Architecture of CA-based SSO Service for Multi-trust Domain

SoHee Park*, JeongNyeo Kim*, SoonJa Kim**
*Information Security Research Division, ETRI
**School of Electrical Engineering and Computer Science, Kyungpook National University
{parksh, jnkim}@etri.re.kr, snjkim@ee.knu.ac.kr

Abstract-*Web portal enterprises are interested in creating of the new and various web services as mashup services with Web 2.0 environment. For this, it is necessary to have the SSO(Single Sign On) service for the user convenience. User can use the various web services by one authentication using the user information sharing between the different websites by SSO. 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). And it is not enough to connect with payment-related service in security aspect. So the web portal enterprises demand the more convenient SSO service with the appropriate security can be used in payment service. This paper proposes the new SSO service for multi-trust domains. It is very useful for converged and mashup services that are constructed by more than two web portals.*

Keywords: SSO, User Authentication, Multi-trust Domain

1. Introduction

The extension of the Internet and the growth of user demand give rise to the various web services like IPTV(Internet Protocol TeleVision), UCC(User Created Contents), 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 boundaries.

So this paper proposes the new SSO service architecture on multi-trust domain by extending the legacy SSO service based on SAML(Security Assertions Markup Language)[3,4,5,6]. 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. The Requirements for SSO Service for Multi-trust Domain

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 of the SSO service for multi-trust domain. But we exclude the requirements of the SSO service for single trust domain.

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

2.1. General Requirements

To support SSO service for multi-trust domain, 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.

2.2. Trusted Third Party Requirements

To support SSO service for multi-trust domain, 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.

2.3. ID Service Provider Requirements

To support SSO service for multi-trust domain, the 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 session of user.
(g) It should obtain the user's agreement about the user information sharing between multi-trust domains if it is needed.

2.4. Service Provider Requirements

To support SSO service for multi-trust domain, 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 users want to use the service that it demands the stronger security level during SSO service on multi-trust domain.

2.5. User Requirements

To support SSO service for multi-trust domain, 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 SPs in other trust domain of

its HIDSP.

3. Architecture of Proposed SSO Service

3.1. Service Architecture

The service architecture of SSO for multi-trust domain is Figure 1. It can be used 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[7]. TTP helps to establish trust relationship between multi-trust domains.

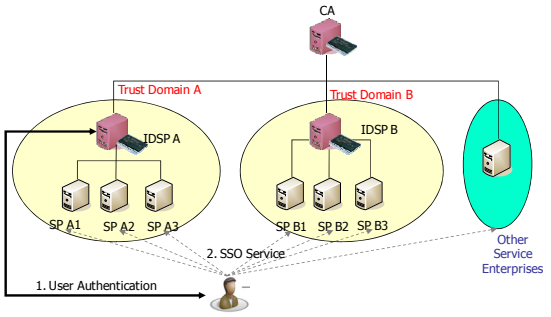

Figure 1. Service architecture

As shown in Figure 1, 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 to establish trust relationship between different trust domains. There are the various mutual authentication mechanisms for this. Server certificates of CA can be used. If we use the server certificates, we don't need additional authentication server for mutual authentication between different trust domains. Also it is possible to connect with e-government for civil application service by using this architecture.

3.2. Functional Architecture

The functional architecture to satisfy the requirements defined in section 2 is Figure 2.

The CA consists of these functions to establish the trust relationship between IDSP A and IDSP B.

- Certificate Issuing
- Certificate Management
- CRL Management

The IDSP consists of these functions for the SSO service in single and multi trust domain.

- ID/PW Authentication
- Federation Establishment/Release
- Multi-Federation Establishment/Release
- Multi-ID Federation Information Management
- ID Federation Information Management
- SSO Process
- Single Logout Process
- Multi-SSO Process
- Multi-Single Logout Process
- Mutual Authentication
- Error Control
- Security Management System Interconnection

The SP consists of the same functions of the IDSP for the SSO service in single and multi trust domain. But the SP includes the web service interconnection function with the web agent of User instead of Mutual Authentication function of IDSP.

