ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Identity Management Systems: Techno-Semantic Interoperability for Heterogeneous Federated Systems

Hasnae L'Amrani[1], Younès EL Bouzekri EL Idrissi[2] & Rachida Ajhoun[1]

[1] Smart Systems Laboratory (SSL), Higher National School of Computer Science and Systems Analysis (ENSIAS), Mohammed V University, Rabat, Morocco

[2] National School of Applied Sciences of Kenitra (ENSAK), University Ibn Tofail, Kenitra, Morocco

Correspondence: Hasnae L'AMRANI, Smart Systems Laboratory (SSL), Higher National School of Computer Science and Systems Analysis (ENSIAS), Mohammed V University, Rabat, Morocco Tel: 212-662-019-225. E-mail: hasnae90lamranii@gmail.com

Received: July 3, 2018 Accepted: July 19, 2018 Online Published: July 28, 2018

doi:10.5539/cis.v11n3p102 URL: https://doi.org/10.5539/cis.v11n3p102

Abstract

The identity management domain is a huge research domain. The federated systems proved on theirs legibility to solve a several digital identity issues. However, the problem of interoperability between federations is the researcher first issue. The researchers final goal is creating a federation of federations which is a large meta-system composed of several different federation systems. The previous researchers' technical interoperability approach solved a part of the above-mentioned issue. However, there are some-others problems in the communication process between federated systems. In this work, the researcher target the semantic interoperability as a solution to solve the exchange of attribute issue among heterogeneous federated systems, because there is a significant need of managing the users' attributes coming from different federations. Therefore, the researcher proposed a semantic layer to enhance the previous technical approach with the aim to guarantee the exchange of attribute that has the same semantic signification but a different representation, all that based on a mapping and matching between different anthologies. This approach will be applied to the academic domain as the researcher application domain.

Keywords: digital identity, federated system, technical interoperability, semantic interoperability, security, cross-domain, ontologies, semantic mapping

1. Introduction

From the beginning, the Internet has been constructed as a space of uncontrolled freedom for the individuals, where everyone is free to expose themselves, consume, tutor themselves, have a social life, etc. Nevertheless, the user needs a solution with a standardized process to manage the use of the internet. Considering, a user has a freedom to use the internet; he has also, rules to respect. The objective of all systems is to have a universal system which response to a universal adaptation and continuous use criteria. The researchers found that, from the beginning phase of system creation, the user is not considered carefully.

In addition, the unconscious of user role train to several identity issues and the digital identity is a serious subject to considere. Because of that, since the design stage, the user requirements should be treated. The seven laws of identity are considered as an ultimate solution to this challenge. However, it still a clear conflict on how the users' identity is treated among different identity management systems. There are several issues related to the creation and management of digital identity within identity management systems. The cross-Domain is the global concern about the migration of identity among identity management systems, especially heteregenuous federated system as the researcher voted system to work on. The researchers found the federated systems the appropriate identity managemnt system to work on, basing on a comparative study done before (L'Amrani et al., 2016). The federation concept provide a solution to degital identity propagation between systems with it ability to garantee the trust among federations.

The problem faced here is the heterogeneity of federation technologies that blocks the insurance of the communication between different federations. Communication means the authentication of users across domains (federations) and the authorization of there access, moreover of the attributes exchange across federations.

The technical interoperability approach is suggested to solve the communication interruption between heterogenous federations. The researchers propose an interoperability component, that translates the different request reaching the component to a standard form and thereafter forwarding it to the destination under the appropriate form.

The actual work objective is the enhancement of the previous technical approach by ensuring a semantic layer to guarantee a complete comprehension of identity among different federated architecture. Here, the researchers propose an enrichment for the technical architecture. The added layer is a semantic treatment to exchange attributes among heterogeneous federations. In contrast whith the technical approach, which is based on the authentication request translation, the semantic layer is based on a method for matching and mapping between different attributes description and representation (domain ontologies), issued from different federation but still having the same semantic signification.

In what fellows, the researchers present an overview of federated systems as well as the presentation of heterogeneous federations' issues. Furthermore, the researchers previous works. Moreover, an arguing why the identity management systems use semantic. Thereafter, the discussion of the proposed approach and the proposed architecture. Finally, we conclude this work with a global summary and future works regarding this subject.

2. Method

2.1 Federated Systems

The federated identity management model describes the most thematic and principal model between his concurrent. Identity federation is defined as the groupement of systems that have evolved trust relationships with each other in order to exchange digital identity information in a secure way. The principal entities of federations' model are the identity provider, service provider and the discovery service WAYF (optional).

