A Mechanism for Federated Identification Services for Public Access Portals Using Access-Cards

Sylvia Encheva
Stord/Haugesund University College
Bjørnsonsg. 45
5528 Haugesund, Norway
sbe@hsh.no

Sharil Tumin
University of Bergen
IT-Department, P. O. Box 7800
5020 Bergen, Norway
edpst@it.uib.no

Abstract

This paper discusses an access control mechanism for public Web portals by sharing users’ data from identity providers across organizations boundaries among federated organizations using a lightweight Web-based application framework.

Each user can subscribe to a portal and be given an access-card which will be used to identify the subscriber at this particular portal or other portals in collaboration. The framework will also implement single-sign-on for member applications of a federation of portals.

1. Introduction

Most public Web portals are not interested in doing their own user management system. Applications are open for anonymous users without any opportunity of finding out the identities of their guests. Library portals and the like often provide a mix of services requiring digital identities to real persons affiliated to real organizations. Without the possibility of identifying users, such portals resort to using users’ computers network addresses as a way to control certain access. For example, certain billable library services are given to clients coming from a certain subnet network address. Such simple control measure can be circumvented by using a Web proxy located within the valid subnet.

A digital identity management system based on self-defined identities created by users themselves like those used by social communities on the Internet for examples Web discussion groups, fan clubs, and hobby groups are not good enough for use on governments or libraries Web portals. Self-defined identity is good for individual user privacy but does not cover accountability and real personality since the identity can be used to identify a fictitious persona.

We present an access control mechanism for public Web portals. The model facilitates sharing of users’ data from identity providers across organizations boundaries among federated organizations using a lightweight Web-based application framework. Each user can subscribe to a portal and be given an access-card which will be used to identify the subscriber at this particular portal or other portals in collaboration. The framework will also implement a single-sign-on (SSO) mechanism for member applications of a federation of portals.

The rest of the paper is organized as follows. Related work may be found in Section 2. The model of the proposed system is presented in Section 3. The access-card details are described in Section 4. System architecture for prototyping the proposed framework is given in Section 5. The paper ends with a conclusion in Section 6.

2. Related Work

Identity management principals in the information society are presented in [3]. Need for federated identities is discussed in [12] and [13].
2.1. CardSpace

Windows CardSpace [1] is a Microsoft’s identity management platform based on .NET framework. It is tightly integrated with Microsoft products running under Windows operating system. The CardSpace architecture consists of service providers called relying parties and a security token server. A card, containing a particular user’s personal information, can be self-issued or managed is used to identify the user to any CardSpace enabled Web applications. A CardSpace card can either be self-issued or centrally managed from a card issuer. CardSpace cards are modeled and have similar functions as digital business cards or membership cards.

2.2. Shibboleth

Shibboleth [10] provides a Web-based platform for Web SSO based on security assertion markup Language (SAML) [9] specification. Shibboleth also provides functionalities that protect users’ privacy. Users have the possibilities to control the amount of personal information to be released to each application. Shibboleth-enabled Web applications simplify management of users’ identities and access controls across different service providers and identity providers.

2.3. OpenID

OpenID [7] is a decentralized digital identity management platform based on user’s own identity by a user defined Uniform Resource Identifier (URI). OpenID eliminates the need for multiple usernames across different Web applications. The user defined URI implements the OpenID identity provider that serves as an authentication server. An application server redirects a user Web browser to the self-defined OpenID identity provider. The user will then do the authentication process and be redirected back to the originating website.

2.4. DotGNU

DotGNU Virtual Identities [2] proposed a peer-to-peer platform for authentication, authorization and sharing resources. Personal information is not copied to service providers, thus protect users privacy. Each user has an identity server and talk to a particular service provider in a peer-to-peer manner when a need for an identification process arises.

3. Trust Model

Most potential users of Web applications provided by government bodies or libraries are members of reputable organizations, such as schools and universities. A digital identity given to a person belonging to these organizations is directly related to that person. The identity management system (IDM) within these organizations can guarantee a high quality users’ data, because it is in the interest of these organizations that these data are as accurate as possible at any one time.

