F-SAMS: Reliably Identifying Attributes and Their Identity Providers in a Federation

David W. Chadwick and Mark Hibbert

School of Computing
University of Kent
{d.w.chadwick,m.j.m.hibbert}@kent.ac.uk

Abstract. We describe the Federation Semantic Attribute Mapping System (F-SAMS), a web services based system that automatically collects, in a trustworthy manner, the semantic mappings of Identity Provider (IdP) assigned attributes into a federation agreed set of standard attributes. The collected knowledge may be used by federation service providers (SPs) to support the dynamic management of IdPs and their assigned attributes.

Keywords: semantic access control, federation interoperability, identity management.

1 Introduction

A federation is defined as "A collection of domains that have established trust and it typically includes a number of organizations that have established trust for shared access to a set of resources" [1]. Although the members of the federation share their resources with other members, they remain in complete control of them and often govern the authorization and access control to their resources through the use of policies about a user's attributes. These members are known as service providers (SPs). The federation members who authenticate and identify the users are known as identity providers (IdPs), those who simply provide attributes about the users, attribute authorities (AAs).

One crucial consideration when establishing a federation is reaching a common understanding of an accepted vocabulary for such things as the user roles and attributes (and their associated privileges) which need to be understood throughout the entire federation. Traditionally, the problem of federation interoperability is addressed by all members of the federation agreeing upon a standard set of attributes that will be assigned to all users by the IdPs/AAs and will be used in access control decisions by the SPs. This is the approach adopted by the UK Access Management Federation (UKAMF) [2], which passes eduPerson attributes [3] between federation members. However, this approach is not scalable and can be difficult to maintain by IdPs and AAs when they have large numbers of users, and/or are members of multiple federations, as the new federation agreed attributes may need to be assigned (or mapped) to each of their users. It also poses difficulties for SPs, since they need to be

P. Herrero et al. (Eds.): OTM 2012 Workshops, LNCS 7567, pp. 231–241, 2012.

sure that each IdP/AA is a trusted member of the appropriate federation and is entitled to assign the federation attributes that it does. The UKAMF partially addresses this problem by regularly distributing metadata between its members, which lists details about the current members of the federation. But it does not yet fully address the trust issues. But by not supporting the federation agreed set of standard attributes, the situation is worse, since SPs will not be able to interpret the semantics of attributes originating from IdPs and AAs outside their domain. However the current federation solution does not mirror the existing physical world.

Consider a university which gets applications for its degree courses from students from every country of the world. Each student presents his/her original paper qualification certificates which are issued by different educational organizations the world over. These have different grading schemes, different pass marks, and different levels of attainment, in short, different attributes issued by different authorities. But the admissions officer needs to know how each of these qualifications maps into the local ones that he is familiar with, in order to know if the student is sufficiently qualified to enroll on the degree course. In the UK, some help is at hand from UK Naric (http://www.naric.org.uk), which provides a directory of foreign educational institutions, the qualifications they offer, and a best guestimate mapping of these into their equivalent UK counterpart. But the mapping is advisory only and each UK admissions officer has to make his own decisions about the trustworthiness and mapping of the foreign qualification attribute. Germany has a more advanced system, in that Uni-Assist (http://www.uni-assist.de) acts as a trusted third party and provides validated mappings of foreign qualifications into their German equivalent. In order to validate the authenticity of the paper certificate, the student has to have it stamped by the German embassy in its country of issuance.

Our Federation Semantic Attribute Mapping System (F-SAMS) system is designed to more closely mirror, and improve upon, the physical world by:

i) allowing IdPs and AAs to send their locally assigned roles and attributes to SPs, rather than having to send a set of standard federation agreed attributes
ii) automating the collection of IdP and AA issued roles and attributes as well as their semantic mappings into a set of federation agreed attributes (the knowledgebase), and
iii) using a novel trust model, builds a trust base that allows SPs to automatically validate unknown IdPs and AAs and their attributes.

The remainder of this paper is structured as follows; section 2 describes the F-SAMS model; section 3 describes the attribute mappings; section 4 explains the crawler which collects the attribute mappings into a knowledge base; section 5 introduces the knowledgebase queries; section 6 discusses related work, whilst section 7 concludes and discusses future directions of F-SAMS research and development.

