情報保護學會論文誌
第11券 第5號, 2001. 10

다중 도메인 환경에서 상호 인증이 가능한 단일 인증 시스템

손 태 식*, 서 정 택**, 윤 혁 중**, 이 철 원**, 김 동 규***

Single Sign-On System enabling Mutual Authentication in Multi Domain Environments

Tae-Shik Sohn*, Jung-Taek Seo**, Hyouk-Jung Yoon**, Cheol-Won Lee**, Dong-Kyoo Kim***

요 약

인터넷의 발달과 함께 인터넷 기술을 기반으로 하는 인트라넷이 널리 보급되고 있다. 인트라넷은 기업, 연구소, 학교 등 같은 목적을 가지는 조직의 정보 공유를 위하여 사용되는 일종의 사설 네트워크이다. 인트라넷 사용의 증가와 함께 인트라넷 환경은 여러 인트라넷이 연관 관계를 가지는 익스트라넷 환경으로 발전하고 있다. 현재 이러한 인트라넷 및 익스트라넷 환경에서는 상호간 정보 공유에 있어 발생 할 수 있는 보안 문제를 해결하는 것이 무엇보다도 중요하다. 따라서 본 논문에서는 인트라넷 및 익스트라넷에서 사용자의 편리성 향상을 위한 단일 인증과 권한 부여 기능을 제공하는 단일 인증 시스템을 제안하고, 제안한 모델을 PKI(Public Key Infrastructure) 기반의 상호 연동을 통해 다중 도메인간에 상호 인증이 가능한 모델로 확장한다.

ABSTRACT

With the development of Internet, it is widely spreaded to a Intranet based on Internet technology. Intranet is a private, unique network to share the information of organization such as incorporate, research institute and university. With the increase of Intranet using, Intranet environment is developing into Extranet environment which is connected many Intranet. Currently such Intranet and Extranet environments, above all, it is important to solve security problems which can appear through use of information between domains. Thus, in this paper, we propose SSO(Single Sign-on System) model with authorization management and single sign-on operation, and we extend it to enable mutual authentication through inter-working based on PKI(Public Key Infrastructure) in Extranet environments.

keyword : *Authentication, Authorization, Single-Sign On, Mutual Authentication, Intranet, Extranet*

Ⅰ. 서 론

인터넷 기술의 발달과 함께 편리한 사용자 인터페이스를 제공하는 웹 기술은 일반 사용자들이 인터넷을 손쉽게 사용하도록 하였다. 일반 사용자들의 인터넷 사용 증가와 함께 기업체, 연구소, 대학 등의 특정 조직체 내에서도 정보 교환을 위한 네트워크에 웹과 같은 인터넷 기술을 적용한 인트라넷 구축이 보편화 되었다. 또한 인트라넷이 구축된 기업체, 연구소, 대학 등이 관련된 업무나 연구, 교육을 수행하는 타

* 아주대학교 정보통신공학과 정보통신 및 시큐리티 연구실(tsshon@madang.ajou.ac.kr)
** ETRI 부설 국가보안기술연구소(seojt@etri.re.kr, cheolee@etri.re.kr)
*** 아주대학교 정보통신공학과 교수(dkkim@madang.ajou.ac.kr)

조직까지 인트라넷의 범위를 확대시켜 정보 시스템을 구축하는 확장된 인트라넷 형태의 익스트라넷도 증가하고있다. 인트라넷 및 익스트라넷은 특정 정보 조직에 맞게 구축된 네트워크 환경에서 TCP/IP 기반의 인터넷 기술을 통해 자유로운 내부 정보 공유는 물론이고 외부 인터넷망과의 연결을 통한 정보 이용도 지원한다. 그리고 개방된 표준 웹 기술을 사용하여 정보를 효율적이고도 저렴한 비용에 처리해 주고 다양한 웹서비스를 통해 조직의 사용자들이 사용하는 다양한 응용 프로그램에 편리한 인터페이스를 제공한다. 또한 TCP/IP와 HTTP 등 표준 프로토콜을 사용하여 플랫폼에 독립적인 네트워크 환경 구축과 추후 확장 편리성 등의 다양한 특징을 가진다.

인트라넷 및 익스트라넷 구축의 이점과 함께 인트라넷 및 익스트라넷은 모든 정보가 공개되고 공유되는 일반적인 인터넷 환경과는 다르게 내부 정보 및 자원에 대한 보안과 상호간 보안이 필요하며 또한 인트라넷과 익스트라넷에서 제공되는 많은 응용 서비스에 대해 사용자의 편리를 위한 단일 인증 기능도 요구된다.

