**UP**GRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by Novática <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*, <http://www.ati.es/>)

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>)

UPGRADE is the anchor point for UPENET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- InfoRewiew, magazine from the Serbian CEPIS society JISA
- Informatica, journal from the Slovenian CEPIS society SDI
- Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
- ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
- Mondo Digitale, digital journal from the Italian CEPIS society AICA
- Novática, journal from the Spanish CEPIS society ATI
- OCG Journal, journal from the Austrian CEPIS society OCG
- Pliroforiki, journal from the Cyprus CEPIS society CCS
- Tölvumál, journal from the Icelandic CEPIS society ISIP



Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: <novatica@ati.es>

UPGRADE Newslist available at
<http://www.upgrade-cepis.org/pages/editinfo.html#newslist>



ISSN 1684-5285

Monograph of next issue (April 2010)

**"Information Technology inTourism Industry"**

(The full schedule of **UP**GRADE is available at our website)

CEPIS UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org

**Vol. XI, issue No. 1, February 2010**



* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by **Novática**, journal of the Spanish CEPIS society ATI (*Asociación de Técnicos de Informática*) at <http://www.ati.es/novatica/>.

# A Privacy Preserving Attribute Aggregation Model for Federated Identity Managements Systems

*George Inman and David Chadwick*

*In order to support attribute based access control (ABAC) in federated identity management most existing solutions, such as Shibboleth and Cardspace, utilise a model in which a single identity provider (IdP) is used to both authenticate the user and provide a set of attribute assertions or claims to the service provider (SP) for authorisation. Since most real world IdPs typically only issue one or very few attributes to users and all users have multiple IdPs, this model has a significant limitation. Users are only able to use one or very few of their attributes to access a service. One solution is to aggregate attributes from multiple IdPs before accessing a service. In this paper we discuss some of the existing attribute aggregation models before introducing our own Linking Service model and its associated protocol mappings.*

**Keywords:** ABAC, Attribute Aggregation, Attribute Assertions, Attribute Release Policies, Information Cards, Liberty Alliance Discovery Service, Linking Service, SAML.

**Authors**

**George Inman** is a research assistant and PhD student in the Computer Science Department at the University of Kent, United Kingdom. He has spent the last 3 years as a member of the Information Systems Security Research Group at Kent, working on Attribute Aggregation and the PERMIS authorisation software suite. Prior to which he received a BSc in Computer Science from the University of Kent. <g.inman@kent.ac.uk>

**David Chadwick** is Professor of Information Systems Security at the University of Kent, United Kingdom. He is the leader of the Information Systems Security Research Group at Kent and a member of IEEE and ACM. His group are the creators of PERMIS (www.openpermis.org), an open source X.509 and SAML supported role based authorisation infrastructure which is part of the US NMI software suite. <d.w.chadwick@kent.ac.uk>

## 1 Introduction

A user's digital identity can be stated as the set of data that can be used to uniquely represent a single person or organisation within a specific context. In the standard model for federated identity management systems (FIMS), such as Shibboleth [1] or Cardspace [2], this context is the federation and the data that makes up the user's identity are the authentication and attribute assertions or claims released by the user's identity provider (IdP) to the service provider (SP). FIMS were often built under the assumption that a federation would offer limited services within a specific security domain such as a university or corporate environment and as such it was reasonable to assume that a user would use a single institutional or corporate IdP for accessing all the SPs in the federation. As these technologies mature however the size and scope of federations become increasingly larger e.g. at the time of writing the UK Access Management federation [3] had 764 member organisations. This means that it has become increasingly likely that a user will have several accounts at different IdPs within the same federation. If one considers the physical world of plastic cards, then users typically have lots of cards issued by many different IdPs. Each card typically only holds one user attribute (club membership, frequent flyer status, type of credit card etc) along with a validity period, a user identifier (usually the friendly name of the holder), a mechanism to authenticate the holder (usually a signature or PIN, but could be a photograph as well), and details of the issuer. Other contents such as holograms and chips are there to ensure the authenticity of the card and the attribute assertion (or claim) that it makes. They do not provide additional attributes of the user. Thus as FIMS expand to Internet scale, users will need to aggregate their attributes from multiple IdPs.