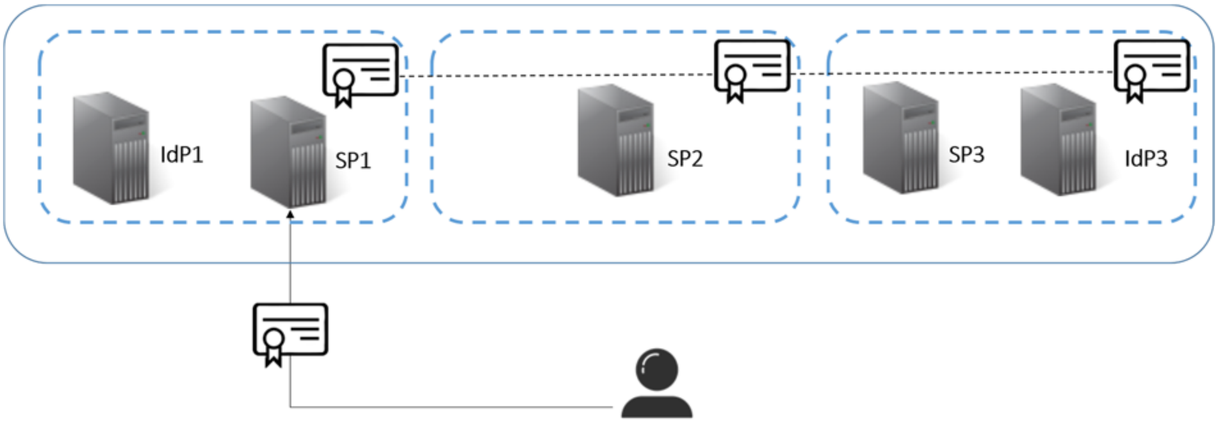

Figure 1. Federation Architecture

2.2 Heterogeneous Federated Systems Issues

The communication process across-federations starts when an external users' request access to a service provider inside the federation where he belongs. This process has two scenarios, the first one is the communication between homogeneous federations and the second the communication among heterogeneous federations. While talking about the homogeneous scenario, the communication interruption issue is not possible. However, it still exists the compatibility issues between versions of same federation technologies.

The serious communication issue among federation come to the world when we have the scenario of heterogeneous federations. The process of communication is interrupted while the service provider of one federation tries to forward the users' request to another heterogeneous federation. The researcher illustrates the communication process interruption by the following use case. This use case is implemented and proved. Furthermore, the interruption of the communication is shown while the request of the service is forwarded from demanded federation to the authentication authority of the user federation.

As a use case we take two federaions based on heteregenuous technologies SAML and WS-Fedeation. First, the user requests a protected service through an HTTP request to the SAML configured service provider. Once the request is received the service provider redirects the user to the WS-Federation configured identity provider authentication service (STS). The request is an URL of the Single-Sign-On service concerning the STS in charge of authenticating the users based on Active Directory and takes as parameters the usual SAML values namely the SAML SAMLRequest request sent in GET to this service. The STS receives the SAMLRequest and RelayState parameters.

Under these conditions, the identity provider returns an access error to the server accompanied by a reference number. This reference number generated by the ADFS service of the STS identity provider informs a request error indicating the revision of the requests' structure. From this use case, the researchers derived two huge issues; the heterogeneity of request structure and the difference of attributes from one federation to another based on the knowledge domain differences.

The first issue is solved with a technical approach discussed in the section of previous works. The second solution is an enhancement of the previous approach with a semantic interoperability layer, which helps to guarantee the attributes exchange among different knowledge domain. In this paper, the authors illustrate the problem, propose an interoperability semantic solution combined with the technical solution and clarify the process of implementation by a design schema and framework conception plus frameworks' interface.

2.3 Previous Work

For each federation technology, there is a specific mechanism to manage digital identity. The researcher previous work aims to ensure a technical interoperability among federated identity management systems to guarantee an interoperable architecture for a transparent communication between heterogeneous federations.

The goal of the previous work is to solve a technical cross-domain issue, for the reason that each system has a different architecture for the management of the digital identity data sent and received. The technical interopearablity approach solves the issues of communication interruption between heterogeneous federations.

As technical existent solutions, they exist narrow configurations in the level of identity provider and service provider, which could be temporary resolution. It could be considered as some ordinary configurations, which do not the response to the research issues. In the referenced work, the researchers presented a standard approach for technical interoperability issues (L'Amrani et al., 2017).

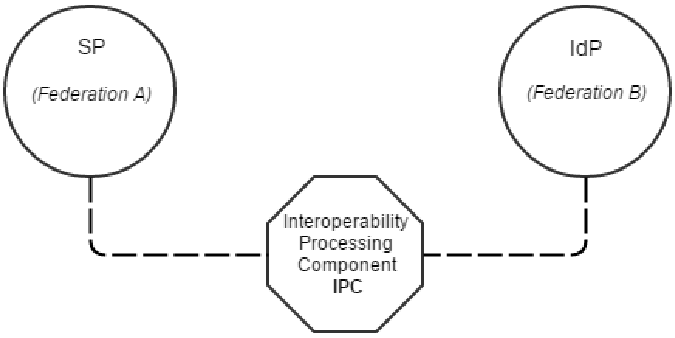

Figure 2. Proposed technical interoperability approach

Figure 2 shows the interoperability processing component place where it can receive federations requests and ensure the translation of those request to the targeted federation.