따라서 내부 네트워크의 여러 자원에 접근하는 사용자에 대한 단일 인증 과정을 통하여 사용자 측면에서는 편리성, 관리자 측면에서는 내부 자원 보호 그리고 연동되어 있는 인트라넷(익스트라넷) 사이 즉 다중 도메인 환경에서는 도메인간 보안 및 단일 인증을 위한 상호 인증 기능 등을 제공해야 한다.

본 논문에서는 우선 인트라넷과 익스트라넷 환경에서의 보안 요구 사항을 알아본다. 그 후 보안 요구 사항을 충족시키기 위한 단일 인증 시스템 모델을 제안하며 여러 인트라넷이 혼합된 다중 도메인 환경에서 도메인 간 상호 인증 및 상호 연동 방안을 제시한다.[1,2,6~9]

II. 인트라넷 및 익스트라넷 환경의 보안 요구 사항

본 논문에서는 인트라넷 및 익스트라넷 환경에서의 보안 요구 사항을 외부 보안과 내부 보안으로 나누어 구분한다. 외부 보안은 인가 받지 않은 외부 사용자의 접근을 통한 내부 기밀 정보의 유출, 웹 기반으로 동작하는 시스템들에서 악성 코드(자바 애플릿, 자바 스크립트, Active X control)의 실행 가능성과 같은 보안 문제들을 가진다. 이러한 외부 보안 문제를 해결하기 위한 보안 요구 사항으로서 방화벽(Firewall) 시스템, 침입 탐지 시스템, 가상 사설망(Virtual Private Network)과 같은 보안 솔루션을 주로 사용한다. 방화벽 시스템이나 침입 탐지 시스템은 외부의 인가 받지 않은 접근을 탐지하여 차단하고 또한 인트라넷과 익스트라넷 환경에서 외부의 인터넷망과 직접적인 연결을 프록시 기법 등을 사용하여 제한한다. 가상 사설망은 두 상대방이 인터넷을 통해 안전하게 기밀 정보를 공유하기 위한 방법으로서 최근 비용 문제와 조직 내부 자료의 보호에 대한 관심 증가 등에 따라 그 사용이 증가하고 있다.

내부 보안은 인트라넷과 익스트라넷에서 서비스를 제공하는 응용 서버들의 정보를 포함하여 네트워크 내의 사용 가능한 모든 자원에 대한 불법적인 접근을 제한하는 것이다. 이러한 내부 정보 및 자원에 대한 접근 제어는 일차적으로 외부 보안 요구 사항의 방화벽 시스템, 침입 탐지 시스템을 통해 비 인가된 외부 사용자의 접근에 대비하거나 사설 전용망을 통하여 외부 사용자가 전송되는 정보를 알아 낼 수 없게 하는 방법이 있다. 하지만 불법적인 방법으로 방화벽 시스템과 침입 탐지 시스템을 뚫고 침입하거나 외부 인터넷망과 연결되어 있는 곳으로 우회해서 내부 자원에 접근하는 등 보안의 위협은 항상 존재하게 된다. 그러므로 내부의 자원의 보안을 위한 보안 요구 사항으로는 인트라넷 및 익스트라넷의 환경에 적합한 인증 기법과 인증 모델[21,22]을 사용하여 인가된 사용자를 가려내고 자원 사용에 대한 접근 제어를 수행하는 것이 필요하다.

앞서 다룬 인트라넷과 익스트라넷 환경의 보안 요구 사항들은 공통적 요소 외에도 익스트라넷 자체의 특성에 기인하는 익스트라넷만의 보안 요구 사항이 또한 존재한다. 익스트라넷 환경은 기존 인트라넷 환경의 정보 시스템 망을 조직의 업무나 연구 등에 관련이 있는 다른 조직을 포함하여 확대한 것으로 이렇게 자신의 인트라넷에 추가되는 여러 조직(Partner)들은 조직 내부의 상황과 목적에 따라서 동적으로 변할 수 있다. 즉, 현재의 협력 관계에 의해서 익스트라넷을 통한 정보시스템 망을 구축했을 지라도 공통의 목적을 위한 연구나 사업이 종료 할 경우 또는 그 외의 상황에 의해서 상호간의 연관 관계가 없어지는 경우에 현재 구축된 익스트라넷 환경의 변화는 필연적이다. 따라서 동적으로 연관 관계가 변할 수 있는 익스트라넷 환경에서 상호간의 신뢰를 바탕으로 한 정보의 공유 및 사용을 위해 도메인간 상호 연동을 통한 상호 인증 기능 제공과 같은 부가적인 보안 요구 사항이 필요하다.[3~5]