The use of multiple IdPs has several advantages to users and SPs. A single IdP is no longer required to issue all of a user's attributes, which is an unrealistic assumption to make. Rather each IdP will issue the attribute(s) for which it is authoritative. This means that a user can pick which subset of their attributes they present to a SP rather than passing their entire set. However this presents a severe limitation since no single IdP knows all the attributes that are required by a SP for authorisation. For example an online bookshop may give a student discount and therefore require both a credit card and a student card to complete the transaction. It is not realistic to expect a university IdP to issue a bank credential or a bank to issue a student credential.

This paper discusses the existing models for the aggregation of authorisation attributes, before describing a new model, which is capable of performing attribute aggregation in a privacy-preserving manner. Prior to developing our new model we generated a set of requirements for attribute aggregation from the answers provided to a widely distributed questionnaire, the results of which are presented in [4].

## 2 Existing Models for Attribute Aggregation

Early models for attribute aggregation often assumed

that a user would have a globally unique identifier [5], such as an X.500 distinguished name, which is contained in each issued credential. Each IdP would use the same identifier to identify the same user and so aggregation is trivial. Whilst most users do hold such globally unique identifiers, e.g. SMTP email addresses, most providers assign locally issued identifiers and passwords to their users, and use the email address as an attribute.

The Liberty Alliance was one of the first groups to address this problem via their identity federation work [6]. In this model the first IdP-SP to authenticate the user asks the user whether she would like to be introduced to other IdPs-SPs in the federation. If the user agrees and subsequently authenticates to another IdP-SP, it invites him to federate his second identity with that of his first. If the user agrees then each IdP-SP creates a random identifier for the user which they exchange. This ensures that neither IdP-SP knows the true identifier of the user but each can refer to the same user via the random identifier created by the other, and can therefore request the user's attributes when providing a service.

In [7] Klingenstein identifies several distinct models for attribute aggregation each of which are discussed below:

In the application database model an SP supplies additional information about the user from a backend database and aggregates this with attributes from the IdP. This model is used primarily to allow an SP to provide persistent user account information. This model has been implemented by the Shibboleth project [8] and used by SWITCH [9] to provide simple static attribute aggregation using a single persistent identifier. The static nature of this scheme is likely to present problems, as it requires each IdP to use the same identifier when referring to the user and provides no mechanisms for the discovery of accounts. This means that each IdP at which the user has an account must be known and configured prior to service provision at each SP which wishes to aggregate user attributes.

Identity Proxying is a model in which a SP trusts a single IdP to issue all a user's credentials. This IdP may then forward the authentication and attribute requests to additional IdPs, aggregate and reassert the returned attributes, ensuring that the SP obtains everything from the IdP it trusts. This is the model utilised by MyVocs [10]. Whilst this model allows for easy integration with existing SPs and IdPs it has several flaws.

The SP cannot be sure which IdP originally issued which credential as they are all repackaged by the trusted IdP before they are received by the SP. There is no clear method for controlling which secondary IdPs will be accessed once its request has been sent. The trusted IdP can view and potentially alter each credential issued by an IdP higher in the chain.

Identity relay is another form of identity proxy, which reduces the level of trust placed in the intermediary IdP by ensuring that the SP receives assertions from each queried IdP. Whilst this model removes some of the inherent flaws in the Identity proxy model created by the repackaging of attributes it still allows signed and encrypted credentials to be substituted with those of another user or omitted entirely prior to them being received by the SP.

Client mediated assertion collection uses an intelligent user agent to guide the user to authenticate to multiple IdPs, pulling attribute assertions from each and presenting the combined set to the SP.

SP mediated aggregation works in a similar manner but has the SP, rather than a user agent, sequentially redirect the user to multiple IdPs for authentication. Whilst both these models demonstrate a high level of privacy protection they require the user to manually authenticate to multiple IdPs, which may prove time consuming and annoying to the user. However this is the model currently used by 3-D secure [11] (Verified by Visa and Master Card SecureCode).

The Identity Federation model as introduced by Chadwick in [12] builds upon the Liberty Alliance work and utilises pair-wise relationships between IdP accounts to create links between them. These relationships are established through a user agent, which sends a user provided secret to each IdP after authentication. The two IdPs can then transfer a random alias to be used when referring to the user. When subsequently contacted by an SP the IdP returns the encrypted alias and details of the other IdP allowing the SP to contact the additional IdP for attributes. This model has the weakness that it may be possible for each IdP to infer which other attributes a user possesses based upon assumptions about which attribute(s) a linked IdP typically issues.

