Service Promotion in a Federation of Security Domains

Abdramane Bah, Pascal André, Christian Attiogbé, Jacqueline Konate

Federation and Promotion of Heterogeneous Domains and Services

Abdramane Bah, Pascal André, Christian Attiogbé et Jacqueline Konaté

LS2N CNRS UMR 6004 - University of Nantes, France
FST-USTTB - University of Science and Technology of Bamako, Mali
{firstname.lastname}@ls2n.fr, jacqueline.konate@gmail.com

ABSTRACT. Service Oriented Architecture (SOA) implemented with web services technologies, provides standardised solutions to share services between various security domains. But acces control to services is defined for each domain, and therefore the federation of security domains brings some flexibility to users of the services. To facilitate the authentication of users, a solution is a federated access control that relies on the identity federation, which allows users to authenticate once in one domain and to access the services of others according to its authorisation attributes. Since the access control requirements of services are specified using domain-specific authorisation attributes, the secure sharing of services in the federation becomes a real challenge. On the one hand, domains cannot abandon their access control models in favour of a global one; on the other hand, the redefinition of the access control requirements of services compromises the existing service consumers. In this paper, we propose the promotion of services as a method that consists in publishing the services of domains at the federation level by redefining their access control requirements with the federation's authorisation attributes. Our promotion method relies on mappings between federation's authorisation attributes and those of domains to preserve existing service consumers and to support domain autonomy. We formally describe interaction and access to promoted services using operational semantics.

RÉSUMÉ. L'architecture orientée services (SOA), mise en œuvre par des services Web, fournit des solutions standards pour partager des services entre divers domaines de sécurité. Cependant, le contrôle d'accès aux services est défini au niveau de chaque domaine de sécurité, et par conséquent la fédération des domaines apporte une certaine souplesse aux usagers des services des domaines. Pour faciliter l'authentification des utilisateurs, une solution est le contrôle d'accès fédéré, basé sur la fédération d'identité et qui permet aux utilisateurs de s'authentifier une fois dans un domaine et d'accéder aux services des autres en fonction de ses droits et attributs. Malheureusement les exigences de contrôle d'accès des services sont spécifiées à l'aide d'attributs d'autorisation spécifiques au domaine, le partage sécurisé des services dans la fédération devient un véritable défi. Les domaines doivent à la fois être autonomes et interopérables vis-à-vis de la fédération. Dans cet article, nous proposons la promotion des services comme solution consistant à publier les services des domaines au niveau de la fédération en redéfinissant leurs exigences de contrôle d'accès avec les attributs d'autorisation de la fédération. Notre méthode de promotion repose sur des correspondances entre les attributs d'autorisation de la fédération et ceux des domaines pour préserver les clients hors fédération. Nous décrivons formellement l'interaction et l'accès aux services promus en utilisant des règles sémantiques opérationnelles.

KEYWORDS : Federated SOA, Service Federation, Web service, Access Control

MOTS-CLÉS : SOA, Fédération de service , Web service, Contrôle d'accès

1. Introduction

Service Oriented Architecture (SOA) implemented through web service technologies provides standardised solutions for sharing resources across organisational boundaries as services. Thus the federation of services from different independent organisations appears as a decentralised collaboration approach which allows the secure sharing of services between users in a trusted environment. However, every organisation in the federation is autonomous and has control over the security and the access to its services according to its own access control (**AC**) policies, such as *Role-Based Access Control* (RBAC), *Mandatory Access Control* (MAC), *Attribute-Based Access Control* (ABAC) [6].

Sharing services in the federation becomes a real challenge due to the AC requirements heterogeneity. On the one hand, the service consumers are not aware of all the AC requirements of services and they are not able to respond to them; on the other hand, the service providers cannot abandon their control models to a global AC model of the federation or map their model with those of all service consumers. In [2] we proposed a method to enable the interaction between independant domain services inside a federation, despite the heterogeneity of their access control mechanisms. However, there are two new issues related to the service sharing challenge in the federation. The first one is the need of a common definition for service access control requirements; the service federation requires that these requirements be defined with mechanisms that can be easily understood by all federated domains. The second issue is the lack of flexibility for discovering and composing despite their security mechanisms, the services defined inside the same federation. Indeed, without such flexibility which can ensure transparency of access, the involved services do not benefit from being in the same federation.

The contributions in this paper solve these issues. First, we propose a global mechanism to define shared access control requirements across the federation. Second, we propose a method for promoting services at the level of the federation without modifying the access modalities of the existing consumers of the services. This promotion is formally defined in order to ensure the secure access to services; it consists in transforming the existing service access control requirements with federated mechanisms in a way that the services can be discovered and used directly at the federation level.