2 The F-SAMS Model

In a F-SAMS federated environment, users can access resources from SPs without any prior interactions taking place between the SP and the user's IdP/AA. Fig. 1 depicts a typical access control request by a user's agent. When the SP receives the

request, it first discovers the user's IdP/AA and then redirects the user's agent to there, along with an authentication and attribute request. As the IdP/AA has no existing relationship with the SP, it does not want to release the user's personal information (attributes) until it knows that the SP is a trusted member of the federation. The IdP/AA queries F-SAMS with the SP's X.509 public key certificate (PKC). F-SAMS looks up the SP in its trust base and returns the result to the IdP/AA. If the SP is a trusted federation member, the IdP/AA can continue with authenticating the user. The IdP/AA returns a signed attribute response to the SP, via the user's agent. When the SP receives the response, it must first validate the IdP/AA and its attributes before granting access to the user. The SP queries F-SAMS i) to determine if the IdP/AA is in the trust base, and ii) to discover the semantics of the IdP/AA's attributes. If the IdP/AA is a trusted federation member, F-SAMS returns a set of mapped federation attributes, which the SP can use to make an access control decision.

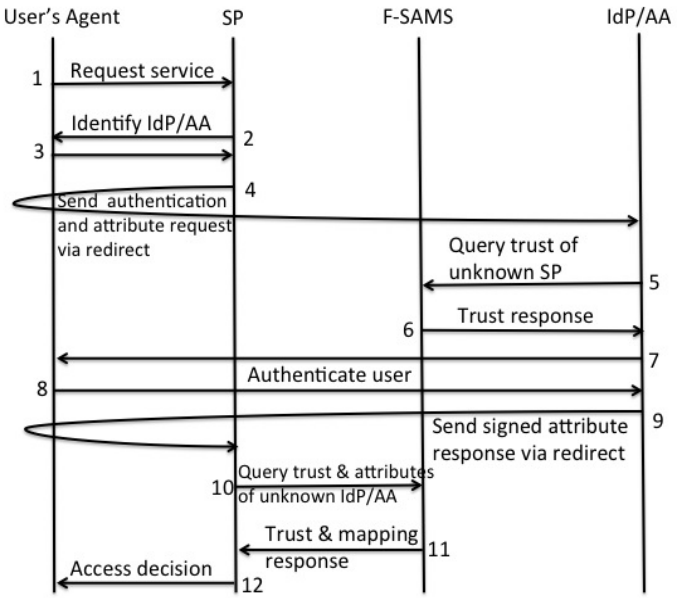

Fig. 1. F-SAMS access control process

The F-SAMS model revolves around the trust and vocabulary expression (TruVEx) document that is published by each IdP/AA member or candidate member of a federation. Each document contains three parts:

- the X.509 PKC of the (candidate) member. This can be a self-signed certificate, or one issued by a CA. The only restriction is that it must contain the uniformResourceIdentifier component of the subject alternative name (SAN) extension and hold the URI of the web location storing the detached signature of the member's TruVEx document. The candidate member determines this URI at the time his PKC is issued, even though the location will initially be empty.

- an attribute mapping part, expressing in RDF the relationships between the attributes in the (candidate) member's local vocabulary and those in the federation vocabulary. Each of the member's vocabularies are aligned with those of the other members using the federation vocabulary as the common ontology that binds them all together. By aligning the vocabularies with the federation ontology, relationships will automatically be inferred between the attributes of the separate organizational vocabularies without any of them possessing prior knowledge of the other vocabularies. The federation vocabulary is published by the federation root of trust (FRoT), the FRoT being the organization that initially establishes the federation and invites other candidate members to join. As the federation evolves, the FRoT may dynamically expand the federation vocabulary to include other attributes that are of interest to the federation's members, and members may update their TruVEx documents accordingly. This allows finer grained access controls to be introduced.
- a friends part, which contains for each friend (i.e. candidate member that this member (the introducer) asserts to be trustworthy): their PKC and the hash of the attribute mapping part of their TruVEx document. The PKC enables the TruVEx document of the friend to be discovered, as the SAN extension points to the TruVEx detached signature and the signature points to the TruVEx document. By including the hash of the attribute mapping part, this stops it from being undetectably altered after the introducer has validated it.

Each member signs his TruVEx document using the private key corresponding to the public key in the first part of the document, and stores the detached signature at the URI contained in the SAN field of his PKC.

An example federation is shown in Fig. 2. where each named square represents the TruVEx document published by a member of the federation.

