情 報 保 護 學 會 誌
第21卷 第4號, 2011. 6

ID 관리 기술 국제표준화 동향 및 향후 전망

조 상 래*, 노 종 혁*, 진 승 헌**

요 약

국제표준화기구 ISO와 ITU-T에서는 ID 관리 기술 관련 표준화를 리드하는 연구그룹을 운용하여 이 분야의 표준화를 주도하고 있다. ID 관리 기술의 표준화를 ISO가 먼저 시작하였으나 현재는 ITU-T가 보다 더 다양한 분야에서 폭넓게 표준 개발을 진행하고 있다. 현재 ID 관리 기술은 기존의 ID 관리 시스템들 간의 상호호환성을 제공하려는 기술에 초점이 맞추어 개발되고 있고 사용자의 개인정보를 공유할 시에는 사용자 중심의 프라이버시 기술을 제공하는 방향으로 진행되고 있다. 본 논문에서는 현재 ISO 및 ITU-T에서 이미 표준화된 ID 관리 관련 국제표준들과 개발 중에 있는 표준초안들에 대해 간단히 소개하고, 기타 다른 표준화 기구들의 동향을 파악하여 향후 추진방향을 제시하고자 한다.

Ⅰ. 서 론

웹 기술의 발달과 서비스의 진화로 사용자의 Identity 정보를 서로 공유하고 관리하는 것은 이제는 웹2.0 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. 이러한 ID 관리의 문제는 단일 도메인에 국한되지 않고 다양한 응용서비스를 제공하는 다중 도메인에 걸쳐 서비스를 제공하기를 요구하여 서로 다른 ID 관리 시스템들 간의 상호호환성을 필요로 한다. 현재 ID 관리 기술은 모든 IT 시스템의 사용자 개인정보 관리에 반드시 필요한 기술로 인식되고 있으며 향후 클라우드 컴퓨팅과 모바일 컴퓨팅에서도 핵심 보안 기술로 다루어지고 있다.

또한 휴대폰을 통해 온·오프라인 환경에서 다양한 서비스를 이용함에 따라 인증정보, 지불정보, 신분증, 정태적/동태적 개인정보, 선호정보 같은 모바일 ID 관리가 중요해지고 있다. 모바일 ID는 휴대성, 이동성, 항시성, 오프라인 상호작용, 고부가가치 등 기존의 ID 개념과는 차별되는 특성을 갖는다. 이에 따라 모바일 ID 보안 기술, 모바일 ID 사용기술, 모바일 ID 기반 서비스 기술 등 새로운 ID 관리 기술이 요구되고 있다.

본 논문에서는 ISO와 ITU-T를 주축으로 진행되고 있는 ID 관리 기술의 국제표준들과 개발 중에 있는 표준초안들에 대해 간단히 소개한다, 또한 두 기관을 제외한 OASIS, Kantara, IETF와 같은 여타의 표준화 전문기관들의 동향도 간단하게 조사하여, 향후 ID 관리 기술의 표준화 추진방향을 제시하고자 한다.

Ⅱ. ISO

본 절에서는 국제표준화기구인 ISO/IEC의 보안분과인 JTC 1/SC27 산하에서 ID 관리 기술의 표준화를 담당하고 있는 WG5에 대하여 소개하고자 한다. SC27은 현재 5개의 작업반을 운영하고 있다.

- WG1 - 정보보호 관리 시스템
- WG2 - 암호 및 보안 메커니즘
- WG3 - 보안 평가 항목
- WG4 - 보안 제어 및 서비스
- WG5 - ID 관리 및 프라이버시 기술

5개의 작업반 중에 WG5에서는 ID 관리와 프라이버시 분야의 표준 및 가이드라인 개발을 위한 요구사항과 개발 내용을 도출하는 작업을 진행하고 있다.

* 한국전자통신연구원 지식정보보안연구부 (sangrae@etri.re.kr, jhroh@etri.re.kr)
** 한국전자통신연구원 지식정보보안연구부 (jinsh@etri.re.kr)

2.1 ID 관리 기술

현재 ID 관리 기술에서는 다음과 같은 표준과제들이 진행되고 있다.

- ISO/IEC FCD 24760-1 - A framework for identity management - Part 1 Terminology and concepts
- ISO/IEC AWI 24760-2 - A framework for identity management - Part 2 Reference architecture and requirements
- ISO/IEC AWI 24760-3 - A framework for identity management - Part 3 Practice
- ISO/IEC CD 29115 - Entity authentication assurance framework

ID 관리 표준은 세 개의 파트로 나누어 진행되고 있다. 먼저 용어 및 개념 부분은 Identity라는 용어에 대한 정의를 시작으로 ID 관리까지 용어를 심도 있게 정의하고 있으며 개념에서는 정의를 보다 쉽게 이해하도록 기본 아이디어와 사용 방법 등을 소개하고 있다. ID 관리 분야의 용어는 그 동안 서로 다른 표준화 기구들에서 같은 용어를 서로 다른 의미로 사용하여 표준을 이해하는데 많은 문제를 일으켰다. 따라서 본 표준은 이러한 문제를 해결하기 위해 이례적으로 용어정의라는 표준과제을 추진하여 향후 이 분야의 초석을 다지려는 의도로 파악되고 있다.

