Interopérabilité et sécurité des systèmes d'information: application aux systèmes de gestion de l'éducation

Abdramane BAH[1], Christian ATTIOGBE[1], Pascal ANDRE[1], Jacqueline KONATE[2]

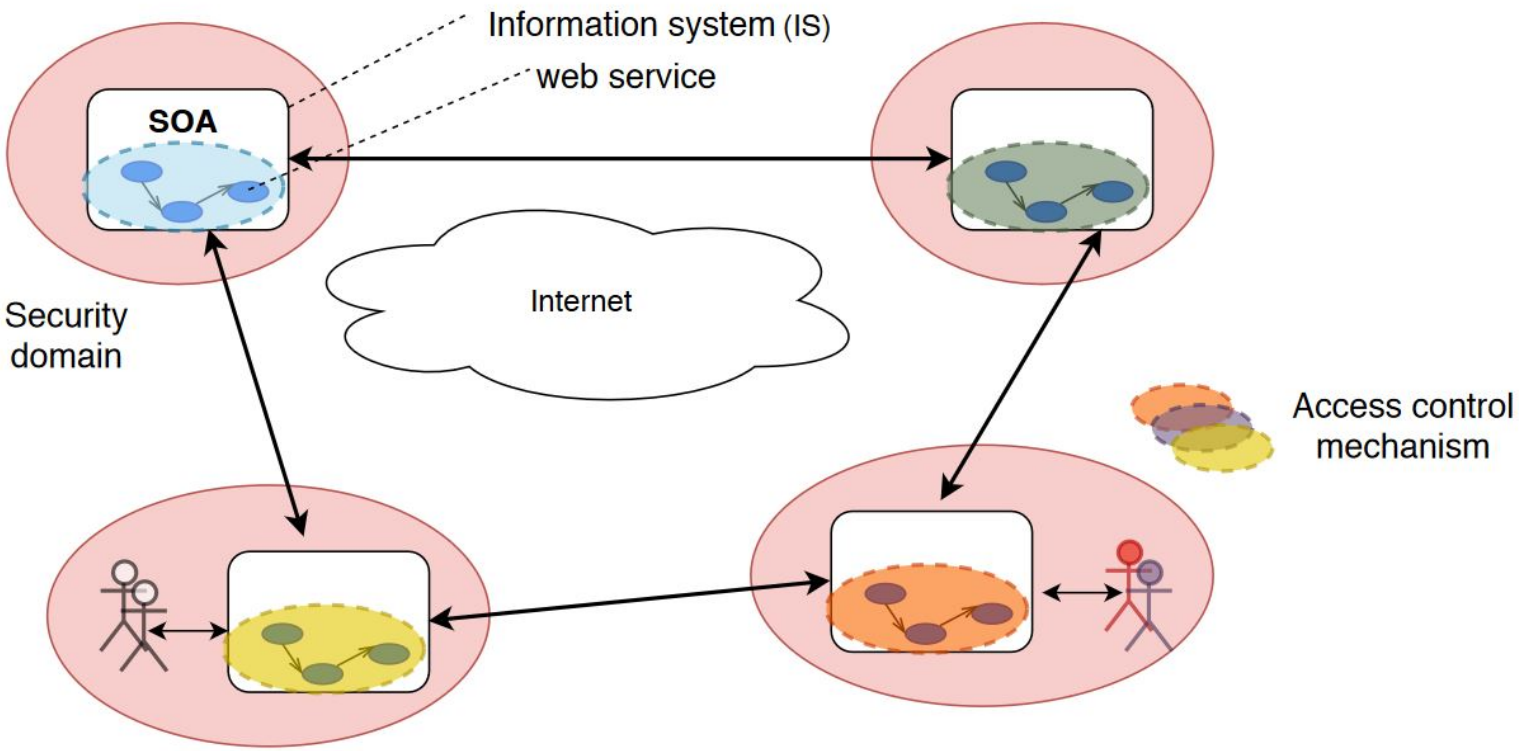
[1] LS2N - Université de Nantes(Equipe AELOS)
[2] Université des Sciences, des Techniques et des Technologies de Bamako (USTTB)

04 Avril 2019

Sommaire

Contexte et problématiques

L'architecture orientée services (SOA) via les services web permet de partager des informations et des ressources entre des domaines de sécurité indépendants.