2.4 The Semantic Requirement to Improve Interopearablity

The primary activity in communities is communication, knowing the identity of the third party with whom you communicate is basic for understanding and evaluating an interaction (Donath, 1996). Identity management is something that we do in traditional communication every day when we decide on what to tell another about ourselves, and what to not say. The researcher exposes a general definition to an identity as a computer representation of an active entity that can be physical (such as a human, a host system, or a network device) or can be a programming agent; this is significantly a definition of the entity identities' in computing (Benantar and USA, 2006). There are several definitions, which we can found in those references (Marit et al., 2003), where they give links between identity, identity management systems and interoperability requirement among those systems.

An entity is the main actor in the communication process. The concept entity is employed in the following to indicate both an individual and an organization (Glässer and Vajihollahi, 2010).

Attribute: An attribute is a feature associated with an entity, like name, Email, national identity code, etc...
Identity: The identity is defined as a conceptual representation of an entity.
Context: A context associated with a specific application domain or case in which an attribute is defined and has a meaning.

Identity management systems contain many models. In the cited reference (L'Amrani et al., 2016), the researcher defined several types of identity management models. The chosen system to work on is the federated system based on the study made in (L'Amrani et al., 2016) reference. Since the federated system is a type of identity management systems, then the federated system needs for semantic integration is clear and by implication is the identity management systems have a part of this need.

Every identity management system is based on the main previous concept, there are many concepts related to this domain but those are the most important to this study. The enormous number of identities that the systems have to manage impose a deep research about a solution to this problem. In addition, the double existence of identities and identity attributes' still an issue, which targets the system performances while the number of items is influential. However, the serious issue about identity management systems is the treatment of attributes that have the same signification semantically, but they are different syntactically. Some statements use different syntaxes, although have the same signification and present the same meaning of one attribute.

2.5 Semantic Interoperability to solve Cross-Domain Issues

In the following schema, the researcher describes the different attributes of users' identity while every user is subscribed in his own federation. As a case study, we take two heterogeneous federations from the academic domain, the federation A present the United Kingdom (UK) or United State (US) academic system and the second show the Moroccan academic system.

Based on (Laformation.ma, 2017), the researcher found that attributes across federation are not the same. In the example of undergraduate and graduate degrees, attributes are treated in a different way. The process of treatment of academic degrees is completely different between Moroccan context and US/UK context. As shown in the schema after (figure 3), the Moroccan universities have a special nomination for the degrees both for undergraduate and graduate. However, the Moroccan context does not make this difference. In addition, there is a huge heterogeneity in the process of giving a special degree. If we take the use case of a Moroccan student who aims to complete his study in the United Kingdom (UK) or United State (US) universities, he should go by a third party to ensure the equivalency of diplomas. In what follows, an example of the third party that ensures matching between academic attributes.

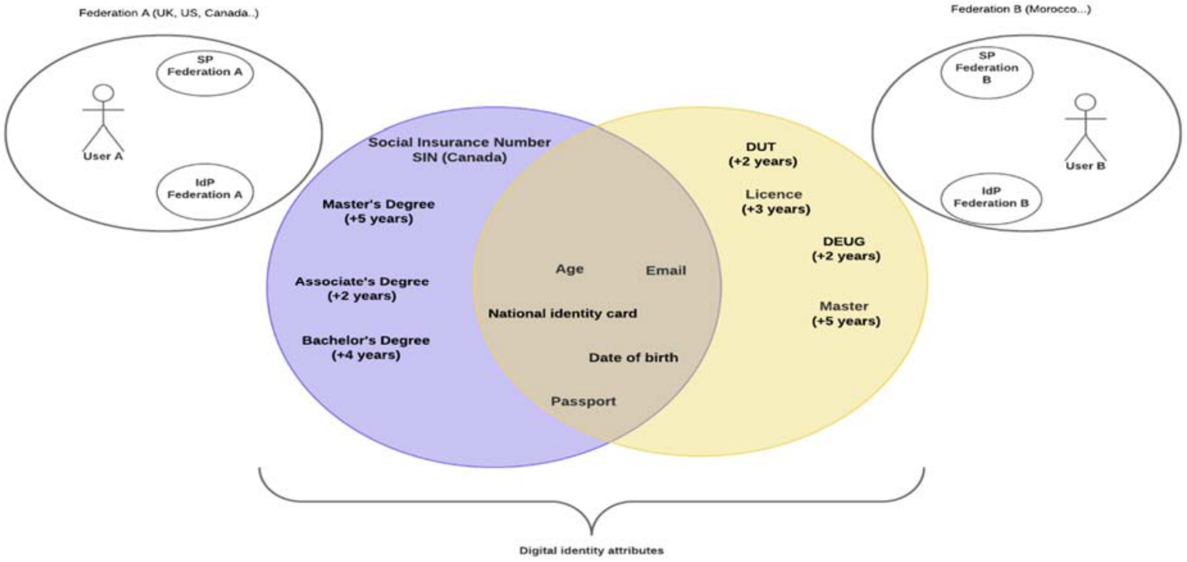
Federation A (UK, US, Canada..)
SP Federation A
User A
IdP Federation A
Federation B (Morocco...)
SP Federation B
User B
IdP Federation B
Social Insurance Number SIN (Canada)
Master's Degree (+5 years)
Associate's Degree (+2 years)
Bachelor's Degree (+4 years)
Age
Email
National identity card
Date of birth
Passport
DUT (+2 years)
Licence (+3 years)
DEUG (+2 years)
Master (+5 years)
Digital identity attributes