두 번째 파트에서는 ID 관리를 하기 위한 참조 아키텍처와 요구사항을 정의하고 있다. 여기서는 실제 Identity가 생성되고 사용, 변경, 효력정지 그리고 폐기까지의 생명주기 관리에 필요한 프레임워크를 정의하고 있다. 이 부분이 ID 관리 프레임워크의 핵심적인 부분이다.

세 번째는 실제 이러한 프레임워크를 어떻게 사용하는 지를 보여주는 부분으로 구성되어 있다. ID 관리 기술은 이미 다양한 분야에서 실제 서비스에 제공되고 있어 실제 적용 사례는 프레임워크 표준을 실제 사용하려는 조직에 많은 도움을 줄 것으로 예상된다.

마지막은 ITU-T와 함께 ID 관리 과정에서 요구되는 개체에 대한 인증 및 보증을 위한 프레임워크와 인증에 영향을 미칠 수 있는 요소들에 대한 기준, 위협 등을 표준화하는 과제이다. 이 부분은 ITU-T 동향에서 보다 자세히 설명할 예정이다.

2.2 프라이버시 기술

현재 프라이버시 기술에서는 다음과 같은 표준과제들이 진행되고 있다.

- ISO/IEC FCD 29100 - Privacy framework
- ISO/IEC CD 29101 - Privacy reference architecture

프라이버시 프레임워크에서는 프라이버시 요구사항을 정의하고 프라이버시 원칙을 기술하고 있다. 동의, 선택, 목적 정의, 수집제한, 사용, 보유, 공개제한 및 최소 데이터 규칙등과 같이 프라이버시 보호를 위해 필요한 정책들을 설명하고 있다. 또한 프라이버시 개발을 위한 개인정보의 수집, 전달, 사용, 저장, 폐기에 이르는 생명주기를 어떻게 처리하는지에 대한 설명도 하고 있다.

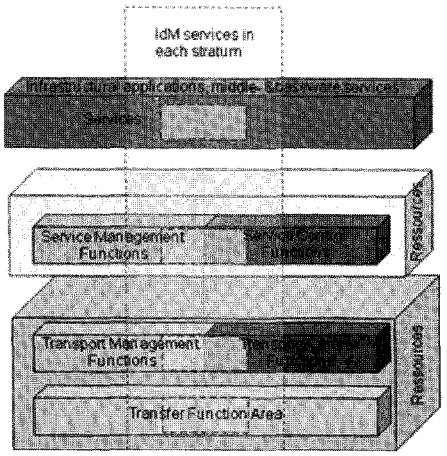
프라이버시 참조 아키텍처에서는 프라이버시 보호를 위해 필요한 요구사항 및 프레임워크를 기술적으로 구현하는데 필요한 지침을 제공한다. 이러한 지침은 프라이버시 기술의 적용이 IT 시스템을 설계할 초반부터 적용되어 개발할 수 있는 기반을 마련하고 있다. 본 표준에는 프라이버시 보호를 위한 제어 기술로 익명화, 블라인드 서명, 생체암호 및 고도화된 프라이버시 보호 기술에 대한 기술도 다루고 있다.

Ⅲ. ITU-T

ITU-T에서는 SG17 WP3 그룹이 ID 관리 기술에 관한 표준화를 리드하는 연구그룹으로, 산하 6개의 연구과제(Question)를 구성하여 관련 국제표준을 개발하고 있다. 이 연구과제들 중 Q.10에서는 ID 관리 기술의 구조와 프레임워크에 대하여 정보통신 환경에서 다양하게 응용될 수 있는 국제표준들의 개발을 담당하고 있다. 현재, Q.10에서는 앞서 언급된 분야로 총 4건의 국제표준을 제정하였으며, 총 12건의 표준초안들이 개발 중에 있다. 본 논문에서는 Q.10에서 개발한 국제표준들과 개발 중에 있는 표준초안들에 대해 간단히 소개한다.

3.1 X.1250

본 표준은 글로벌 ID 관리 시스템 환경에서의 신뢰 및 상호호환성 기능(Baseline capabilities for enhanced global identity management and interoperability)을 제공하기 위한 구조적인 요구사항을 정의하고 있다. 이것



〔그림 1〕 ID 관리 네트워크 계층 상호호환 범위

은 모든 통신, 제어 네트워크, 그리고 서비스에서 사용되는 디지털 아이덴티티(크리덴셜, 식별자, 속성자, 그리고 평판)에 대한 Assertion의 신뢰를 가능하게 한다[1].

