신원 인증 공유를 위한 동적 신뢰 프레임워크

박승철*

A Dynamic Trust Framework for Sharing Identity Authentication

Seung-chul Park*

이 논문은 2012년도 한국기술교육대학교 연구비를 지원받았음

요 약

인터넷 환경에서 신원 인증 서비스를 제공하는 신원 제공자의 신원 인증 결과를 다수의 서비스 제공자가 공유하는 신원 인증 공유는, 반복적인 등록 회피와 싱글 사인온을 통한 사용자 편의성 제고, 신원 제공자로부터의 신원 인증 서비스 아웃소싱을 통한 서비스 제공자의 비용 절감, 그리고 제한된 수의 통제된 신원 제공자에게 한정된 신원 정보 노출을 통한 프라이버시 보호 등의 측면에서 몇 가지 중요한 장점을 제공한다. 그러나 신원 인증 공유 기술이 글로벌 인터넷 차원에서 광범위하게 적용되기 위해서는 신원 제공자, 서비스 제공자, 그리고 사용자간에 신원 인증과 관련된 신뢰 문제가 선결되어야 한다. 본 논문은 신원 인증 공유를 위한 신뢰 프레임워크의 현황을 분석하고, 분석 결과를 바탕으로 신원 인증 공유를 위한 동적인 개방형 신뢰 프레임워크를 제시한다.

ABSTRACT

Identity authentication sharing technology which allows many service providers to share the result of identity authentication of an identity provider provides several important advantages including high usability achieved by avoiding repeated registration of identity information to service providers and single sign-on, cost effectiveness of service providers achieved by outsourcing identity authentication services from identity providers, and privacy protection achieved by exposing identity information only to a limited number of controlled identity providers. However, in order for the identity authentication sharing technologies to be widely deployed in global Internet scale, the trustworthiness issue among the participating identity providers, service providers, and users should be resolved in advance. This paper firstly analyzes existing trust frameworks for identity authentication sharing. And then, based on the result of analysis, this paper proposes a dynamic and open trust framework for identity authentication sharing.

키워드

신원 관리, 인증 공유, 인증 보증, 신뢰 프레임워크

Key word

identity management, authentication sharing, authentication assurance, trust framework

* 정회원 : 한국기술교육대학교(scpark@koreatech.ac.kr)

접수일자 : 2012. 08. 10
심사완료일자 : 2012. 09. 12

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.10.2199

Ⅰ. 서 론

현재의 인터넷 신원 인증 환경에서는 각 서비스 제공자(service provider)가 자신의 사용자들을 위해 별도의 신원 인증 시스템을 구축하여 운용하고, 사용자는 각 서비스 제공자의 신원 인증 시스템에 신원 정보를 제공하고, 신원 증명 정보를 발급받고, 유지하고, 사용한다. 인터넷 기반의 서비스가 다양해짐에 따라 이러한 고립형 인증(isolated authentication) 환경의 사용자는 더 많은 수의 서로 다른 인증 시스템을 사용할 수밖에 없게 된다. 따라서 사용자는 많은 수의 신원 증명 정보(예, 사용자 ID/패스워드, 공인 인증서, PIN(Personal Identification Number), 일회용 패스워드 장치 등)를 관리해야 하고, 사용자의 신원 정보는 점점 많은 수의 서비스 제공자에게 노출될 수밖에 없다[1,2,3]. 그럼에도 불구하고 사용자가 서비스 제공자가 자신의 신원 정보를 어떻게 관리하고 있는 지 확인하고 검증하는 것은 여전히 매우 어렵다. 또한 서비스 제공자의 수가 너무 많고 서비스 제공자의 기술적 수준에 차이가 크기 때문에, 서비스 제공자에 대해 개인 정보 보호 관리 수준을 공인(certification)하는 신뢰 서비스(trust service) 제도를 일괄적으로 도입하는 것도 쉬운 일이 아니다.