Ⅲ. 상호 인증이 가능한 단일 인증 시스템

3.1 제안 시스템 필요성

인트라넷 및 익스트라넷 환경의 내부 보안을 위해 제2장에서 분석된 것과 같은 다음의 보안 요구 사항을 충족시켜야 한다. 우선 내부 자원의 보호를 위하여 비인가 된 사용자의 불법적인 접근을 차단하고 인가된 사용자들에게 부가적인 인증 과정 없이 서비스를 제공하기 위한 단일 인증 기능이 요구된다. 또한 익스트라넷의 특성으로 인해 발생하는 도메인간의 상호 인증 문제를 해결하기 위한 보안 요구 사항으로 단일 인증 시스템간의 상호 연동을 통한 다중 도메인간 상호 인증 기능 역시 필요하다. 이러한 필요성은 분산 네트워크 환경에서 단일 인증 시스템의 적용하는 경우에 인트라넷/익스트라넷, 공개망/비공개 사설망, 회사A망/회사B망 등 네트워크의 특성에 따른 분류되어 적용 되야 함을 말하며 이렇게 네트워크의 특성에 따른 차별화 된 적용은 결국 단일 인증 시스템끼리의 상호 연동 및 상호 인증 기능을 필요로 하게 된다.[2,17]

따라서 본 논문에서 제안하는 다중 도메인 환경에서 상호 인증이 가능한 단일 인증 시스템은 앞서 분석된 인트라넷과 익스트라넷 환경의 보안 요구 사항을 만족시키며 상호간의 신뢰를 바탕으로 한 정보의 공유를 위하여 필요하다.[13,15~17]

3.2 제안 시스템 특징

3.2.1 중앙 집중화된 인증 및 권한 관리

상호 인증이 가능한 단일 인증 시스템은 중앙의 사용자 관리 서버에서 도메인 내의 모든 사용자에 대한 정보를 유지하고 관리한다. 사용자 도메인 내 응용 서버에 대한 인증 요청은 사용자 관리 서버에서 중앙 집중적으로 처리하며, 사용자 인증 과정이 성공하면 사용자가 지니고 있는 정보에 기인하여 사용자가 해당 응용 서버에서 가지는 사용자 접근 권한을 부여한다. 이렇게 사용자 관리 서버에서 도메인 내의 사용자 정보를 관리하고 인증 및 권한 정보를 제어함으로써 도메인내의 사용자에 대해 보다 효율적인 관리가 가능하다.

3.2.2 분산화 된 접근 권한 속성 제어

중앙의 사용자 관리 서버에서 사용자 인증 과정 후에 응용 서버에 대한 사용자의 접근 권한을 부여하지만 각 응용 서버에서는 중앙의 사용자 관리 서버에서 사용자에게 부여한 권한(Role)에 맞는 권한 속성(Privilege)을 자신의 보안 정책에 기반하여 관리한다. 따라서 사용자 권한 관리 및 부여는 사용자 관리 서버에서 중앙 집중적으로 이루어지며 부여된 권한에 대한 권한 속성은 각 응용 서버에서 분산되어 조절된다. 이러한 분산화 된 접근 권한 속성 제어를 통해 중앙 집중화된 사용자 관리의 단점을 보완할 수 있다.

3.2.3 상호간에 독립적인 응용 서버 접근 제어

사용자 관리 서버에서 부여되는 응용 서버의 자원에 대한 사용자의 접근 권한은 각 응용 서버에서 다른 권한 속성을 가질 수 있다. 즉, 각 응용 서버들은 사용자의 같은 접근 권한에 대해 자신의 보안 정책에 따라 다른 권한 속성을 부여할 수 있다. 예를 들면 중앙의 사용자 관리 서버에서 사용자에게 관리자 접근 권한을 부여한 경우 서로 다른 두 응용 서버에서 한쪽의 관리자 권한은 실제적인 관리자이고 다른 쪽의 관리자 권한은 제한된 기능을 가지는 관리자가 될 수 도 있다. 결국 도메인내의 각 응용 서버들에서의 접근 권한 속성은 응용 서버 상호간에 독립적인 특성을 가지며 응용 서버 자신만의 보안 특성에 의한 접근 제어 정책을 가질 수 있게 된다.

3.2.4 도메인간 PKI 기반 상호 연동

여러 도메인간의 상호 인증을 위하여 각 도메인의 사용자 관리 서버는 공통의 비밀키를 공유하여 사용한다. 여기에 사용되는 각 도메인 별 사용자 관리 서버의 비밀키는 사용자 관리 서버의 서명과 인증서를 통해 서로 신뢰하는 도메인간 분배되고 여기서 신뢰 관계는 PKI 기반의 계층적 구조에서 서로를 신뢰하는 인증서 경로를 검증하여 구축된다. 이러한 다중 도메인간 상호 연동은 이미 구축되어 있는 인트라넷 환경의 확장에 있어 필수적이며 PKI를 바탕으로 하여 유연성 및 범용성을 가진다.

