국내외 ID 관리 기술 표준화 동향[주)]

조상래* 진승헌**

웹 기술의 발달과 서비스의 진화로 사용자의 Identity 정보를 서로 공유하고 관리하는 것은 이제는 웹 2.0 시대에는 당연한 기능과 서비스로 제공되고 있다. 기존의 Identity 관리 기술이 인증, SSO 및 인가에 초점을 맞추어 개발이 되었다면 최근의 동향은 사용자의 Identity 정보를 어떻게 프라이버시를 보호하며 안전하게 공유할 수 있는지에 초점을 맞추고 있다. 따라서 본 고에는 현재 인터넷 Identity 관리 기술의 표준화 동향을 분석하고 향후 이 분야의 표준화 개발이 어떤 방향으로 발전해 나갈지 조명해 본다. ▨

목 차

Ⅰ. 서 론
Ⅱ. 국내 표준화 동향
Ⅲ. 국외 표준화 동향
Ⅳ. 향후 표준화 전망
Ⅴ. 결 론

* ETRI 디지털 ID 보안연구팀/선임연구원
** ETRI 디지털 ID 보안연구팀/팀장

Ⅰ. 서 론

인터넷 환경에서 제공되는 정보보호는 시스템간의 연동과 확장성을 위해 반드시 표준을 준용하여야 한다. ID 관리 기술에 대한 표준화는 국제적으로 활발히 진행되고 있으나 개인정보 공유 및 보호 기술에 대한 표준화는 아직 초기 단계이다. ID 관리 분야의 기반기술과 관련하여, W3C 는 XML 전자서명, 암호화, 키 관리에 대한 표준을 제정하고 있고 일부 표준은 IETF(Internet Engineering Task Force)와 공동으로 추진하고 있으며, IETF 는 공개키인증서, 속성인증서, LDAP(Lightweight Directory Access Protocol)에 대한 표준을 제정하고 있다.

주) 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 핵심기술개발사업의 일환으로 수행하였음.[2007-S-601-02, 자기통제 강화형 전자ID 지갑 시스템 개발]

ID 관리와 관련하여, OASIS 는 SAML, XACML, SPML(Service Provisioning Markup Language), XRI 등의 표준을 제정하고 있으며, Sun 을 중심으로 150 여 개 업체가 연합한 Liberty Alliance 와 IBM 과 Microsoft 를 중심으로 여러 업체가 연합한 WS-I(Web Service Interoperability organization)에서 표준화를 진행하고 있다. 개인정보 보호와 관련하여, W3C 의 P3P(The Platform for Privacy Preferences)와 APPEL(A P3P Preference Exchange Language), OASIS 의 XACML, IBM 의 EPAL(Enterprise Privacy Authorization Language) 등의 규격이 제정되고 있다. 2005 년 3 월 OASIS 는 기존의 ID 관리 표준들을 통합 적용한 SAML 버전 2.0 을 공표한 뒤 상호운용성 시험(2005. 7.)을 개최하여 ETRI 를 포함한 8 개 기업이 호환성 인증을 받았고, ITU-T 가 OASIS 와 협의를 통해 SG (Study Group)17 WP2 Q.6 에서 수행하는 SAML 과 XACML 의 표준화 작업에 국내외 전문가들이 참여하였다.

또한 ID 관리와 관련하여, ISO(International Organization for Standardization)는 SC27 WG5 에서 ID 관리와 프라이버시 기술에 대한 표준을 제정하고 있으며, ID 관리와 프라이버시 분야의 향후 표준과 가이드라인을 작성하기 위한 요구 사항과 개발 내용을 도출하는 단계이다. 국내의 경우, 한국정보보호진흥원과 한국정보통신기술협회(Telecommunications Technology Association: TTA)가 정보보호 및 전자서명에 대한 표준을 제정하고 있으며, ETRI 는 TTA 에서 ID 관리, 개인정보 보호와 관련하여 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일 표준화 작업을 국내 표준으로 제정(2006. 12.)하였다.

이와 같이 ID 관리 분야는 현재 점진적으로 표준화에 왕성한 활동을 보이고 있다. 대표적인 국제표준 단체인 ISO 와 ITU-T 는 다양한 표준화 활동을 통하여 ID 관리 분야의 표준화를 주도하고 있고 산업 표준들도 다양한 표준화 활동으로 ID 관리 기술의 표준을 리드하고 있다.

