The Design of SSO Service Architecture for Mashup Service in Web Portals

SoHee Park and JeongNyeo Kim
Information Security Development Division
Electronics and Telecommunications Research Institute
161, Gajeong-dong, Yuseong-gu, Daejeon
Republic of Korea

Abstract: - Web portal enterprises are interested in creating of the new and various web services as mashup services with Web 2.0 environment based on the user participation and sharing these days. And they think the connection of the electronic civil application services of e-government is one of the new business models. For this, it is necessary to have the Single Sign On(SSO) service for the user convenience. SSO is very convenient service. User can use the various web services by one authentication using the user information sharing between the different websites. But the legacy SSO service is not sufficient that the range of user authentication is limited between the cooperated websites within one web portal(single trust domain). Also it is focused on the user friendliness, so it is not enough to connect with e-government in security aspect. So the web portal enterprises demand the more convenient SSO service with the appropriate security can be enough to connect with e-government. This paper proposes the new SSO service on multi-trust domains for converged services and mashup services. It extends the SSO service on single trust domain based on SAML. We define the requirements of the SSO service for web portal on multi-trust domains and design the architecture of the new SSO service satisfying these requirements.

*Key-Words:*Single Sign On, SSO, Single Logout, SAML, ID Management, User Authentication Mechanism

1 Introduction

The extension of the Internet and the growth of user demand give rise to the various web services like IPTV, UCC, Internet shopping mall and etc. And web portal enterprises become to support the new and converged web services as mashup services with Web 2.0 environment based on the user participation and sharing. It means that the web portal enterprises need the new technologies to overstep trust boundary between different web portal enterprises.

To use the various web services supporting many websites, users have to register and use the ID to each website. It isn't convenient to users. The web portal enterprises manage the ID system in each website, so they consume the large amount of cost for ID and user information management[1][2].

To solve these problems, we use the SSO service. Web portals have already supported the SSO service for user convenience. But, the legacy SSO service is not sufficient that the range of user authentication is limited between the cooperated websites within one web portal. And it is focused on the user friendliness, so it is not enough in security aspect. The legacy SSO service is not enough for mashup services because it doesn't support any functions to interconnect with different trust domains. When users want to use the uncoordinated websites, it is impossible without additional authentication mechanism. It means that the legacy SSO service has the limitation based on cooperation relationship between websites. Therefore the web portal enterprises demand the more convenient SSO service with the appropriate security to overstep trust boundary.

So this paper proposes the new SSO service architecture on multi-trust domain by extending the legacy SSO service based on SAML[3]. It is for the new mashup services in web portals. We describe the architecture and service procedures of legacy SSO service in section 2. In section 3, we define the requirements of SSO service for mashup service. And we design the new SSO service architecture is satisfying those requirements and describe the service procedures in section 4. Finally, we conclude in section 5.

2 Architecture and Procedures of Legacy SSO Service

.

2.1 Legacy SSO Service Architecture

Legacy SSO service supports user authentication on single trust domain. It means that the range of user authentication is between the cooperated websites. Fig.1 is the architecture of legacy SSO service.

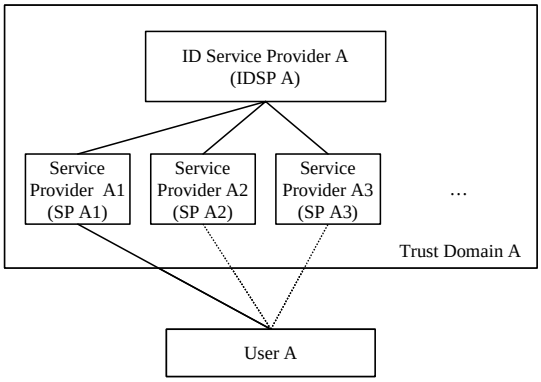

Fig.1 Legacy SSO Service Architecture

The single trust domain consists of the cooperated Service Providers(SPs) and an ID Service Provider(IDSP). In Fig.1, user A registers the ID to IDSP A and can use all web services within single trust domain through SSO service without additional user registration and authentication.

2.2 Legacy SSO Service Procedure

When user A uses the web service of SP A1 in trust domain A, SSO service procedure on single trust domain is Fig.2.