Almost all persons within such organizations have digital identities in connection with their works or studies. Each person will have a unique identity. These digital identifiers can be used by public Web portals remotely to identify real persons from a particular organization within a cooperative framework.

Figure 1. Circles of Trust

Figure 1 shows circles of trust (CoT):

- within an organizations, CoT@domain
- among organizations bind by a master portal
- among federated portals through the master portal.

Identity provider (IdP) provides identity service to any service provider (SP) within an organization. A Web portal (PP) provides collaboration services. Each master portal can in turn be a member of a federation of portals.

Users and service providers belonging to an administrative domain have strong trust relationships. Every user trusts any other user from the same organization by virtue that they trust their administration. Every host trusts any other hosts under the administration of the same domain. All hosts are located behind firewalls at the domain’s Internet borders.

Some service providers from different administrative domains may form a coalition of services, such as online libraries from different colleges and universities. A portal
Figure 2. Access Card

An access-card example as shown in Figure 2 does not disclose its owner domain user identity. Domain user identifiers are normally connected to systems user-identification stored in active directory (AD), network information service (NIS) database or enterprise lightweight directory access protocol (LDAP) server.

An access-card contains three fields of information represented in numerical strings:

1. a unique user-identification number
2. a group of twelve randomly generated four digits pass-codes, and
3. an access-card unique serial-number

A user-identification number is composed of a master PP code, user’s IdP code and a user’s identification code, separated by a hyphen, such as “1325-2212-00032467”.

The pass-codes function as pseudo “one-time” passwords connected to the access-card. The user-identification number and one of the pass-codes are used together to validate the owner of the access-card. If the user passes the validation test then the master PP presents the user with the access-card’s serial-number such as “68564292109”, so that the user will know for sure that she is communicating with a legitimate master PP.

The IdP code part of a user-identification number is related to information about users’ home domain identity provider and authentication/authorization server. The user identification code part of the user-identification number is related to information about a particular user identity. All these relations are stored in a relational database for all subscribed users at a particular master PP.

A user can revoke an old card and can obtain a new card from a master PP at any time. Since a user can subscribe at a different master PP, a single user can own multiple access-cards. However, all these cards are related to user’s domain identity. It is not necessary and desirable to own many access-cards. To minimize the risks involved in relation to that an access-card being stolen or lost, a user is advised to own one access-card at any one time. Users are responsible for the safety of their access-cards.

5. System Architecture

Figure 3 shows typical system architecture that implements a distributive cross-domains authentication and authorization mechanism for Web portals collaborating with domain authentication servers based on Apache HTTP server [8], Python [4, 5] programmable runtime environment and SQLite [6] database.

The framework depends on Web cookies and URL redirects to implement users’ subscription processes and users’ validation processes. Communication and message passing between identity providers, application portals and master portals are accomplished through remote procedure call (XML-RPC) [11].

To preserve states across otherwise stateless hypertext transfer protocol (HTTP) communication, Web cookies are needed. To set a Web cookie in a Web browser, the HTTP server sends the cookie together with the requested Web object as a reply to the client request.
The client saves the cookie and attaches the cookie to its future request to the HTTP server if validity check is true.

GET /appl HTTP/1.0
From: edpst@it.uib.no
User-Agent: HTTPTool/1.0
Cookie: sess=3428763981456690

There are several methods to accomplish clients’ URL redirects:

- A meta refresh which tells the browser to move onto the next page after x seconds.

  <meta http-equiv="refresh" content="0; url=https://sebra.uib.no/validate">

- A frame redirect which loads the contents of another page inside a frame

  <frame name="redirect" src="https://sebra.uib.no/subscribe">
  </frame>

- A header redirect that returns a Location header telling the browser to go to another page in a server response

  HTTP/1.1 200 OK
  Location: https://sebra.uib.no/newsubscription

The first time an unsubscribed user connects to a PP, she will be redirected to her home domain to be authenticated. The PP will provide the user with an access-card if validation is successful. For each access-card the PP saves the user’s identity and domain information in its local database. Next time the user visits the portal, the credential written on the access-card will be used to authenticate that particular user. Using the user’s data previously stored in the database, the portal can identify the user and can also gain more information pertinence to the user by consulting her home domain identity provider by XML-RPC. A slave PP submits a users’ access-card logon information to the master PP during the user validation process.

