Federated Identity Management and Web-Services Framework for Broadcasting - Communications Hybrid Services

Recently, a fusion of broadcasting and communications is accelerating. Under this circumstance, it is expected that television will provide not only public information but also personalized information depending on individual needs. In this article, we describe federated identity management and web-services framework that make it possible for broadcasters to provide personalized services to individual viewers securely.

1. Introduction

July 2011 will be the month in which Japan completes its transition to digital terrestrial broadcasting. This situation encourages viewers to buy or update televisions to ones able to receive digital terrestrial broadcasts and have communications capabilities. An NHK survey conducted at the end of December 2010 has revealed that approximately 100.3 million units (including digital tuners and cable TV set-top boxes (STB)) have been sold to households, and that number is growing steadily.

Television has always been a public broadcast medium, but with the introduction of communications features to receivers, it now has the capability to provide personalized and on-demand services that can meet the individual needs of viewers. In fact, some broadcasters are now starting to offer communications-enhanced services for television. For example, they are developing interactive data broadcasting services, which enable viewers to answer quiz questions or apply for the presents offered by television program. They also have started on-demand video services such as NHK On-Demand, which began in December 2008. Such communications-enhanced services are gaining a growing number of users[1]. However, the communications-enhanced services currently being developed by broadcasters are limited to those handling content and resources managed by themselves and do not yet consider individualized use adequately. In order to stimulate the use of communications services offered through television, it is necessary to make a rich variety of content and resources, including personal information managed by not only broadcasters but also other businesses, accessible.

At NHK STRL, we are conducting research toward making television a means of obtaining personalized information and enabling viewers to use various services securely through a communications network.

In this article, we shall briefly discuss issues related to using personalized services through the television and describe identity federation technology between multiple services. We will also describe a prototype authentication federation system for providing personalized services, the goal of which is to enrich communications services offered through television.

2. Expectations and Issues using Televisions for Personalized Services

Personalized services have been developed in various fields recently, and NHK also began its "NHK Net Club"[2] membership service in 2009. Frameworks for individuals to obtain information themselves through the network are also being studied in the field of government, with initiatives such as the introduction of a citizen ID system together with implementation of a citizen-oriented eGovernment, and key policies for the study of service frameworks in the medical field that will allow individuals to access their own health and medical information[3]. In order to provide these personal information to each user securely, each service provider must manage user identities, including the user's ID, credentials (passwords, etc.), and attributes (address, age, etc.) and provide services as appropriate according to user authentication result.

Personalized services have been thought of as provided mainly through PCs, but for them to be truly popular, they should be accessible through a variety of means besides PCs. In particular, it is hoped that televisions could be used as a familiar access point to obtain personal information because they are present in a high proportion of households and convenient to use.

To use televisions for personalized services, the following requirements must be met.

(1) Authentication effort must be reduced.

Unlike PCs, televisions do not provide an interface such as a keyboard or mouse, so there is a concern that input operations such as entering the user ID and password for authentication will be difficult for users. This burden might become even heavier if the user tries to access a number of personalized services. In order to use multiple personalized services conveniently, the authentication process must be made easier, while ensuring the security of the identities that these services manage independently.

(2) Personalized services must be used securely.

Personalized services might have to handle highly confidential information such as medical or financial data. With such privacy-related information, care must be taken in order that the information does not leak to third parties outside the service providers that hold the

information.

Services handling very confidential information often require biometric authentication such as fingerprints or iris scans, or authentication using a smart card or some other token*1. However, it is inconvenient for viewers to have to buy the equipment necessary for biometric authentication or a smart card reader, particularly when using the television. A balance between service security level and user convenience must be struck whilst taking into account the capabilities and characteristics of television.

(3) Services must make use of the strengths of television.

When using the television for personalized services, we can hope to increase convenience for users, and also improve services in ways that take advantage of characteristics of television, such as linking to broadcast programming.

In this article, we refer to personalized services that satisfy these issues and provide personal information securely and easily as "personalized services in a broadcasting-communications hybrid environment". Such a service is portrayed in Figure 1.