3.2.5 다중 도메인간 상호 인증

공개키 기반 구조를 통해 상호 연동되어 있는 도메인간에 공통의 비밀키를 공유함으로써 자신의 도메인 사용자뿐만 아니라 자신과 같은 비밀키를 가지고 신뢰 관계에 있는 다른 도메인의 사용자에게도 응용 서비스를 제공하는 상호 인증 기능을 지원한다.

3.2.6 클라이언트의 투명성

사용자는 웹 기반의 브라우저를 통해 친숙한 인터페이스를 제공받으며, 자바 애플릿이나 액티브 엑스 컨트롤과 같은 이동 코드 기법을 통해 클라이언트 측에서 필요한 에이전트를 사용자의 부가적인 노력 없이 이용할 수 있다. 이때 자바 애플릿과 액티브 엑스 컨트롤 사용 시 이동 코드 보안의 문제를 해결하기 위해 자바 애플릿의 경우 자바 보안 모델에 명시된 서명된 애플릿 기법[18]을 사용할 수 있고, 액티브 엑스 컨트롤의 경우에도 자바 애플릿 코드 서명 기법과 유사한 방법으로서 액티브 엑스 컨트롤 이동 코드에 대한 서명 값과 인증서를 함께 보내어 웹 브라우저에서 검증하는 코드 서명 기법[19]을 사용 할 수 있다. 따라서 클라이언트는 물론이고 서비스를 제공하는 응용 서버 측면에서도 클라이언트 인터페이스 개발에 대한 큰 어려움 없이 안전한 응용 서비스를 제공할 수 있다.

3.3 제안 시스템 구성 요소

3.3.1 사용자 관리 서버(User Administration Server)

사용자 관리 서버는 도메인 내 응용 서버들의 서비스를 제공받는 사용자 정보를 중앙 집중적으로 관리하여 사용자 인증 기능과 사용자 권한 관리 기능을 제공한다.

사용자 인증 기능은 사용자의 응용 서비스 요청에 앞서 각 사용자들을 인증 하는 것이다. 인증 과정은 사용자의 ID/PW를 기반으로 하는 방법과 좀 더 높은 보안 수준을 위해 ID/PW와 인증서를 함께 사용하여 인증 하는 방법이 있다.

사용자 권한 관리 기능은 서비스를 요청한 사용자에게 알맞은 권한(역할, 레벨)을 사용자 관리 서버가 사용자 인증 과정에서 부여하는 것으로서 각 응용 서버에 대한 사용자의 접근 권한은 사용자 관리 서버에서 중앙 집중적으로 관리된다. 하지만 사용자 관리 서버에서 부여된 권한에 따른 권한 속성은 각 응용 서버의 보안 정책 등에 따라 각 응용 서버마다 독립적으로 관리한다. 또한 사용자 권한 정보의 변경과 그에 따른 사용자 권한 정보의 갱신 기능도 수행한다.

마지막으로 사용자 관리 서버에서는 사용자의 인증 및 권한 부여 과정 후에 사용자가 요청한 응용 서비스를 응용 서버에서 제공받을 수 있는 3-In-1 서비스 티켓을 발급한다. 사용자는 이 서비스 티켓을 사용하여 추후에 부가적인 인증 과정 없이 다른 응용 서버에서 서비스를 제공받는다.

3.3.2 접근 제어 에이전트(Access Control Agent)

접근 제어 에이전트는 도메인의 각 응용 서버에서 사용자의 권한에 따라 자신의 보안 정책을 참고하여 접근 제어 기능을 수행한다. 사용자는 사용자 관리 서버에서 자신의 권한을 부여받게 되고 자신이 부여받은 권한에 맞는 서비스를 응용 서버에게 요청하게 된다. 이때 응용 서버의 접근 제어 에이전트는 자신의 보안 정책에 근거하여 사용자가 가지고 있는 권한에 알맞은 권한 속성을 부여하여 각 응용 서버마다 독립적이고 분산화 된 접근 제어 기능을 수행한다.

