# OASIS SAML(Security Assertion Markup Language) v2.0 고찰 및 활용

조영섭* · 진승헌**

## 1. 서 론

인터넷의 급속한 보급으로 사용자들은 기존에 오프라인으로 수행하던 많은 서비스를 인터넷 상에서 수행하게 되었다. 일반적으로 사용자들은 이러한 서비스를 제공받기 위해서는 인터넷 SP (Service Provider)에 회원 가입 절차를 수행하여 서비스를 이용하기 위한 id와 패스워드 또는 인증서와 같은 credential을 등록하게 된다. 이후, SP를 사용할 때마다 사용자는 자신이 등록한 정보를 이용하여 인증 받게 된다. 그러나 사용자가 사용하는 SP의 수가 증가함에 따라 매번 SP에 인증하는 방식은 사용자의 불편을 초래하게 되었다. 이와 같은 문제를 해결하기 위해, 사용자가 여러 SP를 사용하더라도 한번만 인증 받으면, 추가적인 인증이 필요 없는 SSO(Single Sign-On) 서비스가 필요하다. 일반적으로 SSO 서비스를 제공하기 위해 사용자가 접근하는 SP는 신뢰기관인 IdP(Identity Provider)에게 사용자의 인증을 요청하고, IdP는 사용자 인증을 수행한 후 그 결과를 SP에게 전달하는 과정을 거친다. 이 때, IdP는 사용자 인증 결과를 assertion 이라는 보안 토큰(security token)으로 구성하여 SP에게 전달한다.

SSO 서비스를 제공하는 시스템 구조는 assertion의 형식과 id 관리에 따라 다음과 같은 세 가지 방식으로 구분될 수 있다. 첫 번째는 사유(proprietary) 방식의 구조를 갖는 assertion을 이용하는 것이다. 이 방식은 시스템 구현의 신속성과 편의성에서 장점을 가질 수 있으나 시스템 안전성과 확장성 및 상호운용성이 제약받는다는 단점이 있다. 두 번째 방식은 표준화된 구조의 assertion을 사용하고 IdP에서만 사용자 id와 패스워드를 관리하는 방식이다. 이 경우, 시스템의 안전성과 확장성 및 상호 운용성이 제공되지만 id, 패스워드, 프로파일, 속성 등과 같은 사용자의 모든 ID(Identity) 정보가 IdP로 집중되는 문제가 발생한다. 세 번째 방식은 두 번째 방식과 거의 동일하지만 사용자의 ID 정보를 IdP와 SP에서 각자 관리하는 방식으로 IdP와 SP 사이에 사용자 ID 연계(Identity Federation) 라는 방식을 이용하여 SSO 서비스를 제공한다. 이 방식은 SP들이 각자 사용자의 정보를 관리하며 사용자 인증이 필요할 때만 IdP와 연동하는 방식으로 사용자 정보가 IdP에 집중되는 문제를 해결할 수 있다.

SAML은 IdP와 SP 사이에서 전달되는 사용자 인증 정보를 나타내는 보안 토큰인 assertion을 표준화시킨 것으로 OASIS(Organization for the Advancement of Structured Information Standards)의 보안 서비스 기술 위원회에서 개발한 표준이다. SAML은 사용자 인증여부를 나타

* 한국전자통신연구원 디지털ID보안연구팀 선임연구원
** 한국전자통신연구원 디지털ID보안연구팀 팀장

내는 인증정보뿐만 아니라 사용자의 속성정보와 사용자의 시스템 접근 권한을 나타내는 인가정보를 교환하는 XML 기반 프레임워크이다. SAML은 플랫폼 중립적이며, 기존의 디렉토리 서버의 의존성을 줄이며, 사용자 편의성을 증진시키며, 서비스 제공자의 관리 비용을 감소시키는 등의 장점을 가지고 있다. 이러한 SAML은 웹 SSO, 속성 기반 인가, 웹 서비스 보안 등의 기반으로 활용된다.

본 고는 SAML 표준의 최신 버전인 OASIS SAML v2.0에 대하여 고찰한다. 본 고의 구성은 다음과 같다. 2장에서는 SAML 표준화 진행과정과 관련 표준에 대하여 설명한다. 3장에서는 SAML을 구성하는 표준 스펙과 SAML이 제공하는 기능에 대하여 설명한다. 4장과 5장에서 각각 SAML을 구성하는 핵심 컴포넌트인 SAML assertion의 구조와 프로토콜에 대하여 기술한다. 6장에서는 SAML을 이용하여 온라인상에서 주민번호를 보호하는 서비스에 대하여 설명한다. 마지막으로 7장에서 결론을 맺는다.

## 2. SAML 표준화 과정 및 관련 표준

### 2.1. SAML 표준화 과정

OASIS에서는 2002년 11월에 SAML V1.0 표준을 제정하였고 2003년 9월에는 V1.0을 보완한 V1.1을 제정하였다. SAML V1.1은 많은 벤더(vendor)에 의해 구현되어, 공공, 교육, 산업 분야에서 큰 성공을 거두었다. SAML V2.0은 Liberty Alliance와 Shibboleth의 연구 결과물을 수용하여 SAML V1.1에 ID 연계 기능을 통합하여 2005년 3월에 재정된 통합 표준이다.

다음 그림 1은 SAML 표준의 진행과정을 도식화한 것이다.