Figure 3. Different attributes with same signification across Domains

EduPerson and EduOrg, who has held with funding from Internet2, are Lightweight Directory Access Protocol (LDAP) schema created to cover widely-used individuals and organizational attributes in higher education. The eduPerson purpose class gives a common list of attributes and annotations, describing the existing standards in higher education (Internet2, 2017). However, based on (Chadwick and Hibbert, 2012) study, the EduPerson approach is not scalable, and complex to manage by federation actors when the number of users is large numbers and in the case of been members of multiple federations (Chadwick and Hibbert, 2013).

2.6 Proposed Architecture to Achieve Technical and Semantic Interoperability Levels

The critical concern when establishing a federation is leading to a shared understanding of a standard vocabulary, for example, user roles and attributes which require being known throughout the whole federation. In this work, the researcher focuses on the following dimensions of interoperability:

-Technical: Based on the ability to interchange data, protocols, technical standardization (WP4 and James, 2005).

-Semantic: relates to the ability to exchange meaning between domains.

The schema bellow present the Deployment scenario for the proposed papproaches:

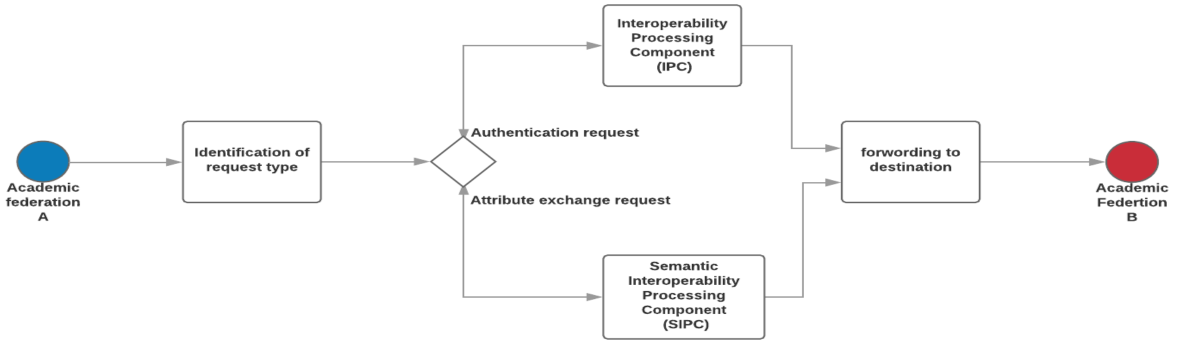
Academic federation A
Identification of request type
Authentication request
Attribute exchange request
Interoperability Processing Component (IPC)
Semantic Interoperability Processing Component (SIPC)
forwording to destination
Academic Federtion B

Figure 4. Proposed approaches deployment scenario

2.7 Semantic Approach

The issue of federation interoperability addressed all the members of the federation accepting a standard collection of attributes which will be allocated to all users by the identity providers (IDPs) and attribute authorities (AAs) furthermore it will be used in access control decisions by the server providers SPs (Chadwick and Hibbert, 2012). Figure 5 presents a general vision about the semantic layer, which will be added to the researcher technical approach.

The case of heterogeneity as shown in the previous section (figure 3), the example of different attributes of different students (users) issuing from different authorities around the world, those) attributes could be a qualification certificate, marks, levels....The real word presents some federations cases where the treatment of semantic difference among graduation attributes is ensured. The first example is in the United Kingdom (UK) universities; they serve to a third party named UK NARIC (NARIC, 2017) to make the equivalency between qualification degrees. It is a governmental establishment, which guarantees the recognition and comparison of international qualifications and skills.

Another experience with the semantic interpretation issue for qualification we can see it in the German authorities. This treatment is ensured by the Uni-Assist. Uni Assist is an organization that supports individuals to grant an approval from the university that he wants to purchase it. The largest base of the universities is connected with the uni-assist. The service should be stamped in the German embassy in the user country (Uni-Assist, 2016).