이 표준은 글로벌 ID 관리 시스템들 간의 상호호환성 및 신뢰를 위한 다음과 같은 요구사항을 정의하고 있다.

- 공통적이고 구조화된 ID 관리 모델 및 상호호환성이 있는 ID 관리 기능들.
- 모든 엔티티들에 대한 보증 레벨을 포함하는 크리덴셜, 식별자, 속성자, 그리고 패턴 ID 서비스의 준비.
- 신뢰받는 ID 제공자, 서비스 및 연계서비스 발견.
- 인가관리 시스템, ID 제공자 그리고 ID Bridge 제공자를 포함하는 연계서비스 제공자들 간의 상호호환성.
- 사용자 개인정보와 아이덴티티 자원의 보호를 포함하는 위험과 위협을 감소하는 보안 및 그 외의 방법.
- 개인정보의 보호 및 정책 실행을 포함하는 감리 및 정책 부합.
- 사용성 및 확장성: 재난 복구, 국제화, 가용성, 신뢰성, 그리고 성능.

[그림 1]은 글로벌 ID 관리 시스템들 간의 상호호환 범위를 네트워크 계층구조로 보여주고 있다.

본 표준은 향후 국내 ID 관리 시스템들 간의 상호호환성을 제공하기 위한 시스템 개발의 요구사항에 사용될 수 있는 내용을 정의하고 있다. 따라서 본 표준은 ID 관리 분야와 웹 서비스 정보보호 분야에 직접적으로 적용되며, 정보보호 산업의 핵심 요소로 활용될 수 있다. 또한, ID 연계의 핵심 기술을 제공함으로써, 기업간 협업을 용이하게 함으로써 새로운 서비스를 창출하고 시장을 활성화할 수 있다.

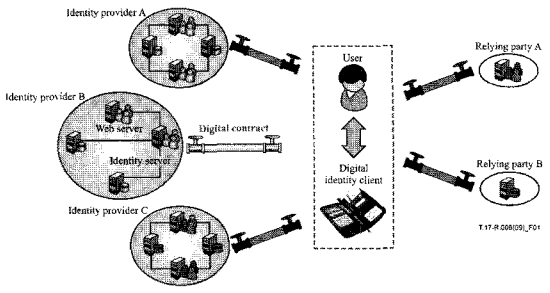
3.2 X.1251

본 표준은 2009년 9월에 표준으로 제정되었다. 표준은 사용자 중심의 ID 관리 프레임워크 (A framework for user control of digital identity)로 온라인 환경에서 사용자의 개인정보를 교환할 때 사용자가 본인 정보에 대해 제어를 할 수 있는 권한을 부여하는 프레임워크 기술이다. 본 표준은 한국전자통신연구원이 개발한 전자ID지갑 기술을 국제표준화한 것으로 ID 관리 기술의 최초 국제표준으로 국내 기술 수준을 한 단계 업그레이드하는 계기가 되었다[2].

[그림 2]는 사용자가 중심에서 개인정보를 제어하는 디지털 아이덴터티 공유 개념을 모델화한 것이다. 기본적으로 사용자의 개인정보를 제공하는 ID 제공자와 사용하는 ID 소비자 사이에 사용자는 디지털 ID 클라이언트를 사용하여 본인의 개인정보를 교환하고 제어할 수 있다. 현재 대부분의 다중 도메인에서의 ID 관리 서비스는 개인의 프라이버시 보호를 위해 사용자 중심의 ID 관리 개념을 도입하여 사용하고 있는 추세이다.

3.3 X.1252

본 표준은 ID 관리 기술의 기본 용어(Baseline identity management terms and definitions)를 정의한 표준으로 향후 ITU-T내에서 ID 관리 기술의 표준초안 개발 시에 활용할 목적으로 2010년 4월에 표준으로 제정되었다. 본 표준은 X.1250과 X.1251을 개발하는 과정 중



〔그림 2〕 디지털 아이덴터티 공유 모델

에 필요성이 제기되어 개발된 표준이다. SG17에서는 그 동안 하나의 표준화 과제로 ID 관리 기술 관련 용어를 정의하는 작업을 2007년부터 진행하였고, 본 표준의 제정을 계기로 향후 관련 표준들의 개발에 많은 도움이 될 것으로 예상된다[3].

용어들은 다양한 경로를 거쳐 선정되었고 아이덴터티 관리 관련하여 아주 공통적으로 사용된다고 믿어진다. 본 표준은 아주 방대한 아이덴터티 관리 관련 용어를 정의하는 것이 목적은 아니다. 대신에 여기에 선정된 용어들은 가장 기본적으로 중요하고 공통적으로 많이 사용되는 아이덴터티 관리 용어들로 구성되어 있다. 몇 가지 중요한 용어에 대한 배경지식이 부록에 수록되어 있다.