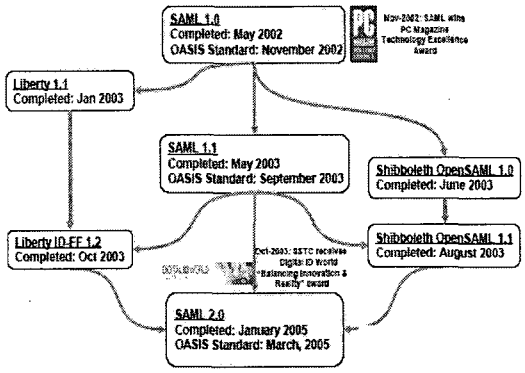



그림 1. SAML Standardization and relationship
출처. Liberty Technology Tutorial from Liberty Alliance

### 2.2 관련 표준

SAML은 다른 표준화 단체들의 표준과 밀접한 연관을 갖고 있다.

▪ **Liberty Alliance**

Liberty Alliance는 연계된 네트워크 ID (Federated Network Identity)를 위한 표준을 제정하기 위해 결성된 산업 컨소시엄이다. 표준은 3단계로 구성된다. 단계 1인 ID-FF(Identity Federation Framework)은 연계 ID를 기반으로 한 SSO 서비스 제공을 위한 표준을 제정하였고 이를 OASIS에 제공하여 SAML V2.0 제정에 도움을 주었다. 단계 2인 ID-WSF(Identity Web Service Framework)는 ID정보를 웹 서비스로 제공하기 위한 프레임워크를 규정하고 있으며, 단계 3인 ID-SIS(Identity Service Interface Specification)는 사용자 프로파일, contact, Geolocation 등과 같은 Identity 서비스 프로파일을 정의한다. SAML V2.0 assertion은 ID-WSF에서 서비스간 보안 정보 교환에 사용된다.

▪ **Shibboleth**

Shibboleth는 교육 관련 온라인 자원들에 대한 접근 제어를 위한 공개 소프트웨어 시스템과 기술

및 정책적 프레임워크를 개발하기 위해 Internet2 컨소시엄에서 진행하는 프로젝트이다. Shibboleth는 SAML 1.x를 사용하였으며 이 경험이 SAML V2.0 표준 제정에 활용되었다.

▪ **XACML**

XACML(eXtensible Access Control Markup Language)는 접근 제어를 위해 OASIS에서 표준화된 XML 기반 언어이다. XACML은 접근 제어 정책 언어와 요청/응답 언어를 기술한다. 정책 언어는 누가 무엇을 언제 접근할 수 있는지를 정책으로 표현하는데 사용된다. 요청/응답 언어는 사용자가 어떠한 자원에 접근할 때, 이러한 접근이 허용되는지를 질의하는 요청과 이에 대한 확인 결과를 나타내는 응답 메시지를 기술한다. XACML과 SAML은 서로 보완적으로 동작하도록 설계되었다. 예를 들어, XACML은 SAML assertion을 수신했을 때, 서비스 제공자가 무엇을 해야 하는지를 기술하는 정책을 제공하며, XACML 기반 속성들은 SAML로 표현될 수 있다.

▪ **WS-Security**

WS-Security는 웹 서비스 표준 메시지 형식인 SOAP(Simple Object Access Protocol) 메시지가 무결성(integrity)과 기밀성(confidentiality)을 유지할 수 있도록 하는 방법을 기술하도록 OASIS에서 제정한 표준이다. WS-Security는 메시지 무결성과 기밀성을 제공하기 위해 X.509 인증서와 Kerberos ticket과 같은 다양한 보안 토큰을 사용한다. WS-Security는 보안 토큰으로 SAML assertion이 사용되는 방법을 기술한 SAML Token Profile을 제정하여 SAML assertion이 SOAP 메시지 보안에 활용될 수 있도록 하고 있다.

▪ **WS-***

WS-*는 IBM과 Microsoft가 주축이 되어 보안을 포함하여 웹 서비스의 다양한 측면에 대한 스펙을 제안하고 있다. WS-*의 보안 역시 WS-Security와 같이 보안 토큰에 기반을 두고 있으며 이러한 보안 토큰으로 SAML assertion이 사용될 수 있다.

## 3. SAML 표준 스펙 및 기능

### 3.1. SAML V2.0 스펙

SAML V2.0은 여러 개의 스펙으로 구성되어 있다. SAML V2.0을 구성하는 주요한 스펙은 다음과 같다.

▪ **Core 스펙**

이 스펙에서는 assertion의 구조와 SAML assertion과 관련된 요청 및 응답 프로토콜에 대하여 기술한다. 이 스펙은 4장과 5장에서 자세히 기술한다.

▪ **바인딩 스펙**

SAML 요청/응답 메시지를 기존에 존재하는 하부 프로토콜로 매핑하는 방식을 기술한다. 메시지를 바인딩하는 하부 프로토콜로는 HTTP, SOAP, Reverse SOAP(PAOS)와 URI 방식이 있다.

▪ **프로파일 스펙**

프로파일은 SAML assertion을 프레임워크나 프로토콜에 어떻게 삽입시키고, 이렇게 삽입된 메시지에서 어떻게 추출하는지에 대한 방법을 규정하는 규칙이다. 이 스펙은 SSO 프로파일, Artifact Resolution 프로파일, Assertion 질의/응답 프로파일, 이름 식별자 매핑 프로파일, SAML 속성 프로파일 등을 규정하고 있다.

