A Reference Model for Authentication and Authorisation Infrastructures Respecting Privacy and Flexibility in b2c eCommerce

Christian Schläger
Department for Information Systems
University of Regensburg, Germany
christian.schlaeger@wiwi.uni-regensburg.de

Thomas Nowey
Department for Management of Information Security
University of Regensburg, Germany
thomas.nowey@wiwi.uni-regensburg.de

Jose A. Montenegro
Computer Science Department
E.T.S. Ingenieria Informatica
University of Malaga, Spain
monte@lcc.uma.es

Abstract

Authentication and Authorisation Infrastructures (AAIs) are gaining momentum throughout the Internet. Solutions have been proposed for various scenarios among them academia, GRID computing, company networks, and above all eCommerce applications. Products and concepts vary in architecture, security features, target group, and usability containing different strengths and weaknesses. In addition security needs have changed in communication and business processes. Security on the internet is no longer defined as only security measures for an eCommerce provider against an untrustworthy customer but also vice versa. Consequently, privacy, data canniness, and security are demands in this area.

The authors define criteria for an eCommerce provider federation using an AAI with a maximum of privacy and flexibility. The criteria is derived concentrating on b2c eCommerce applications fulfilling the demands. In addition to best practices found, XACML policies and an attribute infrastructure are deployed. Among the evaluated AAIs are Shibboleth, Microsoft Passport, the Liberty Alliance Framework, and PERMIS.

1. Introduction

The usage of a service on the internet - maybe to buy a book, or to use a geographic routing service - is not trivial anymore. The purchase of a book is not simply a link to click on but it stands at the end of a sequel of security and data intensive processes - most of them hidden from the user. The business process should be based on a securing infrastructure. AAIs - Authentication- and Authorisation Infrastructures - can provide a secure basis for any business process on the internet. Services start with the identification and authentication of users, entitle the authorisation of subjects and objects by the owner, can contain the management of attributes and policies, and lead to access decision making and enforcement resulting in an access control of some kind. Likely structures for AAIs are shown in Figure 1.

Not looking at AAIs holistically is an approach likely to fail. With the example of PKI we have witnessed that just putting authentication in the centre of business processes is too limited. It is not only a question of ones true identity on the internet but rather a question of rights entitled to a subject or group [10].

The importance of an AAI also lies in its power to connect business partners together. A resilient and trustworthy security infrastructure is needed for clients and providers to exchange any kind of data or to secure information systems inside a company, among a federated circle of vendors etc.

As security threats to eCommerce providers multiply and the public attention shifts towards security breaches eCommerce vendors are under increasingly pressure to provide secure services to their customers. Unfortunately security is not seen or treated as a core competency in eCommerce. Authentication and authorisation are seen as an enabler. These enabling services should be provided out-of-the-box by an eCommerce platform or an application server. On the other side secure online shopping or service usage is essential for customers trusting a provider. Today's internet customers want sophisticated services that guarantee data security, personal data canniness, privacy, and are transpar-

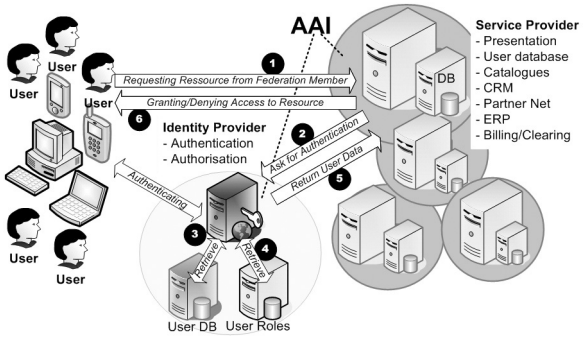

Figure 1. Authentication and Authorisation Infrastructure with IdP and SP

ent for the user. If desired a Single-Sign-On (SSO) should be provided that gives access to a federation of providers.