II. 국내 표준화 동향

국내 정보보호 일반표준은 인터넷보안기술 포럼과 TTA 에서 추진하고 있다. 표준화는 두 가지 방식으로 추진되고 있는데, 한 가지 방식은 사실(de-facto) 표준화 단체가 표준초안을 개발하고 그것을 TTA 에서 정보통신 단체표준으로 개발하는 방식이고, 다른 방식은 TTA 에서 표준초안이 개발되고 관련 PG(Project Group)를 통하여 최종 표준을 확정하여 표준안을 개발하는 방식이다. 현재 국내 개인정보보호 관련 표준화는 표준 기획 단계로, 국외 표준 기구에서 채택된 표준안을 국내 표준으로 추진하는 정도에 머물고 있는 실정이다.

1. TTA 개인정보보호 및 ID 관리 프로젝트 그룹(PG502)

TTA 에서 개인정보보호 관련 표준화는 TC1 PG101 정보보호기반 프로젝트 그룹에서 주로 논의되다가 2008 년 현재는 TC5(정보보호기술위원회) PG502 개인정보보호 및 ID 관리 프로젝트 그룹으로 새로 편성되어 좀더 구체적이고 다양한 ID 관리 분야의 국내 표준개발을 진행할 예정이다.

XACML 1.0 을 바탕으로 XACML 적합성 및 상호운용성 평가 표준을 2004 년에 제정하였고, 확장성 접근제어 생성언어(XACML 1.0) 표준을 국제 표준화 기구 ITU-T 표준 제정에 비해 조금 늦은 2005 년에 제정하였으며, 2007 년에는 XACML 버전 2.0 을 제정하였다. 또한, 2006 년 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일에 대한 국내 표준화를 완료하였으며, SAML 2.0 메타데이터와 인증 문맥에 대한 표준화 작업도 2007 년에 진행하여 12 월에 표준으로 제정되었다.

그리고, P3P 1.1 을 바탕으로 국내 관련 법률을 적용한 개인정보보호정책 설정 및 협상 규격이 2007 년 표준화 과제로 채택되어 같은 해 12 월에 표준으로 제정되었으며, 2008 년 현재 ID 관리 관련 국내 표준은 4 건이 신규 프로젝트로 선정되어 진행되고 있다.

확장형 자원 식별자(XRI) 문법 V2.0 과제는 OASIS 에 표준으로 제정되고 있는 XRI 를 국내 표준으로 수용하여 향후 인터넷에서 사용자의 Identity 를 보다 폭넓게 표현할 수 있는 기반을 마련하는 것이 목적이다. 공통 아이덴터티 데이터 모델과 상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항은 현재 ITU-T SG17 에서 진행하고 있는 Global Interoperable Identity Management 기술 표준을 국내에 수용하여 향후 ID 관리 시스템들간의 상호운용성을 제공하는 기틀을 마련하기 위함이다.

마지막으로 자기통제 강화형 디지털 아이덴터티 공유 프레임워크 기술은 현재 ETRI 에서 기술개발하고 있는 ID 관리 기술을 표준화하여 향후 국내 인터넷 관련 응용 서비스에서 표준화된 사용자 중심의 ID 관리 기술을 개발하여 사용할 수 있는 기반을 마련하는 것을 목적으로 하고 있다.

2. ID 관리 및 개인정보보호 관련 TTA 표준

TTA 에서 제정하거나 진행중인 ID 관련 표준은 <표 1>과 같다.