이러한 문제들을 해결하기 위한 방편으로 지난 몇 년 동안 OpenID[4], Information Card/IMI[5,6], SAML[7] 등과 같은 신원 인증 공유(identity authentication sharing) 기술 개발이 활발히 진행되어 왔다. 신원 인증 공유 기술은 그림 1에서 보는 바와 같이 특정 신원 제공자(IdP - Identity Provider)의 사용자 ID(user identifier)와 신원 증명 정보(credential) 등 신원 정보를 이용한 사용자 인증 결과를 다수의 서비스 제공자(SP - Service Provider)가 공유할 수 있게 한다. 필요한 경우 신원 제공자에 저장된 사용자의 다른 신원 정보들이 서비스 제공자들에 의해 공유될 수도 있다. 신원 인증 공유 환경에서 인터넷 사용자는 자신의 신원 정보(identity information)를 신뢰할 수 있는 신원 제공자에게 등록하고, 해당 신원 제공자가 발급하는 신원 증명 정보만 관리하면 된다. 따라서 신원 인증 공유 기술은 접근하고자 하는 모든 서비스 제공자에게 신원 정보를 반복적으로 등록하고 각 서비스 제공자가 발급하는 신원 증명 정보를 관리해야 하는 현재의 고립형 인증 환경의 불편함으로부터 벗어날 수 있게 하고, 사용자의 신원 정보가 많은 수의 서비스 제공자 대신 제한된 수의 신원 제공자에게만 노출되어 개인 정보 침해 발생 가능성을 줄인다.

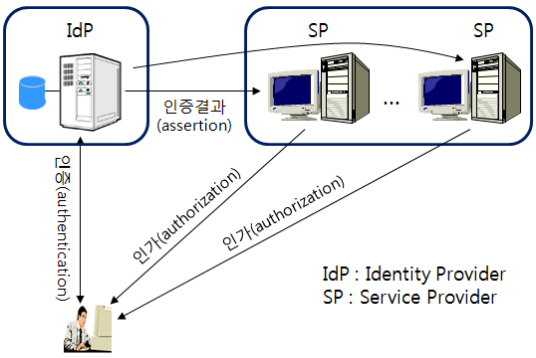

그림 1. 신원 인증 공유 모델
Fig. 1 identity authentication sharing model

또한, 싱글 사인온(SSO - Single Sign-On) 기반의 신원 인증 공유 환경에서 사용자가 인증 제공자에 한번 인증하면, 다른 서비스 제공자를 접근할 때 신원 제공자는 해당 사용자의 인증 결과를 서비스 제공자에게 전달함으로써 서비스 제공자의 추가적인 인증을 불필요하게 하고, 따라서 고립형 인증 모델의 반복적인 로그인과 로그아웃의 불편함을 해소한다. 그리고 신원 인증 공유 환경에서 서비스 제공자는 복잡한 인증 서비스와 신원 정보 관리 서비스를 신원 제공자로부터 아웃소싱(outsourcing)함으로써 자체적인 신원 인증 시스템의 개발과 유지.관리 부담으로부터 벗어날 수 있다. 신원 제공자는 사용자와 서비스 제공자가 신뢰할 수 있는 인증 서비스를 효과적으로 제공함으로써 많은 수의 사용자와 서비스 제공자를 고객으로 유치할 수 있고, 서비스 제공자에 대한 인증 수준과 사용자 수에 따른 신원 인증 비용 부과를 포함하는 다양한 비즈니스 모델을 개발할 수 있을 것이다[3,8,9].

이러한 여러 가지 중요한 장점에도 불구하고 신원 인증 공유 기술이 실제 인터넷 환경에서 광범위하게 적용되기 위해서는, 신원 인증 공유에 참여하는 신원 제공자, 서비스 제공자, 그리고 사용자간에 상호 신뢰 문제가 선결되어야 한다. 서비스 제공자는 신원 제공자의 신원 인증 보증 수준(level of assurance for identity authentication)을 신뢰할 수 있어야 하고, 사용자는 신원 제공자의 신원

정보 보호에 대해 신뢰할 수 있어야 한다. 본 논문은 신원 인증 공유를 위한 기존의 신뢰 프레임워크들에 대해 분석하고, 그 결과를 바탕으로 새로운 동적인 개방형 신뢰 프레임워크(dynamic and open trust framework)를 제시한다. 본 논문이 제안하는 신뢰 프레임워크는 글로벌 인터넷과 다양한 인터넷 서비스를 고려하여 높은 확장성(scalability)와 서비스 유연성(flexibility)을 가지도록 설계되었다.