본 표준의 목적중 하나는 아이덴터티 관리 표준을 개발하고 있는 그룹들이 공통적으로 용어들을 이해하는 것을 돕는 것이다. 용어정의는 가능한 구현 또는 특정 환경과는 독립적으로 만들어졌고 따라서 어떠한 아이덴터티 관리 작업에도 기본적인 정의로 사용될 수 있다. 특정한 경우 또는 문맥에서는 본 표준에서 제공하는 정의보다 좀 더 자세하게 용어가 정의되는 것이 필요한 경우도 있다는 것을 유념하여 사용해야 한다.

본 표준은 아이덴터티 관리를 이용하여 표준화를 추진하는 모든 분야에 적용될 수 있다. 또한 아이덴터티 관리 시스템을 개발하는데 공통으로 사용할 용어가 필요할 시에도 사용될 수 있다.

3.4 X.idmsg

본 표준은 ID 관리 시스템의 보안 지침(Security guidelines for identity management systems)에 대한 표준으로 현재 한국전자통신연구원의 주도로 표준초안이 개발 중에 있다[4].

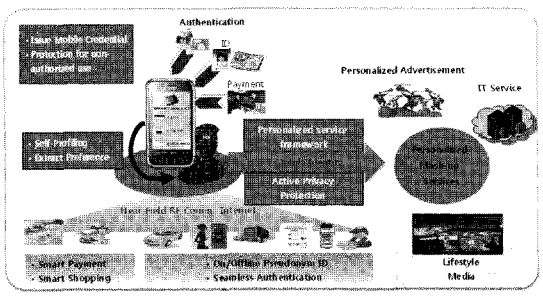
표준은 ID 관리 시스템에 대한 다양한 보안 위협들을 먼저 파악하고 이에 대한 대비책을 마련하는 것으로 시작한다. ID 관리 시스템의 보안 지침은 크게 시스템이 설치될 때, 운영될 때로 나누어진다. 시스템 설치 시에는 주로 사전에 설치되거나 운영되어야할 보안 해결책들이 제시되고 운영 시에는 실제 서비스를 제공할 때 필요한 보안 기술들에 대해 기술하고 있다.

ID 관리 시스템은 크게 서버와 사용자가 사용하는 클라이언트 프로그램으로 구별할 수 있다. 서버 보안의 경우에는 일반적으로 이메일 서버와 같은 응용서버와 크게 다르지 않고 대개의 경우 서버는 기업이 관리하여 비교적 보안 관리가 잘되어 있지만 사용자의 클라이언트 프로그램의 경우에는 훨씬 더 열악한 상황에 있다고 할 수 있다. 또한, 본 표준은 현재 스마트폰이 많이 활성화되고 모바일 환경에서 ID 관리 서비스 요구사항이 늘어남에 따라 모바일 클라이언트에서의 보안 지침에 대해서도 언급하고 있다.

3.5 X.mob-id

현재 스마트폰이 널리 쓰이고 다양한 응용 프로그램들이 모바일 통신을 이용하여 서비스를 제공하는데 개인정보 침해 및 프라이버시 보호 관련하여 해결해야 하는 문제점이 대두되고 있다. 본 표준초안은 모바일 환경에서 사용자의 개인정보를 효율적이고 안전하게 관리하는 프레임워크(Baseline capabilities and mechanisms of identity management for mobile applications and environment)를 한국전통신연구원 주도하에 개발되고 있다. 모바일 ID 관리 프레임워크는 인증, 인가, 개인정보 프로파일링 기술을 바탕으로 스마트 지불, 온오프라인 인증, 모바일 출입증과 같은 다양한 분야에서 사용될 수 있는 기술을 담고 있다[5].

모바일 아이덴터티 관리 서비스 개념은 인증, 아이덴터티, 지불 정보를 통신을 통해 모바일 단말에 발급받아 저장하고 보안성 유지를 제공하며 모바일 아이덴터티를 온·오프라인 환경의 지불, 인증, 아이덴터티 확인에 안전하고 편리하게 사용하고 이 과정에서 동태적 개인정보가 자체 프로파일링 되어 축적된 개인정보를 프라이버시를 유지하고 제공하여 개인화 서비스를 받는 것이다. 스마트 클라이언트는 온·오프라인에서 안전하고 편리하게 신원확인, 인증, 지불하고 개인정보를 능동적으로 보호 및 이용할 수 있게 해주는 휴대 단말 (S/W,