Whilst the SP and client mediated collection models provide secure and privacy-preserving aggregation, they also require the user to choose and authenticate to each IdP in turn due to a lack of links between IdPs. This is likely to prove time consuming if many IdPs are to be queried. Whilst the Identity Federation model is secure and allows multiple IdPs to be queried without multiple acts of authentication it compromises the user's privacy as each IdP queried knows of the existence of at least one of the user's other accounts. Therefore we propose a new model that is a variant of the Identity Federation model and the Identity relay model and utilises a new entity called a Linking Service (LS), which holds the links between user identities and may relay attribute requests between SPs and IdPs.

## 3 A Privacy Preserving Model for Attribute Aggregation

Our model for attribute aggregation assumes that the user is the only person who knows about all of his IdP accounts, and that he does not wish the IdPs to know about each other . We have devised a new federated entity called a Linking Service(LS), the purpose of which is to hold links between the user's IdPs without compromising the privacy of the user. As the IdPs link to the Linking Service they have no knowledge of any other IdP account. Furthermore the LS does not have any knowledge of who the user is or what attributes are held by each individual IdP unless it can be inferred from the IdP's details.

 

### 3.1 Link Registration

Accounts must be linked and configured at the LS before attribute aggregation is initiated. To accomplish this the LS acts as a standard SP and asks the user to login by requesting an authorisation token containing a randomly generated but persistent identifier (PId) from an IdP. This PId will then be used as a pair-wise secret between the LS and the IdP to identify the user's account in all future communications between the two parties. When the LS receives a new PId at login time, it creates a new entry for the user in its internal database. When the LS receives an existing PId at login time, it retrieves the user's existing entry from its database. If the user wishes to link additional IdP accounts to her existing database entry then she authenticates to another IdP requesting another PId which the LS then adds to the same database entry. As the PIds returned from the linked IdPs are randomly generated and not user friendly, the user can choose to add a nickname for each IdP account to her database entry, so that it can be easily identified.

Once all the accounts have been linked the user may wish to set a link release policy (LRP) before aggregation. This LRP policy is used to explicitly define which IdP accounts should be released to which SPs. This is by default a "deny all" policy meaning that no user information will be released to any SPs before specific rules are set. At this point the user may also wish to set non specific rules such as account 1 can be released to any SP.

#### 3.1.1 Level of Assurance

Different IdPs authenticate users in different ways and to different strengths e.g. username and password is weaker than smart card authentication. This is termed the Level of Authentication, or Level of Assurance (LoA). It can be loosely thought of as how sure a relying party can be that the user is really who they say they are. This depends not only on the method of authentication used – which we term the Authentication LoA – but also on the initial vetting and registration process that the user underwent – which we term the Registration LoA. NIST, National Institute of Standards and Technology, has a recommendation that classifies a user's LoA at four levels, with level 4 being the strongest and level 1 being the weakest [13]. A limitation of the NIST recommendation is that its LoA is a compound metric dependent on both the authentication method and the registration process. We believe that they are more useful if they are separate metrics, since IdPs may offer different authentication mechanisms and a static registration mechanism, or may alter the registration procedure that is used with the same authentication method. Thus we introduce the dynamic Session LoA which is computed at login time as the lowest of the user's Registration LoA and the authentication method chosen. We have made provisions to include the Session LoA in our protocol messages. When the LS redirects the user to an IdP during link registration the IdP authenticates the user using its chosen authentication mechanism, which generates an associated Session LoA. The LS then stores this Session LoA as the Registration LoA for this linked account in the user's database entry.

### 3.2 Service Provision Phase

When the user attempts to access a resource the SP can either redirect the user directly to an IdP, or indirectly via the LS. If the user is redirected to the LS then the LS acts as a WAYF forwarding the authentication and attribute request to an IdP of the user's choosing.

Once at the IdP the user is asked to login and to declare whether or not she wishes to aggregate attributes from additional linked accounts. (This may take the form of a tick box placed on the IdPs login page.) If the user decides not to aggregate additional attributes then the IdP returns a standard authentication token and an encrypted set of attributes for the SP. The authentication token contains a random transient identifier to identify the user of this session. If the user wishes to aggregate her attributes then the IdP creates an additional referral attribute containing the encrypted PId for this account that is valid at the LS.

