특집논문-09-14-4-08

IPTV 서비스 제공을 위한 XML 기반의 단일인증 구조

이 승 훈[a], 신 동 일[a], 신 동 규[a]‡

XML-based Single Sign-On Scheme for Internet Protocol TV(IPTV)Services

Lee SeungHun[a], Shin Dongil[a], and Shin DongKyoo[a]‡

요 약

방송 서비스에 가입자 개념을 채택함으로써, IPTV 사업자는 가입자의 결제수준을 기반으로 다양한 등급의 서비스를 제공한다. 가입자로 부터의 수입을 기반으로 하여 IPTV 사업자는 고품질의 서비스를 제공 할 수 있게 된다. 웹 브라우저 기반의 IPTV는 TV 서비스와 더불어 T-커머스 및 E-커머스 서비스도 제공하므로, 사용자는 자주 인터넷 쇼핑이나, 서비스 콘텐츠를 구입하기위해 다른 서비스 도메인에 접속하게 된다. 사용자가 구매한 서비스나 개인적인 서비스를 제공하기위하여 해당 서비스 도메인은 사용자 인증을 요구하게 된다. 현존하는 인증시스템은 한 도메인에서 다른 도메인으로 사용자가 이동했을 경우 재인증 절차를 요구하므로, IPTV 환경에 적절하지 않다. SSO(Single sign-on)구조는 한번 인증된 사용자가 다른 서비스 도메인으로 이동했을 경우 재인증 절차를 요구하지 않는 투명한 인증 서비스를 제공한다. IPTV에서 인증이 필요한 다양한 서비스가 제공되므로, 결제가 필요한 도메인이나 개인 도메인으로 이동시에 이러한 투명한 인증 서비스가 제공되어야 한다. 본 논문에서는 IPTV 환경에 대한 새로운 사용자 인증 구조를 제시하며, 이 구조는 XML 기반의 SSO 표준인 SAML(Security Assertion Markup Language)을 통합한다. 사용자-사례 시나리오를 이용하여 제안된 구조를 검증하였다.

Abstract

By employing the subscriber concept in broadcasting services, IPTV (Internet Protocol Television) operators provide various grades of services to subscribers based on the billing level of the subscribers. With the income from subscribers for a basis, IPTV operators plan to provide high quality services. Since Web browser-based IPTV provides T-commerce and E-commerce services as well as television services, users may frequently visit other service domains to buy goods or content. To provide the user with charged or private services, these service domains request authentication of user. The existing authentication system is not appropriate for the IPTV service environment because the environment unavoidably forces the user to cross from one authentication-based service domain to another. Single sign-on provides a user with transparent authentication services by enabling an authenticated user to move between authentication-based service domains without any re-authentication. Like this distributed environment, since the IPTV service environment also provides a variety of authentication-based services, transparent authentication service needs to be provided to subscribers who want to access charged or private services. In this paper, we propose a new user authentication scheme for the IPTV environment. This scheme integrates the Security Assertion Markup Language (SAML), which is a standard for XML-based single sign on. We validate this scheme using a simple use case scenario.

Keyword : Single sign-on, SAML, Home network, Authentication, Artifact

I. Introduction

As a new media service environment is built in which broad bandwidth communication networks and digitalized broadcasting converge, the distinction between communications and broadcasting will become ambiguous. In this environment, service providers will be expected to provide consumers with converged content services[1]. IPTV (Internet Protocol Television) well reflects this trend as a domain-neutral service. Unlike existing broadcasting services, IPTV operators employ the subscriber concept in their business model and provide various grades of services to subscribers based on various billing levels. This business model enables IPTV operators to expect stable income and gives consumers access to personalized services.

To operate this business model successfully, it is necessary to have a reliable user authentication scheme. However, the relationship between strong security requirements and user convenience is like a two edged sword. When a user requests different services from individual service providers, the user has to visit each service domain individually[2]. In this case, although it is possible to maintain individual security schemes for each domain, the user will have to accept the need for frequent authentication from these domains[3].

In this paper, we propose a new user authentication scheme for the IPTV environment. This scheme integrates the Security Assertion Markup Language (SAML)[4], which is a standard for XML-based single sign-on. We validate this scheme using a simple use case scenario.

a) 세종대학교 컴퓨터공학과
Department of Computer Science & Engineering at Sejong University in Korea
‡ 교신저자 : 신동규(shindk@sejong.ac.kr)
※본 연구는 보건복지가족부 보건의료기술진흥사업의 지원에 의하여 지원받았음. (과제고유번호: A040163)
· 접수일(2009년3월20일),수정일(2009년7월1일),게재확정일(2009년7월1일)

II. Background

Web browser-based IPTV provides various services, just as do the Internet and digital TV[5]. In the IPTV environment, users are forced to provide their information credentials frequently, because they have to access distributed services offered by different service domains. To avoid this inconvenience, the IPTV service environment needs to employee a single sign-on scheme for user authentication. In this section, we illustrate the concepts which support our scheme: IPTV, the security requirements for IPTV, a single sign-on scheme, and the Security Assertion Markup Language (SAML).

