情 報 保 護 學 會 誌
第21卷 第2號, 2011. 4

ITU-T SG17 ID 관리 국제표준화 동향 및 향후 전망

조 상 래*, 진 승 헌**

요 약

국제표준화기구 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 개발중에 있다. 본 논문에서는 Q.10에서 개발한 국제표준들과 개발 중에 있는 표준초안들에 대해 간단히 소개하고, 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.

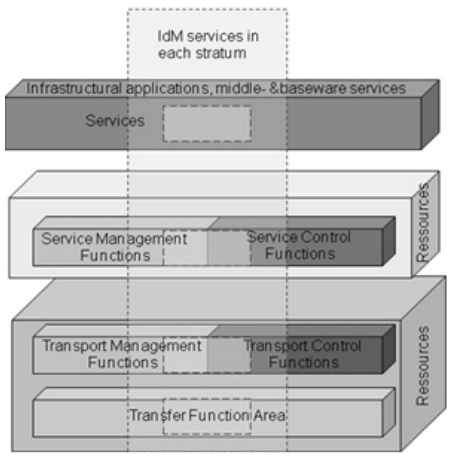
또한 휴대폰을 통해 온·오프라인 환경에서 다양한 서비스를 이용함에 따라 인증정보, 지불정보, 신분증, 정태적/동태적 개인정보, 선호정보 같은 모바일 ID 관리가 중요해지고 있다. 모바일ID는 휴대성, 이동성, 항시성, 오프라인 상호작용, 고부가가치 등 기존의 ID개념과는 차별되는 특성을 갖는다. 이에 따라 모바일ID보안 기술, 모바일ID사용기술, 모바일ID기반 서비스 기술 등 새로운ID 관리 기술이 요구되고 있다.

본 논문에서는 Q.10에서 개발한 국제표준들과 개발 중에 있는 표준초안들에 대해 간단히 소개하고, 향후 추진방향을 제시하고자 한다.

Ⅱ. ITU-T SG17 Q.10

본 절에서는 국제표준화기구인 ITU-T의 보안분과인 SG17에서 ID 관리 기술의 표준화를 담당하고 있는 Q.10의 활동에 대하여 소개하고자 한다.

2.1 X.1250



〔그림 1〕 ID 관리 네트워크 계층 상호호환 범위

본 표준은 글로벌 ID 관리 시스템 환경에서의 신뢰 및 상호호환성 기능(Baseline capabilities for enhanced

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

global identity management and interoperability)을 제공하기 위한 구조적인 요구사항을 정의하고 있다. 이것은 모든 통신, 제어 네트워크, 그리고 서비스에서 사용되는 디지털 아이덴티티(크리덴셜, 식별자, 속성자, 그리고 평판)에 대한 Assertion의 신뢰를 가능하게 한다.

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

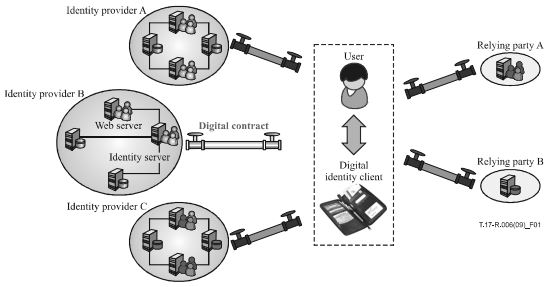
- 공통적이고 구조화된 ID 관리 모델 및 상호호환성이 있는 ID 관리 기능들.
- 모든 엔티티들에 대한 보증 레벨을 포함하는 크리덴셜, 식별자, 속성자, 그리고 패턴 ID 서비스의 준비.
- 신뢰받는 ID 제공자, 서비스 및 연계서비스 발견.
- 인가관리 시스템, ID 제공자 그리고 ID Bridge 제공자를 포함하는 연계서비스 제공자들 간의 상호호환성.
- 사용자 개인정보와 아이덴티티 자원의 보호를 포함하는 위험과 위협을 감소하는 보안 및 그외의 방법.
- 개인정보의 보호 및 정책 실행을 포함하는 감리 및 정책 부합.
- 사용성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

[그림 1]은 글로벌 ID 관리 시스템들간의 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.

2.2 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.



〔그림 2〕 디지털 아이덴터티 공유 모델

[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.

2.3 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 개발시에 활용할 목적으로 2010년 4월에 표준으로 제정되었다. 본 표준은 X.1250과 X.1251을 개발하는 과정중에 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.