Ⅱ. 신원 인증 공유를 위한 신뢰 프레임워크 관련 연구

최근 몇 년 동안 OpenID, Information Card/IMI(Identity Metasystem Interoperability), SAML(Security Assertion Markup Language) 등과 같은 신원 인증 공유를 위한 통신 프로토콜은 다양한 형태로 지속적으로 발전되어 온 반면, 신원 인증 공유에 참여하는 주체들(사용자, 신원 제공자, 서비스 제공자)간의 신뢰 서비스를 제공하기 위한 인프라스트럭처 구축은 아직 미흡한 상태에 있다. 본 논문은 신원 인증 공유를 위해 지금까지 개발된 대표적인 신뢰 프레임워크를 중앙집중형 신뢰 프레임워크(centralized trust framework), 폐쇄형 분산 신뢰 프레임워크(closed and distributed trust framework), 그리고 개방형 분산 신뢰 프레임워크(open and distributed trust framework)로 구분하여 분석한다.

2.1. 중앙집중형 신뢰 프레임워크

신원 인증 공유를 위한 중앙집중형 신뢰 프레임워크는 마이크로소프트에서 개발한 Passport와 그 후속 모델인 LiveID 등에서 채택되었다[10,11]. Passport/LiveID에서는 사용자의 모든 인증 정보가 마이크로소프트에 의해 관리되는 Passport 서버에 등록되고, 유지되고, 관리된다. 그리고 사용자가 서비스 제공자에 로그온하고자 하는 경우, 해당 사용자에 대한 신원 인증 요구는 사용자의 웹 브라우저(UA - User Agent)를 경유하여 Passport 서버에게 전달되고, 모든 인증 서비스는 Passport 서버에 의해 통합적으로 제공된다. Passport/LiveID 시스템에서 사용자와 서비스 제공자(SP)는 전적으로 중앙의 Passport 서버를 신뢰한다. 그리고 Passport 서버 운영 주체는 자체적인 신원 인증 공유 정책을 설정하고(policy maker)과 신뢰 프레임워크(trust framework)를 수립하고, 이 정책과 신뢰 프레임워크에 동의하는 서비스 제공자를 대상으로 서비스 제공자와 맺은 계약(agreement)에 따라 신원 인증 공유 서비스를 제공한다. 따라서 Passport/LiveID 시스템에서 중앙의 Passport 서버와 관리 주체는 그림 2와 같이 인증 정책 결정자(policy maker), 신뢰 프레임워크 제공자(trust framework provider), 그리고 신원 제공자 역할을 동시에 수행하게 된다.

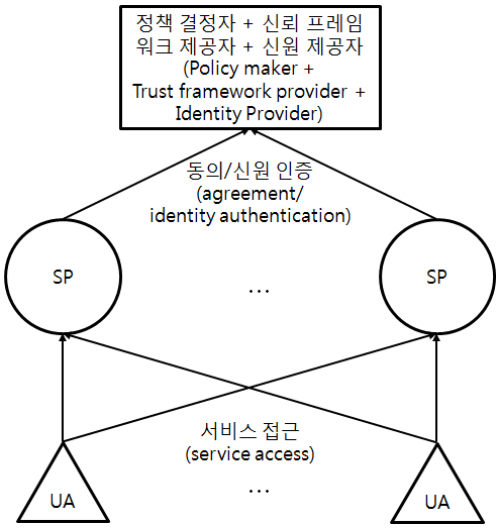

그림 2. 중앙집중형 신뢰 프레임워크
Fig. 2 centralized trust framework

2.2. 폐쇄형 분산 신뢰 프레임워크

Liberty Alliance[12,13] 등은 그림 3과 같이 서비스 제공자(SP)들이 상호 신뢰할 수 있는 다수의 신원 제공자(IdP)들과 함께 하나의 신뢰 동아리(CoT - Circle of Trust)를 형성하는 폐쇄형 분산 신뢰 프레임워크를 채택하였다. 고등교육기관 연합, 관계 회사 그룹, 특정 서비스를 담당하는 정부 기관 등과 같이 동일한 신원 인증 정책을 공유하고 상호 신뢰할 수 있는 그룹은 누구나 신뢰 동아리가 될 수 있다. 신뢰 동아리를 주도하는 특정 기관은 신뢰 동아리의 신원 인증 정책에 동의하고, 해당 동아리가 요구하는 신원 인증 보증 수준을 만족시킬 능력이 있고, 또한 신뢰할 수 있는 다수의 기관을 신원 제공자(IdP)로 지정 또는 공인한다. 사용자는 웹 브라우저와 같은 사

용자 에이전트(UA)를 통하여 신뢰 동아리 내의 신원 제공자들의 일부 또는 전부를 선택하여 자신의 신원 정보를 등록하고, 신원 증명 정보(예, 사용자 ID/패스워드, 공인 인증서 등)를 발급받는다.