1. IPTV (Internet Protocol Television)

Although IPTV extends the PC-based domain and offers the additional content services of the Internet, such as Walled Garden, VOD, and E-Bank, to the TV-based domain, its broader concept means a model accepting various broadcasting channels using ultrahigh speed Internet as a broadcasting media[5]. Since IPTV enables two-way communication between users, video services based on communication services, as well as the existing TV services, can also be offered to many users using the existing network infrastructure and the Internet.

IPTV is emerging as a new trend integrating ultrahigh speed and DTV (Digital Television). By offering the Internet and broadcasting services together, using an existing TV and internet modem, IPTV services can even be provided to users who are familiar with TV services but who have difficulty with PC-based services. Recently, with STB (Set Top Box) becoming more intelligent and being integrated with Internet modems, the role of IPTV has also been changing, becoming a terminal node for supporting home network services[5].

IPTV has the following representative features[6]:

- Interactive services: These allow consumers to actively participate in contents services. In the existing broadcasting services, the consumer's right of choice is very passive, with the consumer being forced to select contents at the time the contents are served. In contrast, IPTV allows a consumer to choose whatever contents he wants, regardless of the time. A consumer can also submit his opinion about contents to a service provider.
- The activation of E-business using T-commerce: Since there are diverse transactions in the IPTV business environment into which internet shopping malls and TV home shopping are integrated, consumers can instantly and easily get information about target goods, along with purchase guidance, through such transactions.
- TPS (Triple Play Service): Simultaneously supports ultrahigh speed internet, Internet phone service and broadcasting service using the internet network infrastructure.

A content provider provides services to IPTV via a streaming server in a broadcasting system using ultrahigh speed internet. Because these services are provided based on IP, the content provider can be aware of the location where the services are requested to ensure that the individual requesting the services can be accurately authenticated. IPTV provides the following custom-made channels and various bidirectional data service, as well as fundamental channels[7].

- T-Commerce: stock market data, shopping, banking, and auctions
- T-info: weather, news, general information, traffic information, and local information
- T-Com: messenger, e-mail, videophone, and SMS
- T-Entertainment: blogs, photos, games, and VOD
- T-Learning: educational programs and language study

2. Security Requirements

Security aspect for IPTV is being considered in IPTV Focus Group of ITU-T, with the standardization efforts of the overall specifications for IPTV[8]. Security requirements on user authentication are as follows:

- The IPTV architecture, as shown in Figure 1, should support authorization and authentication capabilities for the end-user. This can optionally include the capability of a service provider to authenticate and authorize a subscriber, his IPTV terminal device and a different service provider.

- Authentication and Authorization
  (1) For managed services involving protected content, it is typically the case that the subscriber must be authenticated and, subsequent to successful authentication, authorized to access service(s) and the content contained therein.
  (2) Depending on circumstances, authentication and authorization functions may be performed separately on the IPTV terminal device and the subscriber(s). In other cases, additional devices in subscriber premises, such as a delivery network gateway and other subscriber devices may require authentication before service access is authorized.
  (3) The combination of authentication and authorization can be considered to effect positive access control on the terminal device and subscriber for purposes of service and content acquisition prior to use.

The requirements above reflect representative broadcasting middleware standard specifications such as OCAP

