An Architecture for Unifying Web Services Authentication and Authorization

Robert Steele and Will Tao

Faculty of Information Technology, University of Technology, Sydney,
P.O. BOX 123 Broadway N.S.W. Australia 2007
{rsteele, wtao}@it.uts.edu.au

Abstract. Security issues are one of the major deterrents to Web Services adoption in mission critical applications and to the realization of the dynamic e-Business vision of Service Oriented Computing. Role Based Access Control (RBAC) is a common approach for authorization as it greatly simplifies complex authorization procedures in enterprise information systems. However, as most RBAC implementations rely on the manual setup of pre-defined user-ID and password combinations to identify the particular user, this makes it very hard to conduct dynamic e-Business as the service requestor and service provider must have prior knowledge of each other before the transaction. This paper proposes a new Web Services security architecture which unifies the authorization and authentication processes by extending current digital certificate technologies. It enables secure Web Service authorization decisions between parties even if previously unknown to each other and it also enhances the trustworthiness of service discovery.

1 Introduction

As a key factor in the adoption of e-Business, security is an important concern for Web Services adoption [1]. As a new computing paradigm, Web Services applications present security requirements different from those of traditional applications. The challenge in Web Services security is that Web Services applications need to provide controlled disclosure of information rather than the traditional all-or-nothing approach; the authorization procedure is more interactive and complex than the classic user-ID and password combination approach.

2 Unifying Authentication and Authorization in Web Services

2.1 Motivation

In Web Services applications, to carry out a real time, global e-Business transaction, it will be extremely valuable to have a unified architecture to allow service requestors to acquire appropriate privileges automatically and dynamically without necessarily having prior knowledge or relationship with the service provider. And it is also highly desirable that only trusted services can be retrieved in the central registry by service requestors.

B. Benatallah, F. Casati, and P. Traverso (Eds.): ICSOC 2005, LNCS 3826, pp. 582 – 587, 2005.

A new architecture is proposed in this paper for unifying authentication and authorization in Web Services by extending certificate technologies. The architecture allows the service provider to simply define rules to group a large number of current or potential service requestors into appropriate roles, and assigns privileges to service requestors according to the role list, i.e. the architecture utilizes Role Based Access Control (RBAC) in part. Furthermore, before conducting the transaction, the service requestor can decide whether to send a request message or not by checking the service provider's business credentials.

2.2 Overview of the Proposed Architecture

There are several core elements in this new architecture to unify the authentication and authorization in Web Services applications, which are:

1. WS -Business Policy (WSBP)
2. eXtended CA (ECA)
3. eBusiness Passport (EBP)

All new elements are shown in Fig. 1 and the following sections discuss how these elements inter-operate to build a global trustworthy Web Services platform.

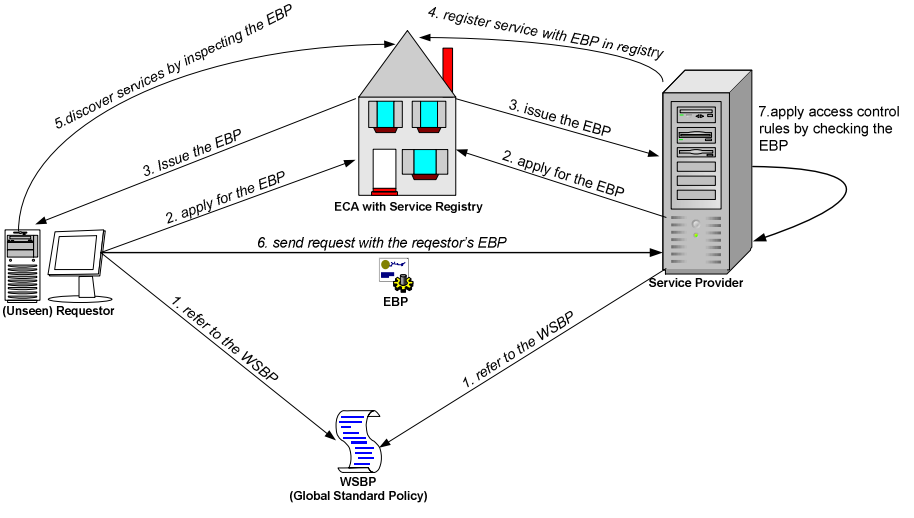

Fig. 1. Overview of Architecture

2.3 WS-Business Policy

WSBP is an important new element in the architecture. It is a standard for describing and evaluating business entities based on their backgrounds and performances. It has a rich set of criteria to enable a fine grained description and evaluation result. All evaluation data is described in XML and constrained by the WSBPXML Schema.