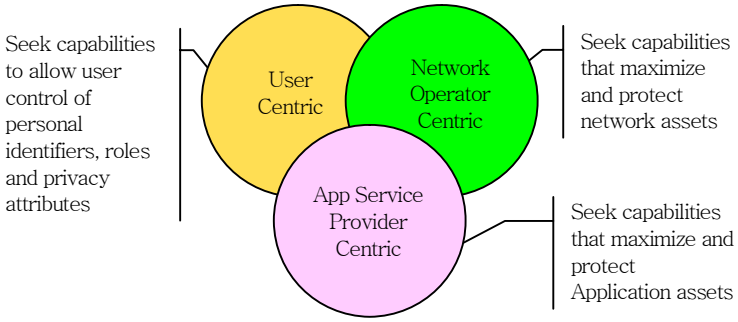
<표 1> TTA ID 관리 관련 표준 목록

관련 분야	표준번호	표준내용	제정 연도	제정 현황
PKI 및 인증	TTAS.KO-12.0012	전자서명 인증서 프로파일 표준	2000	제정 완료
	TTAS.KO-12.0013	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2001	제정 완료
	TTAS.KO-09.0003/R1	부가형 디지털 전자서명방식 - 제 1 부: 기본 구조 및 모델	2005	제정 완료
ID 관리	TTAS.IT-X1141_1	SAML 2.0 주장과 프로토콜	2006	제정 완료
	TTAS.IT-X1141_2	SAML 2.0 바인딩	2006	제정 완료
	TTAS.IT-X1141_3	SAML 2.0 프로파일	2006	제정 완료
	TTAS.IT-X1141_4	SAML 2.0 메타데이터	2007	제정 완료
	TTAS.IT-X1141_5	SAML 2.0 인증문맥	2007	제정 완료
	2008-161	자기통제 강화형 디지털 아이덴터티 공유 프레임워크 기술	2008	진행중
	2008-667	확장형 자원 식별자(XRI) 문법 V2.0	2008	진행중
	2008-668	공통 아이덴터티 데이터 모델	2008	진행중
	2008-669	상호호환성 및 신뢰를 위한 글로벌 ID 관리 시스템 요구사항	2008	진행중

III. 국외 표준화 동향

1. ITU-T FG IdM

2006 년 12 월에 결성된 ITU-T SG17 Focus Group on Identity Management(FG IdM)에서는 포괄적인 IdM 프레임워크 개발을 촉진하고 분산환경에서 자율적인 Identity 발견, Identity 연계 및 구현 수단 개발을 진행하였다. FG IdM 외에도 ITU-T 에는 Identity 관리와 관련된 Study Group 들이 있는데 Q.15/13(NGN Security)에서는 NGN(Next Generation Network) 환



(그림 1) ID 관리 기술의 시장 동향

경에서 보안 요구사항 권고안을 확정하였고 인증, AAA, 보안 메커니즘, NGN 인증서, IdM 보안 등에 관한 권고 초안을 개발 중에 있다. 그리고 A.6/17(Cybersecurity)에서 작성 중인 X.IdM (IdM Security)에 관한 권고안이 Identity 관리 시스템과 관련이 깊고 중요하다.

2006 년 12 월부터 2007 년 9 월까지 진행되는 FG IdM Phase 1 에서는 IdM 과 관련된 활동 중인 표준화 기구, 포럼 및 컨소시엄 목록을 정리하고 일반적인 IdM 프레임워크 요구사항 도출을 위한 사용 사례 시나리오를 작성하였다. 또한 IdM 요구사항 및 기능에 관한 포괄적인 분석 보고서와 함께 IdM 관련 표준화 기구, 포럼 및 컨소시엄에서 작성된 적용 가능한 명세간 차이점과 관련 사용사례를 포함하는 일반적인 데이터 모델 및 관련 스키마 등을 포함한 포괄적인 IdM 프레임워크 개발 문서와 프라이버시 보호 및 IdM 활용 모범사례 보고서 작성을 목표로 활동하였다.

FG IdM 에서는 이미 개발되어 구축된 기존의 ID 관리 시스템들의 전역적 상호운용성(Global Interoperability)을 제공하기 위해 포괄적인 IdM 프레임워크 개발을 빠르게 진행하고 분산환경에서 자율적인 ID 발견, ID 연계 및 구현 수단 개발을 주 목적으로 하고 있다. FG IdM 의 경우 특히 NGN 환경에 맞는 ID 관리 프레임워크 표준화를 목적으로 하고 있어 향후 통신 산업체의 다양한 ID 관리 서비스 요구사항을 만족할 수 있는 표준안을 제시할지 주목을 받고 있다.