The rest of the paper is organised as follows: in Section 2 we formally define the basic concepts of service contracts, security domains, federation of services and the federated service access control. In Section 3, we detail our method for promoting services at the federation level and the semantics of the access to both federated and non-federated services. Section 4 presents the implementation of our method with web service protocols. Related works are discussed in Section 5. We end with a conclusion in Section 6.

2. Service Sharing in a Federation: the Concepts

A service is a self-contained, self-describing processing logic unit for remote access to business information and functionality. A service has two separate parts[3]: a contract s_{cont} and an implementation s_{imp}. The service contract describes the functionalities offered by the service as well as its access policies (e.g. its security requirements); the service implementation achieves these functionalities. We define a *service contract* as a tuple $s_{cont} = \langle I, P_{R[X]}, Edp \rangle$ where I is the interface of the service, $P_{R[X]}$ its constrained policy and Edp the address on which the service receives message invocations; this address is called *endpoint*. I describes the set of operations provided by the service and the protocols used to access them. $P_{R[X]}$ describes the capabilities (e.g. supported encryption algorithms) and the requirements on the invocation message to access the service. We focus on the abstraction of its protection requirements in the form of authorisation attributes or terms $l_r \in R[X]$ where X is the set of attributes used to express the requirements R.

A ***security domain*** is a single unit of security administration; it can be a physical or logical unit; it consists of a set of elements (e.g. human users, applications, services), security authorities, and a security policy in which the elements are managed in accordance with the security policy [8]. A domain d_i is a tuple $\langle U_i, S_i, R_i, SP_i, SS_i \rangle$ where U_i is a set of users, S_i is a set of services, R_i is the service registry, SP_i is the security policy and SS_i the set of security services of d_i. R_i contains the subset of the services of S_i that are published. The permissions to access the services are defined and controlled using $SP_i = \langle AT, AR \rangle$ where AT is a set of the authorisation attributes of d_i and AR is a set of authorisation rules based on the attributes of AT (*e.g.*the rules describe which attributes a_k are authorised to access a service s_i: $\{(s_i, a_k)\}$). The security services SS_i include the authentication service named *local token service* (LTS), the authorisation service (ATS) and the interceptor $Interceptor$. These services are described in the next section. A user u_i of U_i is characterised by its authorisation attributes; $u_i = \langle uID, uAT \rangle$ where uID is his/her identity attributes (e.g. his/her name) and uAT is the set of authorisation attributes such as his/her role (e.g. teacher, manager, administrator).

The access control (AC) relies on two preliminary steps [7]: (1) identification and authorisation of users; (2) authentication of users. The first step consists in assigning an unique identifier and access permissions to users. The authorisation of users is done using AC models such as RBAC or ABAC. A domain's service AC is implemented by the three security services according to a XACML architecture [5] where the $Interceptor$ is the *policy enforcement point* (PEP) and the ATS is the *policy decision point* (PDP). The LTS authenticates the users and delivers a security token as authentication credential used to invoke the service. A *security token* represents a set of *claims* that are declarations made about the user's attributes.

The interoperability between domains requires common collaboration agreements and a secure trusted environment. In such a situation, the federation is one recommended solution [14]. A ***federation of domains*** F is a set of autonomous domains that adhere to common rules and governance policies to control interactions between them [4]. To have an uniform definition with a domain, we define a federation F of n domains $d_i = \langle U_i, S_i, R_i, SP_i, SS_i \rangle$ by the tuple $F = \langle U_f, S_f, R_f, SP_f, SS_f \rangle$ where U_f is the union of domain users ($U_f = \bigcup_{i=1}^{n} (U_i)$); SP_f is the security policy and SS_f the security services of the federation. Initially S_f and R_f are empty. The federation of services consists in sharing the services of the domains in a federation. A ***federated service*** is a service of a domain published at the federation level, and thus, available to other domains. However, in order to federate the domain services, it is necessary to take into account also the AC of users from outside the definition domain of the services. Since each domain is autonomous, the user's authorisation attributes of the domains defined separately can be different or have different semantics for each domain of the federation. This heterogeneity constitutes a challenge for the access control. To overcome this challenge, we have proposed in [2] a method of inter-domain AC for the secure federation of services. This method is based on a federation architecture in which we introduced a new essential component at the federation level: the ***Global Access Control Mediator*** (GACM). The GACM defines the authorisation attributes of the federation called the *federated attributes* (AF) that are independent of those of the domains. The security policy (SP_f) of the federation is made of the federated attributes and a set of authorisation rules (FR) associated to these attributes ($SP_f = \langle AF, FR \rangle$). Initially, FR is empty because the federation F does not dictate domain service access permissions. Federated domains keep the control on their authorisation rules. The federated attributes are used to make mappings between the authorisation attributes of the domains in order to allow AC between them. To achieve the attribute mappings and to establish trust across domains, we introduced an authentication service called *federated token service* (FTS) in SS_f at the level of the GACM.