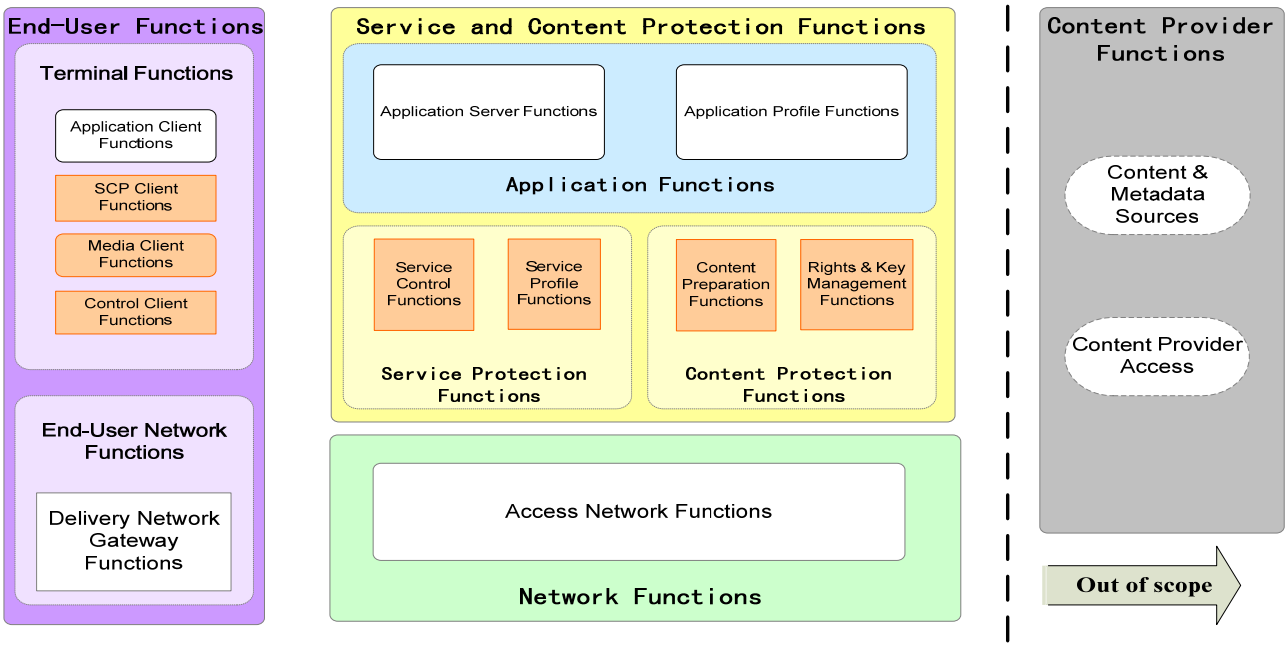


그림 1. 일반적인 IPTV 보안구조
Fig. 1. IPTV General Security Architecture

(OpenCable Applications Platform)[9] and ACAP (Advanced Common Application Platform)[10].

Although progress is being made on the task of standardizing the overall specifications for IPTV, the progress will appropriately reflect representative standard specifications the OpenCable Applications Platform (OCAP) which is standard[11] and Advanced Common Application Platform (ACAP)[12]. In both specifications, requirements related to user authentication are as follows[13]:

표 1. 보안체계 설계 지침
Table 1. Security System design guidelines

Reference	Guidelines
SEC1	Includes the design necessary to communicate the authentication credentials for elements
SEC2	Authentication credentials for PS and critical back-office servers will be provided. The credentials will define specific usage and ensure a source of trust

표 2. 인증기반체계 설계 지침
Table 2. Authentication infrastructure system design guidelines

Reference	Guidelines
SEC1	Includes the design necessary to communicate the authentication credentials for IPCable2Home elements
SEC2	Authentication credentials for CPE and critical back-office servers will be provided. The credentials will define specific usage and ensure a source of trust.

3. Single Sign-On Scheme

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 a 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[14].

There are two approaches for implementing single

sign-on.

- 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 Web Service in the initial SOAP message.

In the first approach, all the old IDs for users are removed and new IDs are assigned from a Central Repository [15]. To access Services, a user must use a new ID. Although this approach is suitable for a single organization, individual organizations may lose the ability to manage security with this system, since all the users' information is stored in 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 their existing ID to access different domains without needing a new ID [14][15]. 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 that the user 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 proprietary authentication schemes in order to communicate with other organizations. The second approach is more appropriate for an IPTV service environment in which all services require user authentication. Figure 2 illustrates the concept of the second approach.

Figure 2 is the prototype of the proposed single sign-on architecture in which the IPTV delivers certain services offered by service providers to the end user regardless of the system environments.

4. 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 [4][16]. 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.

- Authentication Assertion: indicating that a subject was authenticated previously by some means, such as a password, hardware token, or X.509 public key.
- Attribute Assertion: indicating that the subject is associated with attributes.
- Authorization Assertion: indicating that a subject should be granted or denied resource access.

The SAML authority can be classified as authentication

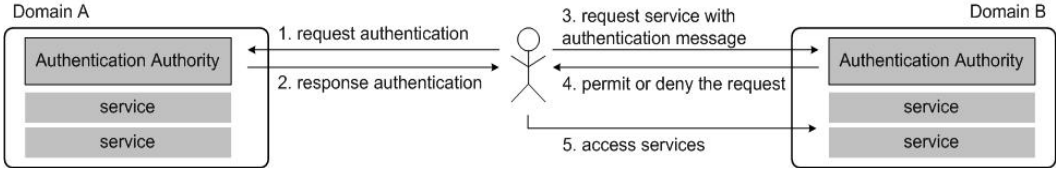


그림 2. 복합 서비스의 단일인증 구조
Fig. 2. Single Sign-On To Multiple Services

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, an IPTV STB keeps its artifact, which verifies that the user has been authenticated once by the SAML authority in the system.