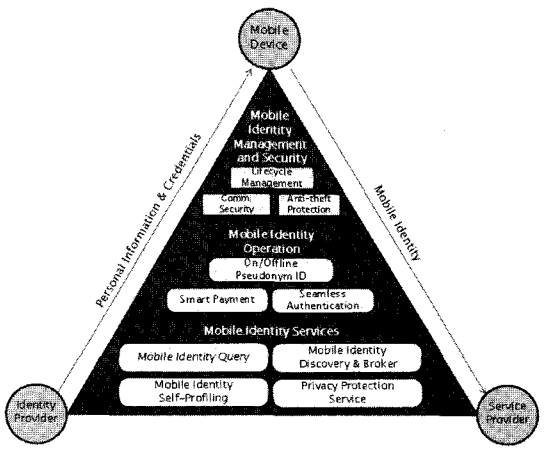


〔그림 3〕 모바일 아이덴터티 관리 서비스 개념도

H/W)로서 모바일 아이덴터티의 보안과 프라이버시 강화, 안전하고 편리한 사용 및 고부가 아이덴터티 기반 서비스 개발을 위한 퍼스널 모바일 아이덴터티 플랫폼이다. [그림 3]은 모바일 아이덴터티 관리 서비스 개념도를 보여준다.

[그림 4]는 모바일 아이덴터티 관리 프레임워크이다. 그림에서 아이덴터티 제공자는 모바일 디바이스가 요청하면 개인정보 또는 크리덴셜을 모바일 디바이스에 제공한다. 이렇게 제공된 정보들은 사용자가 모바일 디바이스를 이용하여 사용하는 다양한 서비스들에서 수집된 정보와 위치정보와 같은 컨텍스트 정보를 더하여 모바일 아이덴터티로 관리된다. 사용자는 서비스 제공자에게 모바일 아이덴터티를 제공하여 다양한 개인 맞춤형 서비스를 받을 수 있다. 프레임워크의 모든 내용은 모바일 디바이스에 설치되어 운영되고 모바일 아이덴터티 오퍼레이션과 서비스 기술들은 필요에 따라 아이덴터티 제공자나 서비스 제공자에 적용되어 사용될 수 있다. 모바일 아이덴터티 프레임워크는 아이덴터티 제공자에게 제공받은 개인정보를 프레임워크 내에 다양한 기술들을 통해 모바일 아이덴터티로 변경하여 관리한 후 다양한 서비스 제공자에게 안전하고 프라이버시가 보장된 방법으로 제공하는 것이 주 목적이다.

본 표준은 모바일 아이덴터티 관리 프레임워크를 정의하여 향후 스마트폰에서 동작하는 다양한 모바일 어플리케이션에 제공될 모바일 아이덴터티 관리, 인증, 프라이버시 기능 및 사용자 인터페이스를 정의하여 모바일 아이덴터티 침해와 분실 도난으로 인한 도용 및 프라이버시 침해를 줄일 수 있고 인증, 지불, 개인정보 기반 서비스를 지원하여 보다 원활한 모바일 인터넷 서비스를 가능하게 한다.



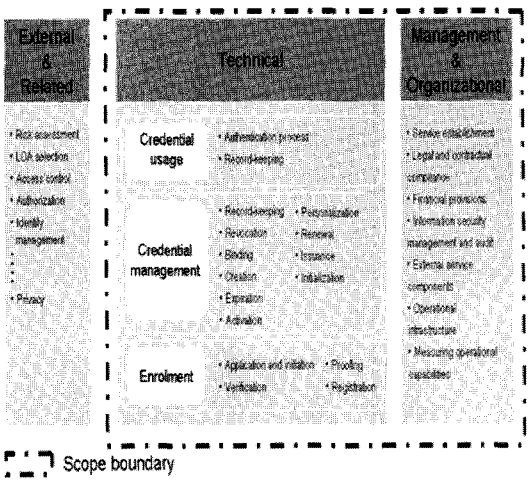
〔그림 4〕 프레임워크 구성도

3.6 X.eaa

인증의 경우 사용자 또는 개체를 검증하기 위해 사용자와 서비스 제공자간에 수행되는데 적용 도메인이 변경되면 새로 인증해야하는 문제점이 있다. 본 표준은 개체 인증 보증 프레임워크(Information technology - Security techniques - Entity authentication assurance framework)로 인증 강도에 따라 레벨을 부여하여 인증 사실에 대한 다중 도메인에서 공유를 가능하게 하는 기술이다[6]. 현재 본 과제를 미국에서 주도적으로 추진하고 있으며 ISO JTC1 SC27과 공동으로 표준을 추진하여 표준이 제정될 경우 인증 분야에서 상당한 영향력이 있을 것으로 예상된다. [그림 5]는 개체 인증 보증 프레임워크의 구성도를 보여준다.

본 표준은 ID관리 서비스 등에서 사용자에 대한 인증에 대한 보증의 정의 기준을 정의한다. 높은 보안성을 요구하는 응용 등에서는 이를 이용하는 사용자에 대한 인증에 대한 보증 레벨 역시 높아야 하는데, 표준에서는 이러한 응용 서비스를 이용하기 위해 사용자가 자신의 신원을 증명(Identity Proofing)하는 방법 및 기준 등을 정의한다. 본 표준은 개체 인증에 대한 보증 프레임워크를 정의하고 있다.