Question de recherche : Comment vérifier les permissions des utilisateurs d'un domaine sur les services des autres ?

Défis et Objectifs

Défis :

1. garantir l'accès aux services malgré l'hétérogénéité des mécanismes de contrôle d'accès des domaines ;
2. garantir que l'accès aux services d'un domaine par des utilisateurs d'autres domaines ne nuira pas à leur sécurité.

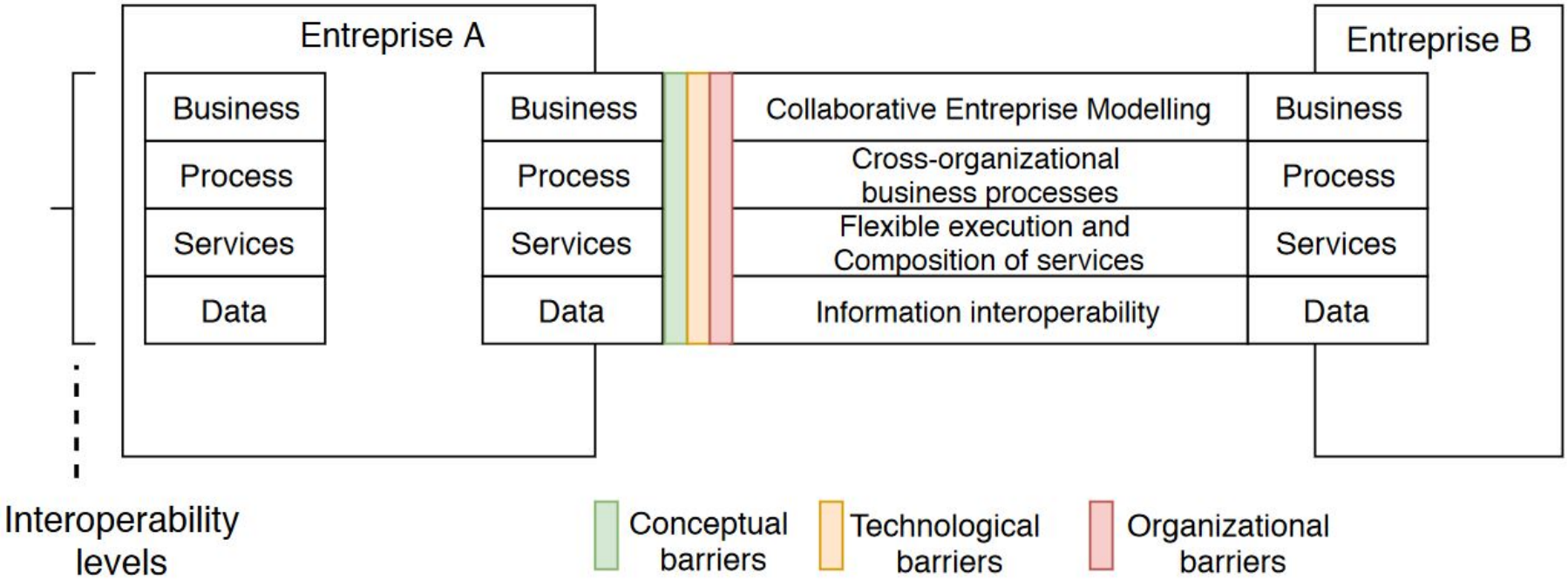
Objectifs :

mettre au point des mécanismes de contrôle d'accès inter-domaines pour :

1. accorder aux utilisateurs des permissions d'accès aux services des domaines ;
2. authentifier les utilisateurs et vérifier leurs permissions d'accès aux services.