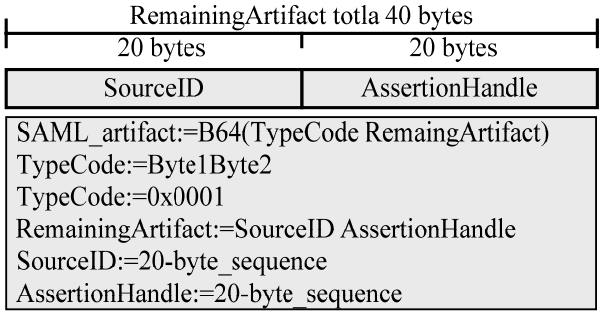


그림 3. Artifact 구조
Fig. 3. The Structure of Artifact

SAML defines an artifact mechanism when the authorization request is too long for an HTTP redirect. The artifact has a role of tokens. It is created within a security domain and sent to other security domains for user authentication.

The artifact format includes a mandatory two-byte Type Code followed by 40 bytes long Remaining Artifact containing a type-code (20 bytes for a Source ID) and a 20-byte random number for Assertion Handle that the servers use to look up an assertion, as shown in Figure 3[15].

III. Single Sign-On Architecture for IPTV Service Environment

The design purpose of this single sign-on architecture is to reduce the time taken by an IPTV user for user authentication, with improved security through the reduced need for the user to handle and remember multiple sets of authentication information. We propose a single sign-on scheme in which an IPTV STB offers his credential information to authentication agent in the trusted domain for

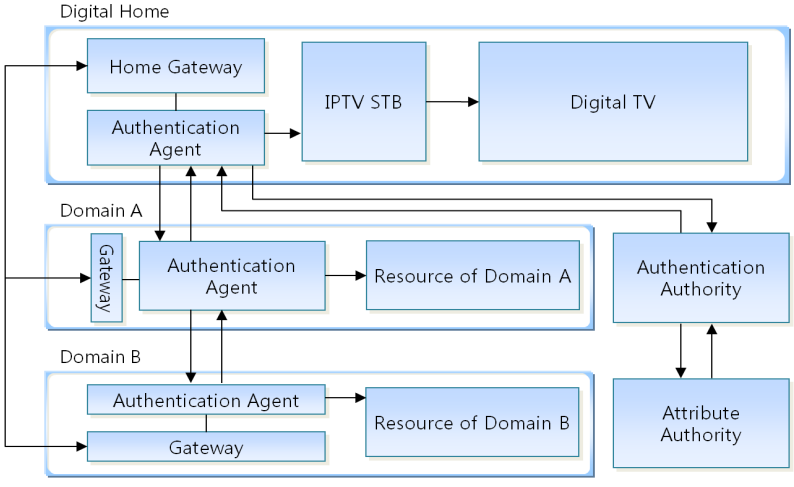


그림 4. 제안하는 단일인증 스키마
Fig. 4. The Proposed Single Sign-On Scheme

obtaining user authentication and access to another domain such as commerce, banking and VOD to get related services using this authentication, based on the SAML standard. Figure 4 explains the concept of this architecture. A user keys in his user name and password to the IPTV STB to access a service. The user credential information is transferred to an authentication agent through a gateway, which connects the IPTV STB and service domains. The authentication agent sends a user authentication request to an authentication authority, in which there is a mutual trust relationship. The authentication authority authenticates the user and returns an authentication assertion to the authentication agent. The IPTV STB then has access to a service in Domain A after successfully getting user authentication from Digital Home. Domain A asks the user's authentication information to the authentication agent of Digital Home, and then the agent sends the authentication assertion to Domain A. Thus, Domain A performs user authentication through the authentication assertion issued by the authentication authority.

In this scheme, user authentication information must be digitally signed and encrypted to guarantee security of the transmission through open networks. Figure 5 shows the procedure for single sign-on in case that a IPTV STB keeps user's authentication information generated from the trusted domain. Each step denoted by an arrow and number in the diagram is explained as follows:

(1) The user's credential information in the IPTV STB is transferred to the Authentication Authority in the trusted domain.
(2) The Authentication Authority generates the authentication information by authenticating the user using his credential information.
(3) The authentication information is encrypted and signed digitally for secure transmission.
(4) The authentication information is transferred to the IPTV STB.
(5) The IPTV STB checks the integrity of the transferred authentication information to protect illegal modification and fabrication.
(6) The authentication information in the IPTV STB is transferred to Domain A for access.
(7) Domain A checks integrity of the received authentication information and decrypt it.
(8) The access is granted if the authentication information is valid.