Together with the complexity of business processes on the internet we see a rise in the need for flexible, dynamic metadata about subjects and objects. Those attributes contain information about a customer and might be processed to generate new data - like role membership, consumer behaviour, patterns, etc. Attributes are optimal for dynamic access control decisions building the basis for a role based, discretionary, or completely attribute based access control [18, 16].

AAIs could be the solution to mediate between different stakeholders in questions of data security, privacy, and trust. Provided that the AAI can gain the trust of users and service providers it could act as a Public Trustee. As described in [5] such a trustee could facilitate the feasibility of multilateral security.

Another factor for the promotion of AAIs is the need of service providers, especially in eCommerce to concentrate on their core competencies and source out non expertise fields or services where no additional competitive advantage can be gained. A federation of eCommerce providers could use a central AAI to outsource security services. As we have shown in [14] eCommerce among other industries searches for means to calculate IT risks and security investments. Joint security services in an AAI can strengthen the security through specialised AAI providers and at the same time reduce costs.

Besides inner organisational usage and GRID computing b2c eCommerce is the main field of activity for AAI products and projects. This paper analyses security needs in business-to-consumer eCommerce applications. Of course AAI research can't be limited to b2c processes. However, b2c eCommerce has the advantage of clearly separable, obvious stakeholders and actors (customers, vendors, intermediate service providers) and well defined communication processes. This allows for a reduction of complexity. Inner organisational AAIs have special needs as far as IT Governance is concerned. Rules applying here can be found in [12] and will be addressed separately.

This paper is structured as follows. In section 2 requirements and criteria are derived from the stakeholders' demands. Section 3 introduces 4 relevant and leading AAIs. In section 4 we match their functionalities with our requirements. Combining best practices and privacy research a reference model is derived in section 5 forming the basis of an AAI fitting our demands. The paper finishes with a conclusion and the outlook for future research and work.

2. Requirements

AAIs are used to connect various actors in communication processes. For eCommerce in a b2c environment the two obvious stakeholders are customers and service providers. In addition external AAI providers should be taken into consideration. This paper concentrates on three main demands (privacy, flexibility, and federation). A broader analysis of demands can be found in [19].

2.1. Privacy

Preserving privacy and customer's data security seems contrary to eCommerce vendors' needs. In eCommerce customers need to be identified and data is desired to gain information about product likings, consumer and payment behaviour. However, this data holds security requirements. A trade-off has to be made between customer and vendor concerning essential data and additional consumer information [6, 5]. AAIs can mediate in this area of conflict. In a federation data about a costumer's payment behaviour or cross selling could be exchanged. On the other hand an AAI could let the customer stay under a pseudonym and filter information. Accordingly the true identity of the customer is only revealed if legally needed or an actual purchase requires it. Anonymity could be guaranteed via a proxy that acts on behalf of the customer or - if a direct interaction is needed - through the usage of anonymous attribute certificates. These certificates could carry authorisation informa-

tion as well as certify a pseudonym. A protocol to obtain such certificates is given in [1].

Managing profile data at one central point holds the benefit of making it easier to keep track of stored data and keeping the information up-to-date. Additionally, it enables the user of an AAI to learn what is stored about his person as required for example by German law. The user can ask for the deletion of private data and could also allow what kind of data from his profile is provided to an eCommerce vendor in a federation.

The EC's Data Protection Working Party monitors closely the functionalities of AAIs and password managers [4]. The Working Party was founded based on Article 29 of the 95/46/EC Data Protection Directive and refers to the aforementioned directive as well as the privacy and telecommunications directive 97/66/EC. Demands include decentralised storage of personal profile data, data canniness, and the already mentioned option for customers to access profile data, control it, and if wanted let it be deleted.

2.2. Flexibility

The process of authenticating and authorising a user doesn't stop with identification and the assignment of rights. AAIs need to be able to manage the whole process as shown in figure 2.