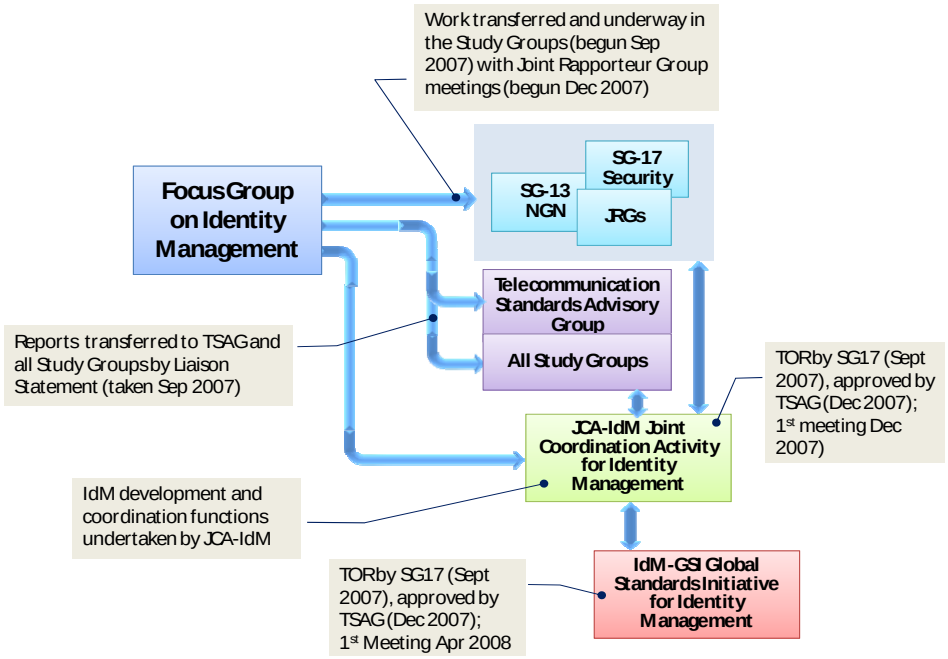
(그림 1)과 같이 ITU-T FG IdM 에서 현재 개발된 IdM 솔루션들의 문제점으로 IdM 관련 일부 기업들은 시장의 특정 영역을 목표로 하고 있고 특정 관점(예: User-centric, Application-centric, Network-centric)에서 자신들의 IdM 솔루션을 최적화하는 노력 진행한 결과 IdM 에 관한 공통의 포괄적 프레임워크 및 아키텍처 부재로 상호연동성에 문제가 있는 Identity 관리 고립 문제 발생을 꼽고 있다.

User-centric 관점(예: ID-WSF, OpenID)에서는 사용자 선호정보(preference)와 사용자 속성정보(attribute)에 대한 통제기능 제공, Application-centric 관점(예: SAML, Shibboleth)에서는 그룹, 역할, 사용자 프로파일, Network-centric 관점(예: ETSI, ATIS, ITU-T)의 경우 위치정보, 네트워크 식별자, 연결성(connectivity) 등을 위주로 IdM 을 특징짓고 있다[7]-[9]. 모든 응용분야에 공통적으로 적용될 수 있는 IdM 솔루션은 존재하지 않으며 포괄적 IdM 인프라구조를 완성하기 위해 현재 또는 미래 네트워크들에 Identity 관련 기능들을 추가할 필요가 있다. 또한 Identity 기능 및 성능이 다른 환경의 IdM 간 연동을 위해 게이트웨이 또는 새로운 프로토콜 개발이 필요하다.

ITU 를 비롯한 많은 기구에서 NGN 아키텍처, 요구사항, 서비스 및 기능에 대한 표준을 개발 중에 있으나 NGN 아키텍처 모델의 통합 요소로서 IdM 이 포함되어 있지 않는 문제점이 있

다. 기본 IdM 아키텍처에 NGN 지원을 위해서 보다 폭넓은 User-centric 관점에서 개선이 필요하며 공공 인터넷 통신망이나 전자상거래 환경 등을 위해 개발된 기본 IdM 아키텍처에 다양한 사용자 역할(예: 정부 사용자, 네트워크 회사 직원, 인가된 ETS, TDR 사용자)과 컨텍스트, 트랜잭션 지원 기능 추가가 필요하다. Network-centric 관점에서 NGN 에 IdM 통합을 위해서는 voice, IPTV, data 서비스 등 다양한 서비스 제공자가 포함된 NGN 환경에서 IdM 솔루션이 제공하는 SSO, 사용자 통제기능을 활용하여 사용자에게 개선된 사용자 경험(user experience)이 제공되어야 하며 상호연동 문제를 최소화하기 위해 NNI(Network-to-Network Interface), ANI(Application-to-Network Interface), UNI(User-to-Network Interface) 구성요소를 위한 SAML 또는 다른 프로토콜 프로파일 개발이 요구된다.