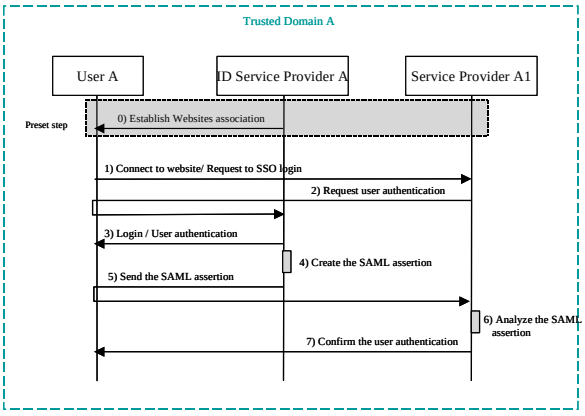

Fig.2 SSO Service Procedure on Single Trust Domain

(0) User A registers the website lists for SSO service to IDSP A.
(1) User A connects to SP A1 and requests the SSO login.
(2) SP A1 redirects the SSO login request message to IDSP A and requests user authentication.
(3) IDSP A shows the ID/PW login page to user A and user A logins to IDSP A using ID/PW.
(4) IDSP A creates the SAML assertion for user A.
(5) IDSP A sends the SAML assertion to SP A1.
(6) SP A1 analyzes the SAML assertion.
(7) SP A1 authenticates user A using SAML assertion and user A can use web service of SP A1.

2.3 Legacy Single Logout Service Procedure

Single logout service can use when user A wants to logout in one time from all web services through SSO in trust domain A. Single logout service procedure on single trust domain is Fig.3.

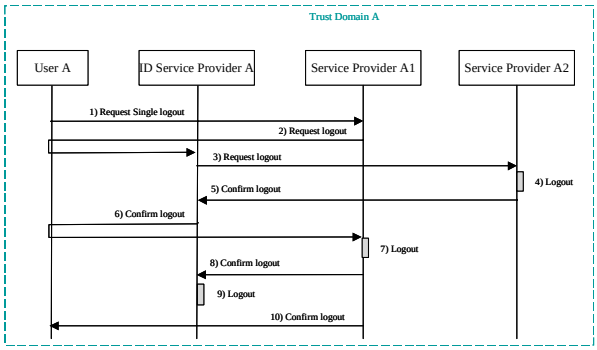

Fig.3 Single Logout Service Procedure on Single Trust Domain

(1) User A requests the Single logout from SP A1.
(2) SP A1 requests logout of user A to IDSP A.
(3) IDSP A requests logout of user A to SP A2.
(4) SP A2 makes user A to logout.
(5) SP A2 sends the logout confirm message to IDSP A.
(6) IDSP A sends the logout confirm message to SP A1.
(7) SP A1 confirms the logout of all websites in trust domain A and makes user A to logout.
(8) SP A1 sends the logout confirm message to IDSP A.
(9) IDSP A makes user A to logout.
(10) SP A1 sends the logout confirm message to user A.

Step(3) ~ step(5) repeat the number of websites that are supporting SSO service to user A.

3 The Requirements of SSO Service for Mashup

For the converged and advanced web services, web portals should support the convenient user authentication mechanism to users by sharing user information between multi-trust domains. So users can use the mashup service by one authentication without additional authentication mechanism. It means that web portals need the interconnection between different trust domains.

We define the requirements for the SSO service on multi-trust domain. But we exclude the requirements for the SSO service on single trust domain.

It consists of general requirements, Trusted Third Party(TTP) requirement, IDSP requirements, SP requirements and user requirement.

3.1 General Requirements

To support SSO service on multi-trust domain for mashup service, the service architecture should consider these general requirements.

(a) It should consider the existence of TTP (ex. Certificate Authority(CA)) to authenticate mutually between trust domains.
(b) It should consider the standardization of ID management method in each trust domain.
(c) It should consider the negotiating procedure for the different authentication method and security level between trust domains.
(d) It should consider the user information protection method against violation of privacy that it can be occurred through the user information sharing.

3.2 Trusted Third Party Requirements

To support SSO service on multi-trust domain for mashup service, TTP should consider these requirements.