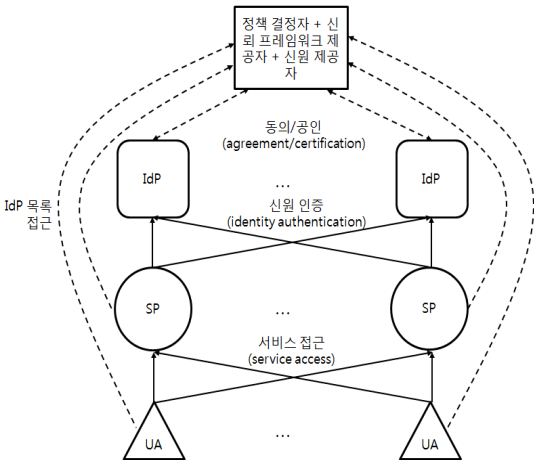

그림 3. 폐쇄형 분산 신뢰 프레임워크
Fig. 3 closed and distributed trust framework

특정 신뢰 동아리의 신원 인증 정책에 동의하고 동아리 주도기관을 신뢰하는 서비스 제공자(SP)는 신뢰 동아리 내의 일부 또는 전부의 신원 제공자의 신원 인증 결과를 공유한다. 서비스 제공자는 특정 사용자에 대해 자신이 신원 인증 결과를 공유하는 신원 제공자의 목록을 제공함으로써 사용자가 인증을 수행할 신원 제공자를 선택할 수 있다. Liberty Alliance에 의해 주로 개발되고 OASIS[14]에 의해 표준화된 SAML은 폐쇄형 분산 신뢰 프레임워크 기반으로 동작하는 대표적인 신원 인증 공유 프로토콜이다. 즉, SAML 공유 인증에서 서비스 제공자(SP)는 신원 제공자(IdP)의 사용자 인증 결과 주장을 담은 어써션(assertion)을 전적으로 신뢰한다는 것을 전제로 동작한다. SAML 기반의 대표적인 신뢰 동아리 그룹은 미국의 대학교 중심의 InCommon[15]이다.

2.3. 개방형 분산 신뢰 프레임워크

개방형 분산 신뢰 프레임워크는 2010년 OIX(Open Identity Exchange)[16]의 도움을 받아 미국 정부의 ICAM(Identity, Credential, and Access Management) 위원회에서 처음 그 개념이 제시되었다[17,18]. 그림 4는 기존의 개방형 분산 신뢰 프레임워크 모델을 보여준다.