3.3.3 클라이언트

클라이언트는 응용 서비스를 제공받는 주체로서 인증 과정에서 필요한 ID, PW, 인증서 등의 정보를 사용자 관리 서버와의 인증에서 사용한다. 인증서 같은 경우에는 인증 과정 전에 미리 발급 받아 디스켓이나 스마트카[10]드에 저장하여 사용한다. 클라이언트는 인증서 기반의 인증 과정에서 미리 인증서를 발급 받아야 한다는 부가적인 노력 외에 단일 인증 기능을 사용하기 위한 별도의 프로그램 실행과 같은 작업이 필요 없다. 즉 인증서를 이용한 인증 과정에서 필요한 인증서 관련 정보와 서비스 티켓 정보에 접근하는 모듈을 사용자 관리 서버에서 다운로드 받아 사용하게 된다. 이러한 클라이언트 모듈은 엑티브 엑스 컨트롤[19]이나 자바 애플릿[18]으로 구현 가능하다.

3.3.4 3-In-1 서비스 티켓

3-In-1 서비스 티켓은 기존의 커버로스[11,12]나 SESAME(Secure European System for Applications in a Multi-vendor Environment)[14,20] 같은 분산 환경의 인증 시스템에서 사용되는 서비스 티켓과 유사한 개념으로서 하나의 서비스 티켓에 사용자 인증, 사용자 접근 권한 그리고 도메인간 상호 인증에 관련된 정보를 가지고 있다. 기존 SESAME 시스템에서 사용되는 서비스 티켓의 경우에는 실제 서비스 티켓을 발급 받기까지 권한 속성 서버 티켓, 권한 속성 인증서, 키 분배 서버 티켓, 응용 서비스 티켓[14,20] 등 구성 시스템의 여러 과정을 거쳐 다양한 서비스를 제공하기 위한 복잡한 티켓 메커니즘을 사용하여 많은 오버헤드를 유발한다. 또한 커버로스

시스템 역시 서비스 티켓의 발급을 위한 인증 서버와 티켓 발급 서버 등을 거치며 비밀키 관리 문제 및 상호 신뢰에 대한 문제[11,12]를 가지고 있다. 따라서 본 논문에서 제안하는 3-in-1 서비스 티켓은 기존의 하나의 서비스 티켓을 사용하여 필요로 하는 인증 기능과 권한 관리 기능을 제공하며 여러 티켓 발급의 오버헤드를 줄이기 위해 중앙의 사용자 관리 서버에서 인증과 권한 관리 서비스 티켓 발급의 기능을 수행함으로써 그 효율을 높인다.

3-in-1 서비스 티켓의 인증 정보 영역에는 사용자 인증 정보와 사용자를 인증 한 사용자 관리 서버의 서명 값을 가지고 있으며, 권한 정보 영역에는 사용자가 서비스를 요청한 각 응용 서버에 해당하는 사용자 접근 권한 정보를 가지고 있고, 상호 인증 영역에는 도메인간 상호 인증을 위해 사용되는 사용자 관리 서버의 인증서를 가지고 있다. [표 1]은 3-In-1 서비스 티켓의 포맷이다.

Authentication Information Field
- Ticket Serial Number : 티켓의 고유 번호
- Ticket Validity Period : 티켓의 유효 기간
- User ID : 사용자의 식별자
- Issuer Domain ID : 티켓을 발급한 도메인 식별자
- Private User Profile : 사용자의 개인 정보
- User Administration Sign : 사용자 관리 서버의 서명 값

Authorization Information Field
- Access Control Information(ACI)
  : Level(Rule-based Access Control)
  : Role(Role-based Access Control)
  : Normal(Default)
- Private User Profile : 각 응용 서버에서 사용하는 사용자 정보
- Domain ID : 각 응용 서버가 속한 도메인 ID

Multi-Domain Authentication Information
- User Administration Server Certificate
  : 사용자가 속한 도메인 사용자 관리 서버의 인증서

[표 1] 3-In-1 Service Ticket Format

Field Name		Information	
Authentication Information field		Ticket Serial Number	
		Ticket Validity Period	
		User ID	
		Issuer Domain ID	
		Private User Profile	
		User Administration Sign	
Authorization Information Field	Application Server A	Access Control Information	Level
			Role
			Normal
		Domain ID	
		Private User Profile	
	Application Server B	Access Control Information	Level
			Role
			Normal
		Domain ID	
		Private User Profile	
	Etc...		
Multi-Domain Authentication Information		User Administration Server Certificate (User Domain Certificate)	

