# XML BASED SINGLE SIGN-ON SCHEME FOR DEVICE CONTROL IN UBIQUITOUS ENVIRONMENT

*Jongil Jeong*[1], *Seunghun Lee*[2], *Dongil Shin*[2], *Dongkyoo Shin*[2*]

[1] Korea Information Security Agency
78 Garak-Dong, Songpa-Gu, Seoul 138-803, Korea
E-mail: jijeong@kisa.or.kr

[2]Department of Computer Engineering, Sejong University
98 Kunja-Dong, Kwangjin-Gu, Seoul 143-747, Korea
shlee@gce.sejong.ac.kr, {dsin, shindk}@sejong.ac.kr

## ABSTRACT

This paper proposes a single sign-on scheme in which a mobile user offers his credential information to a home network running the OSGi (Open Service Gateway Initiative) service platform, to obtain user authentication and control a remote device through a mobile device using this authentication scheme, based on SAML (Security Assertion Markup Language). Especially by defining the single sign-on profile to overcome the handicap of the low computing and memory capability of the mobile device, we provide a clue to applying automated user authentication to control a remote device via a mobile device for distributed mobile environments such as a home network based on OSGi.

**Keywords:** single sign-on, SAML, home network, OSGi, mobile device

## 1. Introduction

Home network environment consists of different kinds of personal equipment, wireless sensors, middlewares, services, and networked devices in the home [1]. In this environment, middlewares such as UPnP (Universal Plug in Plug) [2], Jini [3], Havi [4], PLC (Power Line Community) [5] play an important role controlling and maintaining a variety of home network component. However, mi[1]ddlewares are not interoperable because each one is dependent on vendors who establish middleware. OSGi (Open Service Gateway Initiative) [6] provides the key to solve such problem. By providing transparent layer on which each middleware can communicate OSGi enables middlewares to be interoperable.

In the OSGi service platform, every service bundle in the gateway operator requires user authentication. By the result, a user should complete authentication repeatedly whenever the user wants to access several number of services. This causes potential security problems as well as the difficulty of user access.

*Coreesponding author
This study was supported by the Seoul R&BD Program (BU070131).

First of all, the main security problem with a home network environment based-on the OSGi service platform is that the security infrastructure is distributed and these architectures usually require that key security features be built into all parts of the system. In addition, a user must memorize usernames and passwords for each service. Additionally, the system's administrator manages many passwords in the database and is faced with potential insecure system problems due to the frequent transmission of these passwords at the sites [7]. SSO (Single Sign-On) is a good alternative to solve these problems. SSO is a security feature that allows a user to log into the many different services offered by the distributed systems while only needing to provide authentication once, or at least always in the same way [8].

In this paper, we propose a single sign-on scheme using SAML for home network service environment based on the OSGi service platform. We simulated this environment by proposing and verifying a messaging scenario through implementation, and defined a profile to implement single sign-on through mobile devices with small memory capacities in distributed OSGi environments, which should exchange and verify a key to authenticate a user.

This paper is composed of four sections. Section 2 includes an overview of OSGi and SAML. In Section 3, we propose a security scheme for user authentication for mobile and home network service environments. Finally we conclude in Section 4.

## 2. Background

Mobile devices open up the possibility of offering home network services regardless of a user's or service provider's location. But the handicaps of mobile devices become the barriers to adopting new security technologies, such as single sign on, in mobile or home network service environments [9]. To overcome these barriers, a lightweight method to avoid key-exchange and message encrypting/decrypting must be considered for a mobile device.

A user in a wide area network can control a remote device within a home network environment via a service bundle in

a gateway operator. To use the service bundle, the user's authentication is necessary. For this functionality, Release 3 of the OSGi service platform defines a "User Admin Service" but only offers authentication for each service unit [10]. For this reason, when a user wants to access various services, a home network environment using the OSGi service platform may have the same primary security problem experienced in a mobile or Web Services environment. SSO can be implemented by exchanging and reusing a user's authentication information, including the fact that the user has previously been authenticated by a specific method among different security domains. We specified the information in a uniform and unified way based on SAML.

## 2.1 OSGi(Open Service Gateway Initiative)framework[6]

OSGi was developed to control and manage services and devices in homes, offices, vehicles, mobiles, and other environments via network and its final goal is to solve problems involving service distribution and the interaction between several home network middlewares.