Figure 6 shows the procedure for single sign-on in case that an IPTV STB keeps an artifact instead of authentication information (that is, "assertion" in the SAML standard) to minimize the computing burden. In this case, an IPTV STB keeps its own string type artifact which verifies that the device or the user it self has been authenticated by some compound methods. Each step denoted by an arrow and number in the diagram is explained as follows:

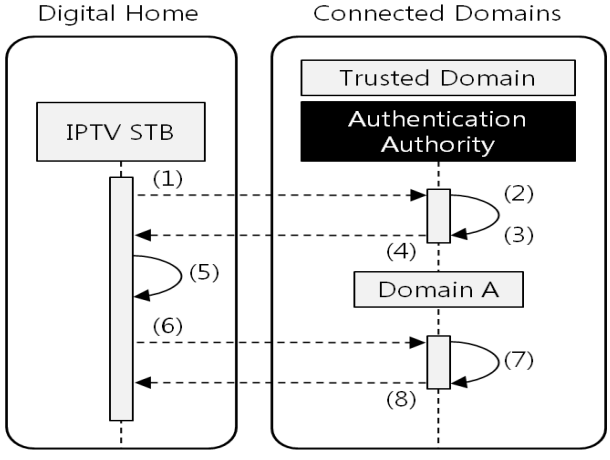


그림 5. 인증 정보를 사용한 단일인증 구조
Fig. 5. Single Sign-On using Authentication Information

(1) The user's credential information in the IPTV STB is transferred to the Authentication Agent in Domain A.
(2) The credential information in the IPTV STB is trans-

ferred to the Authentication Authority in the trusted domain.

(3) Authentication Authority generates authentication information by authenticating the user using his credential information.

(4) The Authentication information is encrypted and signed digitally for secure transmission.

(5) The Authentication information is transferred to the Authentication Agent in Domain A.

(6) The Authentication Agent in Domain A checks the integrity of the transferred authentication information.

(7) The Authentication Agent in Domain A generates an artifact which verifies the user has been authenticated by the Authentication Authority.

(8) The artifact is transferred to the IPTV STB.

(9) The artifact in the IPTV STB is transferred to Domain B for access.

(10) The Authentication Agent in Domain B sends an artifact to the Authentication Agent in Domain A as soon as it receives the artifact from the mobile device.

(11) The Authentication Agent in Domain A checks integrity of the received artifact.

(12) If the artifact is valid, the Authentication Agent in Domain A sends the user's authentication Authentication Agent in Domain A is discarded.

(13) The Authentication Agent in Domain B checks the integrity of the received authentication information and decrypts it.

(14) The Authentication Agent in Domain B generates an artifact which verifies that the user has been authenticated by the Authentication Authority.

(15) The generated artifact is transferred to the IPTV STB.

(16) The access to Domain B is granted if the authentication information is valid.

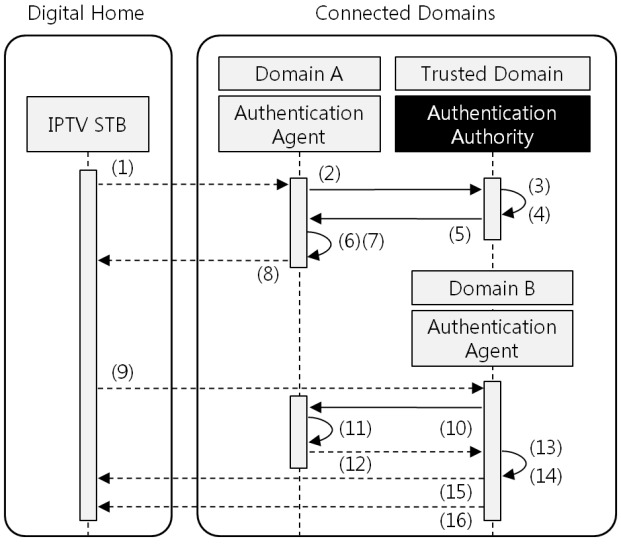


그림 6. Artifact를 사용한 단일인증 구조
Fig. 6. Single Sign-On using an Artifact

The single sign-on scheme using an artifact explained in Figure 6 requires more processing steps than the scheme shown in Figure 4. However the processes which need high computing capabilities are performed by the Authentication Agent, the IPTV STB needs to keep an artifact which is of small size and string type. It can save computing power and memory in the IPTV STB.

The user authentication scheme in each domain may differ depending on the characteristics of each domain. To transfer security tokens regarding user's authentication, which were generated from different user authentication schemes among domains, a framework which does not restrict the representation of security information is needed.