3.4 도메인 내의 인증 및 권한 부여 과정

기존의 SESAME[14,20]나 Kerberos[11,12] 시스템에서의 인증 과정에 비하여 본 제안 시스템은 경량화 된 에이전트기반의 컴포넌트로 구성되어 적용 네트워크에서 효율성과 편리성을 가져 올 수 있다. 실제로 SESAME 시스템의 경우 응용 서버에 접근하여 응용 서비스를 제공받기 위해 필요한 서비스 티켓을 발급 받기 위해서는 우선 인증 서버에서 인증 과정을 수행하고, 그 후 권한 속성 서버에 접근하기 위한 권한 속성 서버 접근 티켓을 발급 받아야 하고, 그 후 권한 속성을 부여받은 후에 키 분배 서버에 접근하기 위한 키 분배 서버 접근 티켓을 발급 받아야 하는 등의 여러 과정을 거친다. 또한 Kerberos[11,12] 시스템의 경우 우선 SESAME[14,20] 시스템과 마찬가지로 인증 서버에서 인증 과정을 수행한 후, 서비스 티켓 발급 서버에서 서비스 티켓을 발급 받기 위한 티켓 발급 서버 접근 티켓을 얻어야 한다. 이처럼 기존의 시스템들은 비록 여러 구성요소로 이루어져 다양한 정보보호 기능을 제공하지만, 현재 인트라넷이나 익스트라넷 환경에 적용하여 높은 효율과 편리성을 갖는데는 시스템 구성 자체에 문제점을 가지고 있다. 따라서 본 논문에서 제안된 시스템은 중앙에 위치하는 도메인의 사용자 관리 서버에서 사용

자 인증과 접근 권한 부여 기능을 수행하며, 이때 인증 된 사용자에게 부여하는 하나의 3-In-1 서비스 티켓을 통하여 편리하게 인증, 접근 제어와 같은 정보보호 서비스를 제공받을 수 있다.

아래에는 도메인 내의 인증 및 권한 부여 과정을 사용자가 도메인 내에서 최초로 인증 과정을 거치며 3-In-1 서비스 티켓을 발급 받는 과정과 3-In-1 서비스 티켓을 발급 받은 후 응용 서버에서 서비스를 제공받는 과정에 대한 설명이다.

[가정]

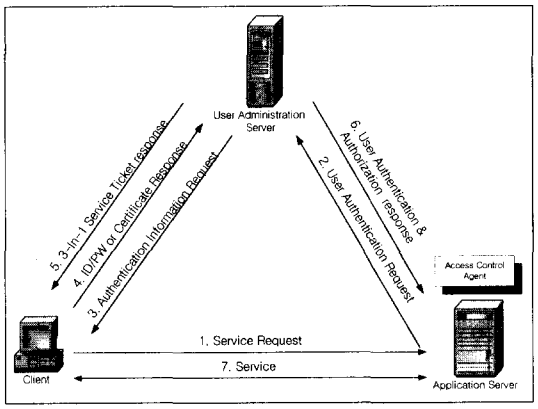
사용자는 사용자 관리 서버에 등록되어 있고 미리 발급 받은 인증서를 가지고 있다. 사용자 관리 서버는 ID/PW와 인증서를 기반으로 한 두 가지 인증 방법 중 하나를 선택하여 [그림 1]과 같이 최초의 인증 과정을 수행한다.

■ 사용자의 서비스 요청 과정

1) 사용자는 응용 서버에 응용 서비스를 요청한다. (서비스 티켓 없이 최초의 요청)
2) 이때 응용 서버는 서비스를 원하는 사용자에 대한 인증 요청을 사용자 관리 서버에게 redirection 한다. 이후 수행되는 인증과정은 ID/PW를 기반으로 하는 인증 기법과 인증서를 기반으로 ID/PW를 함께 사용하는 인증 기법 중 하나를 선택하여 사용할 수 있다.

■ ID/PW 인증(Case 1)

3) 사용자 관리 서버는 사용자에게의 ID/PW 정보를 요청한다.
4) 사용자는 ID/PW 정보를 응답하고 이때 사용자 관리 서버에서 사용자 관리 서버가 가지고 있는 정보와 일치하는 경우 인증 과정을 완료한다.



[그림 1] 도메인 내의 단일 인증 과정(프로토콜 1. 참조)

■ 인증서 기반의 인증(Case 2)

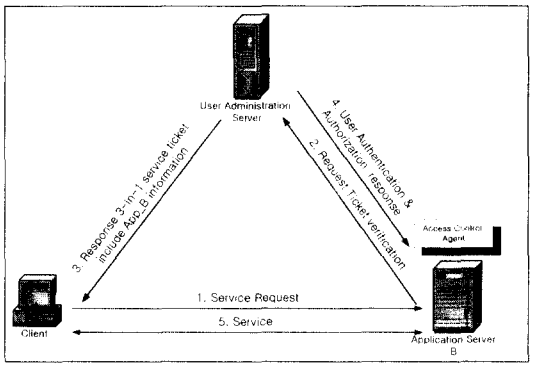
3) 사용자 관리 서버에서 사용자의 인증서 정보를 요구하는 인증서 정보 접근 모듈과 인증서 기반 인증에 사용되는 랜덤 값을 사용자에게 전송한다. 사용자측에서 사용자 관리 서버로부터 받은 클라이언트 모듈이 실행된다. 클라이언트 모듈은 사용자의 비밀키로 암호화된 개인키와 사용자 정보에 접근하기 위해 사용자에게 비밀번호를 요청한다. 사용자의 비밀번호가 승인되면 사용자의 개인키를 사용하여 사용자 관리 서버로부터 받은 랜덤 값을 암호화한다.
4) 암호화된 랜덤 값과 함께 인증서 및 사용자 ID를 사용자 관리 서버에 보낸다. 사용자 관리 서버는 사용자의 공개키를 사용하여 랜덤 값을 복호화한 후 전송전의 랜덤 값과 비교하여 사용자를 인증 한다.