2007 년 9 월 ITU-T SG17 총회에서는 Ad Hoc Group on FG IdM Future 라는 주제로 FG IdM 의 Focus Group 활동 연장 문제에 대한 토의와 향후 ID 관리 표준화의 방향에 대한 포괄적인 문제를 다루기 위해 여러 시간에 걸쳐 회의를 진행하였다. 여러 나라에서 제출한 기고문과 회의에서의 의견을 종합하여 다음과 같은 (그림 2)의 JCA(Joint Coordination Activities)와 GSI(Global Standards Initiative) IdM 을 결성하여 진행하는 것으로 결정하고 2007 년 12 월에 TSAG(Telecommunication Standardization Advisory Group) 승인을 얻어 2008 년 1 월에 서



(그림 2) FG IdM 의 향후 표준화 개발 로드맵

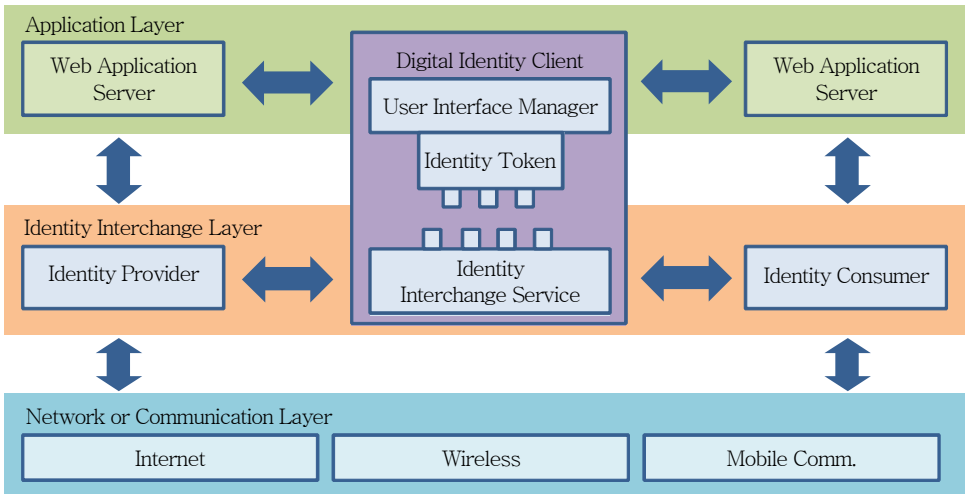
울에서 처음 회의를 진행하였다.

현재 GSI 는 ITU-T 내의 다양한 표준화 단체들이 IdM 의 표준화 개발에 참여하여 의견을 개진할 수 있는 기회를 제공하며 JCA 는 ITU-T 외에 ISO 와 같은 다양한 표준단체들이 모여 상호호환 가능한 IdM 을 주제로 정보를 교환하고 다양한 의견이 토의될 수 있는 자리를 만들어 보다 폭 넓고 심도 있는 표준 결과물을 생성하는 것을 목적으로 하고 있다.

ITU-T SG17 내에서 ID 관리의 표준 개발을 직접적으로 담당하고 있는 곳은 Q6/17 이다. ETRI 는 ID 관리기술인 '자기 통제 강화형 디지털 아이덴티티 공유 프레임워크'에 관한 기고문을 발표하여 X.idif 라는 표준과제로 채택되었고 1 명의 에디터가 선정되어 향후 이 분야에 우리나라의 국제표준화 경쟁력을 제고하는 발판을 마련하였다.

(그림 3)은 ETRI 에서 제안한 Digital Identity 공유 프레임워크로 사이버 스페이스에서의 사용자 중심의 자기통제권이 강화된 전자 ID 지갑을 통하여 다양한 객체들이 서로 사용자의 Identity 정보를 자유롭게 공유할 수 있는 ID 공유 프레임워크에 관한 내용을 담고 있다. 현재 Q6 에서 X.idif 는 ID 관리 분야 표준에 중추적이고 핵심적인 표준으로 자리를 잡을 것으로 예상되며 SG17 에서 IdM 의 표준화 중요성이 부각되어 ID 관리 분야의 표준과제를 전담하는 새로운 Question 을 만드는 것을 심도 있게 논의하고 있고 이에 대한 결정은 2008 4 월 SG17 총회에서 결정될 예정이다.

FG IdM 외에도 ITU-T 에는 ID 관리와 관련된 SG 들이 있는데 Q.15/13(NGN Security)에서는 NGN 환경에서 보안 요구사항 권고안을 확정하였고 인증, AAA(Authentication, Authorization



(그림 3) X.idif 에서 Identity Interchange Layer

and Audit), 보안 메커니즘, NGN 인증서, IdM 보안 등에 관한 권고 초안을 개발 중에 있다.