Revue de littérature

Interopérabilité inter-domaine



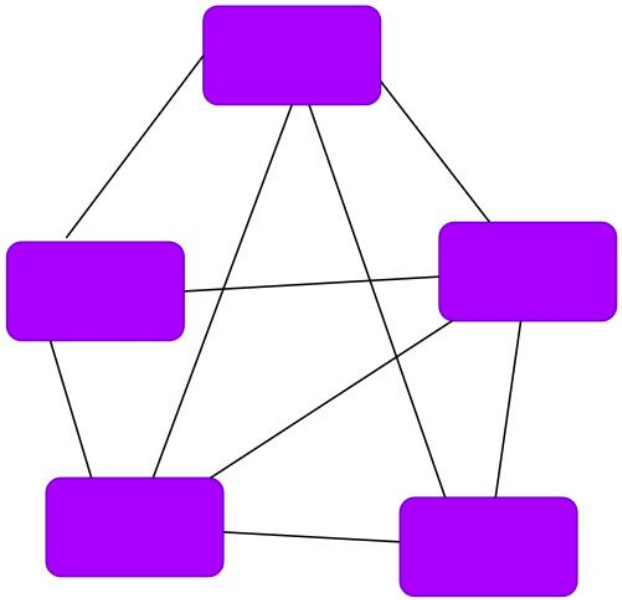
Approches : Standarisation (Intégrée, Unifiée), non-standarisation (Fédérée) [CD06] [Jih07]

Solution : Service-oriented architecture (SOA) [HF10]

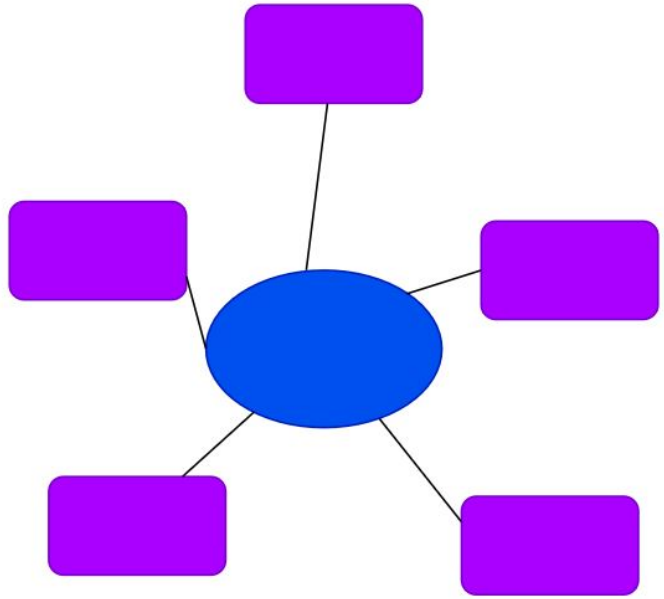
Interopérabilité inter-domaine

Cadre théorique de nos travaux :

- SOA, approche d'interopérabilité : fédéré ; topologie : multi-latérale.



Bi-lateral (point-to-point)



Multi-lateral

Le contrôle d'accès dans les environnements orientés services fédérés

Contrôle d'accès dans les environnements orientés services

Exigences pour le contrôle d'accès fédéré

- Authentification unique fédérée ;
- Autorisation unique fédérée ;
- Autonomie des domaines : contrôle d'accès décentralisé ;
- Adaptation dynamique à l'évolution de la fédération ;
- Confidentialité des informations de sécurité internes.