▪ **메타데이터 프로파일 스펙**

SAML을 기반으로 IdP와 SP가 정보를 교환하기 위해서는 서로가 지원하는 프로토콜, 프로파일, 서비스 엔드포인트(endpoint), 공개키 인증서, provider ID 등과 같은 정보가 필요하다. SAML

은 이와 같은 부가적인 정보를 메타데이터로 부른다. 이 스펙은 메타데이터의 구조를 규정하고 IdP와 SP의 메타데이터를 인터넷 상에서 공개하는 방법과 공개된 메타데이터를 검색하는 방법을 규정한다.

**▪ 인증 문맥(Authentication Context) 스펙**

SP는 사용자에게 제공하는 서비스의 특성에 따라 IdP가 어떠한 방식으로 사용자를 인증했는지를 확인해야 할 필요가 있다. 즉, SP가 사용자에게 자금 이체와 같은 금융 서비스를 제공하는 경우, 사용자의 인증 방식이 최소한 인증서를 이용하거나 또는 인증서와 생체 정보를 이용할 것을 요구할 수 있다. 이와 같은 경우, 사용자에게 서비스를 제공할 것인지에 대한 SP의 판단은 단순히 IdP가 사용자를 인증하였는지에 대한 정보뿐만 아니라 사용자를 어떠한 방식으로 인증하였는지에 대한 부가적인 정보가 필요하다. 이 스펙은 IdP가 사용자를 어떠한 방식으로 인증하였는지를 SP에게 알려주기 위해, 사용자를 인증하는 각각의 방식에 대하여 하나씩 인증 클래스를 정하고 이것이 어떠한 의미를 지니는지를 규정한다.

다음 그림 2는 SAML V2.0에서 제정하는 스펙들의 연관성을 도식화한 것이다.

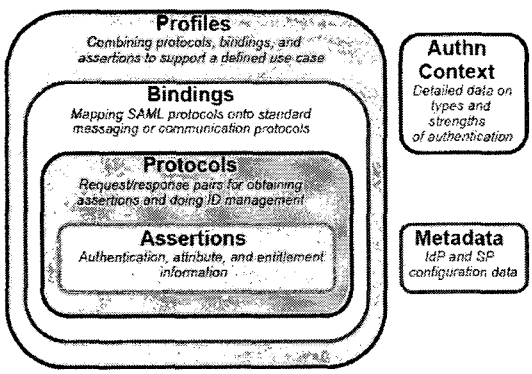



그림 2. SAML Protocol Stack
출처. SAML V2.0 Basics from Sun

### 3.2. SAML 기능

SAML은 다양한 환경에서 다음과 같은 용도로 사용될 수 있다.

**▪ Single Sign-on**

Internet Explorer, Firefox, Mozilla 등과 같은 일반적인 웹 브라우저에서 SSO 서비스를 제공하는데 사용된다. 또한 hand-held 장치와 같은 경우에도 IdP와 통신할 수 있는 기능을 탑재하면 SSO 서비스에 사용될 수 있다.

**▪ Identity Federation**

SAML V2.0은 SP와 IdP 사이에서 사용자가 기존에 가지고 있던 ID들을 연계할 수 있다. 이러한 연계 방식은 사용자의 이름 또는 속성 정보를 이용하여 연계하거나 또는 프라이버시를 보호하기 위해 난수로 이루어진 pseudonym을 생성하여 연계할 수 있다. 이 기능에 대해서는 6장에서 자세히 설명한다.

**Attribute Service**

SAML V2.0 assertion은 IdP와 SP 사이에서 서비스를 수행하기 위해 필요한 사용자 속성 정보를 전달하는 수단으로 사용될 수 있다.

**▪ Single Logout**

SSO를 통해 사용자가 가지게 된 IdP와 SP들의 인증 세션을 한 번의 로그아웃으로 모두 종료시키는 기능을 제공한다.

**▪ Securing Web Service**

SAML Token Profile에서 규정한 방식으로 SAML V2.0 assertion을 사용하여 웹 서비스 메시지의 보안을 제공한다.

## 4. SAML Assertion 구조

본 장은 SAML assertion이 가장 많이 활용되는 인증을 예로 SAML assertion의 구조를 설명한다

SAML 인증 assertion은 어떠한 사용자가 SP 서비스를 사용하기 위해 IdP에서 인정받고, 인증이 성공적으로 수행되면 IdP가 사용자에 대한 인증 사실을 SP에게 전달하기 위해 생성된다. 따라서 SAML인증 assertion은 사용자를 인증한 IdP가 누구이고, 인증 받은 사용자가 누구이며, IdP가 어떠한 방식으로 사용자를 인증했는지에 대한 정보를 포함하고 있다. 다음 그림 3은 SAML 인증 assertion의 개략적인 구조를 보인다.

그림 3의 구조를 구성하는 각각의 필드들의 의미는 다음과 같다.

- **Issuer:** assertion의 발급자로 사용자를 인증한 IdP의 정보를 나타낸다.
- **Signature:** assertion의 내용이 악의적인 사용자에 의해 변경되지 않도록 발급자의 공개키로 전자서명한 내용을 나타낸다.
- **Subject:** IdP가 인증한 사용자가 누구인지를 나타낸다.
- **Conditions:** 발급된 assertion의 유효기간을 설정하고 어떠한 SP를 대상으로 발급되었는지 등에 대한 assertion의 조건을 나타낸다.
- **AuthnStatement:** IdP가 어떠한 방식으로 사용자를 인증하였는지에 대한 정보를 포함한다.