특히, 표준에서는 4가지의 개체 인증에 대한 보증레벨을 정의하고, 각 레벨에 대한 기준 및 가이드라인을



〔그림 5〕 개체 인증 보증 프레임워크 구성도

정의한다. 또한, 인증 위협을 완화하기 위해 사용될 수 있는 통제와 다른 인증에 대한 보증 스킴과 보증 레벨을 매칭시키기 위한 가이드를 제공하며, 4개 보증레벨에 기반을 둔 인증의 결과를 교환하기 위한 가이드도 함께 제공한다. 본 표준은 사용자를 포함한 개체에 대한 인증의 보증 레벨을 정의한 프레임워크를 정의하여 국내 관련 기반 환경을 구축에 기여할 것이다.

3.7 기타 표준초안

Q.10에서 진행되고 있는 추가적인 표준초안 중에 프레임워크 관련 과제들이 다음과 같다. X.giim - Generic identity management interoperability mechanisms은 ID 관리 시스템들간의 상호호환성과 관련된 일반적인 메커니즘에 대한 표준을 개발하고 있다. X.idm-ifa - Framework architecture for interoperable identity management systems는 ID 관리 시스템들 간의 상호호환성에 필요한 프레임워크 구조를 개발하는 표준이다. X.idmgen - Generic identity management framework은 서비스나 사용하는 기술에 독립적으로 적용될 수 있는 ID 관리 구조를 정의하여 향후 ID 관리 시스템들간의 상호호환성을 제공하려 하고 있다.

클라우드 컴퓨팅에서도 ID 관리 기술의 필요성이 제기되고 있는데 본 과제 X.idmcc - Requirement of IdM in cloud computing은 클라우드 컴퓨팅 환경에서 필요한 ID 관리 기술에 대한 요구사항을 정의하는 표준과제이다. X.discovery - Discovery of identity management information는 특정 개체의 식별자와 속성들을 온라인에서 쉽고 안전하게 조회할 수 있는 방법을 표준화하는 과제이다. 이 표준화가 완료되면 향후 보다 많은 응용시스템에서 ID 정보를 이용할 수 있는 방법이 마련될 것으로 기대된다.

X.authi - Authentication integration in identity management는 사용자가 본인이 속한 네트워크에 접속하여 인증을 하면 서비스 이용 시에도 별도의 인증 없이 접근할 수 있는 기술을 표준화한다. 네트워크 계층과 서비스 계층에서 공통으로 사용할 수 있는 통합 인증 기술을 개발하는 것이 본 과제의 목적이다. X.otif - Open identity trust framework는 OpenID와 Information Card 기술 등을 이용하여 사용자의 개인정보를 원활하게 교환하기 위해서 필요한 신뢰 프레임워크를 정의한다. 이러한 신뢰 프레임워크가 표준화되면 향후 ID 제공자와 서비스제공자는 사전의 정책 동의 및 계약이 없어도 사용자의 개인정보를 공유할 수 있다.

X.priva - Criteria for assessing the level of protection for personally identifiable information in identity management는 한국인터넷진흥원에서 개발하고 있는 표준초안으로 개인정보보호 수준 정의를 위한 공통 항목을 정의하고 있다.

기업 및 기관의 개인정보보호 수준을 진단·정의하기 위한 공통 항목으로 개인정보보호를 위한 기반 환경과 처리 단계별 관리 현황, 개인정보 침해사고에 대한 대응 현황에 대한 세부 평가기준을 제시하고 있다. 또한, 특정 개인정보에 따라 보호수준에 대한 기준이 다를 수 있으므로 개인식별 가능성, 민감도 등에 따른 개인정보 분류기준을 제시한다. 기업 및 기관에서는 본 표준에서 제시하는 개인정보 분류기준을 참조하여 보유하고 있는 개인정보를 분류하고, 함께 제시하는 개인정보보호 수준 평가 항목을 각 분류에 적용함으로써 개인정보보호 수준을 진단할 수 있다.

Ⅳ. 기타 국제 표준화 동향

본 장에서는 ISO와 ITU-T를 제외한 다른 국제 표준화 기구들의 동향을 살펴본다.