3. Promotion of Domain Services in the Federation

The services shared by the domains must be visible in a single location at the federation level to facilitate their discovery and composition inside the federation. Redefining service access control requirements with federated attributes is called the *promotion of service*; it must be transparent to existing consumers of the shared services.

Assume we have n domains $d_i = \langle U_i, S_i, R_i, SP_i, SS_i \rangle$, ($i = 1 \ldots n$) that wish to collaborate in a federation $F = \langle U_f, S_f, R_f, SP_f, SS_f \rangle$. The promotion will (1) *Set up the GACM*. The GACM includes the security services that enforce the security policies of the federation. Initially, the security services SS_f include only the FTS, and the security policy SP_f includes only the federated attributes defined in common agreement between the domains. The FTS provides authentication and trust management across domains. The GACM hosted and managed by one of the federated domains, provides secure access to the services that will be shared across domains. (2) *Federate the users of the domains.* The federation of users or *identity federation* allows users to access services from different domains using an unique identity. To federate users, on the one hand the domains negotiate with the GACM to establish the mappings between their authorisation attributes and the federated attributes; on the other hand, they establish locally the mappings between the federated attributes to their authorisation attributes. The federated domain users are initialised with $\bigcup_{i=1}^{n}(U_i)$. From now, we denote by $d_i \sqsubset F$ that a domain d_i is member of a federation F. The federation does not have services yet, $S_f = \{\}$.

To facilitate the discovery and the use of shared services, we need a service registry at the federation level: the *federated (service) registry* R_f. The federated domains will publish in this registry the contracts of the services they wish to share with the federation.

To promote a service s in the federation F, we create a new federated service contract s_{fcont} from the existing service contract $s_{cont} = \langle I, P_{R[AT]}, Edp \rangle$. The AC requirements $R[AT]$ of the existing service contract should be redefined using the federated attributes $af_j \in AF$ to create the access control requirements of the federated service contract. Considering that an AC requirement is a *term* t_r built with the domain authorisation attributes $at_i \in AT$, the AC requirement for the federation results in transforming the domain attributes at_i in t_r with the federated attributes af_j. This results in AC requirements $R[AF]$ for the federated service policy $P_{R[X]}$. The mappings m between the domain authorisation attributes AT and the federated ones AF are already defined in the domains as functions: $m : AT \rightarrow AF$; they are basically, sets of couples $\{(at_i, af_j)\}$.

A federated service authorisation requirement is obtained by transforming each term t_r found in the existing service contract with the mapping m; this results in a set of terms built with AF: $R[AF]$. The federated service contract $s_{fcont} = \langle I, P_{R[AF]}, Edp \rangle$ is then published in the service registry of the federation (see Figure 1) which contains the services s_f promoted by the domains ($\exists d_i \sqsubset F \wedge s_f \in S_i$); they are called the *federated services* instead of *promoted services* in order to be aligned with federated attributes $R_f =$

$\{s_f, ...\}$. The implementation of a federated service remains in the domain that provides it. The promotion process is summarised in appendix A.

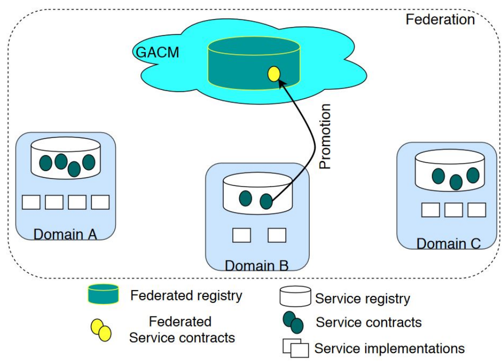

Figure 1. *Overview of service promotion*

The federated services are considered as provided by the federation represented by the GACM. Not all the services of a domain are visible at the federation level. We distinguish two categories of services: (1) the *local services*; (2) the *federated services*. The local services are published only in the service registry of the domains; they are shared at the domain level. The AC requirements of a local service are specified with the domain authorisation attributes. As a result, accessing to local services outside their definition domains requires a common understanding of the authorisation attributes of all the others domains of the federation. The federated services are published in the service registry of the federation. The AC requirements of federated services are specified with the authorisation attributes of the federation that are understandable by all domains. The federation of services facilitates the use and composition of the services of different domains in terms of access control. In addition, the federation of services is transparent to service consumers because it does not change the services calling rules. We formalise, with semantic rules, the processing of the calls of the two categories of services. The semantic rules are listed in appendix B.