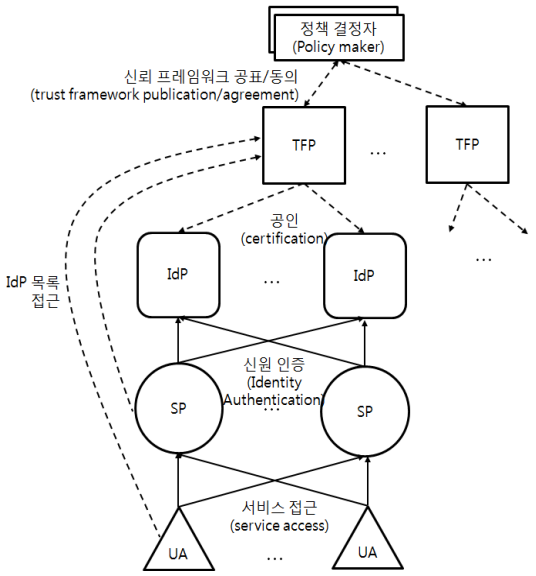

그림 4. 개방형 분산 신뢰 프레임워크
Fig. 4 open and distributed trust framework

개방형 분산 신뢰 프레임워크의 가장 큰 특징은 특정 신원 인증 정책 결정자(예, 정부, 통신 사업자 연합회, 은행 연합회, 대학교 연합회 등)가 자신의 신원 인증 정책에 맞는 신뢰 프레임워크를 공표(publication)한다는 것이다. 서로 다른 정책 결정자는 서로 다른 신뢰 프레임워크를 공표할 수 있다. 공표된 신뢰 프레임워크에 따라 신원 인증 보장 수준(LoA - Level of Assurance for identity authentication) 공인 등의 신뢰 서비스를 제공할 수 있는 기관은 누구나 정책 결정자에 의해 신뢰 프레임워크 제공자(TFP - Trust Framework Provider)로 인정받을 수 있다.

특정 신뢰 프레임워크 제공자(TFP)는 정책 결정자를 대신하여 신원 제공자(IdP)에 대해 신원 인증 보장 수준을 공인하고, 공인된 신원 제공자 정보를 서비스 제공자(SP)와 사용자 에이전트(UA)에게 제공한다. 2012년 현재 미국 정부의 ICAM 위원회에 의해 인정된 신뢰 프레임워크 제공자는 OIX, InCommon, 그리고 Kantara Initiative[19]이다.

특정 신원 제공자는 해당 정책 결정자가 인정한 신뢰 프레임워크 제공자로부터 특정 정책 결정자가 제시하는 특정 신원 인증 보장 수준을 공인받고, 공인된 신원 인증 서비스를 사용자 에이전트와 서비스 제공자들에게 제공한다. 사용자 에이전트와 서비스 제공자는 신뢰 프레임워크 제공자들을 접근하여 공인된 신원 제공자 목록을 다운로드할 수 있고, 공인된 신원 제공자로부터 신원 인증 서비스를 제공받는다.

Ⅲ. 신원 인증 공유를 위한 개방형 동적 신뢰 프레임워크 제안

그림 5는 본 논문이 제안하는 개방형 동적 신뢰 모델을 보이고 있다. 제안된 동적 신뢰 모델에서 특정 정책 결정자의 신뢰 프레임워크를 집행하는 신뢰 프레임워크 제공자(TFP)들은 하나의 신뢰 제공자 네트워크(TFPNET – Trust Framework Provider NETwork)를 형성하고, 신뢰 프레임워크 제공자들은 이 TFPNET를 통하여 자신의 신원 제공자(IdP) 공인 정보를 상호 공유한다. 신원 제공자 정보 공유 방법은 TFPNET 구현에 따라 다를 수 있다. 예를 들면 다수의 신뢰 프레임워크 제공자들이 신원 제공자 정보를 유지하고 관리하기 위한 하나의 서버를 공유할 수도 있고, 각각 자신의 서버의 정보를 상호 공유할 수도 있을 것이다.

특정 정책 결정자는 다른 정책 결정자와의 합의에 의해 신뢰 프레임워크를 상호 신뢰하는 연방화(federation)를 실현할 수 있다. 이 경우 특정 정책 결정자의 TFPNET은 다른 정책 결정자의 TFPNET와 연동되어 상호 신뢰 서비스를 공유할 수 있다. 사용자 에이전트(UA)와 서비스 제공자(SP)는 LCSP(LoA Certificate Status Protocol)을 통하여 TFPNET의 신뢰 프레임워크 제공자(TFP)들이 제공하는 신뢰 서비스를 필요할 때 마다 언제든지 접근할 수 있다.

사용자 에이전트(UA)와 서비스 제공자(SP)는 LCSP를 통하여 특정 신원 인증 보증 수준(LoA)의 공인 신원 제공자 목록을 확인할 수 있고, 특정 신원 제공자의 공인 상태를 확인할 수 있다. 뿐만 아니라, LCSP는 연방화를 통해 연동된 다른 TFPNET의 신뢰 서비스에 대한 접근도 가능하게 함으로써, 서로 다른 정책 결정자의 TFPNET간의 상호 연동성(interoperability) 실현의 핵심 수단 역할을 수행한다.

TFPNET(연방화된 TFPNET 포함)은 다양한 정책 결정자에 따라 다수가 존재할 수 있으며, 어떤 TFPNET을 선택할 것인지는 전적으로 사용자와 서비스 제공자에게 달린 문제이다.