(a) It should support the assurance information of the important servers(IDSPs or SPs) to others.
(b) It should create the assurance information of standard format.
(c) It should deliver the assurance information to each server in secure channel, and it can support the additional security services(ex. Integrity or Non-reputation) if they are needed.

3.3 ID Service Provider Requirements

To support SSO service on multi-trust domain for mashup service, IDSP should consider these requirements.

(a) It should support the mutual authentication method to establish trust relationship with other IDSP.
(b) It should create the SAML assertion for not single trust domain but multi-trust domain if other IDSP requests SSO service of users belonging to its own trust domain.
(c) It should analyze the SAML assertion that be created by other IDSP and reconfigure that SAML assertion to new SAML assertion for its own trust domain.
(d) It should deliver the SAML assertion to other IDSP in secure channel, and it can support the additional security services(ex. Integrity or Non-reputation) if they are needed.
(e) The user authentication information for multi-trust domain should be separated from one for single trust domain and managed in the different way.
(f) The user authentication information of other trust domain should maintain temporally during one SSO service of user.
(g) It should obtain the user's agreement about the user information sharing between multi-trust domains if it is needed.

3.4 Service Provider Requirements

To support SSO service on multi-trust domain for mashup service, SP should consider these requirements.

(a) It should support the SSO login for users belonging to other trust domain.
(b) It should request user authentication to IDSP for SSO login for users belonging to other trust domain.
(c) It should analyze the reconfigured SAML assertion for multi-trust domain that it is received from IDSP.
(d) It should maintain the security level of user authentication for multi-trust domain during one SSO service of user.

(e) The access control for SSO service should be managed in the same way both single and multi-trust domains.
(f) It should request the additional authentication information to users if they want to user the service that it demands the stronger security level during SSO service on multi-trust domain.

3.5 User Requirements

To support SSO service on multi-trust domain for mashup service, user should consider these requirements.

(a) It should agree at the sharing of user information in using SSO service on multi-trust domain if it is needed.
(b) It should configure Home IDSP (HIDSP). HIDSP is ID management server of the user information in its own trust domain.
(c) It should inform its HIDSP to SPs in other trust domain.

4 Architecture and Procedures of Proposed SSO Service

4.1 SSO Service Architecture on Multi-trust Domain

Fig.4 is the architecture of SSO service on multi-trust domain for the various web services and mashup service. It is based on SAML. The single trust domain consists of the cooperated SPs and an IDSP by one web portal. There are TTP like CA on the top of this architecture[4]. TTP helps to establish the trust relationship between multi-trust domains.

In Fig.4, user A belongs to IDSP A in trust domain A. User A registers the ID to IDSP A and can use all web service within the trust domain A through SSO service without additional user registration and authentication. If user A demands the web service in other trust domain B, the mutual authentication between IDSP A and IDSP B is needed. There are the various mutual authentication mechanisms. Server certificates of CA can be used for this. If we use the server certificates, we don't need additional authentication server for mutual authentication between different trust domains.

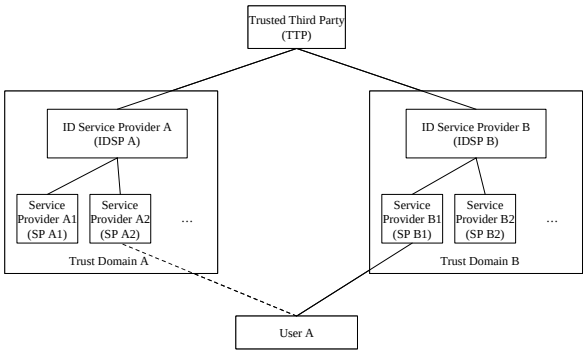

Fig.4 SSO Service Architecture on Multi-trust Domain

4.2 SSO Service Procedure on Multi-trust Domain

When user A use the web service of SP B1 in trust domain B, SSO service procedure on multi-trust domain is Fig.5.