4. Implementation of the Promotion of Services

Web services technologies such as SOAP, WSDL, UDDI provide a SOA implementation through standard internet protocols (e.g. HTTP). A web service contract is described using the WSDL, WS-Policy, and WS-SecurityPolicy standards [1] providing a framework to specify the service policy [3]. The interest of SOA is noticeable when reusable services can be composed to create new services or applications.

The services of each domain are implemented with the SOAP, WSDL and UDDI web service technologies. Service contracts are described with WSDL and the service's security policies; the access control requirements are specified with the WS-SecurityPolicy standard. The promotion of services which involves a local domain and the federation is implemented with three software modules (Figure 2) and involves the following steps:

– the module *extract-mod* extracts the WSDL contract (*localContract*) of the service to be promoted from the service registry of the local domain;

– this contract (*localContract*) is passed to the module *promotion-mod* to obtain the promoted service contract (*promotedContract*);

– the promoted contract (*promotedContract*) is published by the module *publish-mod* as a federated service in the service registry of the federation. The federated service has additional information about the domain that is not in the promoted service contract.

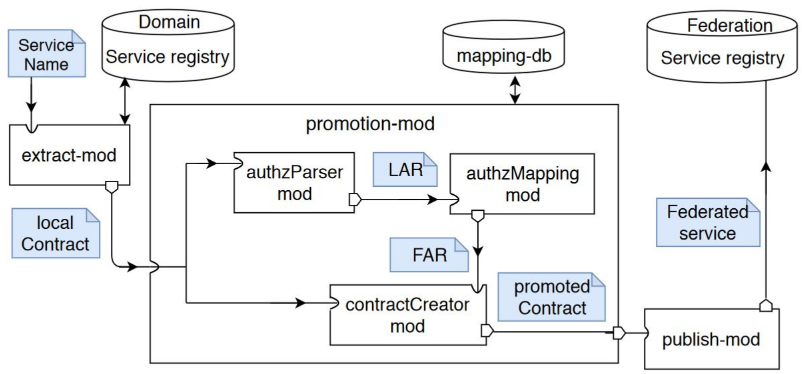

Figure 2. *Overview of the implemented software modules to achieve service promotion*

We implemented the *promotion-mod* module in Java using the Java API for XML Processing (JAXP). Its three sub-modules are: (1) the access control requirements parser *authzParser-mod*; (2) the access control requirements mapping module *authzMapping-mod* and (3) the promoted service contract construction module *contractCreator-mod*. The sub-module *authzParser-mod* receives as input the *localContract* and it outputs the list of access control requirements named *LAR* contained in this file. The *LAR* list contains the access control requirements specified with the domain-specific authorisation attributes and possibly the attributes of the domain's LTS implemented with WS-Trust. Then, the *LAR* list is passed as input to the sub-module *authzMapping-mod* which computes another list of access control requirements (named *FAR*) specified with the authorisation attributes of the federation. The mapping between the authorisation attributes of the domain and those of the federation is already defined in the mapping database *mapping-db* of the domain. The *FAR* list is transmitted as input to the *contractCreator-mod* sub-module which creates the *promotedContract* from the *localContract* by replacing the access control requirements in the *LAR* by the access control requirements given in the *FAR*. An illustration example of the service promotion is given in Appendix C.

5. Related Work

One main concern about service sharing in a federation is how to make domain services available to the service consumers in other domains. The authors in [13] argue that a federation is not supposed to define a centralised service registry and it is not desirable to publish or search in the service registry of each domain; which can be cumbersome with a large number of registry and published services. They propose the communication between the service registries of the domains through notification messages of interest or availability of services satisfying a given description. Sellami et al. [12] propose to organise service registries as communities according to the functionalities of the services they advertise in order to reduce the search space of service consumers. A service registry can belong to different communities at the same time with different degrees of membership. Compared to these techniques, we gather the services into the service registries (central and local) according to the description of their security properties. The service discovery is thus well targeted and effective in the federation. In [15] an approach similar to ours is given for the service discovery in ubiquitous computing. In their agent based system, when a service search fails in a (domain) Directory Agent (DA), that registers Service Agents records, the request is sent to one of the Federation Guide (our GACM) which returns a list of (DA) likely to respond. The service consumers no longer need to know the details of all domains providing the services, they only need those of the federation.