2. ISO

Identity 관리와 연관된 ISO 의 표준화 활동들로는 인터넷 기반 PKI 에 대한 ISO 9594-8(X.509 PKI 인증서 및 인증서 취소 목록, IETF RFC 3280 과 관련), 전자 거래(Electronic Transaction)에서 활용되는 전자 Identity 에 대한 명세 ISO/IEC 15944-1(Information technology - Business agreement semantic descriptive techniques - Part 1: Operational aspects of Open-Electronic Data Interchange(EDI)), 생체인식정보 교환 표준형식을 개발하는 ISO/IEC 19794, Identity 관리 프레임워크를 연구하는 ISO/IEC JTC1 SC27(Information Technology - Security Techniques - A Framework for Identity Management) 등이 있다. SC27 WG5 에서는 Identity 개념, Identity, 식별(identification) 및 식별자(identifier), Identity 생명주기, Identity 인증, 정보사회에서 Identity 관리, 정보기술과 Identity 관리, 정보보안과 Identity 관리 등 포괄적인 Identity 관리에 대한 표준 개발을 진행하고 있다.

ISO/IEC JTC1 SC27 에서 진행 중인 IdM 표준화 작업은 Identity 와 Identity 정보 관리에 대한 정의, Identity 정보를 안전하고 신뢰성 있게 그리고 프라이버시 규정에 맞도록 관리하는 프레임워크, Identity 및 Identity 정보 생명주기 전반에 걸친 보호 등을 포함하고 있다. SC27 WG5 에서 작성 중인 Working Draft 24760 과 관련된 표준화 문서로는 ISO/IEC 27002(Code of practice for Information security management), ISO/IEC 9798(Entity Authentication), 그리고 ISO/TC/215 WG Glossary 등이 있다.

WD 24760 에는 IdM 과 관련된 용어 정의, Identity 개념, Identity 와 식별자 Identity 속성(attribute), 연계(federated) 및 부분(partial) Identity, Identity 모델, Identity 생명주기('Not Established', 'Created', 'Activated', 'Suspended', 'Terminated', 'Archived')와 Identity 관리, IdM 의 비즈니스 정책, 제도 및 법률 측면, IdM 관련 인증, 인가, SSO, 연계 등과 관련된 내용을 포함하고 있다. Identity 식별자 중 정보 객체 식별자로는 IETF RFC 14422 UUID, IETF RFC 2141 URN, 디지털 인증서로는 ISO 9594-8 X.509 등이 이용될 수 있다.

3. IETF

IETF 에서 개발된 표준 중 Identity 관리와 연관된 RFC 들로는 자원이나 개체 식별을 위한 RFC3986(Uniform Resource Identifier), URI 를 포함하는 식별자에 대한 표준들인 RFC3987 (Internationalized Resource Identifier), RFC2822(Internet Message Format), RFC2141

(Uniform Resource Name), RFC4122(Universally Unique IDentifier, Globally Unique IDentifier), RFC4474(Enhancements and Authenticated Identity Management in the Session Initiation Protocol), RFC4484(Trait-Based Authorization Requirements for the Session Initiation Protocol) 등이 있다.

이 밖에도 인증과 증명서 분야에서 Public Key Infrastructure(X.509)(pkix), Extensible Authentication Protocol(eap), Provisioning of Symmetric Keys(keyprov), 접근과 라우팅을 위한 식별자 및 결정 분야에서 Host Identity Protocol(hip), Telephone Number Mapping(enum), 디렉토리, presence 및 가용성 분야에서 Geographic Location/Privacy(geopriv), Session Initiation Protocol(sip), Session Initiation Proposal Investigation(sipping), SIP for Instant Messaging and Presence Leveraging Extensions(simple), 그리고 발견 및 상호연동 분야의 Cross Registry Information Service Protocol(crisp) 워킹그룹들이 Identity 관리와 관련된 표준화 활동을 진행 중에 있다.

4. W3C

W3C(World Wide Web Consortium)에서는 Identity 관리와 관련된 XML 권고안들을 개발하였는데 대표적인 예로는 XML 문서의 ID 속성인 xml:id 의미를 정의하는 xml:id Version 1.0, 웹 정보 및 프로토콜 메시지 부분에 대한 전자서명 규격을 정의하는 XML Signature WG 의 권고안, XML 문서 전체 및 부분에 대한 암호/복호 절차, 암호화된 부분 지정 및 정당한 수신자가 복호화 할 수 있는 정보 지정을 위한 XML 문법을 정의하는 XML Encryption WG 의 권고안, 공개키 등록 및 분배 프로토콜을 정의하는 XKMS(XML Key Management Specification) 등이 있다.