5.1 Subscription process

An unsubscribed user can subscribe for membership and be given an access-card at any public portal belonging to a federation. The only condition is that the user’s domain IdP is known to the master PP and they are allowed to exchange massages through XML-RPC.

The subscription process flow is shown in Figure 4 and is described in detail below:

1. A user requests a subscription at a particular PP. In relation to the browser Internet address, the PP suggests a domain IdP which the user can accept or decline. The user can also choose a valid IdP from a list servers.

2. The PP redirects the user to the chosen IdP.

3. The user submits her correct credential, a valid user-identifier and password, to the IdP to be authenticated. If the given credential is valid then the IdP creates a session token for the user.

4. The IdP redirects the user back to the PP together with the session token.

5. The PP sends the session token and IdP’s service address to the master PP using XML-RPC.

6. The master PP requests the user’s identification data from the domain IdP using XML-RPC. The master PP creates a unique subscription data entry for the user into the database.
7. The master PP creates a unique access-card image for the user. The PP presents the access-card image to the user to be printed, saved or copied. The user is now subscribed and owns a valid access-card.

5.2 Validation Process

To be able to make use of any limited access services, a user must pass the validation process as shown in Figure 5 first.

1. A user requests a protected application at a particular PP. The user is not yet validated. The PP asks the user to provide the user-identification number written on the user’s access-card.

2. The PP redirects the user’s Web browser together with the user-identification number to the master PP. The master PP is identified by the master PP code part of the given user-identification number.

3. The master PP asks the user to provide one of the pass-codes randomly chosen by the master PP. The given pass-code is checked for correctness against the recoded value for the user corresponding to the user-identification number. If the pass-code given matches the recorded value, the access-card owner is now validated at the master PP.

4. The master PP connects by XML-RPC to the IdP identified by the IdP code part of the given identification number for user information. A detailed user information is returned by the IdP if the user is still a valid domain user, else nothing is returned.

5. The master PP creates a master portal session ticket for the user and stores it in the database.

6. A signed Web cookie corresponding to the session ticket is given to the user’s Web browser.

7. The master PP redirects the user’s Web browser back to the originating PP with a token corresponding to the master portal session ticket.

8. The PP connects and sends back the token to the master PP using XML-RPC. If the token is still valid at the master PP the user information is then returned.

9. The user is now validated at that particular PP. A signed Web cookie corresponding to the valid session ticket is given to the user’s Web browser and the user can now access the protected application.

The session ticket created at the PP is used for SSO for all applications connected to the particular PP. The master portal session ticket created at the master PP is used to implement SSO to all applications connected to the federation of portals.
6. Conclusion

The framework described in this paper provides a mechanism for using free, easily accessible and light-weight technologies for public Web portals to use a distributed identity providers for a federated users subscriptions, validation and authorization processes. Access-cards belonging to subscribed users can be shared between many portals. Access-cards employ other credentials than the domain user-identifier and password pair during validation processes. These will protect users’ domain credentials form being compromised.

Once a user is validated and proper session tickets are created and stored at PP and master PP, the user can access any protected applications controlled by the federation of portals, given that the user has enough authorization to do so. A master PP can query a user authorization information from the user home domain IdP at any time.

Users can revoke and create access-cards at any time. Since a domain user validity check for a particular access-card is done at real time, a user subscription is automatically revoked when she is no longer a valid user at a particular organization.

References

[1] CardSpace May 17, 2008 [online]
URL-http://netfx3.com/content/WindowsCardspace
Home.aspx


URL-http://openid.net/


[9] SAML, May 17, 2008 [online]
URL-http://wiki.oasis-open.org/security/SstcSaml1xMetadata

[10] Shibboleth, May 17, 2008 [online]
URL-http://shibboleth.internet2.edu/