The response message is returned to the querying entity, either the SP or the LS. If the SP receives the response, then it decrypts the attributes to see if they are sufficient to authorise the user. If they are, the user's request is fulfilled. If they are not, and no referral is present, then the user's access is denied. If a referral is present, the SP forwards this to the LS, via the user's browser, along with the original authentication token, an attribute query and a Boolean attribute stating whether the LS or the SP should perform the attribute aggregation.

If the response is returned to the LS, or the LS is forwarded the message from the SP, it decrypts the PId in the referral and looks up the user's entry in its internal database. The LS checks to see if specific LRP rules exist for the SP and the authenticating IdP, if no rules exist then the LS may ask the user to dynamically create them. If a set of rules do exist the LS will either query each linked IdP for attributes, or return a set of referrals to the SP for it to do the querying, depending upon the Boolean attribute.

A query to an IdP comprises: the original authentication token from the authenticating IdP, the attribute query from the SP, and the encrypted PId for the user account to be accessed. These can be used by the IdP to determine if it trusts the initial act of authentication and to locate the user's internal account. The IdP then generates an attribute assertion containing the user's attributes and encrypts it to the SP. The user is identified using the random transient identifier from the authentication token. The assertion is returned to the SP, either directly or via the LS.

The SP will receive a set of assertions containing an authentication token and multiple attribute assertions from multiple IdPs which all contain the same random transient identifier. Since the SP trusts all the authoritative sources it can be assured that the same user possesses all of the returned credentials, and has been successfully authenticated.

#### 3.2.1 Use of LoA in Service Provision

As discussed in section 3.1.1 the LS stores a Registra-

tion LoA for each IdP account in the user's database entry during the link registration phase. During the service provision phase the LS will only utilise linked IdPs whose Registration LoA's are higher than or equal to the current Session LoA, computed by the authenticating IdP. This prevents the user from creating links with low Registration LoAs and using them at higher Session LoA's. A user can create links at high Registration LoAs knowing that they can still be used at a lower Session LoA, since the SP will only trust them up to the level of the Session LoA.

When a linked IdP receives a request for attributes it must extract the Session LoA from the authentication token and then compare this against its Registration LoA.. If the Session LoA is less than or equal to the latter value then the IdP will release additional attributes to the SP, otherwise it will not.

## 4 Protocol Mappings

Our conceptual model has been mapped to the Security Assertions Markup Language (SAML) v2 protocol during the link registration phase, and to both Liberty Alliance and Cardspace protocols during the service provision phase. Although our model provides for the passing of LoA between the various components this is not currently a part of the SAML v2 agreed specifications. However OASIS is currently working on a SAML profile of the NIST LoA recommendation [14] which we utilise for passing the LoA between our components.

### 4.1 Link Registration Protocol

The link registration protocol utilises standard SAML 2.0 <samlp:AuthnRequest> messages [5] to request user authentication by a selected IdP and return a persistent identifier to the LS. Upon receipt of the PId in the <samlp:Response> message the LS will either find an existing entry in its database or create a new entry. Either way the user can then link additional IdP accounts to this one.

To ensure that the IdP always returns a PId to the LS, the SAML authentication request is constrained in the following ways:

- The Format attribute of the <NameIDPolicy> is set to "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" to ensure that a PId is returned.
- The allowCreate attribute of the <NameIDPolicy> is set to true, which allows the IdP to create a PId if none already exists.

### 4.2 Service Provision Protocols

We have devised a protocol mapping for attribute aggregation using Liberty Alliance protocols and one using CardSpace protocols. Each mapping encodes referrals as Liberty Alliance ID-WSF Endpoint References (EPRs) according to the EPR generation rules defined in Section 4.2 of [15].

Each EPR points to an entity at which the SP can find additional attributes for the user and the EPRs <sec:Token> element contains the encrypted PId of the user.

#### 4.2.1 Service Provision using the Liberty Alliance Discovery Service

Our model requires minor enhancements to the Liberty Specifications which we have discussed with the Liberty Alliance group who recommended that we use the Discovery Service Mapping described below.

After the user contact the SP, the SP issues a SAML authentication request message, which the user's browser passes either to an IdP or a LS. This message asks the IdP to generate a random identifier for the user in the authentication response and to return both attributes and referrals (EPRs) in the response. The SAML response consists of a single SAML assertion containing a single sign on (SSO) assertion with three statements: an authentication statement, an attribute statement containing the user's attributes and an attribute statement containing the EPR(s) of the LS.