The OSGi service platform is divided into two parts: the OSGi Service Framework and OSGi Service. The OSGi framework supports registry and life-cycle management for an OSGi service in Java runtime environment. As a bundle, an OSGi service such as HTTP, Logging, and Device Access Service is defined by Java Interface. A bundle is the minimum unit for managing a framework. A framework manages installing, uninstalling, resolving, stopping, starting, and active life cycle for bundle.

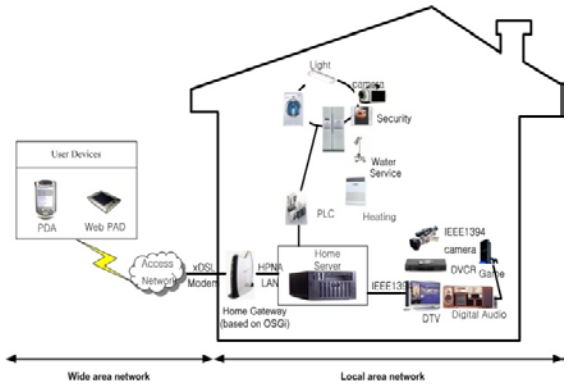


Fig. 1: OSGi architecture

Figure 1 shows the OSGi framework, which connects the wide area network and the local area network. When a user wants to control a device in the local area network, he can control the device through the service being managed by the gateway operator in the wide area network. If there is a trust-relationship between the services, a user who has been authenticated from a service in the gateway operator can avoid any redundant authentication required to use other services.

In order to apply the SSO scheme to the home network as shown in Figure 1, the services extended from core services provided by the OSGi framework should be developed and deployed onto the OSGi framework. Figure 2 shows core services provided by the OSGi framework and extended services.

The description for core services is as follows [11]:

- Device Access Services enables an operator to update, install, or remove device drivers.
- LOG Service gives users a general-purpose message logger for the OSGi environment.
- HTTP Service offers users' access to services on the Internet and other networks.

For experimental purposes, we constructed the following extended services:

- Camera Control Service provides functionality for controlling a surveillance camera, such as camera view, camera on/off, and camera zoom in/out.
- Projector Control Service provides functionality for controlling a projector in a conference room or meeting room, such as projector on/off and adjusting.
- Single Sign On Service makes XML-based queries for user authentication. Also it plays the role of exchanging artifacts between the user and an Authentication Agent. After authenticating the user successfully, Single Sign On Service leads the user to the destination service.

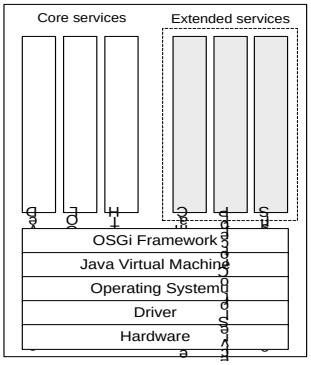


Fig. 2: OSGi framework and extended service

## 2.2 SAML(Security Assertion markup language)

SAML is an XML-based standard framework designed to offer single sign-on for both automatic and manual interactions between systems. It will let users log into another domain and define all of their permissions.

Using a subset of XML, SAML defines the request-response protocol by which systems accept or reject subjects based on assertions [12]. An assertion is a declaration of a certain fact about a subject. An assertion includes the statements generated by the SAML authority, conveying them and verifying that they are true. SAML defines three types of assertions.

- AuthenticationAssertion: indicating that a subject was authenticated previously by some means, such as a password, hardware token, or X.509 public key.
- AttributeAssertion: indicating that the subject is associated with attributes.

•AuthorizationAssertion: indicating that a subject should be granted or denied resource access.

The SAML authority can be classified as authentication authorities, attribute authorities, and policy decision points according to the type of assertions included. The SAML authority can use various sources of information from external policy stores or assertions being received as the input in requests.

SAML defines an artifact mechanism when the authentication request is too long for an HTTP redirect. The artifact has the role of a token. It is created within a security domain and sent to other security domains for user authentication. To achieve single sign-on, a mobile device keeps its artifact, which verifies that the mobile user has been authenticated once by the SAML authority in the system. An artifact is a small string and keeping it in the mobile device can overcome the handicap of having low computing power and a small memory in the mobile device.

## 3. Single Sign-On architecture for mobile and home network service environment

The role of a security domain is to manage and control resources ruled by a specific access control policy. When a subject within a security domain requests resource from another security domain, the subject must be defined in the first security domain and a mutual trust-relationship must exist between the first security domain and the second security domain [13]. Specifically, OSGi recommends the HTTP service to offer users access to the services on the Internet and other networks [14]. Therefore we strongly suggest SSO as a core security scheme to improve user accessibility and security performance in home network environments exploiting the HTTP service.