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. 몇가지 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

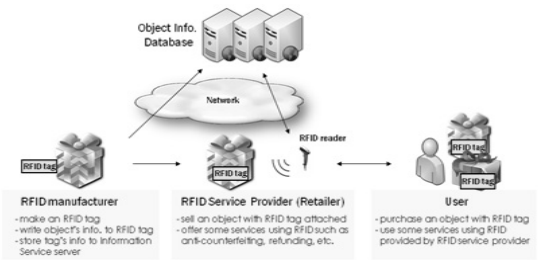
환경과는 독립적으로 만들어졌고 따라서 어떠한 아이덴터티 관리 작업에도 기본적인 정의로 사용될 수 있다. 특정한 경우 또는 문맥에서는 본 표준에서 제공하는 정의보다 좀 더 자세하게 용어가 정의되는 것이 필요한 경우도 있다는 것을 유념하여 사용해야 한다.

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.

2.4 X.1275

본 표준은 RFID를 이용한 응용에서 사용자의 개인정보를 보호하기 위한 지침(Guidelines on protection of personally identifiable information in the application of RFID technology)으로 2010년 12월에 표준으로 제정되었다. 본 표준은 RFID 이용시 사용자의 프라이버시를 보호하기 위한 지침으로 한국인터넷진흥원을 중심으로 프라이버시 문제에 민감한 유럽국가들이 활발히 참여하여 표준을 개발하였다. 본 표준은 ID 관리 보다는 개인정보보호 측면이 많이 부각되어 진해되었고 향후 NFC를 이용한 모바일 응용서비스에서도 개인정보보호 지침으로 사용될 수 있을것으로 기대된다.

[그림 3]은 소규모 상점등의 응용에서 사용되는 RFID의 사용 예를 보여주고 있다.



〔그림 3〕 소규모 상점에서의 RFID 사용 예

2.5 X.1261

본 표준은 인증서 확장 검증 프레임워크(Extended validation certificate framework) 기술로 2010년 12월에 표준으로 채택(Determined)되어 현재 표준승인 절차에 있다. 웹 사이트를 운영하는 법적 실체(legal entity)에 대한 신원확인을 제공하고 그 사이트와 암호화된 통신을 가능케 하는 확장된 검증 인증서 프레임워크를 제안하고 있다. 표준 개발은 미국이 주도적으로 하고 있으며, CA 브라우저 포럼의 규격을 ITU-T 권고로 옮기는 표준으로 현재 일부 국내 인증기관도 이 인증서 규격을 이용해 인증서를 제공하고 있다.

본 표준의 주요 목적은 첫 번째로 웹이나 서비스를 제공하는 사이트의 법인을 식별하는 것이고 두 번째는 해당 사이트와 암호화 통신을 가능하게 하고 마지막으로 법인과의 신뢰관계 구축으로 사이버보안을 강화하여 피싱이나 악성코드 같은 위협으로부터 사용자를 보호하는 것이다.

2.6 X.idmsg

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

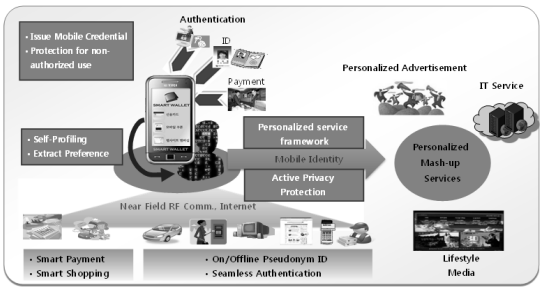
표준은 ID 관리 시스템에 대한 다양한 보안 위협들을 먼저 파악하고 이에 대한 대비책을 마련하는 것으로 시작한다. ID 관리 시스템의 보안 지침은 크게 시스템이 설치될 때, 운영될 때로 나누어진다. 시스템 설치시에는 주로 사전에 설치되거나 운영되어야할 보안 해결책들이 제시되고 운영시에는 실제 서비스를 제공할 때 필요한 보안 기술들에 대해 기술하고 있다.

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.

2.7 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 환경

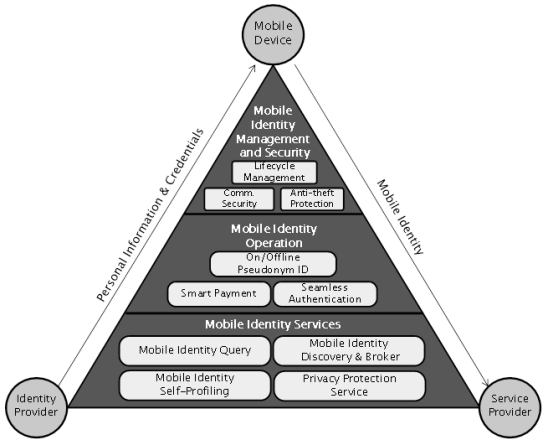
에서 사용자의 개인정보를 효율적이고 안전하게 관리하는 프레임워크(Baseline capabilities and mechanisms of identity management for mobile applications and environment)를 한국전통신연구원 주도하에 개발되고 있다. 모바일 ID 관리 프레임워크는 인증, 인가, 개인정보 프로파일링 기술을 바탕으로 스마트 지불, 온오프라인 인증, 모바일 출입증과 같은 다양한 분야에서 사용될 수 있는 기술을 담고 있다.