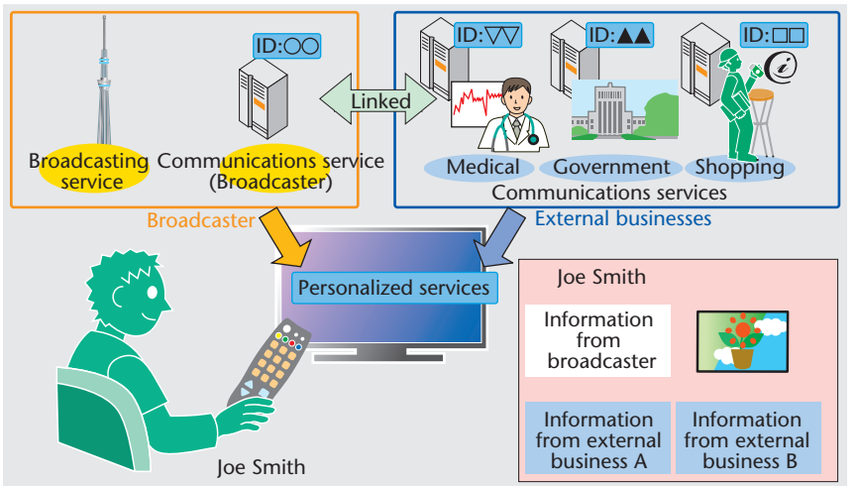

Figure 1: Personalized services in a broadcasting-communications hybrid environment

3. Identity Federation between Multiple Services

There are a number of methods for managing user identities effectively among multiple services, including OpenID[4], which utilizes a single, unified ID with multiple services, and Security Assertion Markup Language (SAML) [5] , which builds trust relationships between services (a circle of trust) beforehand for federated identity management[6].

OpenID is a decentralized model that does not require trust relationships or identity links to be established ahead of time, and this simplicity has lead to broadening usage for popular Web services. However, OpenID involves an exchange of information with unique ID described in Uniform Resource Locator (URL) or eXtensible Resource Identifier (XRI), and it might present a higher security risk than SAML. On the other hand, with SAML, each Service Provider (SP) can protect the user identities managed by themselves, while an Identity Provider (IdP) manages links between the scattered identities of the services within a trusted circle. A pseudonym different from the actual ID is used when linking identities. This avoids any chance of the real user ID being leaked or a breach of privacy by tracing user's name, yet allows security information such as authentication, authorization, and attributes to be exchanged.

For these reasons, we decided to develop an authentication federation system based on SAML, to share authentication information or attributes securely within a trusted circle, and which enables service providers to manage user identities individually. The SAML specification is based on eXtensible Markup Language (XML), so it also has the benefit of being very extensible.

4. User Authentication and Device Authentication

Considering the performance and simplicity of introduction with current televisions, a user ID and password should be a suitable form of authentication for using personalized services through the television. However, for services requiring a high level of security, a more robust form of authentication may occasionally be required. Thus, in addition to user authentication using an ID and password, we studied a more secure authentication that verifies whether or not the device that the user is using is pre-registered as a household television. Using different elements to authenticate is called two-factor authentication, and it is adopted in some of the services as a relatively easy way to strengthen authentication[7].

By checking both user authentication and the legitimacy of the device being used, we can increase the security of authentication. It also enables service providers to control access flexibly according to the users' viewing environments, such as by limiting a service to registered televisions within a household.

5. Authentication Federation System for Personalized Services in a Broadcasting- Communications Hybrid Environment

We now introduce an authentication federation system for personalized services in a broadcasting-communications hybrid environment, which we have developed based on the considerations described above. The system allows viewers to use personalized services from NHK and external service providers securely and easily through data broadcasting service.

*1 A physical device required for use of the service.

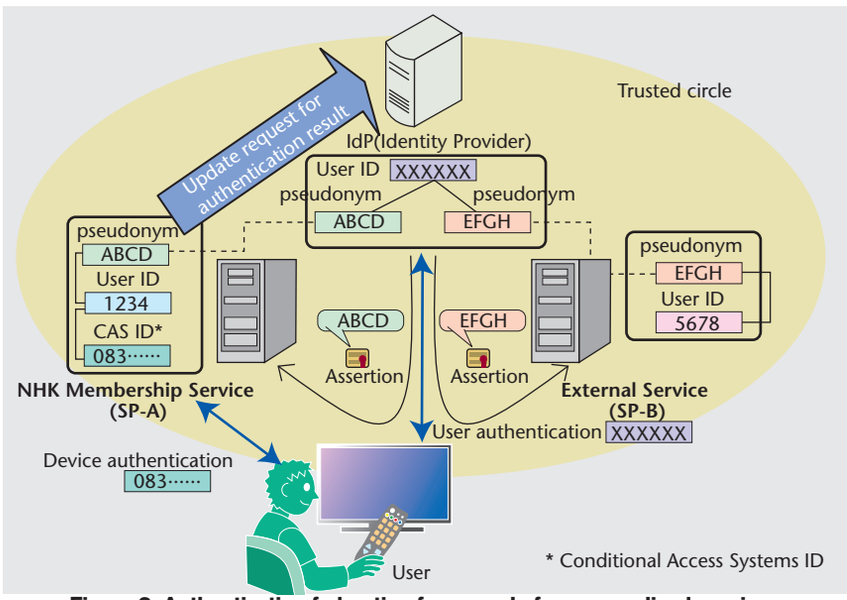

Figure 2: Authentication-federation framework for personalized services in a broadcasting - communications hybrid environment