The user authentication procedure for the architecture shown in Figure 4 is presented in the form of a sequence diagram in Figure 7, where each box in the diagram denotes an entity involved in this process. Figure7 explains the messages between entities applying a user's single sign-on in IPTV STB and two domains, in which there are mutual trust relationships. Steps in Domain B are similar to those in Domain A, since an artifact regarding user au-

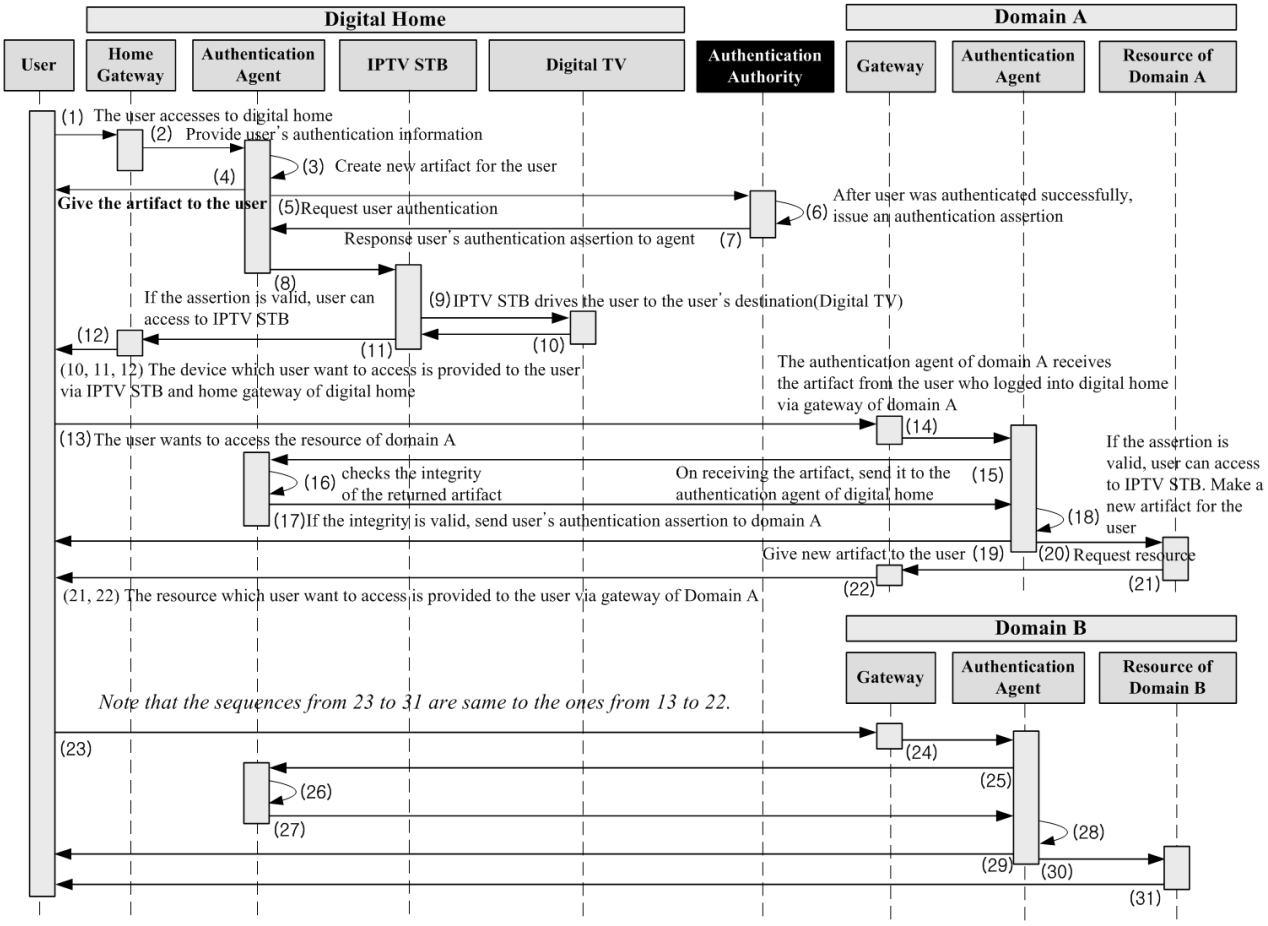


그림 7. 제안하는 단일인증 구조의 순차도
Fig. 7. Sequence Diagram of the Proposed Single Sign-on Architecture

thentication is issued by the Authentication Authority when accessing IPTV STB. The user authentication scheme in each domain may differ depending on the characteristics of each domain. To transfer security tokens regarding user's authentication, which were generated from different user authentication schemes among domains, a framework which does not restrict there presentation of security in formation is needed.

SAML defines the Action element for representing a user's security information. The assertion includes an Authentication Statement element for representing a user's authentication information and the Authentication Statement element, which includes the Authentication Method attribute for supporting various user authentication methods. The user authentication methods supported by SAML are as follows[16].