〔그림 4〕 모바일 아이덴터티 관리 서비스 개념도

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 프로파일링되어 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, H/W)로서 모바일 아이덴터티의 보안과 프라이버시 강화, 안전하고 편리한 사용 및 고부가 아이덴터티 기반 서비스 개발을 위한 퍼스널 모바일 아이덴터티 플랫폼이다. [그림 4]는 모바일 아이덴터티 관리 서비스 개념도를 보여준다.

[그림 5]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



〔그림 5〕 프레임워크 구성도

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.

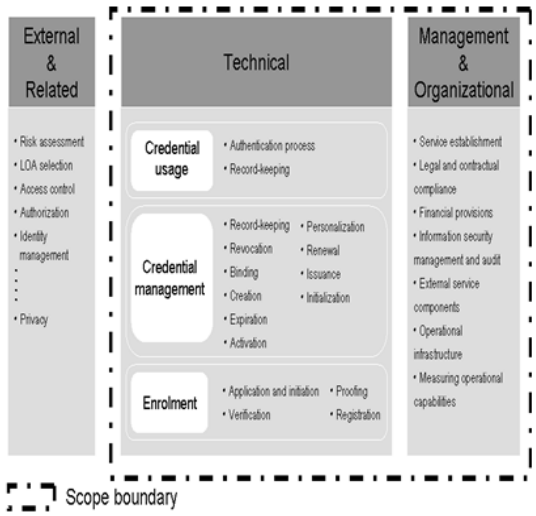
본 표준은 모바일 아이덴터티 관리 프레임워크를 정의하여 향후 스마트폰에서 동작하는 다양한 모바일 어플리케이션에 제공될 모바일 아이덴터티 관리, 인증, 프라이버시 기능 및 사용자 인터페이스를 정의하여 모바일 아이덴터티 침해와 분실 도난으로 인한 도용 및 프라이버시 침해를 줄일 수 있고 인증, 지불, 개인정보 기반 서비스를 지원하여 보다 원활한 모바일 인터넷 서비스를 가능하게 한다

2.8 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. 현재 본 과제를 미국에서 주도적으로 추진하고

있으며 ISO JTC1 SC27과 공동으로 표준을 추진하여 표준이 제정될 경우 인증 분야에서 상당한 영향력이 있을것으로 예상된다.

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 정의한다. 또한, 인증 위협을 완화하기 위해 사용될 수 있는 통제와 다른 인증에 대한 보증 스킴과 보증 레벨을 매칭시키기 위한 가이드를 제공하며, 4개 보증레벨에 기반한 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.



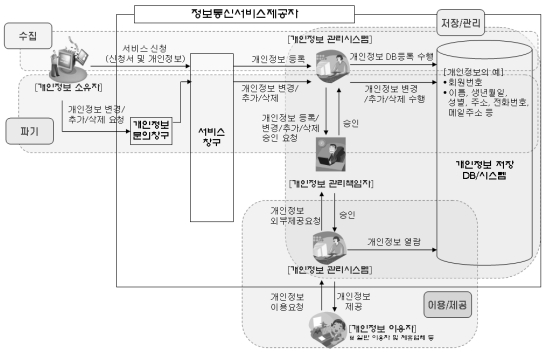
〔그림 6〕 개체 인증 보증 프레임워크 구성도

[그림 6]은 개체 인증 보증 프레임워크의 구성도를 보여준다.

2.9 X.priva

한국인터넷진흥원에서 개발하고 있는 표준초안으로 개인정보보호 수준 정의를 위한 공통 항목(Criteria for assessing the level of protection for personally identifiable information in identity management)을 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. 단, 본 표준은 개인정보보호 수준을 정의하기 위한 기본적인 항목만을 제시하며, 실제 이를 적용하여 개인정보보호 수준을 평가하는 구체적인 방법론은 기업 및 기관에 따라 각기 다를 수 있기 때문에 본 표준에서 제외한다.



〔그림 7〕 개인정보 생명주기 모델

[그림 7]은 정보통신 서비스 제공자가 개인정보 소유자의 개인정보를 수집하고, 이를 저장 및 관리하며 제휴업체 등과 같은 개인정보 이용자에게 고객의 개인정보를 제공하는 개인정보 생명주기에 따른 일련의 개인정보 처리 흐름이다.