A web crawler starts from the TruVEx document of the FRoT, and crawls the web picking up the TruVEx documents of other federation and candidate members and from these it constructs the centralized federation knowledgebase and trust base.

The notion of a "friend" is used in the TruVEx document to refer to an organization whose attribute mappings are trusted by the organization asserting the friendship (the introducer). This "friendship" is not required to be mutual; instead it merely indicates that one organization (the introducer) trusts, or has confidence in, another organization's semantic attribute mappings. All candidate members are given a trust score based on this friendship. As more members add a candidate member to their friends' parts, then the candidate organization's trust score increases until it is sufficient to reach the trust threshold required to become a member of the federation. The new member is then assigned a level of trust by F-SAMS, but this trust level decreases, the further the member is away from the FRoT. A member's trust level is used in computing the trust score of new federation candidates that this member introduces (as a friend). A fuller description of the trust model and trust scoring mechanism is outside the scope of this document.

A TruVEx document is signed for two reasons: the first is to prove the integrity of the document's content, and the second is to verify the assertions made about friends that the introducer trusts. This is similar to a signed X.509 PKC where the signer asserts that the public key mentioned in the certificate belongs to the named subject of the certificate. In the F-SAMS case, the introducer is asserting that he has confidence that his friend's attributes do map into the federation agreed ones as specified in the friend's TruVEx document.

Members can update and re-sign their TruVEx documents as often as they want, with the following provisos:

- each time the document is signed its detached signature must be stored at the signature URI contained in the SAN field of the signer's PKC (otherwise no-one will be able to verify the document's integrity)
- if a member changes his asymmetric key pair or PKC or attribute mapping part he must notify the introducers who have his details stored in the friends' parts of their TruVEx documents (see Fig.2).

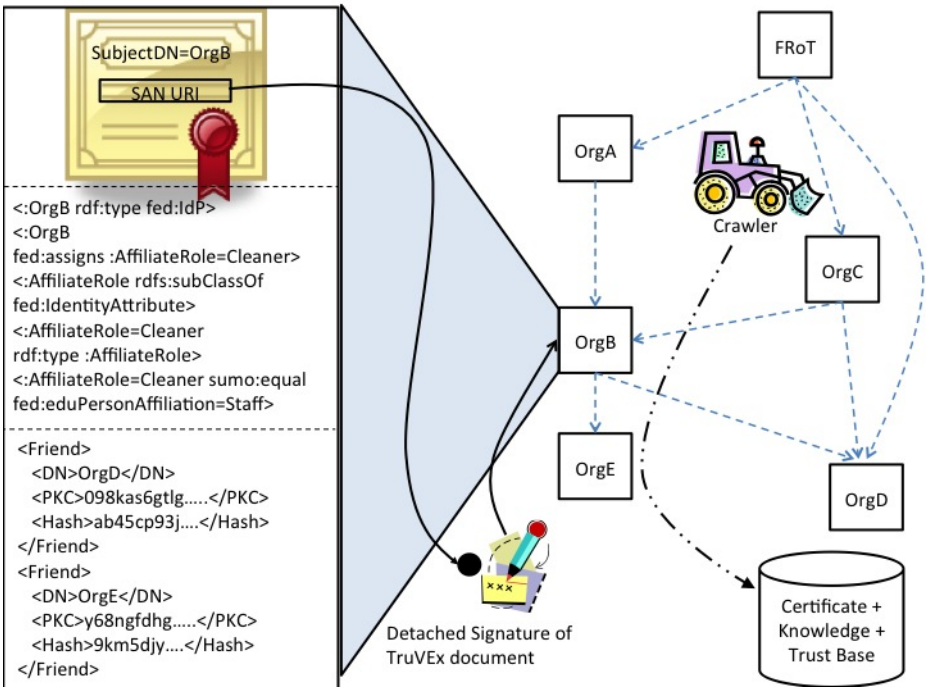

Fig. 2. A TruVEx document from an example F-SAMS federation

A member can update his friends list as often as he wishes without notifying anyone. However, when a member updates the attribute mapping part of its TruVEx document, this alters the hash value so that it no longer matches those published by the introducers of this document. For the document to remain trusted and for F-SAMS to process it, each introducer must re-validate and re-publish the new hash of the attribute mapping part. To assist with the automation of updating the attribute mapping part, members should maintain a separate list of introducers (LOI) that will contain the email addresses of their introducers. The LOI can then be used to inform the introducers when the attribute mappings are updated. The introducers can either confirm the mappings are valid and update their friend's entry accordingly, or if the mappings are no longer valid, the friend's entry can be removed as this member is no longer trusted by the introducer. If the introducer does nothing, it is equivalent to the latter.