There are two approaches for implementing SSO.
•The first approach is to maintain an authentication list for all users in a central repository.
•The second approach is to include authentication information for each Web Service in the initial SOAP message.

In the first approach, all the old IDs for users are removed and then new IDs are assigned from the Central Repository [15]. To access Services, a user must use a new ID. Although this approach is suitable for a single organization, each organization may lose its control for the administration because all the users' information is stored into the Central Repository. In addition, it is difficult to expect extensibility from this approach. This approach is not suitable for distributed mobile environments such as Web Services, which is a set of domain-specific services.

In the second approach, all users can use the existing ID to access different domains without needing a new ID [15], [16]. This approach is suitable for a distributed environment that is a set of domain-dependent distributed services. In such an environment, when a user wants a number of domains, each domain requests the user to provide authentication. In this case, the user is authenticated by a domain and his authentication information is attached to a message to be transferred to other domains. Using this approach, attaching authentication information to the message and transferring the message to other domains, none of the organizations need to change their peculiar authentication scheme in order to communicate with other organizations.

The second approach is more appropriate for a home network service environment in which all services require user authentication. Figure 3 illustrates the concept of the second approach.

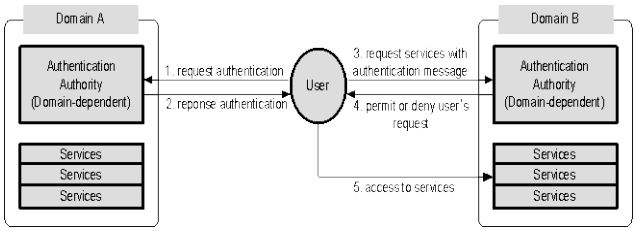


Fig. 3: An approach to implementing Single Sign-On using attached authentication message

Figure 3 is the prototype of the proposed Single Sign-On architecture in which the OSGi delivers certain services offered by service providers to the end user regardless of the system environments.

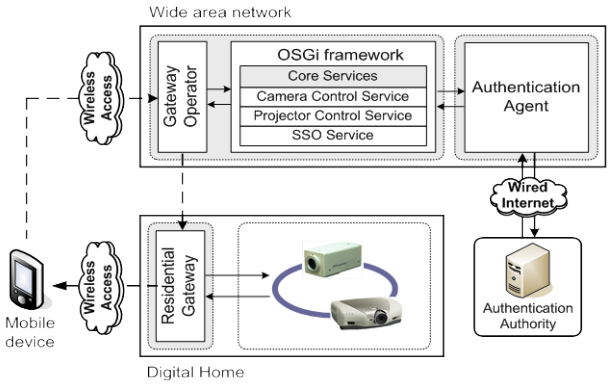


Fig. 4: Proposed Single Sgn-On Scheme

We propose a single sign-on scheme in which a mobile user offers his credential information to the home network for obtaining user authentication and access to multiple service bundles. In our implementation for the simulation, a mobile user gains access to services being managed by a gateway operator with the SAML-based information related to his own authentication in order to control a remote camera and projector. The concept of this architecture is explained in Figure 4. A mobile user keys in his username and password to a mobile device in order to access the Camera Control Service in the gateway operator of the Wide Area Network. This user credential information is transferred to the SSO Service through the gateway operator, which connects the mobile device and Wide Area Network. A more detailed description of our proposed architecture is as follows.

The user authentication procedure for the architecture is presented in the form of a sequence diagram in Figure 5, where each box in the diagram denotes an entity involved in this process. Figure 5 explains the messages between entities applying a user's single sign-on among services, in which there are mutual trust relationships.