Limites des solutions existantes

- L'authentification unique limitée à deux domaines ;
- Hétérogénéité des modèles d'autorisation des domaines n'est pas prise en compte ;
- L'autorisation inter-domaine repose sur des mappings d'identité ;
- Le contrôle d'accès de la composition de services est complexe

Contributions

(1) Méthode de contrôle d'accès fédéré pour SOA

Pour répondre aux exigences de contrôle d'accès fédéré (page 8)

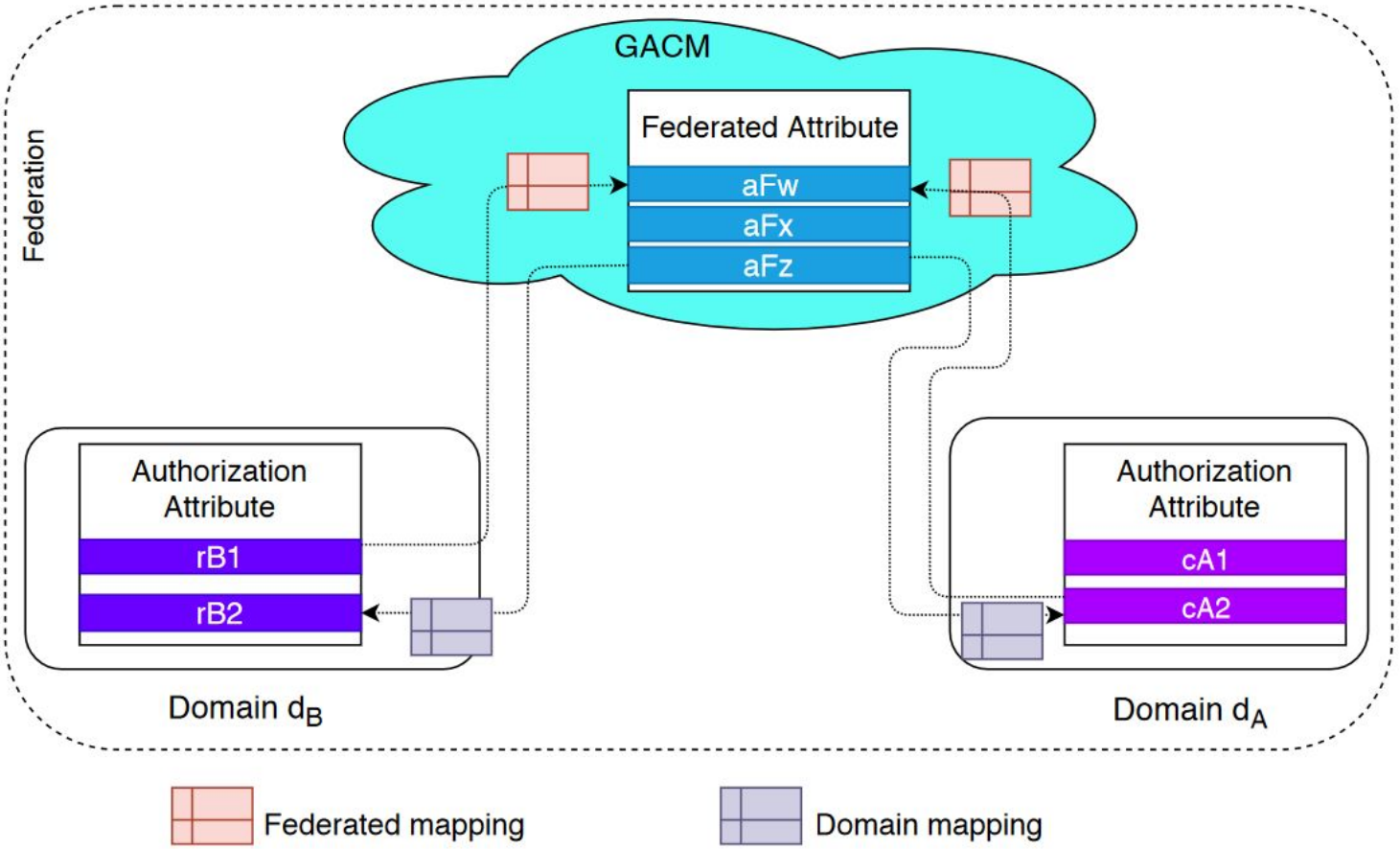
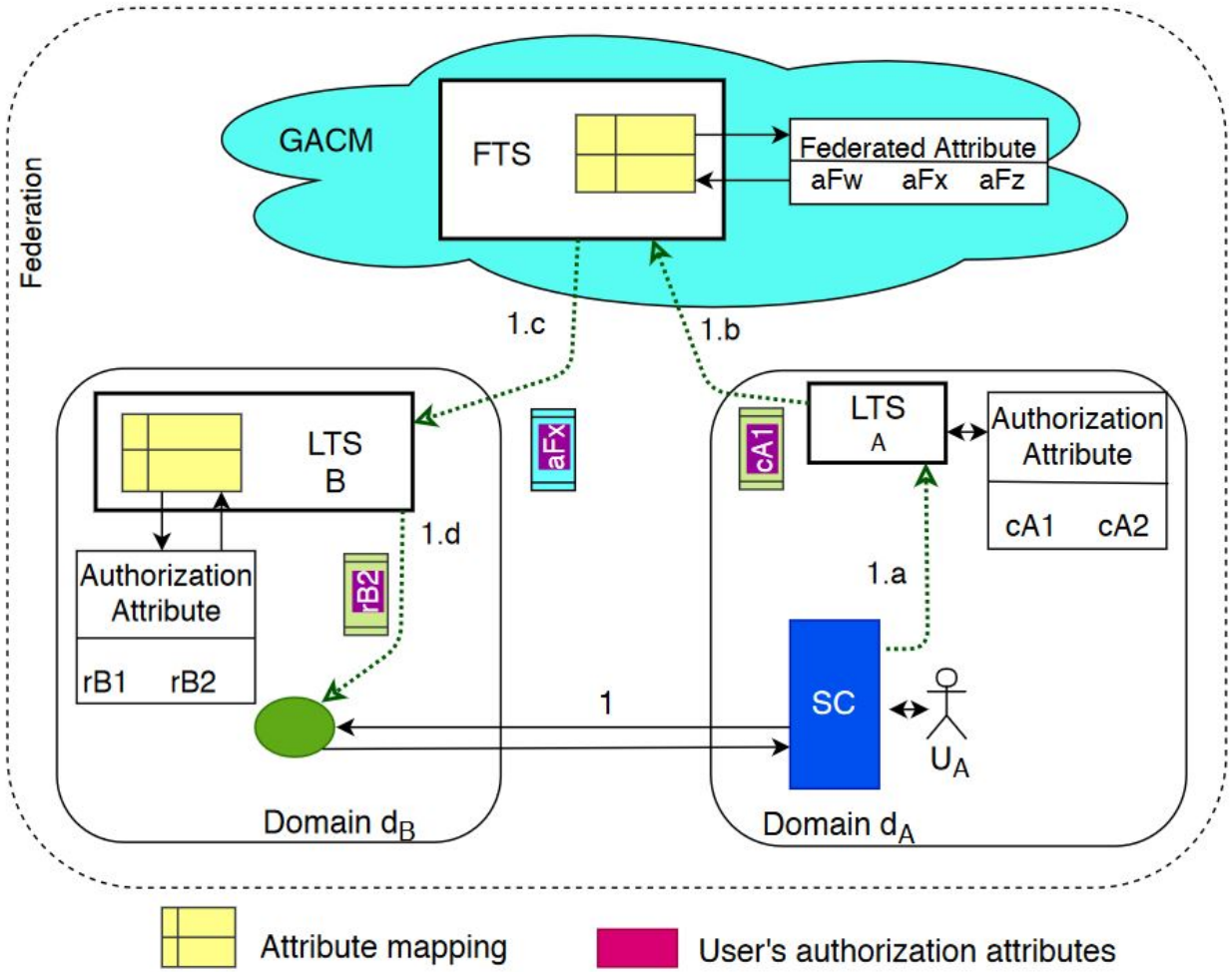