- Password
- Kerberos
- Secure Remote Password (SRP)
- Hardware Token
- SSL/TLS Certificate Based Client Authentication

- X.509 Public Key
- PGP Public Key
- SPKI Public Key
- XKMS Public Key
- XML Digital Signature
- Unspecified

```
<element name ="AuthenticationStatement"
        type="saml:AuthenticationStatementType"/>
<complexType name="AuthenticationStatementType">
  <complexContent>
    <extension base="saml:SubjectStatementAbstractType">
      <sequence>
        <element ref="saml:SubjectLocality" minOccurs="0">
        <element ref="saml:AuthorityBinding" minOccurs="0"
                maxOccurs="unbounded"/>
      </sequence>
      <attribute name="AuthenticationMethod"
                type="anyURI" use="required"/>
      <attribute name="Authentication"
                Instant type="dateTime" use="required"/>
    </extension>
  </complexcontent>
</complexType>
```

그림 8. 인증 구조의 XML 스키마
Fig. 8. XML Schema of Assertion

```
<saml:Assertion AssertionID="00cda300-0d5de-8521-83c5-c2d9f6847b91"
                IssuerInstant="2008-09-07T14:12:01Z"
                Issuer="gce.sejong.ac.kr"
                MajorVersion="1" MinorVersion="0"/>
  <saml:Conditions NotBefore="2008-09-07T14:12:01Z"
                   NotOnOrAfter="2008-09-07T18:12:01Z"/>
    <saml:AuthenticationStatement
                   AuthenticationMethod="password"
                   AuthenticationInstant="2008-09-07T14:12:01Z">
      <saml:Subject>
        <saml:NameIdentifier NameQualifier="gce.sejong.ac.kr">
                   JogilJeong
        </saml:NameIdentifier>
      </saml:Subject>
    </saml:AuthenticationStatement>
</saml:Assertion>
```

그림 9. 인증 예시
Fig. 9. An Assertion

Figure 8 shows an assertion schema and Figure 9 shows the assertion statement, which contains an authentication assertion issued by SAML authority (refer to step (4) of Figure 5)[17]. This message was verified by a simulation in which three domains were constructed in which there is a mutual trust relationship, and the SAML library was used which was built from previous work[18].

Figure 10 is a sequence diagram describing the flow of a scenario based on the proposed SSO architecture. Each of the boxes in the diagram denotes an entity involved in the flow and arrows represent the delivery of messages and the paths used for their delivery. We assume each of parties trust mutually.

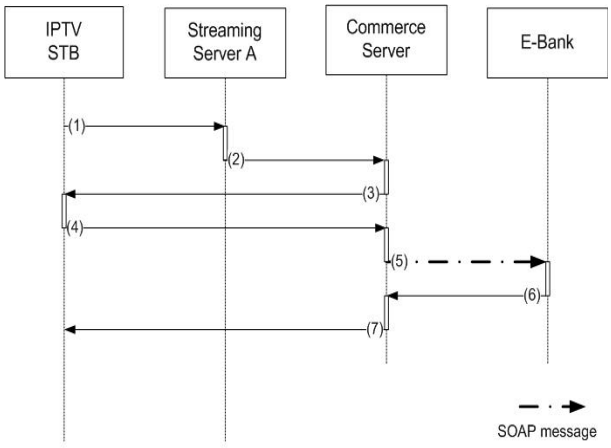


그림 10. 제안하는 단일인증 구조의 시나리오 기반 순차도
Fig. 10. Sequence Diagram of the Scenario Based on the Proposed Single Sign-On Architecture

The following is a detailed description of the diagram:

(1) A user accesses Streaming Server A, which is a home shopping channel, through IPTV STB.
(2) The user orders an item he wants to purchase while watching TV.
(3) The Commerce Server requests authentication information from the user in order to get the consumer's information.
(4) The user provides his certificate and information about a bank with which he has an account to the Commerce Server.

(5) The Commerce Server requests that the E-Bank settle the user's purchase order. The user's certificate is sent to the E-Bank through a SOAP message.
(6) The E-Bank notifies the Commerce Server when the settlement has been completed.
(7) The Commerce Server sends the E-Bank notification to the user.

In step 1, device authentication can be used rather than user authentication because the Authentication Level of Streaming Server A is low. In steps 3, 4, 5, and 6, user authentication is strongly recommended rather than device authentication because the highest Authentication Level is used for the Commerce Server and E-Bank.

IV. Conclusion

IPTV needs to ensure interoperability, so that users and service providers do not need to depend on specific service environments and satisfy security requirements in each environment. User authentication is especially necessary because a security scheme for both charged and free services is required in the IPTV service environment. However, for a user to be authenticated by every service is a very troublesome task. These redundant tasks are the main defect threatening to damage the accessibility of services. To solve this problem, we proposed a single sign-on scheme for user authentication among service domains.

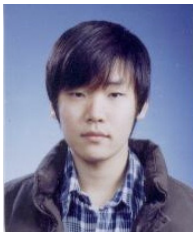
It is expected that IPTV STB will play the role of a home server in a home network. A security scheme for IPTV should also be advanced. Considering the alternative of using a repository for certificates and the importance of user authentication when accessing services, the proposed single sign-on scheme employing the extensibility of SAML can be used to create a more efficient structure.