If the message is passed to the IdP via the LS then the LS formulates a new authentication request to the IdP using the Enhanced Client or Proxy (ECP) Profile of SAML [16]. If the SSO response contains the EPR of the LS, the latter may choose to perform attribute aggregation as described below and return either additional EPRs or attribute assertions in it's response to the SP. Otherwise the LS simply returns the SSO response to the SP.

Once the SP receives the SSO assertion it attempts to resolve any referral EPRs using the Liberty Alliance ID-WSF Discovery Query profile [17]. The DiscoveryQuery operation (Section 3.3 of [17]) enables an IDWSF discovery service to be queried for relevant endpoint references that can be used to access other web-based services. The DiscoveryQuery itself consists of a Query message and a QueryResponse. The Query message contains the <sec:Token> element of the relevant EPR and the SSO authentication assertion, included as SOAP headers [18].

We define two Query messages: the first is sent from the SP to the LS and asks for the EPR of each linked IdP's Discovery Service; the second is sent from either the LS or the SP to an IdP, and asks for the EPR of its SAML V2.0 Attribute Authority (AA). In order to make the design more flexible both EPR types are requested in the same Query message. The recipient already knows what type of service it is and therefore understands which EPR type to respond with. It ignores the second type. This means that the SP does not need to know whether it is talking to a LS or an IdP. It can create its DiscoveryQuery messages in exactly the same way to both.

The LS decrypts the PId in the message's SOAP header and uses it to identify a user's database entry. It extracts the Session LoA of the initial authentication and if the SP is performing aggregation returns a QueryResponse message containing additional EPRs pointing to the discovery service of each linked IdP's account with a greater or equal Registration LoA. If the LS is performing aggregation then it sends a DiscoveryQuery message to the discovery services of these IdPs.

The IdP's discovery service identifies the user's account by decrypting the PId. It then maps the random identifier

 

from the authentication assertion into the user's account. The IdP returns a DiscoveryQuery response containing the EPR of its AA where the random identifier is now valid. The SP (or LS) sends a standard <samlp:AttributeQuery> to the AA using the random identifier, whereupon the AA returns a standard <samlp:Response> encrypted so that only the SP can retrieve the attributes.

#### 4.2.2 Service Provision using the CardSpace Protocols

Our protocol mapping requires only minor changes to the CardSpace Identity Selector client and to the WS-Trust protocol [19]. After the user connects to the SP and is referred back to his Identity Selector, this picks up the SP's security policy using the WS-Metadata exchange protocol [20] as now. If the SP has stated in its service policy that it is capable of accepting referral attributes, a check box labelled "do you want to use your linked cards in this transaction?" appears below the authorisation dialogue. If clicked, the Identity Selector attempts to get the users claims using a modified WS-Trust message containing a new Boolean attribute "aggregateIdentities". This states that referrals should be returned along with the user's attributes. Assuming that the user's authentication credentials are correct, the IdP returns a WS-Trust RequestSecurityTokenResponse message contains a SAML authentication assertion, a SAML attribute response containing the user's attributes and a SAML attribute response containing referral(s) to the user's LS(s). Cardspace relays these assertions to the SP so that it can perform attribute aggregation using the Liberty Alliance Discovery protocol described above.

## 5 Comparison with Existing Models

Our model removes the potential privacy problems present in existing identity federation models by introducing a level of indirection through the use of a linking service. This prevents IdPs from having direct knowledge of additional user accounts. The persistent links between each IdP and the LS in turn alleviates the need for additional acts of authentication by the user. User consent is provided through a Link Release Policy which allows the user to set specific rules for which linked IdPs can be released to each SP she communicates with. Our model minimises the trust that is needed in the LS by not revealing the user's identity or any user attributes to the LS, and by removing the possibility of the LS tampering with or replacing the user credentials by allowing the SP to aggregate all the user's attributes if it so desires.