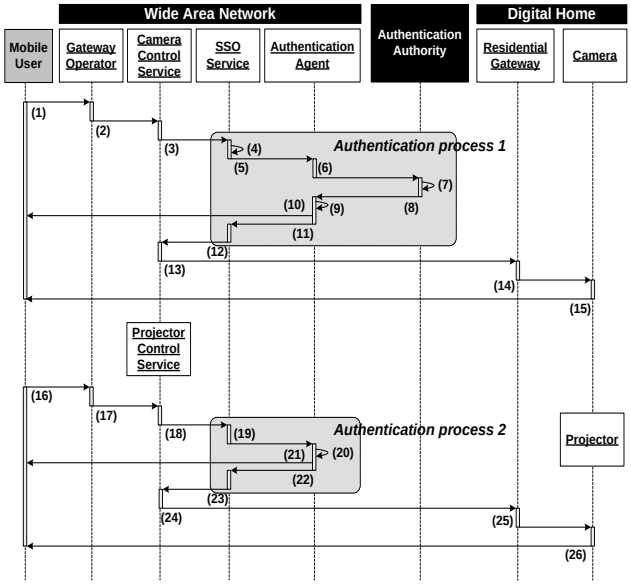


Fig. 5: Sequence Diagram of the Proposed Single Sign-on Architecture

A description of each step is as follows:
(1) The mobile user keys his name and password into his mobile device in order to access the Camera Control Service via the gateway operator.
(2) The gateway operator transfers the user's credential information to the Camera Control Service. When the user's password is transmitted, the password must be encrypted to prevent its exposure.
(3) The Camera Control Service requests user authentication from the SSO Service, providing the user's credential information.
(4) The SSO Service makes a SAML-based authentication query and signs it digitally to be trusted by the Authentication Authority.
(5) The SSO Service sends the signed authentication query to the Authentication Agent.
(6) The Authentication Agent requests user authentication from the Authentication Authority.
(7) The Authentication Authority verifies the signed authentication query, decrypts the user's password, authenticates the user, makes an authentication assertion, and signs it digitally.
(8) The Authentication Authority sends this signed authentication assertion to the Authentication Agent.
(9) The Authentication Agent verifies the signed authentication assertion, evaluates it, and signs the evaluated result digitally. If the result is valid, the Authentication Agent generates an artifact for the mobile user.
(10) The artifact is assigned to the mobile user who wants to access the Camera Control Service.
(11) The Authentication Agent returns the evaluated result to the SSO Service.
(12) The SSO Service leads the mobile user to the Camera Control Service.
(13), (14), and, (15) The Camera Control Service controls the Camera via the Residential gateway in the Digital Home. Before granting access to the Camera, the Residential Gateway must verify the signed result.
(16) The mobile user who wants to access the Projector Control Service via the gateway operator provides the artifact received from the SSO Service (refers to step (10)).
(17) The gateway operator transfers the artifact to the Projector Control Service.
(18) The Projector Control Service requests user authentication from the SSO Service, providing the artifact instead of the user's name and password.
(19) The SSO Service sends the artifact to the Authentication Agent. The SSO Service no longer makes an authentication query.
(20) The Authentication Agent compares the artifact received from the SSO Service (refers to step (10)) with the original artifact (refers to step (9)). If the result is valid, the Authentication Agent removes the original artifact and generates a new artifact for the mobile user.
(21) The new artifact is assigned to the mobile user who wants to access the Projector Control Service.
(22) The Authentication Agent returns the signed evaluated result to the SSO Service.
(23) The SSO Service leads the mobile user to the Projector Control Service.
(24), (25), and (26) The Projector Control Service controls the Projector via the Residential gateway in the Digital Home. Before granting access to the Projector, the Residential Gateway must verify the signed result.

```
<saml:Assertion AssertionID="00cda300-0d5de-8521-83c5-c2d9f6847b91"
      IssueInstant="2004-08-02T13:33:02Z" Issuer="1st_security.com"
      MajorVersion="1" MinorVersion="0">
    <saml:Conditions NotBefore="2004-08-02T13:33:02Z" NotOnOrAfter="2004-08-02T13:38:02Z"/>
       <saml:AuthenticationStatement  AuthenticationMethod="password"
                                      AuthenticationInstant="2004-08-02T13:33:02Z">
            <saml:Subject>
              <saml:NameIdentifier NameQualifier="1st_security.com">jijeong</saml:NameIdentifier>
            </saml:Subject>
       </saml:AuthenticationStatement>
       <saml:AttributeStatement>
            <saml:Subject>
                <saml:NameIdentifier SecurityDomain="1st_security.com" Name="samler"/>
            </saml:Subject>
            <saml:Attribute AttributeName="jobattribute"
                            AttributeNamespace="http://1st_security.com/test/schema/sec1.xsd">
              <saml:AttributeValue>
                  <Customer>
                     <company>sjcredit</company>
                     <email>uuu7@1st_security.com</email>
                  </Customer>
              </saml:AttributeValue>
            </saml:Attribute>
       </saml:AttributeStatement>
</saml:Assertion>
```

Fig. 6: Assertion with Authentication and Attribute Statement

The steps in Authentication process 2 are similar to those in Authentication process 1, since the Authentication Authority when accessing a certain service issues an artifact regarding user authentication. The user authentication scheme in each service may differ depending on the characteristics of each service. To transfer a security token, regarding a user's authentication, which was generated from a different user authentication scheme among the various services, a framework that does not restrict the representation of security information is

needed.