References

[1] Rittwik Jana and Serban Jora, "From IPTV to Mobile TV to IMS-TV?: Implications and standards for a network operator", 15th International World Wide Web Conference 2006 (WWW2006), Edinburgh, Scotland, May, 2006.
[2] A. Volchkov, "Revisiting single sign-on: a pragmatic approach in a new context," IT Professional, Volume: 3 Issue: 1, Jan/Feb, 2001, pp. 39-45.
[3] T.A. Parker, "Single sign-on systems-the technologies and the products," European Convention on Security and Detection, Brighton UK, May. 16-18, 1995, pp. 151-155.
[4] Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) http://www.oasis-open.org/committees/security/
[5] Torbjörn Cagenius, Andreas Fasbender, Johan Hjelm, Uwe Horn, Ignacio Más Ivars and Niclas Selberg, "Evolving the TV experience: Anytime, anywhere, any device," Ericsson Review, No: 3, 2006, pp. 16-18.
[6] A Benjamin, I want my IPTV:Internet Protocol television predicted a winner, IEEE DISTRIBUTED ONLINE Computer Society Vol.6, No.2, 2005.
[7] H. Junqiang, Q. Dayou, Y. Haijun, W. Ting, S. Weinstein, M. Cvijetic, S. Nakamura, Triple play services over a converged optical_wireless network.
[8] FG IPTV-DOC-0188, Output Document: IPTV Security Aspect at 7thFGIPTVmeeting,Qawra, St Paul's Bay, Malta, 11-18 December 2007.
[9] OpenCable Applications Platform (OCAP): http://www.opencable.com/ocap/
[10] Advanced Common Application Platform (ACAP): http://www.atsc.org/standards/a101.html
[11] T. Pilioura, A. Tsalgatidou, S. Hadjiefthymiades, "Scenarios of using Web Services in M-Commerce, ACM SIGecom Exchanges," Vol.3,No.4,January 2003, 28-36.
[12] B. Pfitzmann, B. Waidner, "Token-based web Single Signon with Enabled Clients", IBMResearchReportRZ3458(#93844),November 2002.
[13] J.I. Jeong, D.K. Shin, D.I. Shin, K.Y. Moon, "Java-Based Single Sign-On Library Supporting SAML (Security Markup Language) for Distributed Web Services," LectureNotesinComputerScience3007, (2004).
[14] G. Ben, H. Whitney, H. Andre, J. Murali, D.V. Prasad, T. Ravi, W. "David, Professional Web Services Security, Wrox", 2002.
[15] Birgit Pfitzmann. Privacy in enterprise identity federation | Policies for Liberty single sign on. In Proceedings: 3rd Workshop on Privacy Enhancing Technologies (PET 2003), Dresden, March 2003, Lecture Notes in Computer Science.
[16] OASIS Standard, Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0: http://docs.oasis-open.org/security/saml/v2.0/
[17] B. Pfitzmann, B. Waidner, "Token-based web Single Signon with

Enabled Clients," IBM Research Report RZ 3458 (#93844), November 2002.
[18] J.I. Jeong, D.K. Shin, D.I. Shin, K.Y. Moon, "Java-Based Single Sign-On Library Supporting SAML (Security Markup Language) for Distributed Web Services," Lecture Notes in Computer Science 3007, 2004.

저 자 소 개



이 승 훈

- 2005년 : 명지전문대학 행정정보학과
- 2007년 : 한국교육개발원 전자계산학
- 2007년 8월 ~ 현재 : 세종대학교 컴퓨터공학과 석사과정
- 주관심분야 : 상황인식미들웨어, 웹기반 멀티미디어

신 동 일

- 1988년 : 연세대학교 전산과학과(이학사)
- 1993년 : M.S. in Computer Science, Washington State University
- 1997년 : Ph.D in Computer Science, University of North Texas
- 1997년 9월 ~ 1998년 2월 : 시스템공학연구소 선임연구원
- 1998년 3월 ~ 현재 : 세종대학교 컴퓨터공학과 부교수
- 주관심분야 : 상황인식 미들웨어, 무선인터넷, 게임, 지능형 에이전트, HCI

신 동 규

- 1986년 2월 : 서울대학교 계산통계학과 (이학사)
- 1992년 8월 : Illinois Institute of Technology 컴퓨터과학과 (공학석사)
- 1997년 8월 : Texas A&M University 컴퓨터과학과 (공학박사)
- 1986년 2월 ~ 1991년 8월 : 한국국방연구원 연구원
- 1997년 9월 ~ 1998년 2월 : 현대전자 멀티미디어연구소 책임연구원
- 1998년 3월 ~ 현재 : 세종대학교 컴퓨터공학과 교수
- 주관심분야 : 상황인식 미들웨어, 웹기반 멀티미디어, 데이터베이스, 데이터마이닝