FIGURE – Architecture de contrôle d'accès proposée

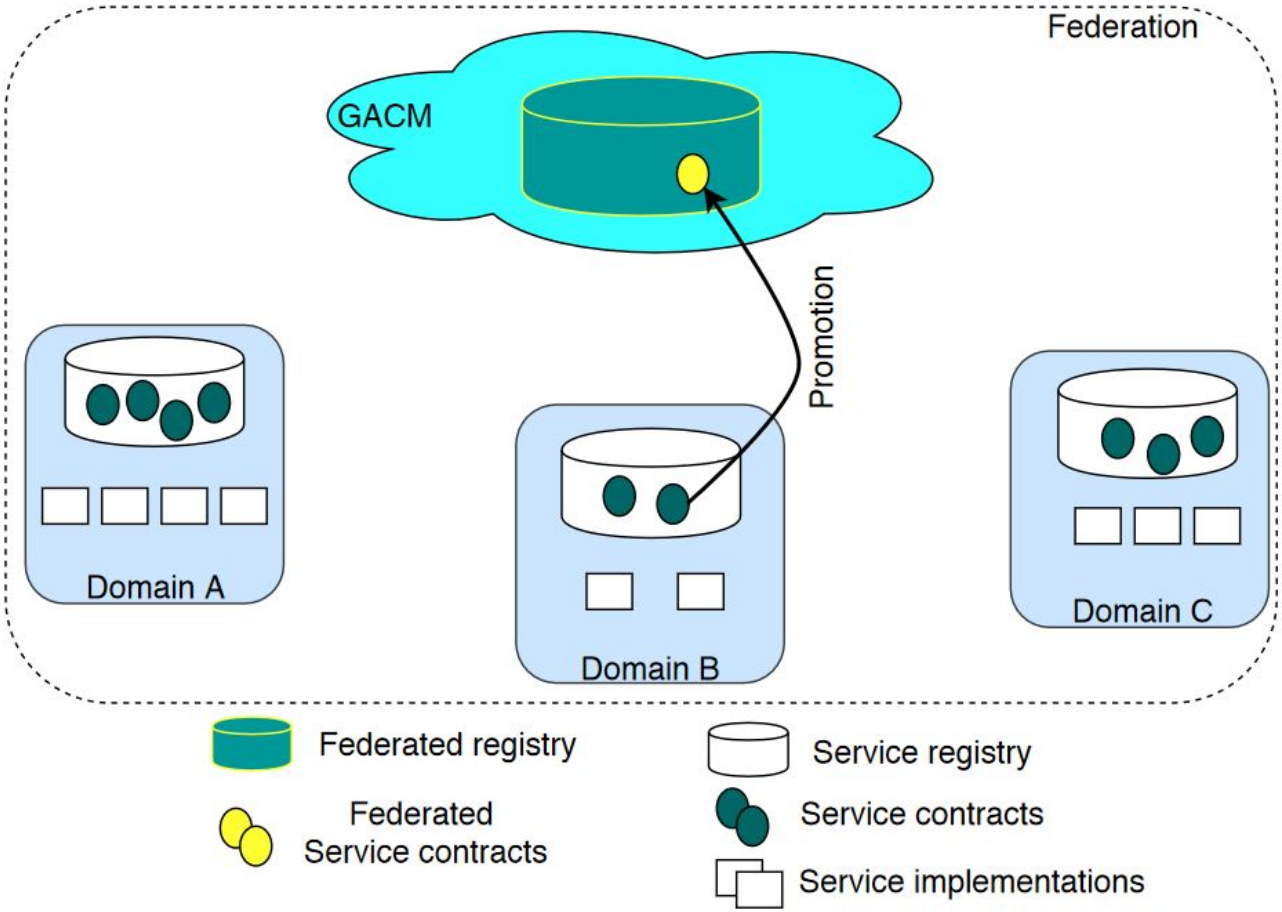
(1) Méthode de contrôle d'accès fédéré pour SOA