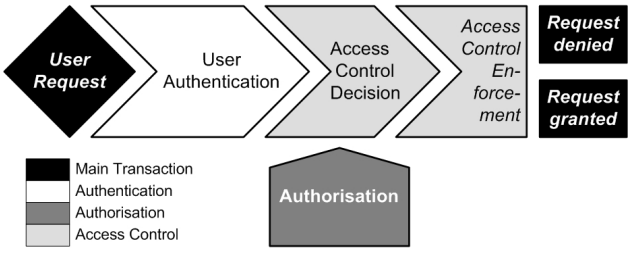

Figure 2. Simple Access Control

Access decisions should no longer be based on a static assignment of roles but pay tribute to the dynamic and changing nature of eCommerce. In addition an eCommerce federation might feature a huge customer base let alone the vast potential of customers in the whole World Wide Web. If access decisions are to be taken they should make use of the information a customer generates during his membership. That information could be positive experiences in his payment behaviour at one vendor or throughout a federation. Again attribute infrastructures and reasoning techniques would be suitable to handle the amount, variety, and changing nature of customer data.

2.3. Federation

In the past, processes in b2c eCommerce were structured like n:1 - meaning that one eCommerce provider had n customers that used his services. Of course with the success of eCommerce a customer soon had accounts at several eCommerce providers. Problems like the maintaining of all these accounts, different levels of security at each vendor, security breaches etc. occurred. eCommerce providers missed the interconnection of user data to fight fraud and gain competitive data. Consequently, the idea of federations was born. Ideally providers are joined together in a structure like n:m meaning in a federation each vendor providing different or complementary services. If common services like a customer database are outsourced a structure like n:1:m develops (figure 1). AAIs can provide their service as a central point of security, authentication, and authorisation in these federations. Two main factors promote the usage of AAI federations in b2c eCommerce. First the additional amount and quality of information about a customer and second the possibility to outsource non core competencies like security features to a trusted partner. As far as AAIs are concerned it is possible for the eCommerce provider to outsource every step from authentication to the enforcement of access control decisions to the AAI. In this scenario the AAI would work as a proxy server for the entire communication.

3. Leading AAIs

In 2005 we have analysed seven major AAIs [19]. As shown in [19] four AAIs are especially relevant in b2c eCommerce in consideration of privacy, flexibility, and federations: the Web-Focused AAIs Shibboleth, Microsoft Passport, the Liberty Alliance Framework and the PMI PERMIS.

3.1. Shibboleth

Shibboleth is an AAI from the U.S. Internet2 Organization connecting over 200 American universities [2].

In Shibboleth each university can alternately be service (SP) or identity provider (IdP). A student from university A trying to gain access to a resource at university B will be asked by the SP to name his or her IdP (home university A) via a so called Where-Are-You-From-Server. The IdP authenticates the user acknowledging this process via a SAML response. Privacy is respected in Shibboleth twofold. First the request is anonymous and second the user decides in his Shibboleth profile what kind of attribute he wants passed along The identity of the user is not revealed but a dynamic handle is generated identifying the request. The Shibboleth SP asks the IdP for further attributes about the user using them to compute and enforce an access control decision.

Shibboleth doesn't specify the means of authentication and the access control. Each member can use whatever mechanism seems fit to them or is already in place, therefore reducing the contribution of Shibboleth to a system of partners that trust each other as far as the authentication mechanism is concerned and for the dispersal of attributes.

3.2. Microsoft Passport

Microsoft Passport, although often criticised, is the first and was the largest commercial AAI so far. Passport concentrates on Single-Sign-On (SSO) for the user who gets is passport account with every hotmail account. Passport relies heavily on the usage of cookies imitating to some extend Kerberos's ticket functionalities. The login to a SP is redirected to Passport requiring his username and password. The SP's ID is transmitted via URL encoding enabling Passport to redirect the client and storing several cookies. At the SP a software is needed - the so called Passport-Manager. This software reads URL encoded data and stores additional cookies into the SP's domain permitting an access control decision. At another vendor the passport cookies are used to enable a SSO [11]. The vendor decides about access of resources using his authorisation and access control mechanism of choice. Passport is a SSO system meaning that it only asserts the user's authentication.