■ 3-In-1 서비스 티켓 발부 과정

5) 사용자 관리 서버는 첫 번째로 사용자가 인증이 되었음을 증명하는 인증 정보를 3-In-1 서비스 티켓의 인증 정보 영역에 생성하고 사용자 관리 서버의 서명 값을 첨부한다. 그 후 이 값을 사용자 관리 서버간의 비밀키로 암호화한다. 두 번째로 사용자가 서비스를 요청한 응용 서버에 대한 사용자의 접근 권한을 부여하고 응용 서버가 서비스에 필요한 사용자 정보와 함께 사용자 관리 서버와 응용 서버의 비밀키로 암호화한다. 그리고 마지막으로 사용자 관리 서버의 인증서를 포함하여 사용자에게 3-In-1 서비스 티켓의 포맷으로 전송한다.
6) 마찬가지로 응용 서버는 자신에게 응용 서비스를 요청한 사용자의 고유 정보와 사용자의 권한 정보를 사용자 관리 서버로부터 제공받는다.
7) 인증 및 권한 부여 과정을 성공적으로 마친 사용자는 응용 서버에서 요청한 서비스를 제공받는다.

[가정]

사용자는 3-In-1 서비스 티켓을 이미 발급 받은 상태이다. 다시 새로운 응용 서버(응용 서버 B)에 서비스를 [그림 2]와 같이 응용 서비스를 요청한다.



〔그림 2〕 단일 인증 과정-서비스 티켓 사용(프로토콜 1.참조)

1) 사용자는 3-In-1 서비스 티켓을 사용하여 응용 서버 B에 서비스 제공 요청을 보낸다.
2) 응용 서버 B는 사용자의 3-In-1 서비스 티켓이 정당한 인증 과정을 통해서 발급 된 것임을 알기 위해 사용자 관리 서버에 검증을 요청한다.
3) 사용자 관리 서버는 사용자 인증 정보를 검증하고, 검증이 통과 된 경우에 응용 서버 B에 맞는 권한 정보를 3-In-1 서비스 티켓에 첨부하여 사용자에게 갱신된 3-In-1 서비스 티켓을 전달한다.
4) 또한 응용 서버 B에게 사용자 고유 정보와 권한 정보를 응용 서버 B와 사용자 관리 서버간의 비밀키로 암호화하여 보낸다.
5) 응용 서버 B는 사용자의 3-In-1 서비스 티켓이 정당함을 알고 사용자에게 부여된 권한 정보에 따라 알맞은 서비스를 제공한다.

〔표 2〕 인증 프로토콜 기호 설명

기호	설명
App_Server_N	응용 서버 N
ux_pub	사용자 x의 공개키
ux_pri	사용자 x의 개인키
ca_x_pub	인증서 발급 기관의 공개키
ca_x_pri	인증서 발급 기관의 개인키
x_pub	사용자 관리 서버 x의 공개키
x_pri	사용자 관리 서버 x의 개인키
Rand	임시 난수 값
E_{mk}	사용자 관리 서버간의 비밀키
Sign(m)	메시지 m의 사인 값
TSN	서비스 티켓 시리얼 번호
TVT	서비스 티켓 유효 기간
PUP	사용자 프로파일 정보
IDI	서비스 티켓 발부 식별자
User_ACI	사용자의 접근 권한 정보
E_{kx}	응용 서버 x와 사용자 관리 서버의 비밀키로 암호화
D_{kx}	응용 서버 x와 사용자 관리 서버의 비밀키로 복호화
Admin_X_Cert	사용자 관리 서버 X의 인증서
Client_X_Cert	사용자 X의 인증서
Domain_X_UAS	도메인 X의 사용자 관리 서버

〔프로토콜 1〕 인증 과정 및 서비스 티켓 발급 과정(그림 1, 2 참고)