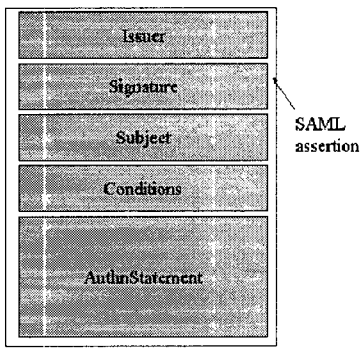



그림 3. SAML Assertion 추상적인 구조
출처. SAML V2.0 Executive Overview from OASIS

SAML V2.0 assertion의 구조는 XML 스키마로 표현되어 있으며, 위에서 설명한 인증 사실뿐만 아니라 속성정보와 인가 정보를 포함하고 있다. 또한 많은 부분에서 open 타입인 any 타입을 지원하여 응용 환경에 따라 확장할 수 있도록 한다. 다음 그림 4는 SAML V2.0 assertion 요소(element)를 도식화한 것이다.

그림 4에서는 assertion 요소에는 자식 요소만 표현되어 있으며 그림 3에서 설명한 issuer 등은 assertion 타입의 속성(attribute)으로 표현된다.

IdP는 사용자를 인증한 후, 여러 가지 상황을 고려하여 그림 4에 부합하는 인증 assertion을 발급하게 된다.

예를 들어, user.com이라는 회사에 다니는 honggildong이라는 사용자를 IdP에서 2006년 3월 1일에 사용자를 X.509 인증서를 이용하여 인증하였으며, 유효기간은 1일이며 이용자는 www.sp.com으로 제한한다는 내용을 표시하는 assertion은 다음과 같이 생성될 수 있다.

assertion을 **bold** 형식의 내용을 중심으로 순서대로 설명하면 다음과 같다.

- **urn:oasis:names:tc:SAML:2.0:assertion**
  - assertion의 네임스페이스를 나타낸다.

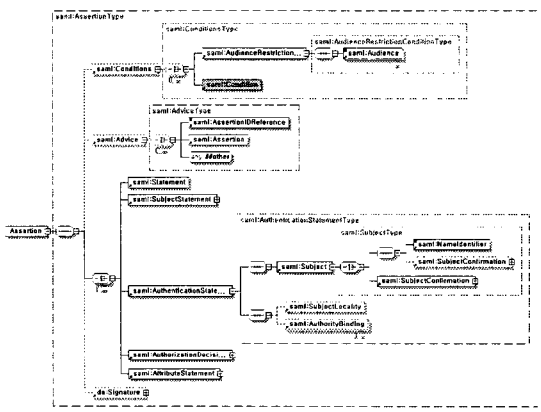


그림 4. SAML V2.0 assertion 요소

```
<saml:Assertion
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    Version="2.0"
    IssueInstant="2006-03-01T12:00:00Z">
  <saml:Issuer>
    www.idp.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:1.1:
              nameid-format:emailAddress">
      honggildong@user.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
      NotBefore="2006-03-01T12:00:00Z"
      NotOnOrAfter="2006-03-02T12:00:00Z">
    <saml:AudienceRestriction>
      <saml:Audience>
        www.sp.com
      <saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement
      AuthnInstant="2006-03-01T12:00:00Z"
      SessionIndex="12345678">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:X509
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
</saml:Assertion>
```

- **2.0** - assertion의 버전이 SAML V2.0 임을 나타낸다.
- **2006-03-01T12:00:00Z** - assertion의 발급 일자가 2006년 3월 1일 12시 임을 나타낸다.
- **wws.idp.com** - assertion의 발급자인 IdP의 이름이 www.idp.com 임을 나타낸다.
- **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** - 사용자의 이름 형식이 e-mail 임을 나타낸다.
- **honggildong@user.com** - 사용자의 이름이 user.com의 honggildong 임을 나타낸다.
- **2006-03-01T12:00:00Z** - assertion이 2006년 3월 1일 12시 이전에 사용되어서는 안 됨을 나타낸다.
- **2006-03-02T12:00:00Z** - assertion이 2006년 3월 2일 12시 이후에 사용되어서는 안 됨을 나타낸다.
- **www.sp.com** - assertion은 www.sp.com 이라는 이름을 가진 SP를 대상으로 하는 것이기 때문에 다른 SP에서는 이 assertion에 믿고 사용자 인증을 확인하면 안 됨을 나타낸다.
- **2006-03-01T12:00:00Z** - IdP가 사용자를 인증한 시각이 2006년 3월 1일 12시 임을 나타낸다.
- **12345678** - 사용자의 SSO와 Single Logout을 관리하기 위해 생성하는 인증 세션 번호를 나타낸다.
- **urn:oasis:names:tc:SAML:2.0:ac:classes:X509** - IdP가 X.509 인증서를 이용하여 사용자를 인증했음을 나타낸다.

## 5. SAML 프로토콜

SAML V2.0은 assertion의 발급, Identity 연계, 단일 로그아웃 등과 같은 기능을 제공하기 위해 다음과 같은 프로토콜을 제공한다.

- **Authentication request** - SP가 사용자를 인증하기 위해 IdP에게 사용자 인증을 요청하는 프로토콜이다.
- **Assertion query and request** - 이미 사용자가 인증되어 IdP가 사용자 인증 assertion을 발급한 상태에서, SP가 발급된 assertion을 IdP에게 요청하거나 IdP가 사용자를 재 인증하기를 원할 때 사용되는 프로토콜이다.
- **Artifact resolution** - IdP가 사용자를 인증한 후 assertion을 발급하고 이를 가리키는 난수인 artifact를 사용자 브라우저를 통해 SP에게 전달하였을 때, SP가 전달받은 artifact를 이용하여 해당되는 assertion을 IdP에 요청하는 프로토콜이다.
- **Name identifier management** - IdP와 SP가 자신이 관리하는 사용자 계정을 난수인 pseudonym을 생성하여 서로 연계시키는 프로토콜이다.