The member's X.509 PKC is used for verification of the distinguished name (DN) and public key of the member. Note that a member may assert its own DN, by issuing a self-signed certificate, but its friends will validate this when they add the member to their friends' lists. The PKC is used by the crawler to confirm the subject's DN with the one constructed from the friend assertions made by already trusted introducers in their TruVEx documents. The PKC is also used to confirm that the TruVEx document was signed by the correct entity. Thus F-SAMS does not rely on, nor require, any CA infrastructure. The validated member's PKC is stored in the certificate base by the crawler, for subsequent use by other federation members.

The FRoT's TruVEx document contains additional information to the members' TruVEx documents. It contains the SP members part and the federation vocabulary part. The SP members part contains a list of (possibly self-signed) X.509 PKCs of SPs that are trusted members of the federation. The FRoT has validated that these public keys do belong to the named SP members. They can be used for authenticating the SPs in message exchanges. The federation vocabulary part contains the vocabulary that the members of the federation will base their attribute mappings on.

3 The Attribute Mappings

The attribute mapping part of a TruVEx document conveys via RDF statements which attributes the IdP/AA assigns to its users and shows how they relate to the federation's attributes. The federation vocabulary is made up of a subset of concepts and object properties from the SUMO upper common ontology [4], supplemented by F-SAMS, as shown in Fig. 3 and Table 1. The F-SAMS upper common ontology in Fig. 3 shows how the SUMO (sumo) and F-SAMS (fed) concepts and object properties connect. We have extended the SUMO Attribute concept to include IdentityAttribute, with a subclass of EmailAddress. This allows IdPs/AAs to define their own identity attributes (as subclasses) and map them into the federation vocabulary. The Organization concept from SUMO has been extended to include the three types of organization that F-SAMS will encounter: IdP, AA, and SP. IdPs/AAs will classify themselves as one or both of these, whilst the FRoT will classify the SPs. Fig. 3 also shows the object properties (defined in Table. 1) used in F-SAMS.

Table 1. The relationships used by F-SAMS

Relationship	Object property	Definition of object property
Superior role/attribute	sumo:subAttribute	The object of the triple is a subordinate attribute of the subject of the triple
Equivalent or better	sumo:equal	The subject of the triple is at least equivalent to the object of the triple
Property of	sumo:property	The object of the triple is an attribute of the subject (any entity) of the triple
Assigns	fed:assigns	The object of the triple is an identity attribute assigned by the subject of the triple

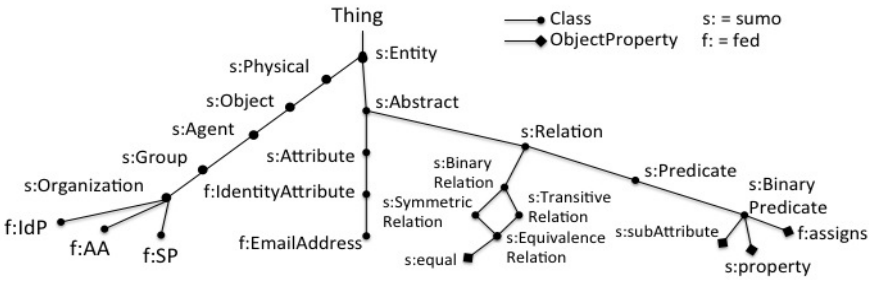

Fig. 3. The F-SAMS upper common ontology

This upper common ontology is then extended by the FRoT to include the federation's application specific objects and attributes. All concepts in the F-SAMS ontology are related using the rdfs:subClassOf property. Individuals are connected to their concept via the rdf:type property. All attributes are represented as type/value pairs (e.g. Role=Professor), and are instances of their attribute type concept. These attributes may be hierarchically related to each other (i.e. superior or subordinate) and the SUMO property subAttribute is used to define the subordinate attribute relationship. When an IdP/AA asserts that one of its attributes is equivalent to a federation attribute, the SUMO equal relationship is used. When an IdP/AA wishes to map one of its identity attributes to a non-equivalent federation attribute, the IdP/AA attribute must be superior to the federation attribute.