WS-SecurityPolicy, WS-Trust and WS-Federation provide standard mechanisms for expressing the security requirements of the services. The heterogeneity comes from AC models and the authorisation attributes of domains. Preuveneers et al. [10] have proposed to align the authorisation attributes of domains by declaratively defining equivalence relations between their names and their values. The authors in [6] proposed to make the service AC at the consumer side based on collaboration contracts as proposed in [9]. While this approach preserves the autonomy of domains in terms of security, it is difficult to adapt domains to the authorisations changes at service providers side. The mapping of attributes was also proposed in [11]. It consists in transforming the local attributes using derivation rules to federated attributes, which are attributes defined by the domains but recognised by the federation. The federated attributes used in our approach are defined by the federation and are independent from the authorisation attributes of the domains. Using federated attributes, the same service can be shared locally, and in different federations, using heterogeneous security informations; we ensure the autonomy of domains in terms of securing services, while minimising dependencies with the federation.

6. Conclusion

To meet the challenge of sharing and composing securely the services inside a federation of heterogeneous domains, we have proposed the promotion of services outside their definition domains. The services promoted by the domains become federated services. With our promotion technique, the usage of promoted services remains simple and transparent within the federation. To master the secure access to services and their composition, we have formally defined the interaction and the access to services (federated or not), using operational semantic. We have implemented, as a proof of concept, the proposed promotion of services in JAVA with the JAXP API. The services are implemented with SOAP, WSDL and UDDI web service technologies. The service access control policies are specified with WS-SecurityPolicy. We applied it to a WSDL contract of a secure service whose authorisation requirements are specified in accordance with the WS-Trust specification. A primary benefit of the promotion of services is to easily create applications and new services by composing federated services with their security requirements. Our experimentations confirm that service promotion breaks barriers to service interoperability through the expression of service access control requirements with a common agreed upon dialect of the federation.

As for perspectives, it would be more convenient to use or extend the dialect used in one federation; for this purpose, a standard dialect like that of the WS-Federation specification could be adapted. To gain more accuracy, we plan to experiment with the calling rules of federated services on the basis of the authorisation conditions that we have defined. This will then be reused for studying the performance of the secure composition of federated services and evaluate its relevance for large distributed applications across federations.

7. References

Aruna S and VIT Vellore. Security in Web Services- Issues and Challenges. *International Journal of Engineering Research and*, V5(09):IJERTV5IS090245, September 2016.

Abdramane BAH, Pascal André, Christian Attiogbé, and Jacqueline Konaté. Federation of Services from Autonomous Domains with Heterogeneous Access Control Models. In *18th International Information Security for South Africa Conference*, Johanesbourg, August 2019.

Elisa Bertino, Lorenzo Martino, Federica Paci, and Anna Squicciarini. *Security for Web Services and Service-Oriented Architectures*. Springer, 2010.

Nick Duan. Design Principles of a Federated Service-oriented Architecture Model for Net-centric Data Sharing. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 6(4):165–176, October 2009.

David Ferraiolo, Ramaswamy Chandramouli, Rick Kuhn, and Vincent Hu. Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC). In *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control - ABAC '16*, pages 13–24. ACM Press, 2016.

Samira Haguouche and Zahi Jarir. Managing Heterogeneous Access Control Models Cross-Organization. In Javier Lopez, Indrajit Ray, and Bruno Crispo, editors, *Risks and Security of Internet and Systems*, volume 8924, pages 222–229. Springer, Cham, 2015.

Vincent C. Hu, David Ferraiolo, and D. Richard Kuhn. Assessment of access control systems. Tech. Report NISTIR 7316, National Institute of Standards and Technology, September 2006.

International Telecommunication Union. *Baseline identity management terms and definitions*, 04 Avril 2010.

Michael Menzel, Christian Wolter, and Christoph Meinel. Access control for cross-organisational web service composition. *Journal of Information Assurance and Security*, 2(3):155–160, 2007.

D. Preuveneers, W. Joosen, and E. Ilie-Zudor. Policy reconciliation for access control in dynamic cross-enterprise collaborations. *Enterprise Information Systems*, 12(3):279–299, 2018.

Carlos E. Rubio-Medrano, Ziming Zhao, Adam Doupe, and Gail-Joon Ahn. Federated Access Management for Collaborative Network Environments: Framework and Case Study. In *Proc. of the 20th ACM Symposium on Access Control Models and Technologies - SACMAT '15*, pages 125–134. ACM Press, 2015.

Mohamed Sellami, Olfa Bouchaala, Walid Gaaloul, and Samir Tata. Communities of Web service registries: Construction and management. *Journal of Systems and Software*, 86(3):835–853, March 2013.

Ignacio Silva-Lepe, Isabelle Rouvellou, Rahul Akolkar, and Arun Iyengar. Cross-domain service management for enabling domain autonomy in a federated SOA. In *2010 International Conference on Network and Service Management*, pages 475–480. IEEE, October 2010.

Zhiying Tu, Gregory Zacharewicz, and David Chen. A federated approach to develop enterprise interoperability. *Journal of Intelligent Manufacturing*, 27(1):11–31, February 2016.