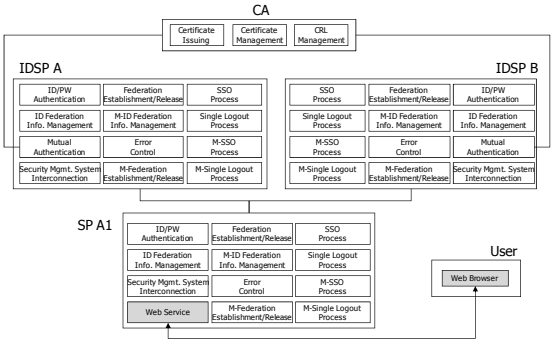

Figure 2. Functional architecture

4. Service Procedures for Proposed SSO Service

4.1. SSO Service Procedure

When User A use the web service of SP B1 in trust domain B, SSO service procedure for multi-trust domain is Figure 3.

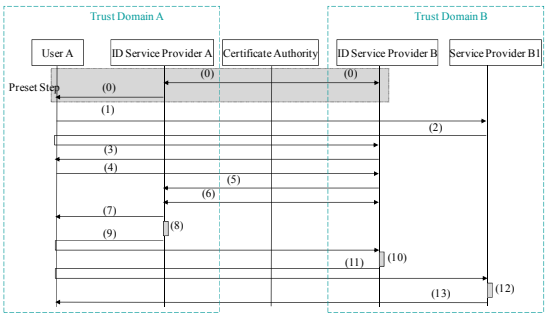

Figure 3. SSO Service Procedure

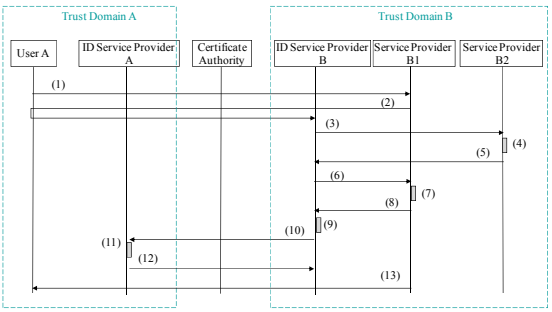

Figure 4. Single Logout Service Procedure

(0)CA issues the server certificate to IDSP A and IDSP B. User A registers the website lists for SSO service t 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 IDSP B of the HIDSP(IDSP A).
(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 authentication information. This SAML assertion is for multi-trust domain. So it can be used in SSO service for multi-trust domain.
(9)IDSP A sends the SAML assertion to IDSP B through the 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.

4.2. 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 B. Single logout service procedure on multi-trust domain is Figure 4.

(0) User A requests the Single logout from SP B1.
(1) SP B1 requests logout of User A to IDSP B.
(2) IDSP B requests logout of User A to SP B2.
(3) SP B2 is logged out User A
(4) SP B2 sends the logout confirm message to IDSP B.
(5) IDSP B sends the logout confirm message to SP B1.
(6) SP B1 confirms the logout of all websites in trust domain B and it logged out User A.
(7) SP B1 sends the logout confirm message to IDSP B.
(8) IDSP B is logged out User A and it removes the authentication information of User A.
(9) IDSP B requests logout of User A to IDSP A.
(10) IDSP A is logged out User A.
(11) 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 mashup services in web portals. We defined the requirements of SSO service for multi-trust domain in section 2. And we designed new SSO service architecture is satisfying those requirements and described the service procedures in section 3 and 4. Finally, we concluded in section 5. We used the CA that is one of TTPs to establish the security relationship between different trust domains. So we don't need additional authentication server for mutual authentication between different trust domains.

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] T. 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] Assertions and Protocols for the OASIS SAML V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[5] Bindings for the OASIS SAML V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

[6] Profiles for the OASIS SAML V2.0, http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[7] 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.