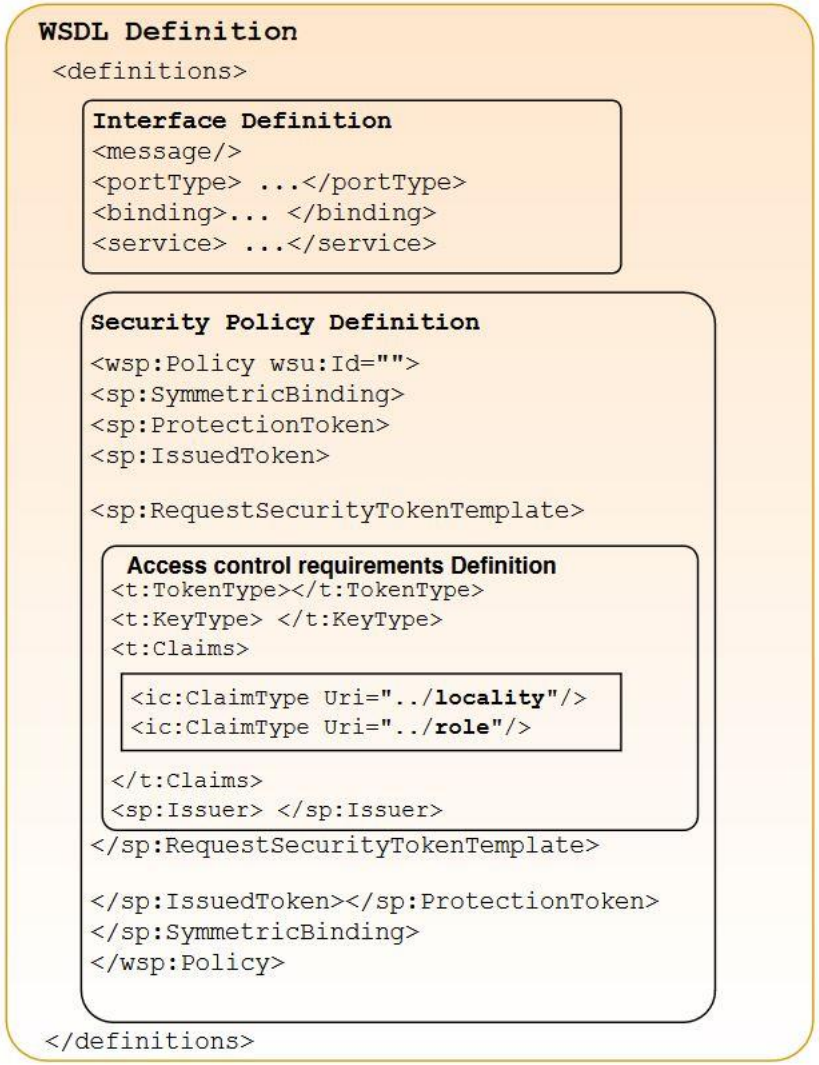
Module de promotion de services

ECAL: Exigences de contrôle d'accès local

ECAF: Exigence de contrôle d'accès fédéré



3.3. Promotion de services: illustration

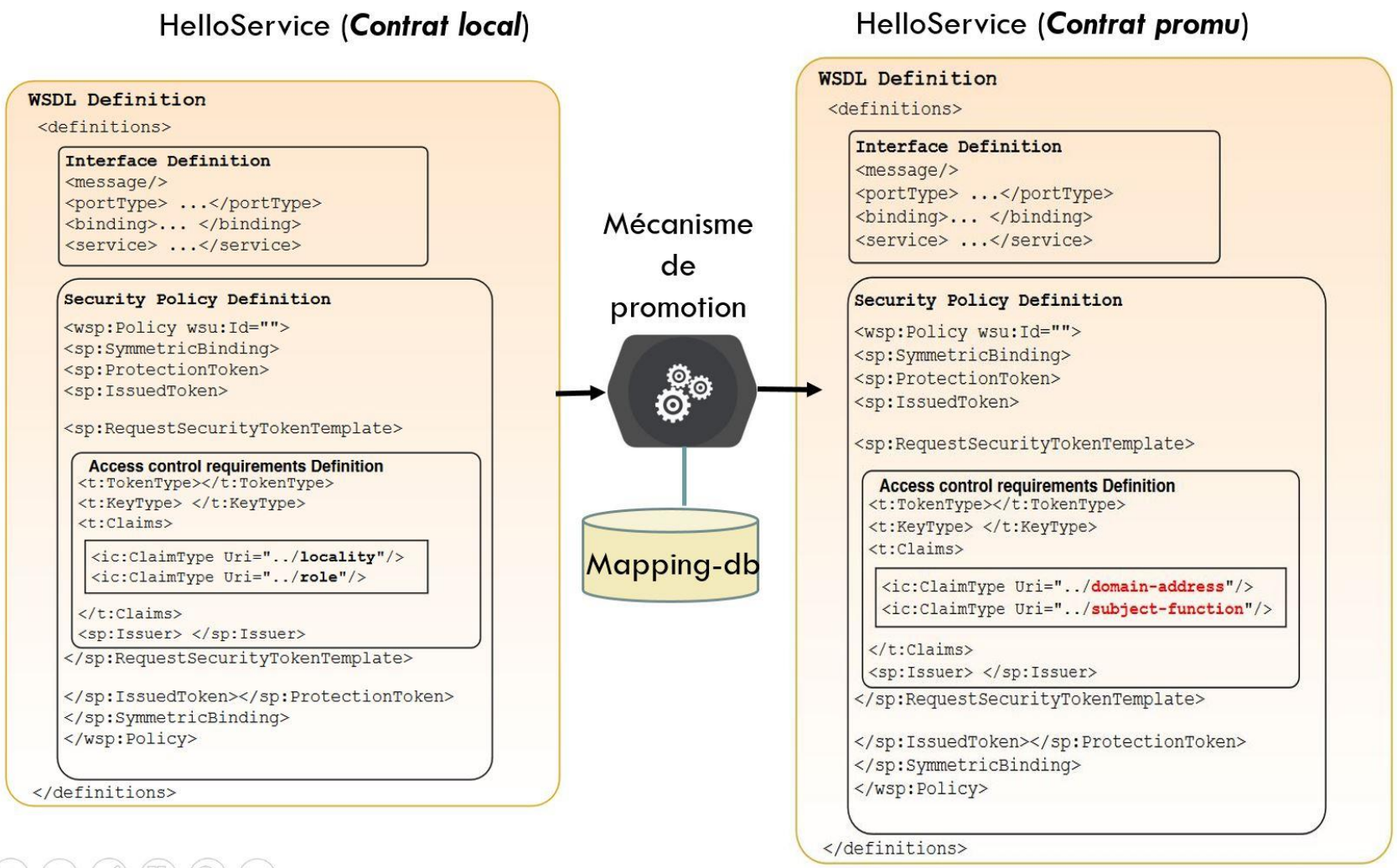


Nous illustrons la promotion du service avec un service web nommé **HelloService** fourni par le **domaine IUG**

HelloService nécessite un jeton de sécurité qui doit contenir certains attributs d'autorisation de l'utilisateur du service : rôle et localité.

HelloService doit être partagé dans la **fédération ICV** dont les attributs fédérés sont : domain-address, subject-function, subject-activitystatus.

3.3. Promotion de services: illustration



SOMMAIRE

1. Contexte
2. Problématique
3. Contributions
   1. Propositions
   2. Mise en œuvre
   3. Expérimentations
4. **Bilan et perspectives**

Résultats

(Q1) Interopérabilité de contrôle d'accès (modèles, mécanismes et attributs)

1. Une **méthode de mapping d'attributs** (améliore l'état de l'art)
   - Préserve l'autonomie des domaines
   - Facilite et favorise la participation à de nouvelles collaborations

2. Un **mécanisme de contrôle d'accès basé sur le mapping** (nouveau)
   - Supporte l'autorisation basée sur le mapping
   - Permet de préserver les mécanismes de contrôle d'accès existants des domaines

Résultats

(Q2) Interopérabilité des services en termes de contrôle d'accès

1. La promotion de services (nouveau)

- Assure la visibilité et l'accessibilité des services à plusieurs niveaux
- Plusieurs points d'accès sécurisés à un même service
- L'autonomie de sécurité n'est plus une barrière à la collaboration

Perspectives

1. Médiation des protocoles de fédération (e.g. SAML, WS-Federation) par le GACM (Interopérabilité inter-fédérations)

2. Langage de contrôle d'accès pour la définition des politiques de mapping

3. Extension des politiques de mapping avec des permissions individuelles

4. Intégration des mécanismes de sécurité des services web (e.g. WS-Trust) dans les moteurs d'orchestration de services fédérés

MERCI POUR VOTRE ATTENTION