Passport uses a central database to keep all client information, a matter of discussion in recent years. In addition the Microsoft policy of so called "security through obscurity", not providing consistent information about the stored data and its protection is widely criticised. Several security vulnerabilities were found and fixed in the past [7]. Passport's future is uncertain. After most of its main clients abandoned it (e.g. eBay in 2004) rumours are that it will be used only internally for Microsoft services or integrated into an existing web based service.

3.3. The Liberty Alliance Framework

Liberty was the open source community's answer to Microsoft Passport in 2001. Governmental and Non-Profit organisations as well as well know IT players like SUN or IBM are building the consortium. In Liberty a Circle of Trust (COT) establishes a Liberty system [8, 9]. Each partner provides the authentication for his users with his own methods while they themselves can login to all other partners in a SSO. The user authenticates at his IdP and if he wishes a cookie is stored under a common domain where every member hosts a server so they all can access the cookie. If a user moves to a COT member the cookie is read, the IdP asked for appropriate authentication, and an assertion is awaited. Communication is based on the SAML protocol.

Liberty resembles more a framework than an actual AAI. A COT has to decide on the implementations. The creation of a COT has to be planned carefully due to its openness. The SAML assertions can carry any attribute the COT agrees upon. Liberty is distributed. The IdP is not fixed like in Shibboleth or centralised like in passport. It is possible to login at different points of the COT thus resulting e.g. in different user names or attributes that are transferred. The identity of the user is not revealed in the process of requests and assertions.

3.4. PERMIS

The EU project PERMIS [3] is closely integrated into the target system. This can be e.g. an apache web server. Instead of using the apache security functionality like .htaccess PERMIS is used to derive the role name of a user and a PERMIS policy is used to control access. The target application is also responsible for user authentication as PERMIS is authentication agnostic.

PERMIS uses X.509 attribute certificates (AC). These bind the distinguished name of the user to a role. An XML policy authorises roles and targets. ACs and their revocation lists are stored in LDAP directories. If a user wants access to a target the PERMIS access control enforcement function will delegate his request to the access control decision function which determines the correctness of the AC and its compliance to the policy. If access is granted the decision is given back to the enforcement function which grants the access or not.

The centrally stored ACs can contain any information an Attribute Authority has assigned. Of course different authorities can work together creating an attribute storage LDAP. Attributes are validated via the authorities' signatures. The decision and enforcement functions have to be implemented into the web server at the SP.

4. Matching AAIs and Requirements

4.1. Privacy

Shibboleth doesn't disclose the user's real name and he or she can decide what kind of attributes can be passed along. However, all of these available attributes are provided whether or not needed for an access control decision. A real name or address is never needed. However, if a situation would occur in which the user would have to disclose his or her real name to the vendor, a matching could be made to all available attributes.

In Passport the user needs to trust Microsoft to not misuse his data. This data consists of his profile and also his customer behaviour. However, the user has no opportunity to see, control, let alone delete this information. Microsoft

does not even have a privacy policy. The cookies stored contain profile data the user cannot decide upon.

Liberty, with a decentralised structure and a focus on just authentication, naturally opposes Microsoft. As several possibilities to enter the COT are possible a SP can just be sure that the actual IdP has authenticated the user. Different usernames and profile information can be given and nevertheless federated in Liberty. However, a COT can decide to exchange attributes of the user. Again, due to the distributed nature it is nevertheless impossible to be sure to gather all bargain relevant attributes at all federated partners. To be fair the Liberty framework is just a framework indeed with guidelines for an actual implementation. No Liberty system equals the other and users should be careful to look at the privacy policy of the system in question.

PERMIS uses just a distinguished name (DN) for the storage and retrieval of attributes. Privacy can be guaranteed if the certificates are bound to a pseudonym and the authentication disables a matching between name and DN. As certificates are publicly available and the content is not encrypted a provider or attacker getting the DN can access all available attributes. This is again an unnecessary disclosure of personal information.