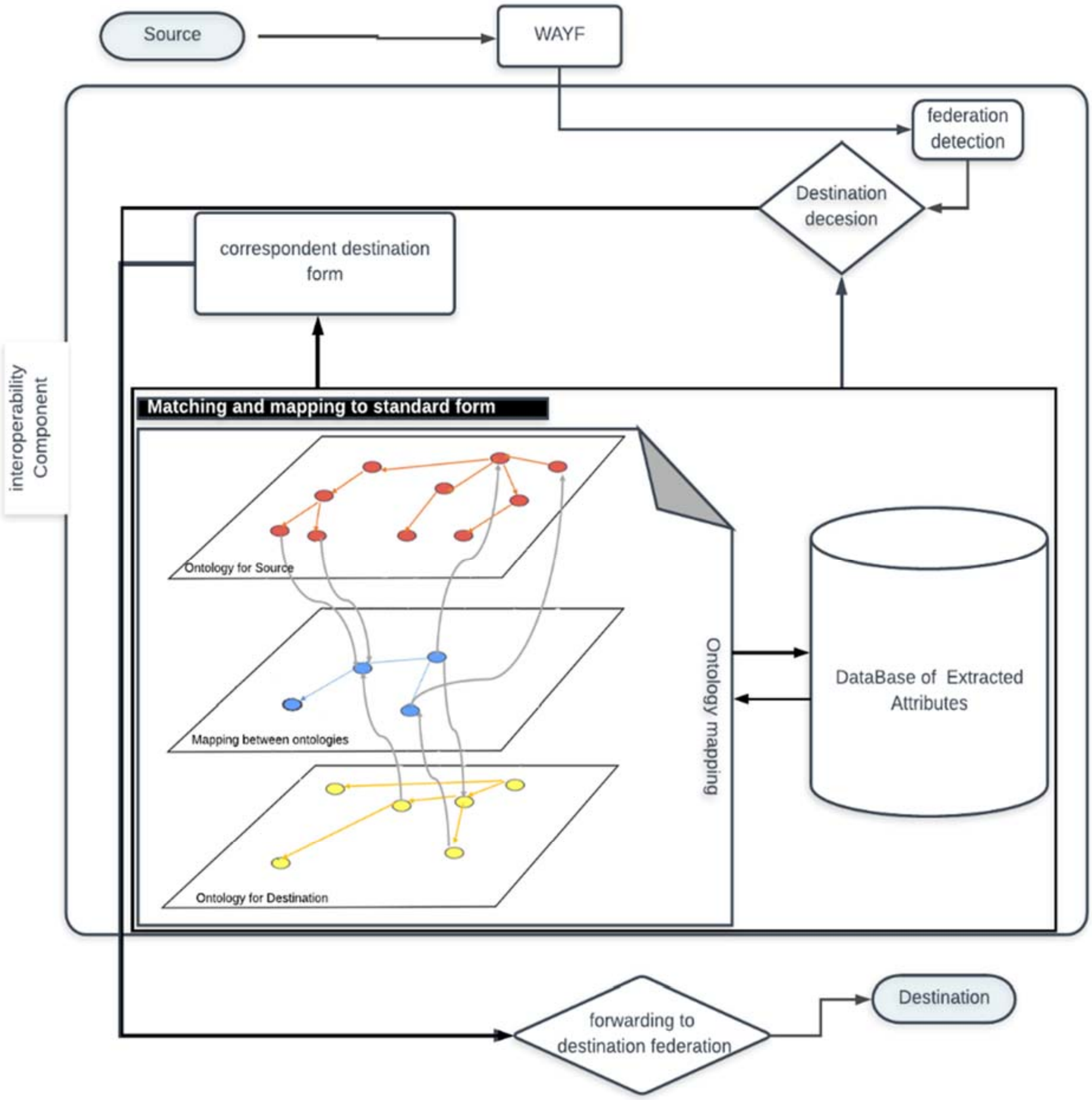
Source
WAYF
federation detection
Destination decesion
correspondent destination form
interoperability Component
Matching and mapping to standard form
Ontology for Source
Mapping between ontologies
Ontology for Destination
Ontology mapping
DataBase of Extracted Attributes
forwarding to destination federation
Destination

Figure 5. Proposed semantic interoperability approach

3. Results and Discussion

3.1 Techno-Semantic Approach

As cited in (Microsoft 2017), there is always a deep need to interoperate other management knowledge format and schemes. In contrast with the traditional top-down approach, the suggestion of a bottom-up approach which based on a semantic mapping among resources description and attributes management across heterogeneous management domains is a good concern. Issues, which can target different ontologies of the same knowledge domain, those ontologies, can differ from each other because they provide a less or more information about the same domain. In view of the fact that mapping between different ontologies from a heterogeneous academic domain is the proposed solution.