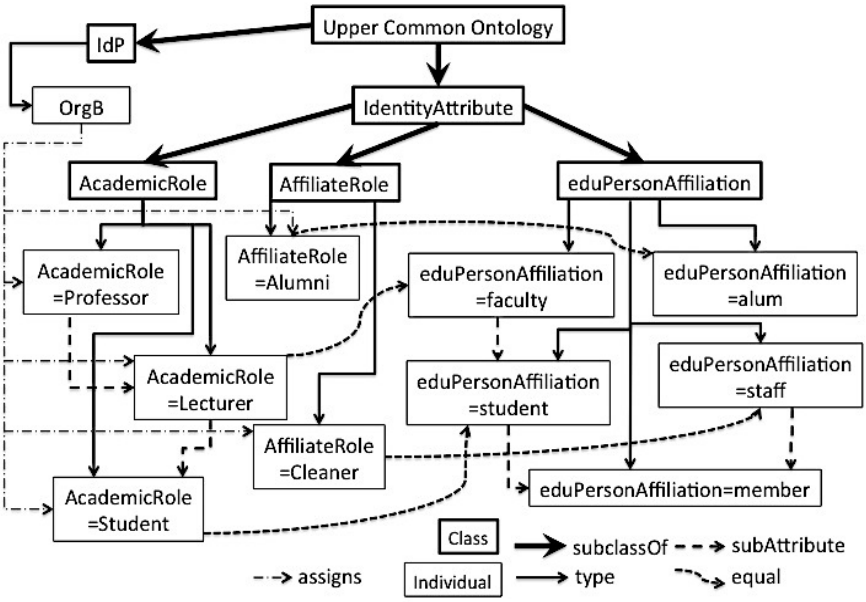

Fig. 4. Example attribute mappings

A pictorial example of (a subset of) a federation vocabulary that might be used by an academic federation is shown on the right hand side of Fig. 4. This is taken from the eduPerson schema [3]. The left hand side shows the mappings that might be made by the OrgB IdP, which issues two types of attribute: academic roles (in a hierarchy) and two unrelated affiliate roles. OrgB is linked to its attribute values using the assigns property. Some of these can be mapped into equivalent federation eduPerson Affiliation attribute values. Other relationships can be inferred from these mappings. For example, the AcademicRole=Lecturer attribute is equivalent to the eduPerson Affiliation=faculty attribute. As AcademicRole=Lecturer is a subAttribute of AcademicRole=Professor, it can be inferred that AcademicRole=Professor is also equivalent to eduPersonAffiliation=faculty. Similarly, eduPersonAffiliation=member is a subAttribute of eduPersonAffiliation=student, and the latter is a subAttribute of eduPersonAffiliation=faculty, therefore both AcadmicRole=Lecturer and Academic Role=Professor will inherit the privileges of eduPersonAffiliation=faculty, eduPerson Affiliation=student and eduPersonAffiliation=member. Fig. 2 shows part of Table 2 represented as RDF in OrgB's TruVex document.

Table 2. Example triples from Fig.4

Subject	Predicate	Object
AcademicRole	subClassOf	IdentityAttribute
eduPersonAffiliation	subClassOf	IdentityAttribute
AcademicRole=Professor	type	AcademicRole
OrgB	assigns	AcademicRole=Professor
AcademicRole=Professor	subAttribute	AcademicRole=Lecturer
AffiliateRole=Cleaner	type	AffiliateRole
eduPersonAffiliation=staff	type	eduPersonAffiliation
eduPersonAffiliation=staff	subAttribute	eduPersonAffiliation=member
AffiliateRole=Cleaner	equal	eduPersonAffiliation=staff

4 The Crawler

The crawler is the element of F-SAMS that discovers the vocabularies, verifies the documents, and builds the knowledgebase, trust base and certificate base. The crawler runs periodically to maintain and update the information. The crawler is initialized with the PKC of the FRoT and the URI of the FRoT's TruVEx document. The crawler begins by retrieving the FRoT's TruVEx document, which it verifies with the PKC, before dissecting it to extract the various parts. The FRoT's federation vocabulary part contains the federation ontology, which F-SAMS uses as the foundation for the knowledgebase. The SP members part is used to create the list of SP PKCs in the F-SAMs certificate store. Only these SPs will be entitled to use the web service to validate IdPs/AAs and their attributes. The FRoT's friends' information is used to create the crawler's initial list of friends (LOF). As the FRoT is fully trusted, its friends are trusted to join the federation as IdPs/AAs, and their certificates are added to the F-SAMs certificate store. However, their trust levels are set to a reduced level.