4.2. Flexibility

As shown, AAIs should provide methods to manage the entire process of authentication and authorisation. Attributes and the inference of attributes with rules are the most flexible solution to deduce access rights or role memberships. To conclude a trusted access control decision all necessary attributes but not more should be compiled and the appropriate rules should be executed.

Unfortunately none of the analysed AAIs uses an attribute infrastructure to manage dynamic information about subjects and objects. PERMIS makes use of sophisticated certificates able to hold any attribute imaginable but uses the data only to store the user's role name for a resource. Shibboleth, Passport and Liberty could provide the service provider with any kind of data through SAML assertions or the cookie stored data but it is not used for more then role transportation. Furthermore there is not filtering of attributes to the actual need.

Shibboleth relies entirely on the authentication and access control mechanisms in place of its partners. Due to its historical background the systems in use at universities are not touched. The allocated attributes however are standardised. Therefore the subject authorisation can be called "guided" by Shibboleth.

Passport is a SSO system taking care of authentication for its vendors. Authorisation and access control still have to be managed by the SPs. Profile data is accessible but not filtered for the SP.

Liberty like Passport provides a SSO. The roles of SP and IdP change but could also be hold simultaneously by a COT partner. Attributes can be transferred but again there is no filtering. Another drawback for flexible attribute based authorisation is the uncertainty to accumulate all attributes.

PERMIS is authentication agnostic depending therefore on another system. The access control decision is made and enforced by PERMIS. Attributes are gathered and managed by the system, however PERMIS in its current state is role based, meaning that attributes are role names for various resources. The correctness of attributes is guaranteed by an attribute authority; as is the policy in use. Flexibility as far as targets are concerned is limited due to the close integration of PERMIS into the target.

4.3. Federation

The term federation for b2c eCommerce applications has been coined especially in the Liberty project. Together with Shibboleth and Passport federations are a key element in these AAIs. The potential to outsource customer data and security problems is least developed and intended in Shibboleth. Passport as a commercial SSO provider naturally provides SPs with the most potential to outsource AAI elements. PERMIS again needs an authentication mechanism. This provided it could be a suitable AAI for a federation if the limitation of the close integration into the target server is acceptable.

5. Reference model

Our proposed reference architecture can be seen in figure 3. The architecture enables the process of requesting a resource as given in figure 4. The starting point is the user's request. In the event of a request (step 1 in figure 3) the user is redirected to the AAI's central authentication and authorisation service (step 2) carrying wit him some kind of resource ID. The system grants or denies the requested action. User involvement is needed only to authenticate (step 3). Entities involved are the user, the federation member who's resource is requested, and the AAI including means to store and alter user data, attributes, and policies.

We will sketch out the entire process of authentication and access control using an attribute infrastructure and policies to derive an access control decision. To formulate rules and policies (accumulation of rules) XACML - the eXtensible Access Control Markup Language has become standard [15]. Inference algorithms compute attributes of subjects and objects to decide whether or not access is granted. XACML can also be used to deduce role memberships from attributes. It might be possible to compute all the customers purchasing events resulting in a role membership granting for example rebates or special payment options. For every