4.1 Liberty Alliance

Liberty Alliance project는 연계 ID 관리를 위한 가이드라인과 실례 그리고 공개 표준을 개발할 목적으로 2001년에 결성되었고, ID들이 연계되고, 공유함으로써 사용자에게 SSO, Single Logout 등의 편리함을 제공한다. Liberty Alliance project는 크게 세 개의 모듈로 구성되어 있다. 여러 사이트의 사용자 계정을 연결하는 ID의 연계를 다루는 ID-FF, ID서비스의 생성, 검색, 사용을 위한 프레임워크를 제공하는 ID-WSF와 ID-WSF 위에서 일정, 주소록, 달력, 위치추적, 사용자 상태나 경고등을 위한 ID 기반의 서비스를 다루는 ID-SIS로 구성되어 있다. ID-FF는 OASIS의 SAML 2.0으로 표준화되었고. Identity 서비스를 평가하고 검증할 수 있는 Identity Assurance Framework를 개발하였고 엔티티들간의 Identity 정보의 원활한 교환과 프라이버시 제한을 정책으로 설정할 수 있는 Identity Governance Framework 표준안도 현재 개발되어 발표되었다.

2009년 4월에 Liberty Alliance의 모든 결과물은 향후 ID 관리 기술 등의 통합 및 조화를 목적으로 설립된 Kantara Initiative에 헌정되고 별도의 활동을 중단하였다. 이러한 움직임은 향후 ID 관리 기술이 ID 관리 시스템들 간의 상호호환성을 해결하려는 움직임의 일환으로 해석되고 있다.

4.2 Kantara Initiative

Kantara Initiative는 2009년 4월 DataPortability Project, the Concordia Project, Liberty Alliance, ISOC, ICF, OpenLiberty.org와 XDI.org가 연합하여 결성이 되었으며 디지털 아이덴터티에 대한 중심축으로 산업계에서 필요한 다양한 ID 관리 요구사항을 반영하여 상호운용성과 조화를 기반으로 표준을 개발하는 것을 목적으로 한다.

아이덴터티 관련 기술 사양을 개발하기 위해 Kantara Initiative는 다양한 그룹들을 운영하고 있는데 사용자에게 보다 안전한 ID 관리 서비스를 제공하려는 목적에서 Clients WG(Work Group)와 Comsumer Identity WG를 운영하고 있으며 ID 관리 기술 분야인 Federation, Identity and Access Services, Identity Assurance 그리고 IdP Selection WG를 운영하여 보다 구체적인 ID 관리 기술의 사양을 개발하고 있으며 전자정부, 의료와 정보통신과 같은 구체적인 분야의 ID 관리 관련 사양도 개발하고 있는 것이 특징이다.

4.3 OASIS

OASIS에서 제정한 ID 관련 표준들로는 SAML, XACML, SPML, XRI, WS-Security(Web Service Security) 등이 있으며, 현재 OepnID와 CardSpace가 서로 상호 운영할 수 있는 표준인 Identity Metasystem Interoperability를 개발 중에 있다.

Identity Metasystem Interoperability 작업반은 마이크로소프트에서 개발한 Information Card 기술을 광범위한 웹 서비스에 적용하기 위해 출범했다. Information Card는 사용자가 패스워드를 입력하지 않고 다양한 웹 사이트에 인증을 할 수 있고 개인정보도 공유할 수 있는 기술로 마이크로소프트 운영체제에 제공되고 있다.

Identity in Cloud (IDCloud) 작업반은 클라우드 서비스 환경에서 ID 관리 시스템에 잠재적으로 존재하는 보안 위협을 대처하기 위해 만들어졌다. 클라우드 시스템의 특성상 다양한 종류의 ID 관리 시스템들이 사용될 것으로 예상되어 본 과제는 이러한 환경에서 상호호환성을 제공하는 것으로 목적으로 요구사항 및 사용 시나리오를 도출하는 작업을 진행하고 있다.

이중 XRI는 인터넷 규모의 URI 기반 추상화된 ID를 정의하는 명세와 XRI 데이터 공유를 위한 조율 프로토콜, 도메인 상호간에 자원 공유 등을 명세하고 있음. 또한 XDI는 XRI에 기반을 둔 dataweb 구축을 목표로 인터넷 규모의 멀티 도메인들 간에 XRI와 XDI 기본 스키마에 기반을 둔 XML 도큐먼트를 상호간에 서로 공유하고 링킹, 동기화하는 표준화를 제안하고 있음.

4.4 IETF

IETF에서 개발된 표준 중 ID 관리와 연관된 RFC들로는 자원이나 개체 식별을 위한 RFC3986 (Uniform Resource Identifier), URI를 포함하는 식별자에 대한 표준들인 RFC3987 (Internationalized Resource Identifier), RFC2822 (Internet Message Format), RFC2141 (Uniform Resource Name), RFC4122 (Universally Unique Identifier(UUID) URN Namespace), RFC-4474 (Enhancements for Authenticated Identity Management in the Session Initiation Protocol), RFC4484 (Trait-Based Authorization Requirements for the Session Initiation Protocol) 등이 있다. IETF는 주로 인터넷 프로토콜 관련 보안 기술들을 주로 표준화하는 단체로 ID 관리 관련해서는 주로 식별자나 개별 프로토콜 기술의 표준화로 기여를 하고 있다.