- **Name identifier mapping** - 서로 다른 두 SP가 사용자 프라이버시를 보호하면서 one-time으로 사용자를 식별하는데 사용되는 프로토콜이다.
- **Single logout** - SSO를 통해 생성된 사용자 인증 세션을 한 번에 모두 로그아웃시키는데 사용되는 프로토콜이다.

본 장에서는 위와 같은 프로토콜 중에서 가장 핵심적인 기능을 수행하는 Authentication request 프로토콜에 대하여 설명한다.

SAML V2.0의 Authentication request protocol은 다음 그림 5와 같은 AuthnRequestType을 이용하여 요청 메시지를 생성한다.

그림 5의 AuthnRequestType을 구성하는 필드들의 의미는 다음과 같다.

- **Issuer** - assertion의 발급자로 IdP를 의미한다.
- **Signature** - assertion의 내용이 악의적인 사용자에 의해 변경되지 않도록 발급자의 공개키로 전자서명한 내용을 나타낸다.

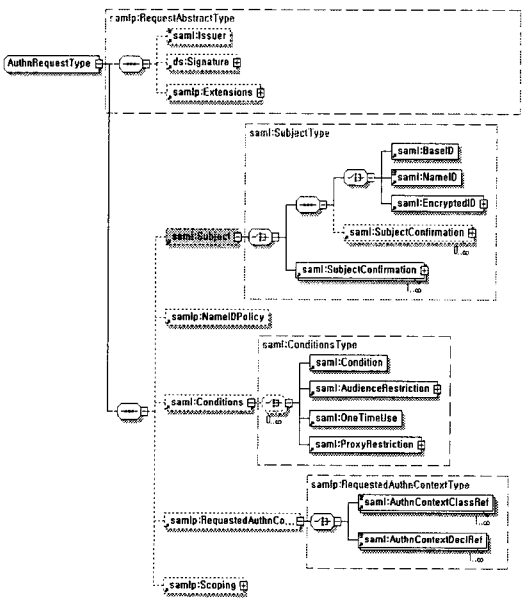



그림 5. SAML V2.0 AuthnRequestType

- **Extensions** - 응용 환경에 따라 요청 메시지를 확장할 수 있도록 한 확장 필드이다.
- **Subject** - SP가 IdP에게 인증을 의뢰한 사용자에 대한 정보를 나타내는 필드이다.
- **NameIDPolicy** - IdP가 인증 assertion을 발급할 때 표시되는 사용자의 식별자를 제약하는 필드이다.
- **Conditions** - SP 입장에서 IdP가 assertion을 발급할 때 유효기간 등과 같은 조건을 어떻게 설정해 주기를 바라는 지를 나타낸다.
- **RequestAuthnContext** - SP 입장에서 IdP가 사용자를 어떠한 방식으로 인증하기를 바라는 지를 나타낸다.
- **Scoping** - IdP가 SP의 인증 요청을 다른 IdP에게 요청할 수 있는지 즉 proxying이 얼마나 가능한 지를 나타낸다.

다음은 SP가 사용자 인증을 IdP에게 요청하는 AuthnRequest 메시지의 예이다. AuthnReuqest 메시지가 SOAP으로 바인딩되어 있다.

이 인증 요청 메시지는 www.sp.com이라는 SP가 user.com에 다니는 honggildong이라는 사용자를 IdP에 인증 요청하는 메시지이다.

```
<env:Envelope
  xmlns:env=
      "http://www.w3.org/2003/05/soap/envelope/">
  <env:Body>
    <samlp:AuthnRequest
      xmlns:samlp=
        "urn:oasis:names:tc:SAML:2.0:protocol"
      ForceAuthn="true"
      AssertionConsumerServiceURL=
        "http://www.sp.com/authService"
      ID="SPauthRequest_1"
      Version="2.0"
      IssueInstant="2006-03-01T12:00:00Z"
      <saml:Subject
        xmlns:saml=
          "urn:oasis:names:tc:SAML:2.0:assertion"
        <saml:NameID
          Format="urn:oasis:names:tc:SAML:1.1
                  :nameid-format:emailAddress">
          honggildong@user.com
        </saml:NameID>
      </saml:Subject>
    </samlp:AuthnRequest>
  </env:Body>
</env:Envelope>
```

이 인증 요청 메시지를 **bold** 형식의 내용을 중심으로 순서대로 설명하면 다음과 같다.

- **http://www.w3.org/2003/05/soap/envelope/** - 프로토콜 메시지를 포함하는 SOAP 메시지의 네임스페이스를 나타낸다.
- **urn:oasis:names:tc:SAML:2.0:protocol** - 요청 메시지의 버전이 SAML V2.0 임을 나타낸다.
- **true** - IdP는 반드시 대화식(interactive) 으로 사용자를 인증해야 함을 나타낸다.
- **http://www.sp.com/authService** - IdP가 이 요청에 대한 응답 메시지를 SP에게 반환하는 위치를 나타낸다.
- **SPauthRequest_1** - 이 요청 메시지의 유일한 식별자를 나타낸다.
- **2.0** - 요청 메시지가 SAML V2.0을 따르고 있음을 나타낸다.
- **2006-03-01T12:00:00Z** - 이 요청 메시지의 생성 시각을 나타낸다.
- **urn:oasis:names:tc:SAML:2.0:assertion** - 사용자를 나타내는 이 구조는 4장에서 설명한 SAML V2.0의 assertion에서 정의한 Subject 구조를 따르고 있음을 나타낸다.
- **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress** - 사용자의 이름 형식이 e-mail 임을 나타낸다.
- **honggildong@user.com** - 사용자의 이름이 user.com의 honggildong 임을 나타낸다.