Yuanmin Chen, Wei Mao, and Xiaodong Li. Federation framework for service discovery in ubiquitous computing. In *2008 11th IEEE International Conference on Communication Technology*, pages 600–602, Hangzhou, China, November 2008. IEEE.

A. Promotion Process

Preliminary. We have a mapping function m between the authorisation attributes AT_i of the domain d_i and the federated attributes AF_j; $m : AT_i \to AF_j$. We generalise the application of the mapping function to a set of elements by using the notation *map*(m, s_a) where s_a is a set of attributes. The *map*(m, s_a) results in a set s'_a of attributes. We also use the converse function m^{-1} in the same way. ACR stands for access control requirements. Promoting a service $s_i = \langle I, P_{R[AT_i]}, Edp\rangle$ of $d_i = \langle U_i, S_i, R_i, SP_i, SS_i\rangle$ where $SP_i = \langle AT_i, AR_i\rangle$ with $AT_i = \{at_u\}\, u \in 1..q \wedge q \in \mathbb{N}$, $AR_i = \{(s_u, at_v)\}\, u, v \in \mathbb{N}$ into the federation $F = \langle U_f, S_f, R_f, SP_f, SS_f\rangle$, consists in performing the following steps.

– Copy the service contract $\langle I, P_{R[AT_i]}, Edp\rangle$ of s_i from the service registry R_i;

– Isolate the local ACR terms $R[AT_i] = \{t_1, t_2, ...\}$ from $P_{R[AT_i]}$; each term is an ACR specified with the local authorisation attributes $at_u \in AT_i$;

– Transform $R[AT_i]$ into the federated ACR $R[AF_f]$ by applying m on the set of terms $R[AT_i]$ to change the attributes $at_u \in AT_i$ with the federated attributes $af_j \in AF_f$: *map*$(m, R[AT_i])$;

– Create a new federated service contract $s_{fcont} = \langle I, P_{R[AT_f]}, Edp\rangle$ with the federated ACR $R[AT_f]$;

– Publish the service contract s_{fcont} in the service registry R_f of the federation F.

The following rule formally defines the promotion of domain services in the federation:

$$\frac{\begin{array}{c} F = \langle U_f, S_f, R_f, SP_f, SS_f\rangle \\ d_i = \langle U_i, S_i, R_i, SP_i, SS_i\rangle \qquad s_i = \langle I, P_{R[AT_i]}, Edp\rangle \\ d_i \sqsubset F \wedge s_i \in S_i \qquad R[AF_f] = map(m, R_l) \\ s_j = \langle I, P_{R[AF_f]}, Edp\rangle \end{array}}{F = \langle U_f, S_f, R_f \cup \{s_j\}, SP_f, SS_f\rangle} (\text{promotion}, d_i, s_i)$$

B. Promotion rules

In the following semantic rules, the function *localToken*(s_i, u_i, s_j, ss_i) is used to get the local security token st_i delivered by a security service ss_i on behalf of the user u_i to call a service s_j from a service s_i; *domainToken*(s_i, tk_i, s_j, ss_j) is used from the service s_i of a domain d_i to request a security token tk_j required by a service s_j from the security service ss_j of another domain d_j of the federation F on behalf of a user of a domain d_i authenticated by its local security token tk_i. The expression *CallAttempt*(s_i, u, s_j) denotes a call attempt to a service s_j from a service s_i on behalf of a user u, and *SecureCall*(s_i, tk, s_k) denotes the secured call by providing the required token tk. Finally, in the semantic rules, the symbols $\rightsquigarrow$ means "*results in*".

When a service s_1 of a domain d_i calls another service s_2 of the same domain d_i on behalf of an authorised user u of d_i, then the security token associated to u by the service security ss of d_i is used to call s_2.

$$\frac{\begin{array}{c} d_i = \langle U_i, S_i, R_i, SS_i, SP_i \rangle \\ u \in U_i \quad s_1 \in S_i \quad s_2 \in S_i \\ s_2 \in R_i \quad s_2 = \langle I, P_{R[AT_i]}, Edp \rangle \\ ss \in SS_i \quad tk = \mathit{localToken}(s_1, u, s_2, ss) \end{array}}{\mathit{CallAttempt}(s_1, u, s_2) \ \rightsquigarrow \ \mathit{SecureCall}(s_1, tk, Edp)} (\mathit{intradomainLocalServCall})$$

Local services can still be called by authorised domains; that is an inter-domain service call. When a service s_i of a domain d_i calls on behalf of a user u_i of d_i a service s_j of another domain d_j of the federation F, then the security token tk_j obtained from the security service ss_j of d_j with the local security token tk_i associated with the user u_i by the security service ss_i of d_i, is used to call the service s_j of d_j.