본 표준은 기업 및 기관 스스로 자사의 개인정보보호 수준을 평가해보고, 이를 통해 개인정보보호 수준을 강화함으로써 개인정보 침해사고로 인한 사회적·경제적 피해를 감소시키는데 기여할 수 있을 것으로 기대한다.

2.10 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 framework 은 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 이용시에도 별도의 인증없이 접급할 수 있는 기술을 표준화한다. 네크워크 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.

Ⅲ. 기타 국제 표준화 동향

본 장에서는 ITU-T를 제외한 다른 국제 표준화 기구들의 동향을 살펴본다. ITU-T와 동급으로 간주되는 ISO의 ID 관리 기술 동향을 알아보고 산업계 표준 기구인 Kantara Initiative에 대해서도 간략하게 소개한다.

3.1 ISO

ISO는 JTC 1/SC27/WG5에서 ID 관리 프레임워크 국제표준 개발을 진행중에 있으며, ID 관리 프레임워크 개발을 위해 선행되어야 할 작업으로 ID 온톨로지 정의를 들고 있다. ID 온톨로지는 실제적인 ID 관리에 필요한 용어와 개념 공유를 위해 필수적이며, ID 관리 프레임워크 이용자에게 ID 관리와 관련된 일관성 시각을 제공하는 한편 서로 상이하거나 연관된 목적을 가진 다른 사용자와의 협력을 가능하게 하는 중요한 역할을 담당하고 있는 단일 도메인에서 사용하는 가장 기본적인 ID 관리시스템의 프레임워크에 대한 표준을 개발하고 있다. 현재 앞에서 언급한 'Entity Authentication Assurance'의 표준 같은 경우 ITU-T와 함께 ID 관리 과정에서 요구되는 객체에 대한 인증 및 보증을 위한 프레임워크와 인증에 영향을 미칠 수 있는 요소들에 대한 기준, 위협 등을 정의하는 작업을 수행하고 있다.

3.2 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.

Ⅳ. 결 론

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. SG17 중심으로 ID 관리 포커스 그룹을 시작할 당시에는 이미 산업계에서는 다양한 ID 관리 기술들이 활발하게 사용되고 있어서 국제표준으로 추진하기에는 때 늦어 감이 없지 않았다. 하지만 당시 포커스 그룹에서는 다양한 ID 관리 시스템들이 존재하지만 이 시스템들 간의 상호호환성이 부재하여 서비스 연동이 힘든 점에 주목하여 글로벌 ID 관리 상호호환성 기술 표준으로 방향을 잡아 지금까지 국제표준을 선도하고 있다.

Q.6에서 Q.10으로 변경되면서 ID 관리 기술만을 중점적으로 연구하게 되어 현재는 다양한 ID 관리 분야의 표준들이 제정되고 개발되고 있다. 현재 ID 관리 분야는 하나의 큰 우산 아래 다양한 표준들이 모여 하나의 거대한 생태계를 이루고 이 안에서 상호연동하여 사용자에게 다양한 ID 관리 서비스를 제공하는 것을 목적으로 표준화가 추진될 예정이다.

참고문헌

[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] ITU-T Recommendation X.1275, “Guideline on protection of personally identifiable information in the application of RFID technology”, ITU-T SG17, December 2010.

[5] Anthony M. Rutkowski, “Draft New Rec. ITU-T X.1261 (X.EVcert), Extended validation certificate (EVcert) framework for determination”, ITU-T SG17, TD1170Rev.3, December 2010.

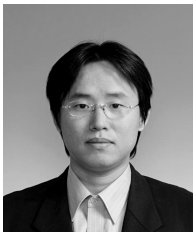
[6] Sangrae Cho, "Revised text of draft Recommendation ITU-T X.idmsg: Security guidelines for identity management systems". ITU-T SG17, TD1324, December 2010.

[7] 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.

[8] 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.

[9] Hyangjin Lee, Inkyoung Jeun, "Revised draft text of X.priva : Criteria for assessing the level of protection for personally identifiable information in IdM", ITU-T SG17, TD0640, September 2009.

〈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

진 승 헌(Jin Seung-Hun)
정회원
1993년 2월 : 숭실대학교 전자계산학과 졸업
1995년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과(정보보호) 박사
1994년 12월~1996.4월 : (주)대우통신 종합연구소 연구원
1996년 5월~1999년 5월 : (주)삼성전자 통신연구소 전임연구원
1999년 6월~현재 : 한국전자통신연구원 인증기술연구팀 팀장
관심분야 : 인증, ID관리, 개인정보보호, 모바일 지불결제, 정보보호