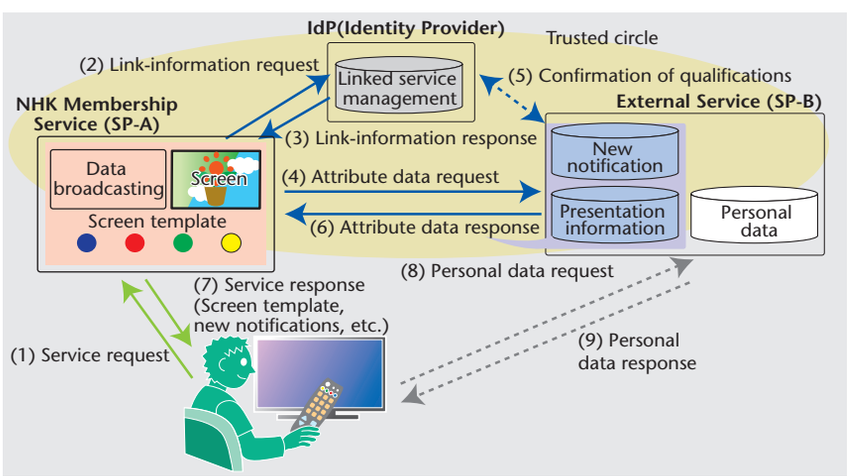

Figure 3: Attribute exchange framework

5.1 Single Sign-on through Federated Authentication of the User and Device

The authentication federation system uses pseudonyms to link identities within a trusted circle, formed beforehand among the NHK membership service (SP-A), external services (SP-B), and the IdP. The IdP provides centrally managed authentication information in the form of certificates called assertions. In this way, the user is able to perform authentication once and then use multiple personalized services (single sign-on)[8].

User is authenticated by the IdP, which links and manages user identities. But identifying information or authentication procedures for televisions or other devices are often managed exclusively by a particular business such as the vendor*2 or platform operator. Making all service providers manage device-related information separately leads additional risks in terms of cost and security. To deal with these problems, we extended the SAML protocol so that the management and authentication of user devices can be done by specific service providers, and the result of this authentication can be associated with the user authentication result and shared within the trusted circle. In this way, even if a service provider does not manage and authenticate the device being used, it can use the two-factor authentication result, and can flexibly provide services that take the user's access environment into account[9]. The authentication mechanism for the system is shown in Figure 2.

5.2 Exchange of Attribute Data

New kinds of personalized services that use broadcasting as a starting point can be provided when they are implemented together with broadcasting services, such as prompting viewers to access an external service that handles their health information while viewing health programs on television, or recommending program content related to what the viewer is currently viewing. To implement such services, fundamental information for a broadcasting-communications hybrid service must be distributed by the broadcaster.

With this system, some of the attribute data that is not particularly confidential, such as user-menu, presentation-style data, and existence of new information, can be retrieved from external providers by the broadcaster and presented within the broadcaster's data-broadcast framework to present services suited to the user and deliver notifications on a per-household basis. For the attribute data exchange framework, we used the ID-Web Service Framework (ID-WSF)[10] specification created by the Liberty Alliance Project. The process of exchanging attribute data is shown in Figure 3.

5.3 Secure Presentation of Private Information

For linking to public services, which handle personal information related to health or social security, such confidential information shall not be sent via the broadcaster, and must be provided directly to the user. With this system, the television obtains detailed personal data directly from the external provider in XML format and a presentation template from the

*2 The company or manufacturer of a product, etc.