The WSBP has two parts, which are:

1. WS Business Policy-Common (WSBP-C)
2. WS Business Policy-Industry (WSBP-I).

WSBP-C is used to describe the common attributes of all business entities, such as registration date, number of employees and credit rating. The WSBP-I is industry sector specific evaluation criteria, where all criteria are tightly bound as evaluation criteria relevant to that particular industry.

The reasons for making WSBP into two parts are:

1. It is hard to evaluate all business entities which can be from all different locations and industries by using only common universal criteria.
2. It is not unusual that one business entity covers multiple industries. In this case, the business can be evaluated with one WSBP-C and multiple WSBP-I.

An evaluation result must have only one WSBP-C result and at least one WSBP-I. The criteria of WSBP are globally unified. The key role of WSBP is to provide a globally agreed set of criteria/ factors for evaluating business entities by a unified standard. Fig. 2 shows a potential WSBP instance - a real case might be more comprehensive and detailed.

```
<?xml version="1.0" encoding="UTF-8"?>
<WSBP xmlns="http://it.uts.edu.au/xml/ns/wsbp">
    <WSBP-C Name=" UTD Sydney Pty Ltd">
        <Type>Private</Type>
        <RegisteredLocation>Syd,AU</RegisteredLocation>
        <NumberOfEmployees>122</NumberOfEmployees>
        <Credit rating="8.5" rater="RoyalUnion" />
        <Certificate standard="ISO9000" />
     </WSBP-C>
     <WSBP-I Sector="Tech" Industry="ICP&amp;amp;ISP">
           <RegisteredUsers>5033051</RegisteredUsers>
           <GooglePageRank>8</GooglePageRank>
           <PageViews>10343305</PageViews>
     </WSBP-I>
  </WSBP>
```

Fig. 2. Potential WSBP Instance

By having a global standard for business evaluation (Fig. 1 Step 1) and if the results of such an evaluation can also be *authoritatively certified*, providers will be able to assign certain provider-specific roles to a requestor, even a previously unseen service requestor, based on the particular business characteristics of the requestor that have been certified. Due to the global standard, providers will be able to design mappings in advance that map requestors presenting certain certified business criteria to access roles through their knowledge of the criteria provided by WSBP.

2.4 ECA and EBP

An extended CA, the ECA does not only issue digital certificates but also evaluates business entities according to WSBP. In practical operation, the ECA's job might actually be more like a proxy as the ECA may only convert the certified paper documents into electronic form. For example, the documents may have actually been certified by a relevant government authority. After checking these stamped documents which are provided by business entities (Fig.1 Step 2), the ECA represents the evaluation results in electronic form against WSBP, along with the business entities' public key, all digitally signed by the ECA's private key. The signed evaluation results are named an e-Business Passport (EBP) (Fig.1 Step 3). The EBP is a special form of digital certificate which carries business entities activities and performance, also with their public key. As such it does not just provide authentication as a normal certificate does but also contains information to drive authorization decisions, allowing all business entities to be virtually connected. Because an EBP is digitally signed by the ECA's private key, it can be verified by the ECA's public key and no one can tamper with the data in the EBP, also, as the public key of the particular business entity has been signed in the EBP, the sender of the EBP can be easily authenticated. This ensures an EBP can not be forged and as long as the ECA is trusted, the information inside the EBP is trustworthy. An EBP will expire after a certain time to provide better trust and security and it is also renewable.

2.5 ECA and Service Providers

The ECA also allows service providers to register their services into a central registry to overcome some shortcomings in UDDI such as lack of access control and trustworthy service discovery [3] [4].

The service provider applies for an EBP based on relevant WSBP as Fig.1 Step 1 and 2 indicate. If the provided documents are qualified, the ECA will issue an EBP to the service provider (Fig.1 Step 3), and register this service provider's service into the central registry along with their EBP and all other necessary information such as WSDL (Fig.1 Step 4). If the EBP expires; the service will be removed from the central registry automatically to keep the registry a store of more current service information. A service provider can renew the EBP to prevent its expiration.

In current UDDI, there is no effective way to decide which service is reliable and trustworthy. For our architecture, only trusted services can be registered in the central registry and no longer certified and trusted services are removed immediately, allowing the central registry to always maintain fresh and trusted services.