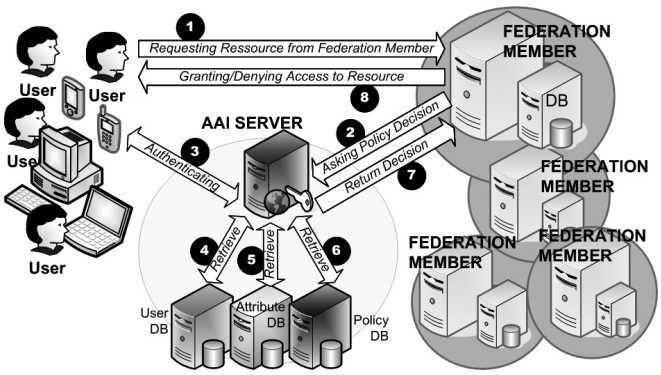

Figure 3. AAI Reference Architecture with Attribute Infrastructure

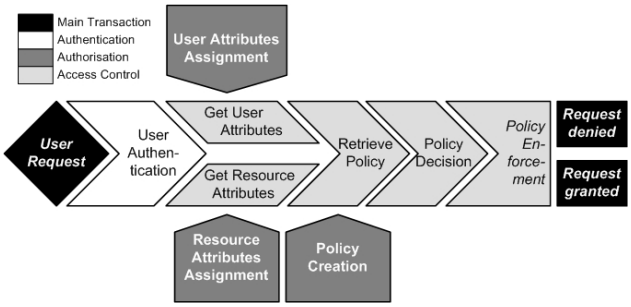

Figure 4. Reference Model, needed AAI processes

step we will look at the introduced AAIs and decide if a best practice approach is to be found. In addition the potential of the technologies mentioned above are taken into consideration.

5.1 Authentication

For our reference model we decided to use username and password or a PKI certificate with pseudonyms to guarantee privacy (step 3 in figure 3).

Widely promoted but seldom used PKI was supposed to be the solution of choice for authentication but only PERMIS recommends the usage of PKI as authenticator. Due to its advantages we recommend the usage of PKI for our reference model in the case where no anonymity is desired or a certificate using a pseudonym rather then a real name. However, due to PKI's disadvantages the usage of usernames and strong passwords [10] seems more likely. An AAI provider could act as a Certificate Authority but more realistically an existing third party PKI would be used.

5.2 Authorisation

We have decided on an attribute based access control model therefore needing a corresponding authorisation process.

Vendors authorise users via the creation of policies and attribute assignments to their resources. Clients can have attributes per se (creation of a new account), explicitly assigned by the vendor, or derived from their behaviour or features (age, location, and alike).

In Shibboleth the users' roles are passed along from the IdP to the SP. The Shibboleth role is derived from his position at the IdP (his home university), however, the role is static and the roles rather trivial (student, employee, ...).

As shown in Figure 4 the authorisation is not part of the direct process of requesting a resource. Naturally authorisation happens prior to the access request. Authorisation has to be done for subjects requesting and objects being requested. In our reference architecture attributes are assigned to users and resources. These attributes have to be compliant with the XACML policy in use. A federation needs to agree on a set of attributes. As [16] has shown attributes can derive from an ontology or even be deducted from unstructured information.

Attributes about a user can be hold either centrally (as given in figure 3), locally at the vendors site, or hybrid storing the attributes partly centrally and to some extend at the vendors site. As the user may have experiences and accounts at different federation's vendors, in an extreme case locally means at m sites (m being the number of vendors in a federation).

The attributes for resources are stored locally at the respective vendor's site. They are collected in the access control process. As a storage format PERMIS proposes X.509 attribute certificates. However, these certificates do not comply fully with the ITU-T standard. In [13] we have shown a fully compliant prototype to generate, delegate, and manage X.509 attribute certificates.

The rules to access a resource are put together into policies. Again policies can be stored in three different ways: first, completely central at one of the AAI servers (again see Figure 3 for an example), second, locally at the vendor's site or third, a centrally stored master policy is enhanced by more detailed and individual policies from the respective vendor. As an example the AAI server could gather the user's payment behaviour from every federation member, translate the events with a common policy to a user class (e.g. gold user, standard user, etc.). The local policy would then state whether for a resource of a certain value he is privileged to pay by invoice, credit card or gets a discount.

5.3 Access Control

Our reference architecture uses XACML policies to decide on access.

In our model access control is split into policy decision and policy enforcement - as usual in attribute based access control schemes. Using attributes and a policy to decide on access rights, the place of decision and enforcement can differ. Taking the example above an eCommerce provider who forwarded a request to the AAI takes the decis ion and enforces it with its own means - e.g. the Apache build in access control functionalities. This would be the usual scenario. Using the AAI's central server as a proxy is the other option (figure 5). The request for a resource and the denial of access would be handled by this server. However, the feasibility is questionable. The proxy becomes a single-point-of-failure and a bottleneck for the entire federation.