Figure 6 is an assertion statement issued by the SAML authority (refers to step (7) of Figure 5; its signed information is removed). This message was verified by a simulation where two services were constructed with a mutual trust relationship and the SAML libraries, which were built from previous work [17].

Fig. 7: Conference room viewed by the Camera Control Service

Figure 7 shows the views of conference rooms from the Camera Control Service. In Figure 7, CH#0 and CH#2 show one room and CH#3 and CH#4 show the other room. The mobile user can view each room to select a room for a meeting and then turn on the projector of the selected room using the Projector Control Service before the meeting.

Fig. 8: Conference room where the projector is on

Figure 8 shows the room where the projector is on for the meeting.

## 4. Conclusion

In home network environments based on the OSGi framework, there exist some barriers to distributing automated user authentication due to the limited capabilities of mobile devices. To overcome these problems, we proposed a security scheme to exchange user authentication information based on SAML under an OSGi-based home network environment. This scheme supports the efficient and secure transfer of a user's credential information between a mobile device and home networks, for service networks, and offers access to related domains without the burden of a repeated log-in process.

Since the proposed Single Sign-On scheme is designed to recognize the individual authentication scheme in each domain, OSGi framework-based systems, which are applied in our proposed architecture, can have the Right of self-government as well as extensibility.

## 5. REFERENCES


[1] Digital Home Working Group Std., “Digital Home White Paper”, DHWG, 2003.

[2] Dong-Sung Kim, Jae-Min Lee, Wook Hyun Kwon, In Kwan Yuh, “Design and implementation of home network systems using UPnP middleware for networked appliances”, IEEE Transactions on. Consumer Electronics. Vol. 48. Issue. 4. pp. 963-972, 2002.

[3] S. Landis, V. Vasudevan, “Reaching out to the cell phone with Jini”, HICSS. Proceedings of the 35th Annual Hawaii International Conference on. System Sciences. pp. 3821-3830, 2002.

[4] R. Lea, S. Gibbs, A. Dara-Abrams, E. Eytchison, “Networking home entertainment devices with HAVi”, IEEE Transactions on Vol. 33. Issue. 9. pp. 35-43, 2000.

[5] H.C. Ferreira *et. al.*, “Power line communications: an overview”, IEEE AFRICON 4th. Vol. 2. pp. 558-563, 1996.

[6] Choonhwa Lee, D. Nordstedt, S. Helal, “Enabling smart spaces with OSGi”, IEEE Pervasive Computing. Vol 2. Issue. 3. pp. 89-94, 2003.

[7] A. Volchkov, “Revisiting single sign-on: a pragmatic approach in a new context”, IT Professional 3, Issue. 1. pp. 39-45, 2001.

[8] T.A. Parker, “Single sign-on systems-the technologies and the products”, European Convention on Security and Detection. 16-18. pp. 151-155, 1995.

[9] T. Pilioura, A. Tsalgatidou, S. Hadjiefthymiades, “Scenarios of using Web Services in M-Commerce”, ACM SIGecom Exchanges. proc. pp. 28-36, 2003.

[10] Y.G. Kim *et. al.*, “A Service Bundle Authentication Mechanism in the OSGi Service Platform”, AINA 2004. Proc. pp. 420-425, 2004.

[11] OSGi Alliance Std., “OSGi Service Platform Release 3”, OSGi Alliance, 2003.

[12] E. Maler, P. Mishra, R. Philpott, “Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1”, OASIS Committee Specification. 2003.

[13] G. Ben, H and Whitney *et. al.*, “Professional Web Services Security”, Wrox, 2002.

[14] OSGi Alliance Std., “Secure Provisioning Data Transport using Http”, RFC36. http://www.osgi.org/, 2002.

[15] Birgit Pfitzmann., “Privacy in enterprise identity federation | Policies for Liberty single signon”, In Proceedings: 3rd Workshop on Privacy Enhancing Technologies (PET 2003), Dresden, March 2003.

[16] A. Pashalidis and C. J. Mitchell, “A taxonomy of single sign-on systems“, Lecture Notes in Computer Science, vol.2727. Springer-Verlag, July 2003, pp. 249–264. 2003.

[17] J. Jeong *et. al.*, “Java-Based Single Sign-On Library Supporting SAML (Security Markup Language) for Distributed Web Services”, Lecture Notes in Computer Science 3007, 2004.