3 Unified Authentication and Authorization

EBP is the key enabler to apply provider-side rules to achieve dynamic authorization as it carries with it certified WSBP criteria about the requestor business. However, as when a requestor carries out a transaction with a service provider, certain sensitive information may be passed in service requests, the service requestor also needs to determine whether they wish to invoke services from a particular provider. This can be achieved by requestor-side rules (Fig. 1 Step 5). The service requestor can check

the provider's EBP at service discovery time and pass the provide EBP through the requestor-side rule engine. The risk in the requestor-side has been greatly decreased by pre-checking the providers' EBP. The SOAP request will only be made when the requestor finds the provider which meets the service requestor's requirements.

If the service requestor decides to conduct the transaction with a particular service provider, the service requestor will send its EBP to the provider in the SOAP header, as Fig.1 Step 6 indicates. After receiving the EBP, the service provider uses the ECA's public key to verify the EBP, the public key of the requestor inside the EBP to verify the sender and all other WSBP related information for determination of what privileges to grant. If the EBP is valid, the provider-side rule engine parses the XML document and the service requestor will be granted appropriate roles or be rejected automatically, depending on the provider's rules (Fig. 1 Step 7). After finishing the processing, the rule engine generates the highly secured tokens for maintaining the session with the requestor, encrypts the information by the requestor's public key, puts the encrypted information into the SOAP header and sends it back to the service requestor. Fig. 3 provides an example of simple pseudo-code to demonstrate provider-sides rules and how a mapping from WSBP criteria contained in the EBP to roles might work. The important point is that every service-provider will have its own specific implementation and provider-specific roles, and the implementation and roles are totally de-coupled from the service requestor. As such the service requestor does not need to know how the service provider implements its EBP rule mapping, and the rules can be very complex to meet real business requirements.

```
if (credit > 8)
    addRoles(requestor,GOLD)
else (credit between {5 to 8} && city==MY_CITY)
    addRoles(requestor,GOLD)
else
    addRoles(requestor,SILVER)
```

Fig. 3. Potential rules for mapping from WSBP criteria contained in an EBP to access roles

To accelerate the procedure of conducting real time business, service requestors are supposed to be recognized globally by only presenting their EBP. However, in the complexity of real world business transactions, exceptions will always occur. So in our architecture, the current user-ID and password based RBAC system still can be used to catch these exceptions. When the transaction can not simply use the EBP to allocate privileges, the service requestor can still be assigned the user-ID and password to get privileges manually. So the architecture will not lose any flexibility by adding the new functionalities described.

4 Related Work

There are already many standards and research activities for enhancing the security aspects in Web Services. All the standards, WS-Trust, WS-Federation, Shibboleth, SAML etc still build on the assumed token model, i.e. that the possible values inside

the claim of a security token are not standardized or enumerated. To overcome this, we have proposed WSBP as a standard for even the possible "wording" of claims in our tokens, which is the EBP. This allows rules to be designed for a service in advance, referencing standard WSBP terms. Such rules can be applied to even previously unknown clients.

Smart certificates [2], is the closest research work to our proposed architecture, as it extends X.509 certificate for enabling flexible RBAC for web servers. However, as this work does not entail the proposal of a standard for the certificate contents, it doesn't enable the type of dynamic e-Business we are addressing and this work has not been extended into the Web Services domain.

5 Conclusion

The architecture utilizes and extends the digital certificate concept to introduce the idea of an e-Business Passport and a unified business policy to enable fine grained authorization for any business transaction partners where the service requestor and service provider do not necessarily need any previous negotiations before transaction. Also, it greatly enhances the trustworthiness in service look up, both for service requestors and service providers. The architecture can be used to boost trustworthiness in global dynamic e-Business. Our current ongoing research work includes finalizing a complete WSBP-C schema and implementing a prototype system.

References

1. Ciganek, A. P., Haines, M. N. & Haseman W.D.: Challenges of Adopting Web Services: Experiences from the Financial Industry, Proceedings of the 38th Annual Hawaii International Conference on System Sciences (2005)
2. Park, J.S. & Sandhu, R.S.: RBAC on the Web by Smart Certificates, Proceedings of the fourth ACM workshop on Role-based access control (1999) 1-9
3. Steele, R., Dai, J., UDDI Access Control for the Extended Enterprise: Proceedings of the International Conference on Web Information Systems and Technologies(2005)
4. Yang, S.J.H., Hsieh, J.S.F., Lan, B.C.W & Chung, J.Y,: Composition and evaluation of trustworthy Web Services, Proceedings of the IEEE EEE05 international workshop on Business services networks(2005)