The researcher work is about techno-semantic interoperability to solve CrossDomain issues. In this paper, the researcher proposes a semantic layer to improve the technical interoperability solution. The techno-semantic proposed architecture aims to create an interface to ensure semantic interoperability between heterogeneous federations. In figure 6, the researcher gives a federated architecture of technical and semantic approach where he shows several components of technical and semantic architecture. The objective of the merger between two approaches is giving a height performance solution to the Cross-domain issues. Where the process of communication will be transparent on both authentication and attributes exchange levels.

The techno-semantic approach is a combination of a technical approach already proposed in (L'Amrani et al., 2017) and a semantic layer (figure 6) added to the first one. As shown in figure 6 the architecture contains a component for the semantics treatment of attributes received from the different federation. Here we can have the same technology for identity federation treatment [SAML (OASIS, 2017), WS-Fedearion (Microsoft, 2017)...] but it could be different in the semantic of attributes.

The researcher proposes a common interface to communicate between heterogeneous federations. The common interface federated to ensure semantic interoperability between different federations is an intermediate ontology. Ontologies encompass attributes which have the same meaning but different representation. The researcher is in beginning stage on ontologies conception, however, to find more information about ontologies mapping, many studies done about this subject (García-Barriocanal et al., 2011), (Cox, 2015).

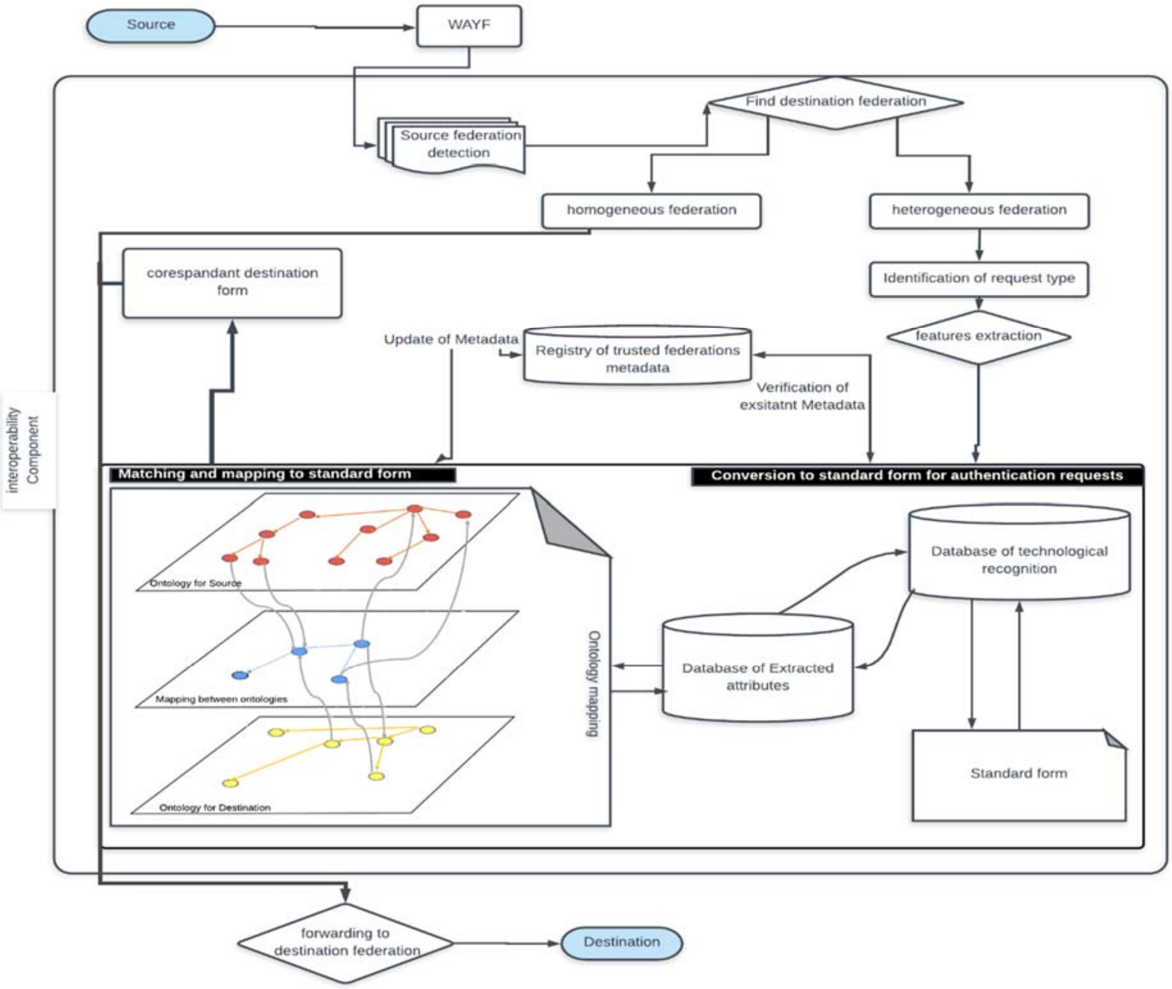
Source
WAYF
Find destination federation
Source federation detection
homogeneous federation
heterogeneous federation
corespandant destination form
Identification of request type
features extraction
Update of Metadata
Registry of trusted federations metadata
Verification of exsitatnt Metadata
interoperability Component
Matching and mapping to standard form
Conversion to standard form for authentication requests
Ontology for Source
Mapping between ontologies
Ontology for Destination
Ontology mapping
Database of technological recognition
Database of Extracted attributes
Standard form
forwarding to destination federation
Destination