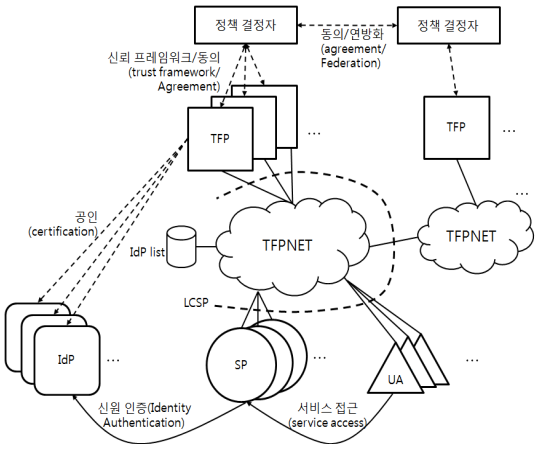

그림 5. 개방형 동적 분산 신뢰 프레임워크
Fig. 5 open, dynamic and distributed trust framework

그림 6은 제안된 개방형 동적 분산 신뢰 프레임워크의 신뢰 서비스 제공 시나리오를 개략적으로 보여주고 있다. 개방형 동적 분산 신뢰 프레임워크 환경에서 사용자는 사용자 에이전트(UA)를 통해 자신이 이용하고자 하는 신원 제공자(IdP)의 신원 인증 보증 수준(LoA)에 대한 정보를 요청한다.

이에 대해 신원 제공자는 자신이 지원하는 신원 인증 보증 수준 정보와 자신을 공인한 TFPNET에 대한 정보(LoA_Info_Respond(LoA, TFPNET))를 사용자 에이전트에게 응답한다. 사용자 에이전트는 해당 신원 제공자의 공인 상태를 해당 TFPNET을 통해 확인(verify)할 수 있다.

TFPNET을 통해 신원 제공자의 공인 상태를 확인한 사용자는 자신의 사용자 에이전트와 신원 제공자가 지원하는 신원 인증 공유 프로토콜(예, OpenID, Inforamtion Card/ IMI, SAML 등)을 사용하여 자신의 신원 정보를 해당 신원 제공자에 등록한다.

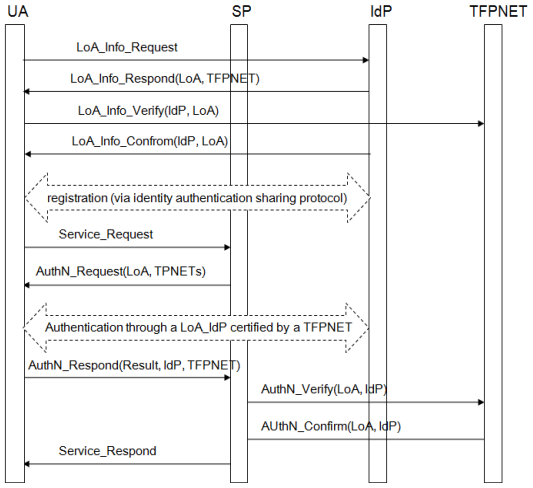

그림 6. 개방형 동적 분산 신뢰 프레임워크 동작 시나리오
Fig. 6 operation scenario of open, dynamic and distributed trust framework

사용자가 자신의 사용자 에이전트를 통해 특정 서비스 제공자(SP)의 서비스를 요청하면, 해당 서비스 제공자는 자신이 요구하는 신원 인증 보증 수준(LoA)과 자신이 신뢰하는 TFPNET에 대한 요구사항을 포함하는 인증 요구 메시지(AuthN_Request(LoA, TPNETs))를 사용자 에이전트에게 보냄으로써 신원 인증을 요구한다.

사용자 에이전트는 서비스 제공자의 신원 인증 요구사항을 만족시키는 신원 제공자를 선택하여 신원 인증 공유 프로토콜로 신원 인증을 수행하고, 인증 결과와 인증을 수행한 신원 제공자, 그리고 신원 제공자를 공인한 TFPNET 정보를 포함하는 신원 인증 응답 메시지(AuthN_Respond(Result, IdP, TFPNET))를 서비스 제공자에게 전달한다. 서비스 제공자는 신원 인증 결과 확인 후, TFPNET를 접근하여 인증을 수행한 신원 제공자의 신원 인증 보증 수준(LoA)에 대한 공인 상태를 확인함으로써 인증 결과에 대한 신뢰도를 판단하고, 최종적으로 사용자가 요구한 서비스를 응답하게 된다.