이와 같은 요청 메시지에 대하여 IdP는 응답 메시지를 생성하여 SP에게 전달한다. 다음 그림 6은 인증 요청 메시지에 대하여 생성되는 응답 메시지 타입을 도식화한 것이다.

그림 6에서와 같이 인증 요청에 대한 응답 메시지는 StatusResponseType과 Assertion으로 구

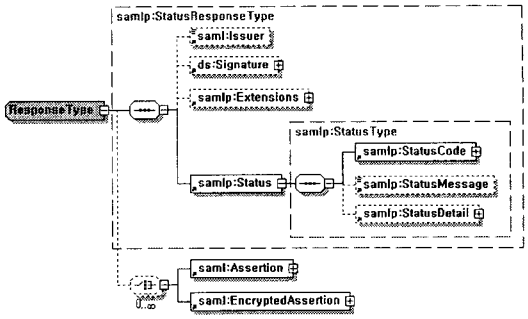



그림 6. SAML V2.0 ResponseType

성된다. StatusResponseType은 다른 프로토콜에서 공통적으로 사용되는 응답 메시지이다. IdP는 사용자의 인증이 성공한 경우 4장에서 설명한 assertion을 응답 메시지에 추가한다. 보안성을 높이기 위해 assertion은 암호화되어 포함될 수 있다.

SAML V2.0에서 공통적으로 사용되는 StatusResponseType에 포함되는 필드는 다음과 같은 의미를 지닌다.

- **Issuer** - 응답 메시지를 생성한 IdP의 이름을 나타낸다.
- **Signature** - 응답 메시지의 보안을 위해 IdP가 생성한 전자서명 값을 포함하는 필드이다.
- **Extensions** - 응용 환경에 따라 응답 메시지를 확장할 수 있도록 한 확장 필드이다.
- **StatusCode** - 응답 결과를 나타내는 code 값을 포함하는 필드이다. SAML V2.0 에서는 "urn:oasis:names:tc:SAML:2.0:status:Success" 등과 같은 urn으로 정의되어 있다.
- **StatusMessage** - 관리자에게 반환될 수 있는 추가적인 응답 메시지를 나타내는 필드이다.
- **StatusDetail** - 응용 환경에 따라 응답 메시지를 추가할 수 있도록 구성된 open 타입이다.

## 6. 응용 예: ID 연계 기반의 온라인 주민번호 보호서비스

본 장에서는 SAML V2 assertion을 이용한 응용 예로, ID 연계를 통해 온라인상에서 주민번호를 보호하는 서비스에 대하여 설명한다. 본 서비스는 ETRI에서 개발한 ID 관리 시스템인 e-IDMS(ETRI IDentity Management System)를 통해 구현되어 있다.

### 6.1 인터넷 주민번호 사용의 문제점

현재, 인터넷 서비스를 이용하기 위해서는 웹사이트 가입시, 가입자의 실명확인을 위해 주민번호를 입력하여야 하는 것이 일반적이다. 또한, 사용자가 성인사이트를 이용하기 위해서는 성인인증을 위해 추가적으로 주민번호를 입력하여야 한다. 사용자가 Id나 패스워드를 분실하였을 경우, 분실자 확인을 위해 주민번호를 입력해야 하는 것 또한 일반적이다. 이와 같이 주민번호가 인터넷 상에서 광범위하게 사용되는 것은 주민번호가 자체적으로 개인의 신상정보를 가지고 있기 때문에, 서비스 제공자들이 쉽고 편리하게 사용자의 신원을 확인할 수 있기 때문이다.

그러나 온라인상에서의 주민번호를 사용하는 것은 주민번호가 가지는 다음과 같은 특성 때문에 다양한 문제를 발생시킨다.

- **개인정보 포함** - 주민번호에는 생년월일, 성별, 출생지 같은 개인정보가 포함되어 있다. 따라서 주민번호를 획득하면 개인의 정보를 알 수 있게 된다.
- **단일 식별성** - 주민번호는 한 개인을 유일하게 식별할 수 있는 단일 식별자이다. 단일 식별자는 한 개인의 모든 정보와 활동을 연결할 수 있는 수단이 되기 때문에 프라이버시 보호 측면에서 큰 문제를 갖는다.

또한 인터넷 상에서 주민번호를 이용할 경우, 본인확인 수단이 부재하기 때문에 많은 문제가 발생된다. 즉, 오프라인의 경우, 주민등록증을 통해 본인 여부를 확인할 수 있는 반면, 온라인상에서는 주민번호를 입력하는 사람이 주민번호 소유자 본인인지 확인할 수 있는 방법이 없다. 현재 주민번호가 광범위하게 노출되어 있는 상태에서 다른 사람의 주민번호를 입력하는 주민번호 도용을 막을 방법이 없으며 미성년자가 성인의 주민번호를 사용하는 것을 막을 방법이 없는 실정이다.