Figure 6. Techno-semantic interoperability approach

Coming back to the previous example an AS, DUG, DUT degrees have the same signification (studying 2 years) however, each academic system make its own treatment for the process of managing the qualification associated to a degree. Here we should use a mapping technique between those different federations' ontologies, which can establish a calculation to ensure if an attribute in federation A has the same signification in federation B.

3.2 Proposed Conception

The illustration below includes the conceptual design of both the technical and the semantic approach (Techno-Semantic approach). This representation is a class diagram, which explains the flow exchange between the main entities of researchers' approach.

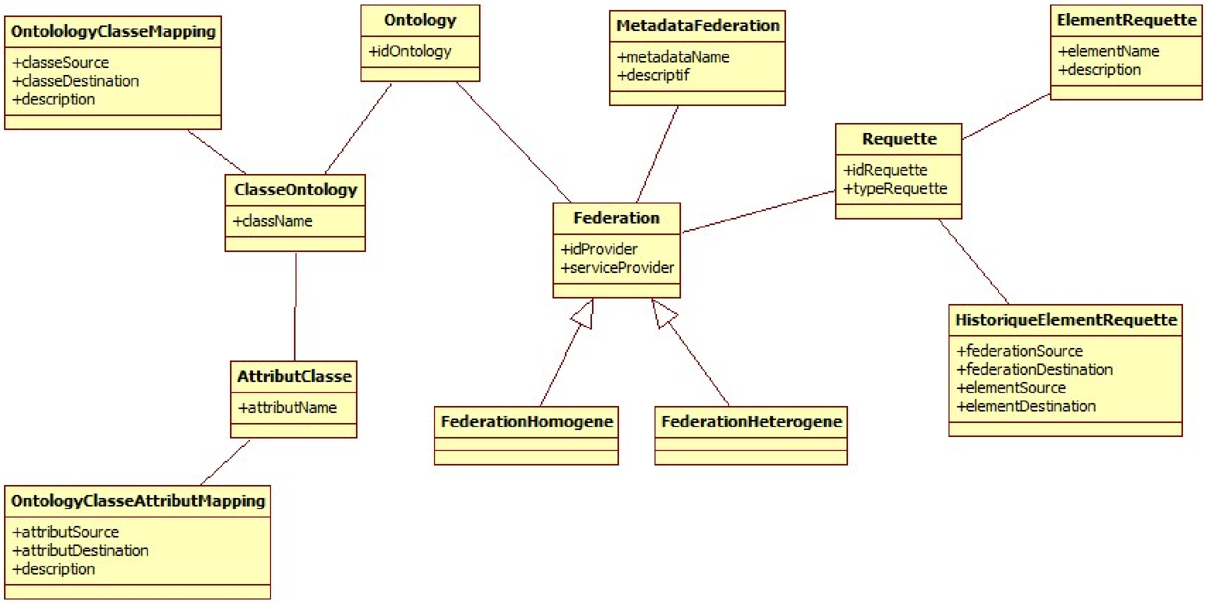

Figure 7. Framework Conception

- The central entity is the federation-Entity, which involves the attributes Identity Provider, Service Provider

- Towards the right, we put the entities that handle the technical approach (the Requests, the Elements of requests and the History of the exchanged requests).

- Towards the left, we find the entities that concern the semantic approach (the ontology, the class of the ontology, the attribute of the class, the Mapping between the classes and the Mapping between the attributes of the classes).

3.3 Discussion

This work aims to improve an intermediate framework that has as functioning, preserving technical interoperability between heterogeneous federated systems in distributed environments. This solution solves the problem of the heterogeneity of the authentication and authorization requests between these different federations by a technical architecture that helps the matching between the requests basing on the translation process to a standard form thereafter transforming to the targeted federation.

The problem posed in this solution is; does this solution support the difference in the content of the query? At this point, we can note that in a query, we can send several attributes with the purpose of sharing and exchange between the federations after a successful process of authentication and authorization.