5. OASIS

OASIS(Organization for the Advancement of Structured Information Standards)에서 제정한 ID 관련 표준들로는 SAML, XACML, SPML, XRI, WS-Security 등이 있다. SAML 표준에서는 주체(subject)에 대해 발행된 assertion 구조 및 assertion 처리를 위한 관련 프로토콜들에 대해 정의하고 있으며 XACML 은 정보시스템에 의해 관리되는 자원에 대한 접근허용 여부를 정의하는 XML 언어 기반 보안정책 기술언어 표준이다[4]. SPML 은 사용자, 자원, 서비스 프로비저닝 정보교환을 위한 XML 기반 프레임워크를 정의하고 있으며 XRI 는 위치, 응용, 전송 프

로토콜과 독립적인 URI 와 호환성 있는 추상적 식별자와 해결 프로토콜에 대한 표준을 정의하고 있다[5],[6]. WS-Security 표준에서는 웹 서비스 messaging 에 적용되는 무결성 및 비밀성 지원을 위한 프로토콜을 정의하고 있다. 또한 XDI 는 XRI 에 기반을 둔 데이타웹(dataweb) 구축을 목표로 인터넷 규모의 멀티 도메인들 간에 XRI 와 XDI 기본 스키마에 기반을 둔 XML 문서를 상호간에 서로 공유하고 연결(linking), 동기화하는 표준화를 제안하고 있다.

6. WS-I

WS-I 는 SOAP, WSDL(Web Service Description Language), UDDI(Universal Description Discovery and Integration)로 구성되는 웹 서비스에 대한 표준을 제정하는 조직으로 웹 서비스의 보안과 관련된 표준 또한 제정하고 있으며 향후 표준 로드맵도 제시하고 있다. WS-Security 는 SOAP 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 보호 수준(Quality of Protection)을 제공하기 위한 스펙이다. WS-Security 는 바이너리 보안토큰을 인코딩하는 방식과 X.509 인증서 또는 Kerberos 티켓 등을 사용하는 방식 등을 정의하고 있다. 특히, 이 스펙은 OASIS 에 제안되어 WSS(Web Service Security)라는 명칭으로 표준화가 진행되고 있다.

WS-Trust 는 신뢰관계를 형성하는 방법으로, 당사자간에 직접 신뢰관계를 형성하는 방법과 신뢰할 수 있는 중간 계층을 통해 신뢰관계를 형성하는 방법을 소개한다. WS-Policy 는 수신자와 송신자가 보안에 대한 요구사항과 자신이 지원 가능한 보안 정도를 명시하는 방법을 제공한다. WS-Federation 은 사이트 또는 조직간 ID 연동을 위한 스펙으로 WS-Security, WS-Policy, WS-Trust 및 WS-Secure Conversation 기반 위에서 구현된다. 현재, WS-Federation 이 SAML 을 채택하여 사용할지에 대해서는 미지수이다. WS-Trust, WS-Policy, WS-Federation 은 현재 버전 1.0 표준안이 나온 상태이다. WS-I 는 또한 OASIS 와 같은 중립적인 표준 단체에 WS-Federation 을 비롯하여 WS-Trust, WS-SecureConversation, WS-SecurityPolicy 를 상정할 예정이다.

7. Liberty Alliance

Liberty Alliance 프로젝트는 연계(federated) ID 관리를 위한 가이드라인과 실례 그리고 공개 표준을 개발할 목적으로 2001 년에 결성되었고, 웹 서비스의 소비자들이 ID 정보에 대한 프라이버시와 보안을 유지하면서 온라인 업무를 어디에서든지 더 쉽게 할 수 있게 하는 것을 목표로 하고 있다. (그림 4)는 Liberty Alliance 기술의 개념과 Liberty Alliance 에 참여하는 기관을

<자료>: Liberty Alliance Tutorial, http://projectliberty.org/

(그림 4) Liberty Alliance

보여준다.

ID 들이 연합되어 연결되고, 공유함으로써 사용자에게 SSO, 단일 로그아웃(Single Logout) 등의 편리함을 제공한다. Liberty Alliance 프로젝트는 크게 세 개의 모듈로 구성되어 있다. 여러 사이트의 사용자 계정을 연결하는 ID 의 연합(federation)을 다루는 ID-FF, ID 서비스의 생성, 검색, 사용을 위한 프레임워크를 제공하는 ID-WSF 와 ID-WSF 위에서 일정, 주소록, 달력, 위치추적, 사용자 상태나 경고 등을 위한 ID 기반의 서비스를 다루는 ID-SIS 로 구성되어 있다[1]-[3].