## 7 Conclusions and Future Work

As federations and their associated identity management systems grow in size and complexity it becomes more likely that user's will have multiple accounts at different IdPs. Unfortunately most existing systems do not support the use of attributes from more than one IdP. To counteract this deficiency we have designed and developed a linking service, which allows a user to link his various IdP accounts together in a privacy-preserving manner. These accounts can then be used automatically during service provision to access and return attributes from multiple authoritative sources, without requiring the user to authenticate separately to each IdP. We have mapped our conceptual model onto existing standard protocols based on SAML, Liberty Alliance and CardSpace, and have implemented the SAML and Liberty Alliance specifications which will be released as open source software as part of the PERMIS software suite [21]. We intend to implement the CardSpace protocols in the near future.

## Acknowledgements

The authors would like to thank the UK JISC and EC FP7 for funding this work under the Shintau and TAS3 projects respectively.

## References

[1] R. L. "Bob" Morgan, Scott Cantor, Steven Carmody, Walter Hoehn, and Ken Klingenstein. "Federated Security: The Shibboleth Approach". Educause Quarterly. Volume 27, Number 4, 2004.

[2] Arun Nanda. "Identity Selector Interoperability Profile v1.0" Microsoft Corporation, April 2007. See <http://download.microsoft.com/download/1/1/a/11ac6505-e4c0-4e05-987c-6f1d31855cd2/Identity-Selector-Interop-Profile-v1.pdf>.

[3] The UK Access federation. <http://www.ukfederation.org.uk/>.

[4] David Chadwick, George Inman, Nate Klingenstein. "Authorisation using Attributes from Multiple Authorities – A Study of Requirements". Presented at HCSIT Summit - ePortfolio International Conference,16-19 October 2007, Maastricht, The Netherlands.

[5] OASIS. "Assertions and Protocol for the OASIS Security Assertion Markup Language. (SAML) V2.0", OASIS Standard, 15 March 2005.

[6] Liberty Alliance. "ID-FF 1.2 Specifications". Available from <http://www.projectliberty.org/liberty/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>.

[7] N. Klingenstein. "Attribute Aggregation and Federated Identity", pp.26, 2007. International Symposium on Applications and the Internet Workshops (SAINTW'07), 2007.

[8] Shibboleth "NativeSPAttributeResolver". Available from <https://spaces.internet2.edu/display/SHIB2/NativeSPAttributeResolver>.

[9] SWITCH "SAML 2 V0 Platform". Available from <http://www.switch.ch/aai/support/presentations/opcom-200909/AAI-OpCom-VOPlatform.pdf>.

[10] Jill Gemmill, John-Paul Robinson, Tom Scavo, Purushotham Bangalore."Cross-domain authorization for federated virtual organizations using the myVocs collaboration environment" Concurrency and Computation: Practice and Experience. Published online July 2008 at <http://www3.interscience.wiley.com/journal/120780040/abstract?CRETRY=1&SRETRY=0>.

[11] 3-D secure. See <http://en.wikipedia.org/wiki/3-D_Secure>.
[5] W. Johnston, S. Mudumbai, M. Thompson. "Authorization and attribute certificates for widely distributed access control". Proceedings of Seventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 1998 (WET ICE '98), pp.340-345, 17-19 Jun 1998.
[12] David Chadwick. "Authorisation using Attributes from Multiple Authorities" in Proceedings of WETICE 2006, June 2006, Manchester, UK (best paper award in Security Workshop).
[13] NIST LoA. <http://www.nist.gov/>.
[14] OASIS. "Level of Assurance Authentication Context Profiles for SAML 2.0", Working Draft 01. 01, July 2008.
[15] J. Hodges, R. Aarts, P. Madsen, and S. Santor (Editors). "Liberty ID-WSF Authentication, Single Sign-On, and Identity Mapping Services Specification v2.0". Liberty Alliance Project.
[16] SAML Profiles.
[17] J. Hodges, C. Cahill (Editors). "Liberty ID-WSF Discovery Service Specification V2.0". Liberty Alliance Project.
[18] J. Hodges, J. Kemp, R. Aarts, G. Whitehead, P. Madsen. "Liberty ID-WSF SOAP Binding Specification v2.0" Liberty Alliance Project.
[19] OASIS, "WS-Trust 1.3", OASIS Standard, March 2007.
[20] Doug Davis, Ashok Malhotra, Katy Warr, Wu Chou, "Web Services Metadata Exchange (WS-MetadataExchange)", World Wide Web Consortium, Working Draft WD-ws-metadata-exchange-20090625, June 2009.
[21] See <http://www.openpermis.org and http://sec.cs.kent.ac.uk/permis>.

 