This whole approach is applied to the academic context. Even though the field of academic knowledge is the same, the attributes can change between use cases. In the examples noted in Figure 2 it is clear that in the same context (academic context) and even in a common domain of knowledge, a problem of the heterogeneity of attributes representation exists. There are several parameters to consider when discussing data exchange between different federations and in the same knowledge domain.

There are two parameters to discuss their impacts on the exchange of attributes between different federations. It exists evermore issues around the data structure that can be different from one federation to another and from one knowledge domain to another. In addition, we can also note the parameter of language, it is possible to be different attributes' language, from one federation to another, also for the case of different areas of knowledge.

4. Conclusion and Fsuture Works

Actually, the researchers are working on the interoperability between federated systems, the researchers tackle all levels of interoperability beginning from the organizational level and ending at the technical level. The authors aim to carry out an interoperability architecture, which simplifies the communication process between homogeneous and heterogeneous identity management solutions.

In this paper, the authors aim to give a global view of identity management issues. We can define the semantic treatment of attribute exchange among federated systems. The communication process between the federated system should be transparent

and flexible. We find the problem of communication discontinuity in the process of requesting and receiving services.

We treated the identities portability issue among federated systems. By an interoperable approach, we can solve this problem. When the researcher compares the communication process between two federations, each one is based on a heterogeneous technology from the other. In addition, the nomination of same attributes is completely heterogeneous. At this level, there are technical and semantic issues in the exchange process between federations. In this work, the solution of interoperable approach is adopted to solve this problem of communication interruption, caused by the heterogeneity of those federations' technologies, standards, and protocols. In addition, the researcher adds a semantic layer to solve the problem of attributes exchange among different academic domain like the UK and Moroccan universities.

Our future goal is to create a global interoperable approach between different federations. All that to guarantee the portability of identity between different domains and a transparent communication between heterogeneous entities. The next step is about the creation of an intermediate ontology to ensure the mapping between different ontologies from same knowledge domain. That will be based on ontologies mapping and alignment for creating correspondences between Ontologies. As there are several methods to achieve this correspondence (Mapping, Merging, articulation), the researcher chooses the mapping technique. The authors are achieving the validation stage; they are working on an implementation as a proof to validate the feasibility of the solution.

References

Benantar, M., & IBM USA. (2006). Access Control Systems Security, Identity Management and Trust Models. Springer.

Chadwick, D. W., & Hibbert, M. (2013). Towards automated trust establishment in federated identity management. Springer, IFIP Advances in Information and Communication Technology, pp. 33-48, https://doi.org/10.1007/978-3-642-38323-6_3.

Chadwick, D. W., & Hibbert, M. (2012). F-sams: Reliably identifying attributes and their identity provider in a federation. In On the Move to Meaningful Internet Systems: OTM 2012 Workshops. Springer, https://doi.org/10.1007/978-3-642-33618-8_32.

Cox, S. J. D. (2015). Ontology for observations and sampling features, with alignments to existing models. *Semantic Web, 8,* 453-470.

Donath, J. S. (1996). Identity and deception in the virtual community.

García-Barriocanal, E., Cebeci, Z., Okur, M. C., & Öztürk, A. (2011). Metadata and Semantic Research.

Glässer, U., & Vajihollahi, M. (2010). Identity management architecture. *Security Informatics, 9,* 97–116, https://doi.org/10.1007/978-1-4419-1325-8_6.

Internet2 (2017). eduperson and eduorg.

Kevin, F., Rob, B., John, K., Hendrik, T., Dave, L., Aidan, B., & Declan, O. (2010). Enabling decentralized management through federation. Computer Networks: Special issue. *Managing emerging computing environment, 54,* 2825-2839. https://doi.org/10.1016/j.comnet.2010.07.006.

L'Amrani, H., Berroukech, B. E., Bouzekri, E. L., Idrissi, Y., & Ajhoun, R. (2017). Toward interoperability approach between federated systems. In BDCA'17 Proceedings of the 2nd international Conference on Big Data, Cloud and Applications. ACM.

L'Amrani, H., Berroukech, B. E., EL Bouzekri EL Idrissi, Y., & Ajhoun, R. (2016). Comparative study between identity management systems: Laws of identity for models' evaluation. In 4th IEEE International Colloquium on Information Science and Technology, (CiSt 2016), pages 736-740.

Laformation.ma (2017). Etudier aux etats-unis.

Marit, H., Henry, K., Christian, K., & Martin, R. (2003). Identity Management Systems (IMS): Identification and Comparison Study. Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG).

Microsoft (2017). Understanding ws-federation.

NARIC, U. (2017). Uk national recognition information centre.

OASIS (2017). Oasis security services (saml) tc.

Uni-Assist (2016). uni-assist.

WP4 and James, B. L. (2005). D4.1: Structured account of approaches on interoperability.

Copyrights