IV. 향후 표준화 전망

국내에서도 이미 웹 서비스를 제공하는 사이트들은 OpenID 와 같은 가벼운 ID 관리 기술을 이용하여 ID 관리 서비스를 제공하고 있으며 공공기관에서도 온라인 신원확인 서비스를 제공하기 위해 ID 관리 기술을 적용하고 있다. 2007 년을 기점으로 ID 관리 기술에서 인증 및 사용자 정보 공유에 대한 요구가 점점 증가하고 있고 이에 대한 프라이버시 보호 요구사항도 점차 대두되어 ID 관리 기술의 국내 표준화가 시급한 상황이며 향후 적용 사이트들간의 상호운용성을 위해서도 관련 표준화 개발이 시급한 실정이다.

국외의 경우에는 이미 여러 가지 ID 관리 기술들에 대한 표준화가 진행되었고 현재는 다양한 ID 관리 기술들간의 상호연동을 통하여 융복합 서비스를 NGN 에서 제공하기 위한 표준화 개발이 진행되고 있다. 국외에서는 ID 관리기술의 변화속도가 빨라 현재는 대형 IT 기업이나 공개 소프트웨어 그룹들이 주로 기술의 개발을 주도하고 있고 표준화 개발은 그 보다는 한 박자

늦게 진행되고 있는 것이 현실이다. 그러나 표준화가 완료되면 향후 기술의 주도권을 주로 외국 업체들이 가지고 국내 시장을 독점할 우려가 있어 이 분야의 기술 개발과 표준화 개발이 시급한 문제로 지적되고 있다.

ID 관리 기술은 인증 및 크리덴셜 관리와 사용자 개인정보의 공유를 통하여 응용 서비스에 다양한 융복합 서비스 창출을 용이하게 해줄 수 있다. 이러한 특성은 인터넷 환경에서는 SNS (Social Network Service)와 IPTV 와 같은 다양한 분야에 적용될 수 있고 디바이스의 제약으로 사용자와의 간편한 상호작용을 요구하는 모바일 또는 유비쿼터스 환경에서 더욱 중요한 역할을 할 것으로 여겨진다. 그리하여 표준화 관련해서도 이 분야의 다양한 표준화 개발이 향후 이루어 질 것으로 예상된다.

V. 결 론

웹에서 제공되는 서비스들이 점점 진화하고 발전함에 따라 Identity 관리 기술도 점점 다양하고 고도화된 기술들을 필요로 하고 있다. 초기의 Identity 관리 기술이 제한된 도메인 내에서 인증, SSO 및 인가 기술에 초점을 맞추어 기술이 개발된 반면 현재의 Identity 관리 기술은 사용자를 중심으로 Identity 정보의 공유에 보다 무게를 두고 개발되며 정보의 공유시 발생할 수 있는 프라이버시 문제에도 많은 연구를 하고 있다.

현재 ID 관리 기술은 기업 또는 산업계의 요구사항에 맞추어 빠르게 발전하고 있다. 하지만 ID 관리 기술의 발전보다 표준화의 개발은 상대적으로 더디어 기술의 상호운용성이나 제공되는 ID 서비스들의 보안성이나 프라이버시 보호가 여전히 부족한 상황이다. 따라서 국내에서 국내 환경에 맞는 안전한 ID 관리 기술의 표준을 개발하는 것이 시급하고 이렇게 확보된 기술을 국외의 여러 표준화 단체들에 적극적으로 국제 표준화를 진행하는 것이 향후 기술적으로 우위를 점할 수 있는 기반을 마련할 것으로 생각된다.

<참 고 문 헌>

[1] Liberty Alliance ID-WSF Data Services Template Specifications, Version 2.0, http://www.projectliberty.org,

[2] Liberty Alliance ID-WSF Specifications, Version 2.0, http://www.projectliberty.org,

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

[4] Security Assertion Markup Language(SAML) OASIS Standard specification, Version 2.0, http://www.projectliberty.org,

[5] OASIS Extensible Resource Identifier (XRI) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xri
[6] OASIS Extensible Resource Identifier (XRI) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xdi
[7] J. Hoyt, OpenID Simple Registration Extension, Version 1.0, http://openid.net/specs/openid-simple-registration-extension-1_0.html
[8] Scott Kveton, The State of OpenID, http://openid.net/pres/openid-solt-final.pdf
[9] D. Hardt, OpenID Attribute Exchange, Draft Version 1.0, http://openid.net/specs/openid-attribute-exchange-1_0-07.html

* 본 내용은 필자의 주관적인 의견이며 IITA 의 공식적인 입장이 아님을 밝힙니다.