Ⅳ. 분석

표 1은 제안된 개방형 동적 신뢰 프레임워크의 특징을 기존 신뢰 프레임워크들과 비교하여 보이고 있다.

표 1. 신뢰 프레임워크 비교
Table. 1 comparison of trust frameworks

	프라이버시 보호	편의성	확장성	유연성
중앙집중형 신뢰 프레임워크 [10,11]]	low	very high	very low	low
폐쇄형 분산 신뢰 프레임워크 [7,12]	medium	medium	low	medium
개방형 분산 신뢰 프레임워크 [17,18]	high	low	medium	high
개방형 동적 신뢰 프레임워크	very high	high	very high	very high

중앙집중형 신뢰 프레임워크 기반의 Passport/Live ID 시스템은 마이크로소프트와 같은 잘 알려지고 충분한 정도의 신뢰도를 가진 하나의 기관을 신원 제공자로 채택한다는 측면에서 신뢰 구도가 간단하고 편리한 장점이 있다. 반면, 모든 사용자의 서비스 제공자 접근 동작이 마이크로소프트의 Passport 서버에 노출되는 데 따른 프라이버시 문제, 인터넷 서비스 제공자의 마이크로소프트에 대한 의존성 심화 문제, 그리고 중앙 서버의 확장성 문제, 그리고 하나의 신원 인증 서버에 의한 다양한 신원 인증 서비스 제공의 어려움으로 인한 유연성 부족 등으로 인해 개방형 환경에 적용되는 데는 어려움이 있다.

폐쇄형 분산 신뢰 프레임워크는 상호 신뢰 관계가 형성되어 있고, 유사한 수준의 신원 인증을 요구하는 특정 그룹내에서 비교적 쉽게 적용될 수 있다. 그러나 신뢰 관계가 사전에 형성되어 있지 않은 일반적인 글로벌 인터넷 환경에서 보편적으로 적용되기 어려워 확장성 측면에서 문제점이 있고, 신원 인증 요구 수준이 다른 다양한 서비스 환경에서 적용되기에도 어려움이 많아 여전히 서비스 유연성이 부족한 문제점이 있다.

기존의 개방형 분산 신뢰 프레임워크는 공인된 신원 제공자 정보를 신뢰 프레임워크 제공자(TFP)로부터 다운로드 형태로 접근한다는 측면에서 정적 신뢰 프레임워크(static trust framework)이다. 이와 같이 정적인 신뢰 프레임워크 환경에서는 서비스 제공자와 사용자 에이전트가 다양하고 많은 수의 신뢰 프레임워크 제공자(TFP)에 의해 공인되는 신원 제공자 정보를 적기에 파악하기 어렵다. 따라서 기존의 정적인 개방형 분산 신뢰 프레임워크를 글로벌 인터넷 환경으로 확장하는 데 어려움을 피할 수 없다. 개방형 분산 신뢰 프레임워크 환경에서 다양한 정책 결정자와 신뢰 프레임워크 제공자, 그리고 신원 제공자에 의해 다양한 신원 인증 서비스가 제공될 수 있지만, 사용자와 서비스 제공자가 자신의 요구사항에 맞는 신원 인증 보증 수준의 신원 제공자를 수작업 형태로 찾아야 한다는 측면에서 서비스 유연성에도 여전한 문제를 안고 있다.

본 논문이 제안한 개방형 동적 분산 신뢰 프레임워크는 신뢰 프레임워크 제공자(TFP)들의 신원 제공자 공인 정보를 TFPNET를 통하여 공유하게 하고, 사용자 에이전트와 서비스 제공자는 LCSP를 통하여 TFPNET의 모든 신뢰 프레임워크 제공자들이 제공하는 신원 제공자 정보를 원할 때 마다 동적으로 접근할 수 있게 한다. 따라서 신뢰 프레임워크 제공자(TFP)의 수가 많아지더라도 이들에 의해 공인되는 신원 제공자 정보를 사용자와 서비스 제공자가 적기에 파악하는 데 어려움이 없으므로 높은 확장성을 보장한다. 또한 사용자와 서비스 제공자가 자신의 요구사항에 맞는 신원 인증 보증 수준의 신원 제공자를 LCSP를 통해 TFPNET에서 쉽게 찾을 수 있으므로 서비스 유연성과 사용자 편의성을 동시에 높일 수 있다.