이와 같이 인터넷상에서 주민번호의 사용은 많은 문제를 발생시키지만, 현실적으로 주민번호 자체를 없애거나 새로운 체계를 만들어 적용하는 것은 많은 사회적 비용이 요구된다. 따라서, 현재는 인터넷상에서 주민번호의 유통을 최소화하여 주민번호의 노출과 유출을 방지하며, 기존에 주민번호를 이용하여 신원확인을 수행하는 인터넷 사이트에 최소한의 비용으로 동일한 서비스를 제공하는 주민번호 보호 서비스에 대한 연구와 구축 및 적용이 진행되고 있다.

### 6.2 온라인상에서 주민번호 보호 방안

6.1 절에서 설명한 문제를 해결하고 인터넷 상에서 주민번호를 보호하기 위해 다양한 방법이 고안되어 왔다. 이러한 방법들의 공통적인 기본 개념은, 일반 웹사이트에서는 회원 가입시점에 주민번호 입력을 금지하고, 신뢰할 수 있는 제3의 기관에서만 주민번호를 관리한다는 것이다. 주민번호 관리기관에서는 본인확인 후 주민번호를 등록한다. 본인확인 방법은 주민등록증 확인을 의미하는 대면확인 방법과, 대면확인 방법의 불편함을 피하기 위해 기존에 대면 확인된 정보를 통해 온라인상에서 본인임을 확인하는 방법이 있다. 후자의 방법은 금융계좌 비밀번호, 휴대폰 SMS 인증

코드를 이용하는 방식이다.

주민번호를 관리하는 기관은 이와 같은 방법들을 이용하여 이용자에게 주민번호 대체 정보를 발급한다. 주민번호 대체 정보는 주민번호의 문제인 개인정보 포함과 단일 식별성을 갖지 않도록 구성된다. 주민번호 대체정보가 발급되면, 사용자는 웹사이트 가입시 주민번호를 입력하는 대신, 주민번호 대체정보를 제시한다. 기존에 직접 주민번호를 입력하던 환경에 주민번호 대체를 적용하면, 주민번호 또는 대체정보 이용을 선택할 수 있도록 하게 되며, 대체정보를 선택하면, 발급 받은 대체 정보를 입력하여 기존에 주민번호를 입력하던 것과 동일한 서비스를 제공하게 된다.

주민번호 대체 정보 발급 방법에 따라 여러 가지 방안이 구분될 수 있다. 공개키 인증서에 포함시키는 방법, ID 연계를 바탕으로 하는 인증확인서에 포함시키는 방안, 가상번호를 발행하여 이용자가 직접 입력하도록 하는 방안 등이 있다.

### 6.3 ID 연계 기반의 주민번호 보호 서비스

e-IDMS에서 구현된 주민번호 보호 서비스는 ID 연계 방식을 이용하여 주민번호 보호 서비스를 제공한다. IDSP(IDentity Service Provider)는 사용자의 주민번호를 관리하는 신뢰기관이며 SP는 사용자에게 서비스를 제공하는 일반적인 인터넷 사이트이다. e-IDMS에서는 SP가 사용자 신원확인을 위해 별도로 사용자의 주민번호를 요구하거나 저장하지 않도록 한다. 이를 위해 e-IDMS에서는 IDSP와 SP가 ID 연계방식으로 동일한 사용자를 식별하고 사용자 정보를 연계하도록 한다.

다음 그림 7은 IDSP와 SP 사이에서 사용자의 ID를 연계하는 기본 개념을 보여준다.

그림 7에서 사용자는 기존의 방식과 유사하게 IDSP와 SP에 가입자 등록을 하며, IDSP와 SP는 사용자 계정을 관리한다. 그러나 IDSP만 사용자의 주민번호를 관리하며 SP는 주민번호를 관리하지 않는다는 점이 기존 방식과 다르다. 다음은 IDSP와 SP가 사용자의 ID를 연계하는 방식이다.

1. **IDSP 사용자 등록** - 사용자는 IDSP에 id(kimcs), 패스워드, 주민번호 및 기타 IDSP에서 필요한 정보를 입력하여 자신의 계정을 생성한다.
2. **웹 사이트 가입** - 사용자는 웹 사이트에 cskim이라는 id를 생성하여 가입한다.
3. **IDSP에 신원확인** - 웹 사이트는 가입자의 신원확인을 IDSP에게 요청한다. 이 때, 웹 사이트의 신원확인 요청은 가입자 브라우저

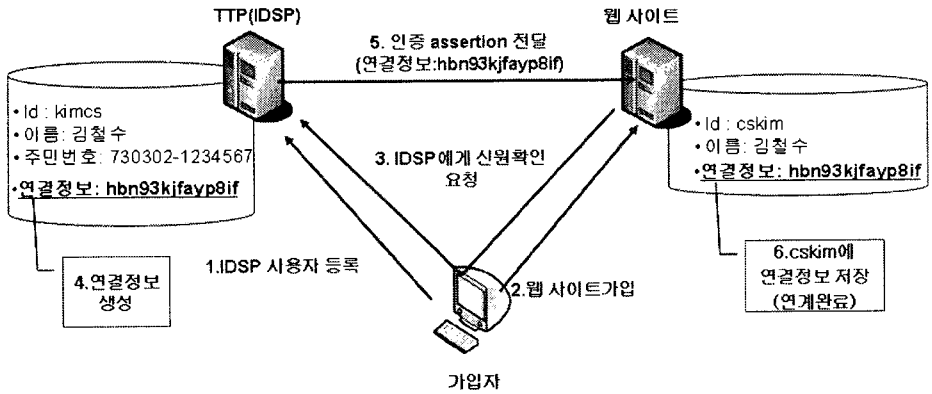



그림 7. IDSP와 SP의 ID 연계

를 통해 IDSP에게 redirect된다.