Our model makes use of a sophisticated attribute infrastructure. The AAI pulls from the vendor's or his central database attributes about the user and the resource (steps 4 and 5 in figure 3). This process can be quite complex. To ensure that no data about prior purchases are transferred from one federation member to the other the AAI has to collect all attributes. It would be unjustifiable to let a vendor retrieve all attributes from his partners thereby gaining unnecessarily knowledge about the user. The AAI asks every provider if he is in possession of attributes. The AAI has to ensure that all available attributes are processed otherwise no reliable decision can be taken.

Next the AAI needs to assemble the needed policies (step 6). Afterwards the access control decision is computed. The outcome of the decision (can subject A access object B each with the corresponding attributes under the rules in policy C) is either Yes, No, or N.A. The latter needing some sort of special handling.

The need to protect private data from other vendors in a federation is very well respected in Liberty. However, Liberty can not guarantee the complete pooling of attributes due to its heavily distributed architecture. There are m-1 ways to authenticate at the vendor's site coming from another partner in the federation. Accordingly there are m-1 possible attribute collections to hand over.

5.4 Privacy

Privacy is a question of knowledge of user data. Therefore it is crucial to know which entity in our model knows what. Obviously the vendor is informed about the client's purchases at his site. He knows neither about his client's purchases nor about other actions at his federation partners. The AAI pulls the attributes, events and status information and hands back only a filtered result or if the PDP is completely centralised the vendor just gets to know the policy decision. If not evitable (e.g. mailing of goods) the user can act anonymously in the federation or under a pseudonym.

The AAI can be a point of attribute verification by the user. As required by law user information can be accessed by the user and deleted if desired. We are aware of the problem of negative attributes. If a user knows that attributes are stored about him that lower his credibility he would erase his account and try to create a new, unburdened one. Therefore it is necessary to discard the idea of negative attributes and rather use positive attributes that improve an initially sceptical rating of the client.

6. Conclusion and future work

In this paper we have analysed the demands on AAIs in business-to-consumer eCommerce as far as the building of a federation, flexibility, and privacy are concerned. After defining the criteria we matched them with four AAIs namely Shibboleth, Microsoft Passport, the Liberty Alliance Framework, and PERMIS. None of the analysed solutions are currently able to attain our goals. As far as flexibility is concerned the solutions are missing the dynamic and complexity of eBusiness. We have introduced the idea to use an attribute based access control mechanisms with XACML policies for that. To assure benefits from a federation we combined the benefits of a central SSO solution like Passport with those of the distributed solution Liberty. PERMIS provided mechanisms to outsource almost every part of the access control process to an AAI. The usage of a common vocabulary has been implemented with success in Shibboleth. We have adopted the idea and promote a wider usage of attributes for the access control. Our distributed AAI respecting privacy and flexibility is an improvement among existing AAIs and AAI concepts in respect to our demands. The produced model so far has been tailored to b2c eCommerce. The next steps in our work will be to broaden the field of application. GRID computing and inner organisational usage will be targeted next. As a proof of concept the described solution is currently implemented using the

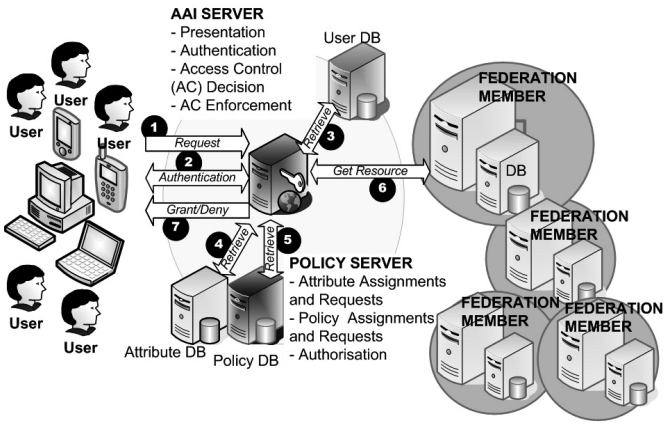

Figure 5. AAI with Attribute Infrastructure acting as a Proxy

Liberty Framework and the ABAC model from [18, 16, 17] as a basis.