The crawler then works through the LOF to read, verify and analyze their trusted TruVEx documents. As it does so, it dynamically updates the knowledgebase from their attribute mapping parts, and its LOF and internal certificate store from their friend's parts. The crawler then proceeds to compute the trust scores of the friends of the friends of the FRoT, using the entries in its LOF. The more friends a candidate member has, the higher its trust score. If a candidate does not have a trust score which passes the required membership threshold, its details (PKC and hash) are still added to the LOF, but the TruVEx document is not read in or processed until its trust score satisfies the membership threshold. Once this occurs, the crawler computes a reduced trust level for this new member, adds its PKC to the F-SAMS certificate store, reads in its TruVEx document, validates it, then includes its friends in its LOF and its attribute mapping part in the F-SAMS knowledge base. The crawler continues this process until either no more entries are added to its LOF, or no more trusted candidates remain unprocessed. Once the crawl is complete, any candidates with a trust score under the threshold are kept in the LOF, but are not included in the trust base, so that SP's only have access to a completely trusted set of IdPs/AAs and their attribute mappings. Periodically, at a frequency determined by the FRoT, the crawler starts to crawl the federation again, starting with the TruVEx document of the FRoT. If a previously trusted member become untrusted, then its details are removed from the F-SAMS certificate, knowledge and trust bases.

5 F-SAMS Queries

To query F-SAMS, the SP establishes a TLS session with the F-SAMS web service, and sends a request containing the PKC and the (unknown to the SP) attribute(s) of the issuing IdP/AA. F-SAMS initially attempts to retrieve the trust score for the IdP/AA from its trust base, and if it is found, will proceed to map the IdP/AA's attribute(s) into federation attributes. The response to the SP contains one of the following:

- a response code of -2 if the IdP/AA is not trusted;
- the trust score of the IdP/AA (which will always be above the membership threshold), followed by one of the following for each IdP/AA attribute:
    - a response code of 1 and the mapped federation attribute, or
    - a response code of 0 and the dominant federation attribute, meaning that the attribute is known to F-SAMS but is not equivalent to or superior to any federation attribute. The dominant federation attribute represents the closest match. The SP can then unilaterally decide to either grant the unknown attribute equivalent or downgraded privileges compared to the dominant federation attribute, or simply ignore it.
    - a response code of -1 when the attribute is unknown to F-SAMS.

As the knowledgebase is built by aligning only vocabularies that are fully trusted, i.e. from IdPs and AAs that have a trust score of at least the threshold, the relationships returned by F-SAMS can be completely trusted even though the trust is transitive and not direct. This is because each SP has complete trust in the FRoT, and through

chains of trust from the FRoT to every IdP/AA member in the federation, trust remains strong regardless of how far that latter is away from the FRoT, since more introducer chains are needed the further an IdP/AA is away from the FRoT.

An IdP or AA may query F-SAMS to determine whether an SP is a trusted member of the federation. An IdP/AA establishes a TLS connection with F-SAMS and sends the SP's PKC. F-SAMS checks the certificate base and returns a binary response of true if the SP is a federation member, and false if not.

6 Related Work

Our work is related to the work presented in [5], OBIS, which enables semantic interoperability within federations. More specifically, the knowledgebase that we present is a relationship lookup service similar to OBIS. However, OBIS is grounded in natural language, whereas F-SAMS is based on the standardized RDF and OWL languages [6, 7]. In addition to the relationship lookup service, we present a federation infrastructure for building the knowledge base and a trust model for dynamically expanding the IdP/AA membership.

The Semantic Access Control (SAC) Model [8] was specifically designed to enforce ABAC policies in heterogeneous and distributed environments. It maps policies to resources dynamically based on the semantics of policies and resources. F-SAMS allows the SP to keep their existing policies, mapping instead the user's attributes into their local SP equivalents.