Séquence d'autorisation inter-domaine



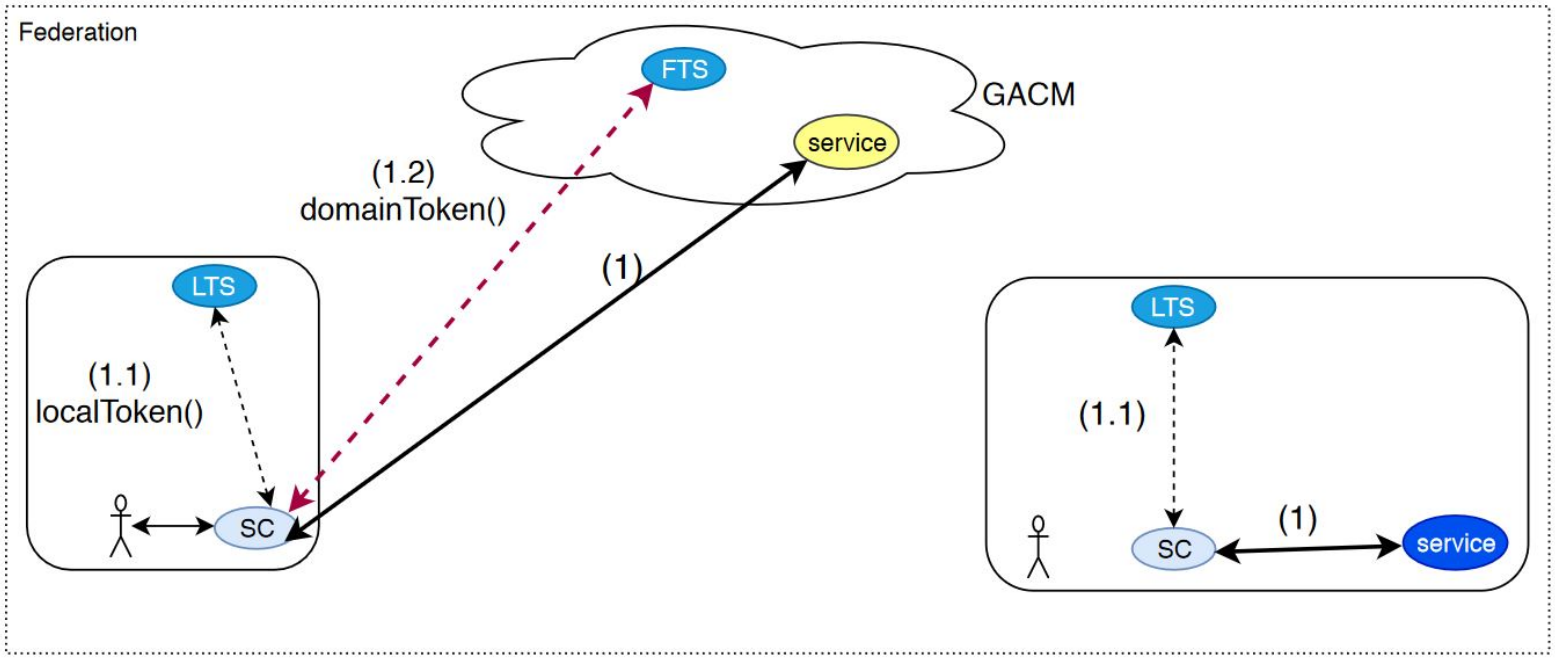
(2) Promotion des services dans la fédération (en cours)

Problématique : Visibilité des services dans la fédération



(2) Promotion des services dans la fédération (en cours)