References

[1] V. Benjumea, J. Lopez, J. A. Montenegro, and J. M. Troya. A first approach to provide anonymity in attribute certificates. In *Proc. of the International Workshop on Practice and Theory in Public Key Cryptography (PKC'04), Singapur, March 2004, Lecture Notes in Computer Science (LNCS) 2947*, pages 402–415, 2004.

[2] S. Cantor. *Shibboleth Architecture Protocols and Profiles Working Draft 05*. Internet2, 2004.

[3] D. Chadwick and A. Otenko. The permis X.509 role based privilege management infrastructure. In *Proc. of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002)*, pages 135–140, 2002.

[4] EC Article 29 Data Protection Working Party. Working document on on-line authentication services. 10054/03/en wp 68. adopted on 29.01.2003. http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp68_en.pdf.

[5] H. Federrath and A. Pfitzmann. Bausteine zur Realisierung mehrseitiger Sicherheit. In *Mehrseitige Sicherheit in der Kommunikationstechnik*, pages 83–104, 1997.

[6] S. Katsikas, J. Lopez, and G. Pernul. Trust, privacy and security in e-business: Requirements and solutions. In *Proc. of the 10th Panhellenic Conference on Informatics (PCI'2005). Lecture Notes in Computer Science*, pages 548–558, 2005.

[7] P. Kormann and A. Rubin. Risks of the passport single signon protocol. *Computer Networks*, 33(6):51–58, October 2000.

[8] Liberty Alliance Project. *Liberty ID-FF Bindings and Profiles Specification*, 2004.

[9] Liberty Alliance Project. *Liberty ID-FF Protocols Schema Specification*, 2004.

[10] J. Lopez, R. Oppliger, and G. Pernul. Why have public key infrastructures failed so far? *Internet Research*, 15(5):544–556, October 2005.

[11] Microsoft. *Microsoft Passport Review Guide*, 2003.

[12] M. C. Mont, R. Thyne, and P. Bramhall. Privacy enforcement for it governance in enterprises: Doing it for real. In L. N. in Computer Science, editor, *Trust, Privacy and Security in Digital Business: Second International Conference, TrustBus 2005*, volume 3592, pages 226–235, 2005.

[13] J. A. Montenegro and F. Moya. A practical approach of X.509 attribute certificate framework as support to obtain privilege delegation. In *Proc. of the 1 st European PKI Workshop: Research and Applications. Samos Island, Greece. June 2004 Lecture Notes in Computer Science (LNCS) 3093*, pages 160–172, 2004.

[14] T. Nowey, C. Klein, K. Plößl, and H. Federrath. Ansätze zur Evaluierung von Sicherheitsinvestitionen. In *Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics*, pages 15–26, 2005.

[15] OASIS. *OASIS eXtensible Access Control Markup Language Technical Committee: eXtensible Access Control Markup Language (XACML)*.

[16] T. Priebe, W. Dobmeier, and N. Kamprath. Supporting attribute-based access control with ontologies. In *Proc. of the 1st International Conference on Availability, Reliability, and Security (ARES 2006), 2006.*, 2006.

[17] T. Priebe, W. Dobmeier, B. Muschall, and G. Pernul. ABAC - Ein Referenzmodell für attributbasierte Zugriffskontrolle. In *Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics*, pages 285–296, 2005.

[18] T. Priebe, E. Fernandez, J. Mehlau, and G. Pernul. A pattern system for access control. In *Proc. of the 18th Annual IFIP WG 11.3 Working Conference on Data and Application Security*, pages 235–249, 2004.

[19] C. Schläger and G. Pernul. Authentication and authorisation infrastructures in b2c e-commerce. In *Proc. of the 6th International Conference on Electronic Commerce and Web Technologies - EC-Web '05. Lecture Notes in Computer Science*, pages 306–315, 2005.