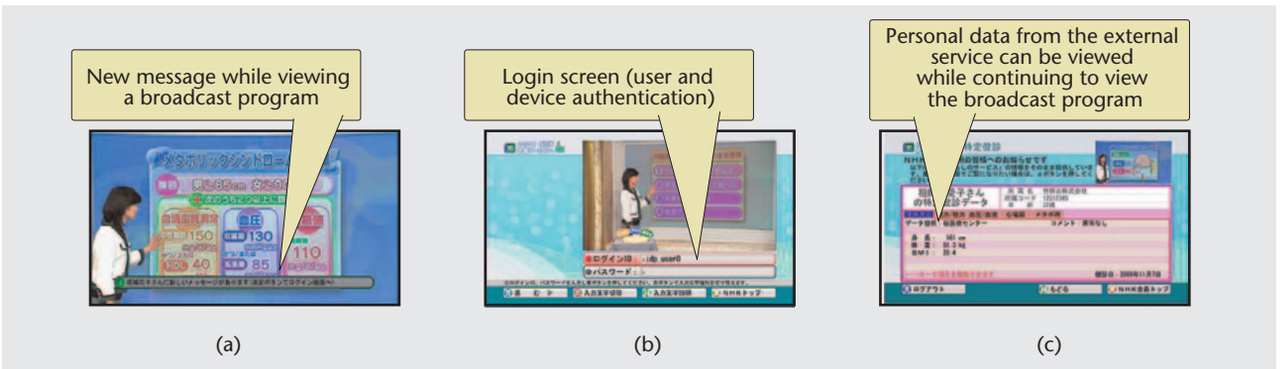

Figure 4: Transition of screens for receiving the personalized services

broadcaster as a stylesheet in XML Stylesheet Language Transformation(XSLT), as shown in Figure 3. And then, it transforms them into Broadcast Markup Language (BML), which is a language for describing data broadcast. In this way, the television can render the personalized service in the BML browser[11].

Figure 4 shows how such personalized services can be provided. Figure 4 (a) shows the screen of broadcast program. The broadcaster uses the attribute data exchange framework to check whether there is any new information for the user at any of the service providers within the trusted circle. If new information is detected, it notifies the pre-registered television of the existence of new information. The television receiving the notice displays a message on the screen, which let the users who are watching the television know the existence of new information.

Figure 4 (b) shows the login screen to use a personalized service. The user is asked to enter a user ID and password, and both the user and the device are authenticated. As described in Section 5.1, when both of these are authenticated once, the authenticated user can use not only NHK membership services, but also various other personalized services within the trusted circle.

Figure 4 (c) shows a screen displaying personal information managed by an external service with a screen template provided by the broadcaster. For example, the user can continue viewing the health program based on the data broadcast service, while securely viewing his or her health data obtained directly from the external service, within the red-framed, external-data presentation region. It is possible to link to on-demand services, such as displaying programs related to the content being viewed.

6. Conclusion

In this article, we discussed identity-management technologies to allow viewers to easily and securely receive personalized services in a broadcasting?communications hybrid environment. The identity web-services federation framework between broadcaster's services and external services enables viewers to enjoy various personalized services without interrupting the broadcaster's service. In the future, we will work on creating more sophisticated communications services linked to broadcasting.

(Chigusa Yamamura and Arisa Fujii)

References

1) K. Ogawa: "The Role of Television in the Network Age: From the 2010 Trend Survey on the Internet Use via Television," NHK Monthly Report on Broadcast Research, June Issue, pp. 90-105 (2010) (Japanese).
2) NHK Net Club, https://pid.nhk.or.jp/pid01/
3) Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society(IT Strategic Headquarters): "A New Strategy in Information and Communications Technology(IT)," http://www.kantei.go.jp/foreign/policy/it/100511_full.pdf .
4) OpenID Foundation: "OpenID Authentication 2.0," http://openid.net/specs/openid-authentication-2_0.html .
5) OASIS: "Security Assertion Markup Language Version 2.0 (SAML V2.0)," http://saml.xml.org/saml-specifications#samlv20.
6) K. Takahashi: "Trends in Identity Management," IEICE Journal, Vol. 92, No. 4, pp. 287-294 (2009) (Japanese).
7) N. Tamura: "Examining the best user authentication possible today," Nikkei Communications, July, No. 558, pp. 19-21 (2010) (Japanese).
8) A. Fujii, S. Fujitsu, K. Ishikawa, T. Yoshimura, G. Eto, Y. Konya, T. Yamada, M. Kawamori, and K. Kawazoe: "A study on Single Sign-On system for a digital TV receiver: A Gateway between Home Server based on Broadcasting and Communication Network," IEICE Technical Journal, Vol. 105, No. 264, MoMuC 2005-44, pp. 77-81 (2005) (Japanese).
9) C. Yamamura, A. Fujii, K. Ishikawa, Y. Homma, T. Obi, M. Yachida, and J. Lee: "User-device authentication federation framework for receiving personalized telecommunication services based on data broadcasting service," IPSJ Forum on Information Technology 2010, L-035 (2010) (Japanese).
10) Liberty Alliance Project: "Liberty Identity Web Services Framework 2.0 (Liberty ID-WSF)," http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates .
11) C. Yamamura, A. Fujii, and K. Ishikawa: "A presentation method for personal information from external provider on data broadcasting," ITE Annual Symposium, 3-7 (2009) (Japanese).