Formalisation des appels de services avec la sémantique opérationnelle structurée



$$\frac{\begin{array}{c} d_i = \langle U_i, S_i, R_i, SS_i, SP_i \rangle \\ u \in U_i \quad s_1 \in S_i \\ s_2 \in S_i \quad s_2 = \langle I, ATQ, Edp \rangle \\ ss \in SS_i \quad tk = \text{localToken}(s_1, u, s_2, ss) \end{array}}{\text{CallAttempt}(s_1, u, s_2) \rightsquigarrow \text{SecureCall}(s_1, tk, Edp)} (intraDomainServiceCall)$$

Conclusion

Bilan

Travaux de la première année

(1) Étude bibliographique

- Contrôle d'accès
- Authentification des utilisateurs (Single Sign-On (SSO), Federated-SSO (F-SSO)
- Contrôle d'accès des services web

(2) Définition du cadre théorique

- Fédération de domaines
- Fédération d'identité (F-SSO) pour l'authentification
- Contrôle d'accès inter-domaine impliquant des modèles d'autorisation hétérogènes

(3) Rédaction de l'état de l'art (v.1)

Travaux de la deuxième année

(1) Définition de la 1^{ere} contribution

(2) Expérimentation du contrôle d'accès

- Services web (SOAP, WSDL, WS-Security, WS-Trust, SAML, XACML...)
- Sécurisation des services web : CXF, Axis2, Glassfish metro
- Framework de contrôle d'accès testés : WSO2, OpenAM,...
- Définition d'une architecture d'expérimentation

(3) Etat de l'art (v.2)

Perspectives

Bilan (suite)

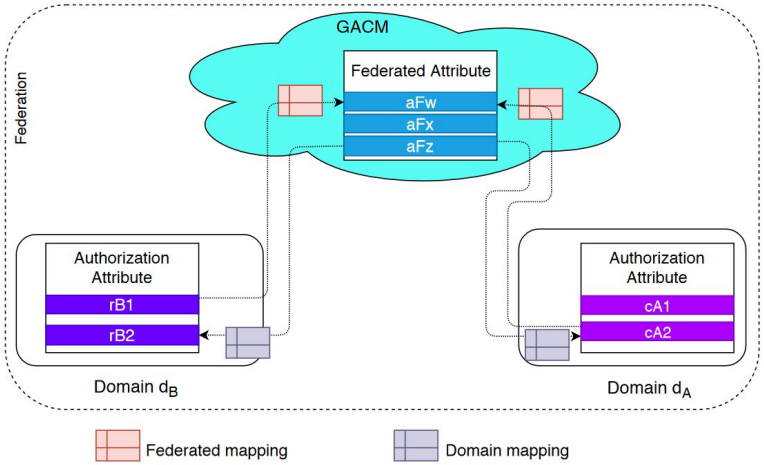
Travaux de la 3eme année

1. soumission de la première contribution ;
2. deuxième contribution en cours.

Plan prévisionnel pour la suite

1. définir le plan de rédaction du manuscrit ;
2. rédiger le manuscrit ;
3. terminer l'expérimentation du contrôle d'accès.

Perspectives



1. Médiation des protocoles de fédération (e.g. WS-Federation, Shibboleth) entre les domaines (troisième article) ;
2. Expérimentation du contrôle d'accès de la composition de services.

Références


David Chen and Nicolas Daclin.
Framework for enterprise interoperability.
In *Proc. of IFAC Workshop EI2N*, pages 77–88, 2006.


Mohammad Kazem Haki and Maia Wentland Forte.
Inter-Organizational Information System Architecture : A Service-Oriented Approach.
In Luis M. Camarinha-Matos, Xavier Boucher, and Hamideh Afsarmanesh, editors, *Collaborative Networks for a Sustainable World*, volume 336, pages 642–652. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.


TOUZI Jihed.
Aide à la conception de Système d'Information Collaboratif support de l'interopérabilité des entreprises.
phdthesis, INSTITUT NATIONAL POLYTECHNIQUE DE TOULOUSE, November 2007.