The Semantic Access Control Enabler (SACE) [9] was developed to enforce RBAC when accessing heterogeneous databases. This approach allows each organization to define their resources as concepts (classes) and then use schema mapping techniques to resolve the semantic interoperability. Thus, the SP's resources in the request can be mapped to concepts representing a resource in the ontology by a trusted third party mediator which makes the access control decisions on behalf of the SP. So the permissions are associated to classes in the ontology rather than to the actual resources. In comparison, F-SAMS leaves the access control decisions in the hands of the SP and maps the requester's roles/attributes into SP understood ones, rather than mapping the requested resources. F-SAMS therefore has wider applicability.

[10, 11] both suggest the use of RDF ontologies to create and manage policies, whereas, [12] extends this presenting the ROWLBAC model, which discusses the use of OWL to represent policies in RBAC. They argue that the use of established access control techniques (such as XACML) requires all roles to be established at initialization time and it is therefore advantageous to use OWL to generate policies. F-SAMS similarly does not require all roles to be known at initialization time, but enables the dynamic mapping of roles/attributes rather than the dynamic generation of policies.

7 Conclusions and Future Work

We have presented F-SAMS, a web services based system for use in federations to enhance interoperability, using semantic mappings to understand attributes from unknown IdPs and AAs. Its trust model allows for the automatic sharing of vocabularies

between members, and using levels of trust, ensures that SPs can have complete trust in the mappings without even knowing the IdP/AA or its vocabulary. Combining a trust base and a knowledge base allows SPs to not only verify attribute assertions from an unknown IdP or AA, but also interpret the unknown request attributes. This provides flexibility within the federation, as IdP/AAs do not have to update their attributes to accommodate the federation attributes. Instead, they can map their attributes into the federation's, where they can be securely collected and stored centrally for SPs to query whenever unknown attributes are encountered. It also means that the SPs and IdP/AAs do not have to engage in any prior trust relationships.

Future work will include the design and building of a vocabulary creator that will allows members to create, edit and sign their TruVEx documents using a GUI. The F-SAMS infrastructure will be extended to allow SPs to dynamically introduce new SPs to a federation, and to include Levels of Assurance in IdPs.

References

1. Federation definition, http://msdn.microsoft.com/en-us/library/ms730908.aspx
2. UK Access Management Federation, http://www.ukfederation.org.uk
3. EduPerson Schema, http://middleware.internet2.edu/eduperson/
4. Niles, I., Pease, A.: Towards a Standard Upper Ontology. In: Welty, C., Smith, B. (eds.) Proc. of the 2nd Int. Conf. on Formal Ontology in Information Systems (FOIS 2001), Ogunquit, Maine, October 17-19 (2001)
5. Ciuciu, I., Zhao, G., Chadwick, D.W., Reul, Q., Meersman, R., Vasquez, C., Hibbert, M., Winfield, S., Kirkham, T.: Ontology-based Interoperation for Securely Shared Services. In: Proc. IEEE Int. Conf. on New Technologies, Mobility and Security (NTMS 2011), Paris, France (2011)
6. RDF Concepts – W3C Recommendation (February 10, 2004) http://www.w3.org/TR/rdf-concepts/
7. OWL – W3C Recommendation (October 27, 2009), http://www.w3.org/TR/owl2-primer/
8. Yagüe, M.I., Gallardo, M.-d.-M., Maña, A.: Semantic Access Control Model: A Formal Specification. In: de Capitani di Vimercati, S., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 24–43. Springer, Heidelberg (2005)
9. Mitra, C.C.P.P., Liu, P.: Semantic Access Control for Information Interoperation. In: Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, pp. 237–246 (2006)
10. Uszok, A., Bradshaw, J., Johnson, M., Jeffers, R., Tate, A., Dalton, J., Aitken, S.: KAoS Policy Management for Semantic Web Services. IEEE Intelligent Systems 19(4), 32–41 (2004)
11. Kagal, L., Berners-Lee, T., Connolly, D., Weitzner, D.: Using semantic web technologies for policy management on the web. In: Cohn, A. (ed.) Proceedings of the 21st National Conference on Artificial Intelligence, vol. 2, Boston, Massachusetts, July 16-20. Aaai Conference on Artificial Intelligence, pp. 1337–1344. AAAI Press (2006)
12. Finin, T., Joshi, A., Kagal, L., Niu, J., Sandhu, R., Winsborough, W.H., Thuraisingham, B.: ROWLBAC - Representing Role Based Access Control in OWL. In: Proceedings of the 13th Symposium on Access Control Models and Technologies, pp. 73–82. ACM Press (June 2008)