$$\frac{\begin{array}{c} F = \langle U_f, S_f, R_f, SS_f, SP_f \rangle \\ d_i = \langle U_i, S_i, R_i, SS_i, SP_i \rangle \quad d_i \sqsubset F \\ d_j = \langle U_j, S_j, R_j, SS_j, SP_j \rangle \quad d_j \sqsubset F \\ u \in U_i \quad s_i \in S_i \quad s_j \in S_j \quad ss_i \in SS_i \\ s_j \notin R_f \quad s_j = \langle I_j, P_{R[AT_j]}, Edp_j \rangle \\ tk_i = \mathit{localToken}(s_i, u, s_j, ss_i) \\ ss_j \in SS_j \quad tk_j = \mathit{domainToken}(s_i, tk_i, s_j, ss_j) \end{array}}{\mathit{CallAttempt}(s_i, u, s_j) \ \rightsquigarrow \ \mathit{SecureCall}(s_i, tk_j, Edp_j)} (\mathit{interdomainLocalServCall})$$

Federated Services Calls. When the service s_j of d_j is a federated service, then the security token used to call s_j is obtained from the security service ss_f of the federation.

$$\frac{\begin{array}{c} F = \langle U_f, S_f, R_f, SS_f, SP_f \rangle \\ d_i = \langle U_i, S_i, R_i, SS_i, SP_i \rangle \quad d_i \sqsubset F \\ d_j = \langle U_j, S_j, R_j, SS_j, SP_j \rangle \quad d_j \sqsubset F \\ u \in U_i \quad s_i \in S_i \quad s_j \in S_j \quad ss_i \in SS_i \\ s_j \in R_f \quad s_j = \langle I_j, P_{R[AT_j]}, Edp_j \rangle \\ tk_i = \mathit{localToken}(s_i, u, s_j, ss_i) \\ ss_f \in SS_f \quad tk_f = \mathit{domainToken}(s_i, tk_i, s_j, ss_f) \end{array}}{\mathit{CallAttempt}(s_i, u, s_j) \ \rightsquigarrow \ \mathit{SecureCall}(s_i, tk_f, Edp_j)} (\mathit{interdomainFederatedServCall})$$

These rules are used to implement the interactions between the services of the domains. A service of any domain can still call another service of the same domain by providing its security requirement. But a service can now call directly a service of another domain promoted at the federation level; in the last case, the security token of the initial caller is used to get via the federation, the right security token for calling the promoted service. Therefore we ensure the simplicity of service composition with respect to heterogeneous security policies, in the context of the promoted service.

Consider a domain $d_j = \langle U_j, S_j, R_j, SP_j, SS_j \rangle$ of a federation $F = \langle U_f, S_f, R_f, SP_f, SS_f \rangle$ with $SP_f = \langle AF_f, FR_f \rangle$ and $AF_f = \{af_u\}\ u \in 1..p \wedge p \in \mathbb{N}$, the calls to the services of d_j received in the call queue of the interceptor of d_j ($Interceptor_j \in SS_j$) are not directly enabled. The calls are first verified according to the access control requirements of the called services, then they are authorised in accordance with the domain's security policy $SP_j = \langle AT_j, AR_j \rangle$ where the attributes $AT_j = \{at_u\}\ u \in 1..m \wedge m \in \mathbb{N}$ and the rules $AR_j = \{(s_u, at_u)\}\ u \in 1..r \wedge r \in \mathbb{N}$. Because local services and federated services are both provided by a domain, the calls to services are handled by the domains.

A call by a service s_i to a service s_j in a domain d_j of F is enabled under the following conditions (Table 1): either s_i is in the domain d_j or s_i is a service of a domain of the federation and s_i satisfies the security requirements of s_j; that is the conformance with the required access rules (denoted $conformance(tk_j, AT_j, P_{R[AT_j]})$ which checks that the token is built with attributes in AT_j and satisfies the requirements in $P_{R[AT_j]}$). Moreover the attributes in tk_j should satisfy the rules in AR_j.