V. 결 론

본 논문에서는 현재 국제표준화 기구들에서 진행되고 있는 ID 관리 기술의 표준화 동향을 고찰해 보았다. ID 관리 표준화는 개별적으로 보안기술 표준으로 주로 산업체의 요구사항을 만족하기 위해 산업표준으로 진행되었고 2005년 이후 ISO에서 ID 관리라는 제목으로 국제표준화를 진행하였다. ISO에서 진행된 ID 관리 표준은 단일 도메인 내에서 ID 관리 서비스를 제공하는 기술에 초점이 맞추어져 있어 다중 도메인에서 서로 다른 ID 관리 시스템들 간의 상호호환성을 필요로 하는 요구사항을 만족하지는 못하고 있다.

ITU-T SG17 Q.10은 2004~2008년 회기에는 Q.6 (사이버보안)로 주로 사이버 보안 기술에 대한 표준화 개발에 주력하였다. 하지만 2006년 말에 SG17에서는 ID 관리 포커스 그룹(Focus Group on IdM)을 결성하여 본격적으로 이 분야의 표준 개발을 시작하였다. 현재 ITU-T에서는 ID 관리 기술 관련하여 기존의 ID 관리 시스템들 간의 상호호환성을 제공하려는 기술에 초점이 맞추어 표준이 개발되고 있고 사용자의 개인정보를 공유할 시에는 사용자 중심의 프라이버시 기술을 제공하는 방향으로 진행되고 있다.

기타 표준기구들에서도 다양한 ID 관리 기술들의 표준화가 진행되고 있지만 아직까지는 ISO와 ITU-T 국제표준으로는 가장 영향력을 행사하고 있다. 하지만 ID 관리 기술의 경우 다분히 산업체에서 비즈니스의 요구사항에 맞추어 기술이 개발되고 나중에 표준화되는 경향이 있어 Kantara Initiative의 움직임에도 주목할 필요가 있다.

참 고 문 헌

[1] ITU-T Recommendation X.1250, "Baseline capabilities for enhanced global identity management and interoperability," ITU-T SG17, September 2009.

[2] ITU-T Recommendation X.1251, "A Framework for User Control of Digital Identity," ITU-T SG17, September 2009.

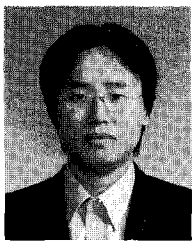
[3] ITU-T Recommendation X.1252, "Baseline Identity Management Terms and Definitions," ITU-T SG17, April 2010.

[4] Sangrae Cho, "Revised text of draft Recommendation ITU-T X.idmsg: Security guidelines for identity management systems," ITU-T SG17, TD1324, December 2010.

[5] Sangrae Cho, "Revised text of draft Recommendation ITU-T X.mob-id: Baseline capabilities and mechanisms of IdM for mobile applications and environment," ITU-T SG17, TD1351, December 2010.

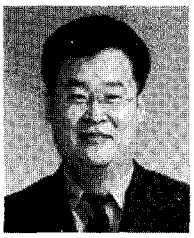
[6] Erika McCallister, "Text for ITU-T Recommendation X.eaa | ISO/IEC 2nd CD29115 - Information technology - Security techniques - Entity authentication assurance framework," ISO/IEC JTC 1/SC 27/WG 5 N59230, December 2010.

〈著者紹介〉



조 상 래 (Sangrae Cho)
정회원
1996년 8월 : Imperial College London 전산학과 졸업
1997년 9월 : Royal Holloway, University of London 정보보안 석사
1997.10 ~ 1999.7 : LG종합기술원
1997년 7월~현재 : 한국전자통신연구원 선임연구원
2009년 1월~현재 : ITU-T SG17 Q.10 Editor
관심분야 : 정보보호, ID 관리, 인증 및 인가 분야

노 종 혁 (Jong-Hyuk Roh)
정회원
1996년 2월 : 인하대학교 컴퓨터공학과 학사
1998년 2월 : 인하대학교 컴퓨터공학과 석사
2006년 8월 : 인하대학교 컴퓨터공학 박사
2000년 12월~현재 한국전자통신연구원 선임연구원
관심분야 : 정보보호, 프라이버시 보호기술, 네트워크 보안 기술, 인증/인가 기술



진 승 헌 (Jin Seung-Hun)
정회원
1993년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 전산학(정보보호) 박사
1996년 4월 : (주)대우통신 종합연구소 연구원
1999년 5월 : (주)삼성전자 통신연구소 전임연구원
1999년 6월~현재 : 한국전자통신연구원 인증기술연구팀장
관심분야 : 정보보호(PKI, 인증/인가기술, 프라이버시 보호기술), 모바일 지불결제, 컴퓨터/네트워크 보안