V. 결 론

신원 인증 공유 기술이 실 환경에서 적용되기 위해서는 신원 인증 공유에 참여하는 신원 제공자, 서비스 제공자, 그리고 사용자간에 상호 신뢰 문제가 선결되어야 한다. 그리고 신원 인증 공유 기술이 글로벌 인터넷 환경에서 광범위하게 적용되기 위해서는 충분한 확장성과 신뢰 서비스 유연성을 가진 신뢰 인프라스트럭처 구축이 요구된다.

본 논문은 기존의 개방형 분산 신뢰 프레임워크의 정적인 특성을 보완한 개방형 동적 신뢰 프레임워크를 제안하였다. 제안된 개방형 동적 신뢰 프레임워크의 확장성과 서비스 유연성, 그리고 편의성은 글로벌 인터넷 환경에서 개방형 신뢰 프레임워크 기반의 신원 인증 공유 기술의 본격적인 도입을 가능하게 할 것이다.

참고문헌

[1] A. Josang and S. Pope, “User Centric Identity Management”, AusCERT Conference, pp. 77-89, May 2005.

[2] FIDIS, “D3.17:identity Management Systems - recent developments”, www.fidis.net, August 2009.

[3] J. A. Grant, “The National Strategy for Trusted Identities in Cyberspace”, IEEE Internet Computing, pp. 80-84, November/December 2011.

[4] OpenID Foundation, ″OpenID Authentication 2.0 - Final″, http://openid.net/specs/openid-authentication-2_0.html, Dec. 2007.

[5] Craig Burton, ″The Information Card Ecosystem: The Fundamental Leap from Cookies & Passwords to Cards & Selectors″, ICF(http://www.informationcard.net), April 2009.

[6] OASIS, ″Identity Metasystem Interoperability Version 1.0″, http://docs.oasis-open.org/imi/ns/identity/v1.0/identity.html, May 2009.

[7] OASIS, ″Security Assertion Markup Language (SAML) V2.0 Technical Overview″, http://www.oasis-open.org, March 2008.

[8] T. E. Maliki and J.-M. Seigneur, “A Survey of User-centric Identity Management Technologies”, Proc. of Int’l Conference on Emerging Security Information, Systems and Technologies, pp. 12-17, 2007.

[9] E. Maler and D. Reed, ″The Venn of Identity - Options and Issues in Federated Identity Management″, IEEE Security & Privacy, pp. 16-23, March/April 2008.

[10] D. P. Korman and A. D. Rubin, ″Risks of the Passport Single Signon Protocol″, IEEE Computer Networks,

Vo. 33, pp. 51-58, July 2000.
[11] http://en.wikipedia.org/wiki/Windows_Live_ID
[12] Liberty Alliance Project, "Liberty ID-FF Architecture Overview", Liberty Alliance, 2004.
[13] http://www.projectliberty.org/
[14] http://www.oasis-open.org/committees/security/
[15] http://incommon.org/
[16] http://openidentityexchange.org/
[17] D. Thibeau and D. Reed, "Open Trust Frameworks for Open Government : Enabling Citizen Involvement through Open Identity Technologies", http://openid.net/, Aug. 2009.
[18] M. Rundle, et. al., "The Open Identity Trust Framework(OITF) Model", http://openidentityexchange/, March 2010.
[19] http://kantarainitiative.org/

저자소개

박승철(Seungchul Park)

1985.2 : 서울대 계산통계학과 졸
1987.2 : KAIST 전산학과 석사
1996.8 : 서울대 컴퓨터공학과 박사
ETRI 연구원, 한국IBM
현대전자 네트워크연구소장, 현대네트웍스(주)
연구소장 역임
현재 한국기술교육대학교 부교수
※관심분야 : 광대역통신망, 멀티미디어통신, P2P 스트리밍, 신원 관리