$\mathit{SecureCall}(s_i, tk_j, Edp_j) \in Interceptor_j\!\downarrow\!CallQueue$	
$s_i \in S_j \vee (\exists d_i \sqsubset F \wedge s_i \in S_i)$	$SP_j = \langle AT_j, AR_j \rangle$
$\exists s \in S_j \wedge s = \langle I, P_{R[AT_j]}, Edp \rangle$	$Edp_j = Edp$
$conformance(tk_j, AT_j, P_{R[AT_j]})$	$\forall at_u \in tk_j.(s, at_u) \in AR_j$

Table 1. *Conditions for a service s_i calling s_j*

$\mathit{SecureCall}(s_i, tk_f, Edp_j) \in Interceptor_j\!\downarrow\!CallQueue$	
$\exists d_i \sqsubset F \wedge s_i \in S_i$	$SP_j = \langle AT_j, AR_j \rangle$
$\exists s \in S_j \wedge s = \langle I, P_{R[AT_j]}, Edp \rangle$	$Edp_j = Edp$
$m = \{(at_j, af_f)\} \wedge tk_j = mapToken(m, tk_f)$	
$conformance(tk_j, AT_j, P_{R[AT_j]})$	$\forall at_u \in tk_j.(s, at_u) \in AR_j$

Table 2. *Conditions to enable calls with federated attributes*

For the conditions (Table 2) to enable the calls to s_j from s_i via the federation level with a token tk_f, the reverse mapping from the federated token (denoted by $mapToken(m, tk_f)$) should be in conformance with the local requirements of s_j.

C. Authorization requirements of HelloService

We illustrate the service promotion with a simple web service named *HelloService* provided by a domain *IUG* identified by the URI `http://iug.net`. The contract of *HelloService* extracted from *IUG*'s service registry is available at `http://bit.ly/2Dib6Lh`. *HelloService* requires a security token issued by the security token service (STS) of *IUG* named *iugSTS*. This token must contain some authorisation attributes of the user on whose behalf the service is called. The access control requirements are claim requirements as defined in the WS-Trust specification.

The claims are expressed using a dialect that indicates the used syntax and semantics. However, WS-Trust does not define any dialect for the expression of claims. *IUG* has its own dialect identified by the URI `http://schemas.iug.net/authorizations/attributes`. Each authorisation attribute of *IUG* is identified by an URI. For example, the URI of the user's role is `http://schemas.iug.net/authorizations/attributes/role`.

The service *HelloService* must be shared in the federation *ICV* made of different domains. Each domain expresses its authorisation attributes using its own dialect. To foster a common understanding of authorisation attributes, *ICV* has a dialect for its federated attributes that are shared by all domains. This dialect is identified by the URI `http://federation-icv.org/ac/ws/authorizations/attributes`. *IUG* defines mappings between the URIs of its authorisation attributes and those of the federation. For example, the user role of IUG `http://schemas.iug.net/authorizations/attributes/role` corresponds to the URI `http://federation-icv.org/ac/ws/authorizations/attributes/subject-function` of the federation.

To promote *HelloService* in the federation *ICV*, its contract is passed to the *promotion-mod* module which replaces each access control requirement expressed with the dialect of *IUG* by the corresponding one expressed with the dialect of the federation, using the mappings defined by *IUG*. The attributes of the *iugSTS* issuing the security token in *IUG* are also replaced by those of the STS of the federation. The result of this promotion available at `http://bit.ly/2UGqOuf` is published in the service registry of *ICV*. Thus, other domains can discover the *HelloService* and understand its access control requirements.

Listing 1 – Authorization requirement of HelloService

```
<sp:AsymmetricBinding>
 <wsp:Policy>
  <sp:InitiatorToken>
   <wsp:Policy>
    <sp:IssuedToken sp:IncludeToken="http://docs.oasis−open.org/ws−sx/ws−securitypolicy
          /200702/IncludeToken/AlwaysToRecipient">
         <sp:RequestSecurityTokenTemplate>
             <t:TokenType>http://docs.oasis−open.org/wss/oasis−wss−saml−token−profile−1.1#
                  SAMLV1.1</t:TokenType>
             <t:KeyType>http://docs.oasis−open.org/ws−sx/ws−trust/200512/PublicKey</t:KeyType
                  >
             <t:Claims Dialect="http://schemas.iug.net/authorizations/attributes" xmlns:authz="http://
                  schemas.iug.net/authorizations/attributes">
                 <authz:ClaimType Uri="http://schemas.iug.net/authorizations/attributes/country"/>
                 <authz:ClaimType Uri="http://schemas.iug.net/authorizations/attributes/role"/>
                 <authz:ClaimType Uri="http://schemas.iug.net/authorizations/attributes/status"/>
            </t:Claims>
         </sp:RequestSecurityTokenTemplate>
     <wsp:Policy>
     <sp:RequireInternalReference/>
     </wsp:Policy>
     <sp:Issuer>
       <wsaw:Address>http://iug.net/ss−services/sts/iugSTS</wsaw:Address>
     </sp:Issuer>
    </sp:IssuedToken>
   </wsp:Policy>
  </sp:InitiatorToken>
  <sp:RecipientToken> ... </sp:RecipientToken>
    ...
 </wsp:Policy>
</sp:AsymmetricBinding>
```