1. **연결정보생성** - IDSP는 사용자를 인증하고 SP와 연결정보를 위한 pseudonym "hbn93kjfayp8if"를 생성한다.
2. **인증 assertion 전달** - IDSP는 가입자의 ID연계 정보와 신원확인 정보를 SAML V2.0 assertion으로 생성하고 이를 웹 사이트에 전달한다.
3. **연결정보 저장** - 웹 사이트는 IDSP에서 생성한 연결정보를 가입자 계정에 저장 관리한다.

ID 연계는 추후 SP가 사용자를 인증할 때, SP에서 사용자 인증을 수행하지 않고 IDSP에게 인증을 요청할 수 있다. 이것은 IDSP가 관리하는 도메인에서 사용자에게 SSO 서비스를 제공할 수 있도록 한다.

ID 연계를 통해 제공되는 주민번호 보호서비스를 다음과 같은 장점을 가진다.

- **사용자 불편 최소화** - 사용자는 주민번호를 입력하는 대신, IDSP의 id만 기억하고 있으면 된다. 연결정보의 전달은 사용자가 직접 알지 못하게 백그라운드로 진행된다. 또한 사용자는 연결정보의 내용을 직접 알 필요가 없다.
- **사업자 도입/운영 비용 최소화** - 별도의 클라이언트 측의 툴킷이 필요 없기 때문에 도입 및 유지보수 비용이 크게 절감되고, 유무선 동일한 방식으로 동작하기 때문에 무선용 시스템 구축이 용이하다.
- **강력한 프라이버시 제공** - 연결 정보를 SP 사이트마다 다르게 사용하므로 연결정보에 의한 단일 식별성 문제를 해결할 수 있으며, 주민번호는 물론 실명을 입력하지 않기 때문에 프라이버시가 효과적으로 보호된다.
- **표준화된 기술** - OASIS에서 제정한 표준 기술인 SAML V2.0을 채택하여 개발되었으므로, 안정성, 보안성, 확장성이 보장되어 있고, 상호 호환성도 높다.
- **부가적인 서비스 제공 가능** - 인터넷 ID 관리 서비스가 본래 제공하는 SSO, ID 정보 관리, 개인정보 보호가 기본적으로 제공된다.

## 7. 결 론

인터넷 서비스가 다양해지고 보안의 중요성이 높아짐에 따라, 사용자의 신원을 확인하고 이 정보를 유통하는 기술은 매우 중요하다. OASIS는 이와 같은 필요성을 충족시키기 위해 사용자의 인증 정보, 속성 정보, 인가 결정 정보를 표현하고 전달하는 표준화된 XML 프레임워크를 개발하였다.

본 고는 OASIS에서 표준화된 SAML V2.0에 대하여 고찰하였다. 먼저 SAML 표준화 과정과 관련 표준에 대하여 기술하였고, SAML이 제공하는 기능 및 스펙들에 대하여 간략하게 기술하였다. SAML V2.0의 스펙 중에서 가장 중요한 SAML Assertion의 구조와 프로토콜에 대하여 기술하였다. 또한 SAML V2.0 assertion을 이용하여 온라인상에서 주민번호를 보호하는 서비스에 대하여 기술하였다. SAML V2.0은 향후 인터넷 상에서 안전한 서비스를 제공하기 위한 필수적인 보안 요소로 널리 활용될 것으로 예상된다.

## 참 고 문 헌

[1] Eve Maler, SAML V2.0 Basics, Sun Workshop, May 2005.

[2] Liberty Alliance, Liberty Technology Tutorial, 2005, http://www.projectliberty.org/ resources/ LibertyTechnologyTutorial.pdf

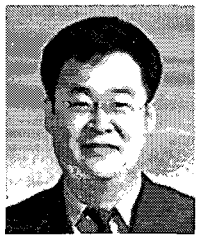
[3] Liberty Alliance Project, http://www.projectliberty.org/

[4] OASIS SAML, http://www.oasis-open.org/

committees/security/
[5] OASIS Web Services Security, http:// www.oasis-open.org/committees/wss/
[6] OASIS XACML, http://www.oasis-open.org/committees/xacml/
[7] Paul Madsen, et. al., SAML V2.0 Executive Overview, OASIS SAML Committee Draft 01, April 2005.
[8] Shibboleth, http://shibboleth.intenet2.edu/
[9] WS-*, http://www.ws-i.org/
[10] 한국전자통신연구원, "인터넷 ID 관리 서비스 기술 백서 v2.0", 2005.

조 영 섭

· 1993년 2월 인하대학교 전자계산공학과 졸업
· 1995년 2월 인하대학교 대학원 전자계산공학과 석사
· 1999년 2월 인하대학교 대학원 전자계산공학과 박사
· 1998년 12월~현재 : 한국전자통신연구원 디지털ID보안연구팀 선임연구원
· 관심분야 : Digital Identity Management, 인증인가, 정보보호, EC



진 승 헌

· 1993년 2월 숭실대학교 전자계산학과 학사
· 1995년 2월 숭실대학교 대학원 전자계산학과 석사
· 2004년 2월 충남대학교 대학원 컴퓨터과학과 박사
· 1994년 12월~1996년 4월 (주)대우통신 종합연구소 연구원
· 1996년 5월~1999년 5월 (주)삼성전자 통신연구소 전임연구원
· 1999년 6월~현재 한국전자통신연구원 디지털ID보안연구팀장/선임연구원
· 관심분야 : Digital Identity Management, PKI, PMI, 인증인가