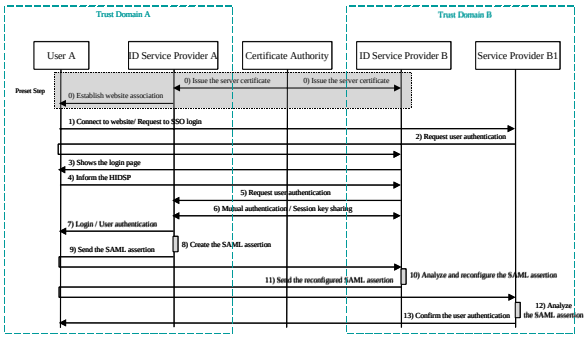

Fig.5 SSO Service Procedure on Multi-trust Domain

(0) CA issues the server certificate to IDSP A and IDSP B. User A registers the website lists for SSO service to IDSP A.
(1) User A connects to SP B1 and requests the SSO login.
(2) SP B1 redirects the SSO login request message to IDSP B and requests user authentication.
(3) IDSP B shows the ID/PW login page to user A.
(4) User A informs the HIDSP to IDSP B.
(5) IDSP B requests the user authentication to IDSP A.
(6) IDSP A and IDSP B authenticate mutually using the server certificate.
(7) IDSP A shows the ID/PW login page to user A and user A logins to IDSP A using ID/PW.
(8) IDSP A creates the SAML assertion for user A using user A's information. This SAML assertion is for multi-trust domain.

(9) IDSP A sends the SAML assertion to IDSP B in secure channel.
(10) IDSP B analyzes the SAML assertion and reconfigures new SAML assertion for trust domain B.
(11) IDSP B sends the reconfigured SAML assertion to SP B1.
(12) SP B1 analyzes the reconfigured SAML assertion.
(13) SP B1 authenticates user A using the reconfigured SAML assertion and user A can use web service of SP B1.

4.3 Single Logout Service on Multi-trust Domain

Single logout service can use when user A wants to logout in one time from all web services through SSO in trust domain B. Single logout service procedure on multi-trust domain is Fig.6.

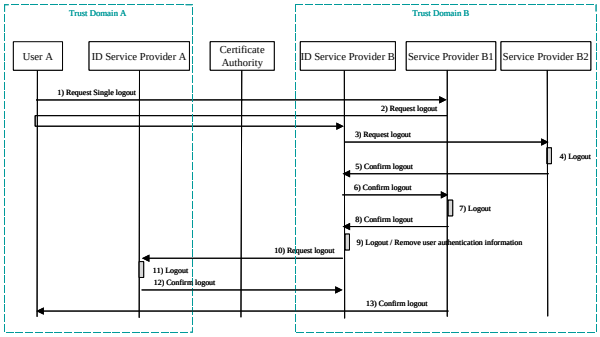

Fig.6 Single Logout Service Procedure on Multi-trust Domain

(1) User A requests the Single logout from SP B1.
(2) SP B1 requests logout of user A to IDSP B.
(3) IDSP B requests logout of user A to SP B2.
(4) SP B2 makes user A to logout.
(5) SP B2 sends the logout confirm message to IDSP B.
(6) IDSP B sends the logout confirm message to SP B1.
(7) SP B1 confirms the logout of all websites in trust domain B and makes user A to logout.
(8) SP B1 sends the logout confirm message to IDSP B.
(9) IDSP B makes user A to logout and removes the authentication information of user A.
(10) IDSP B requests logout of user A to IDSP A.
(11) IDSP A makes user A to logout.
(12) SP B1 sends the logout confirm message to user A.

Step(3) ~ step(5) repeat the number of websites that are supporting SSO service to user A.

5 Conclusion

This paper proposed the SSO service architecture on multi-trust domain by extending the legacy SSO service based on SAML. It is for the new mashup services in web portals. We described the architecture and service procedures of legacy SSO service in section 2. In section 3, we defined the requirements of SSO service for mashup service. And we designed new SSO service architecture is satisfying those requirements and described the service procedures in section 4. Finally, we concluded in section 5.

The web portals can support more secure and friendly web service to users and manage the user information more effectively through this proposed SSO service architecture. Also users can use the various web services securely and conveniently.

This paper will be able to contribute to the web service market promotion including new web services creation and activations in web 2.0 environment.

References:

[1] Tim O'Reilly, *What is Web 2.0,* http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html, 2005
[2] ETRI, *The White Paper of Internet ID Management Service,* 2006
[3] OASIS SAML, http://www.oasis-open.org/committees/security
[4] R. Housley, S. Santesson, *Update Directory String Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,* RFC4630, 2006