1. 인증서를 이용한 사용자 인증(그림 1의 3,4번 과정)
   User Admin Server_A to Client_A=Send Rand
   Client_A to User Admin Server_A=E_{ua_pri}〔Rand, ID〕 || Client_A_Cert
   * Client_A_Cert = $Sign_{ca\_pri}$(ua_pub)
   User Admin Server_A=Verify(Client_A_Cert) = $Verify_{ca\_pub}$($Sign_{ca\_pri}$(ua_pub))
   D_{ua_pub}〔E_{ua_pri}〔Rand, ID〕〕

2. 사용자의 3-In-1 서비스 티켓 발부(그림 1의 5,6번 과정)
   User Admin Server_A to Client_A : 3-In-1 Service Ticket=E_{mk}〔m, $Sign_{a\_pri}$(m)〕 || App1 || Admin_A_Cert
   * m=〔TSN, TVT, PUP, IDI〕, App1=E_{ka}〔PUP, User_ACI〕
   User Admin Server_A to App_Server_A : App1
   * App1=E_{ka}〔PUP, User_ACI〕

3. 새로운 응용 서버에 대한 정보 추가(그림 2의 3,4번 과정)
   User Admin Server_A to Client_A : Added App2 information to 3-In-1 Service Ticket
   Added 3-In-1 Service Ticket=E_{mk}〔m, $Sign_{a\_pri}$(m)〕 || App1 || App2 || Admin_A_Cert
   * m=〔TSN, TVT, PUP, IDI〕, App1=E_{ka}〔PUP, User_ACI〕, App2=E_{kb}〔PUP, User_ACI〕
   User Admin Server_A -> App_Server_B : App2
   * App2=E_{kb}〔PUP, User_ACI〕

〔프로토콜 2〕 상호 인증 과정(그림 3 참고)

1. 그림 3의 도메인간 상호 인증 과정에서의 가정 부분(도메인 A에서 서비스 티켓 발급)
   Domain_A_UAS to Client_A : 3-In-1 Service Ticket=E_{mk}[m, Signa_pri(m)] || App1 || Admin_A_Cert
   * m=[TSN, TVT, PUP, IDI], App1=E_{ka}[PUP, User_ACI]
   User Admin Server_A to App_Server_A : App1=E_{ka}[PUP, User_Role]

2. 그림 3의 상호 인증 과정
   1) Client_A to App_Server_B : Service Request(Send Service ticket)
   2) App_Server_B to Domain_B_UAS : Authentication Req(Indirection Client_A service request with Service Ticket)
   E_{mk}[m, $Sign_{a\_pri}$(m)] || App1 || Admin_A_Cert
   Domain_B_UAS : Verify(Admin_A_Cert)=$Verify_{ca\_pub}$($Sign_{ca\_pri}$(a_pub))
   Dmk[E_{mk}[m, $Sign_{a\_pri}$(m)]]
   Verify(Client A authentication information)=$Verify_{a\_pub}$($Sign_{a\_pri}$(m))
   3) Domain_B_UAS to Domain_A_UAS : Request User information
   4) Domain_A_UAS to Domain_B_UAS : Response Update user information or Unchanged user information
   5) Domain_B_UAS to Client_A : Response 3-In-1 Service Ticket include App2
   3-In-1 Service Ticket=E_{mk}[m, $Sign_{a\_pri}$(m)] || App1 || App2 || Admin_A_Cert
   * m=[TSN, TVT, PUP, IDI], App2=E_{kb}[PUP, User_ACI]
   Domain B to App_Server_B : App2
   * App2=E_{kb}[PUP, User_ACI]

〔프로토콜 3〕 상호 연동 과정(그림 4 참고)

1) CA to Domain_A_UAS, Domain_B_UAS, Domain_C_UAS : Issue Certificates
2) Domain_A_UAS to Domain_B_UAS : E_{b_pub}[mk, $Sign_{a\_pri}$(mk)] || Admin_A_Cert
   Verify(Admin_A_Cert)=$Verify_{ca\_pub}$($Sign_{ca\_pri}$(a_pub))
   D_{b_pri}[E_{b_pub}[mk, $Sign_{a\_pri}$(mk)]]
   $Verify_{a\_pub}$($Sign_{a\_pri}$(mk))
3) Domain_B_UAS to Domain_C_UAS : E_{c_pub}[mk, $Sign_{b\_pri}$(mk)] || Admin_A_Cert || Admin_B_Cert
   Verify(Admin_B_Cert)=$Verify_{ca\_pub}$($Sign_{ca\_pri}$(b_pub))
   D_{c_pri}[E_{c_pub}[mk, $Sign_{b\_pri}$(mk)]]
   $Verify_{b\_pub}$($Sign_{b\_pri}$(mk))

Ⅳ. 도메인간 상호 인증 및 연동

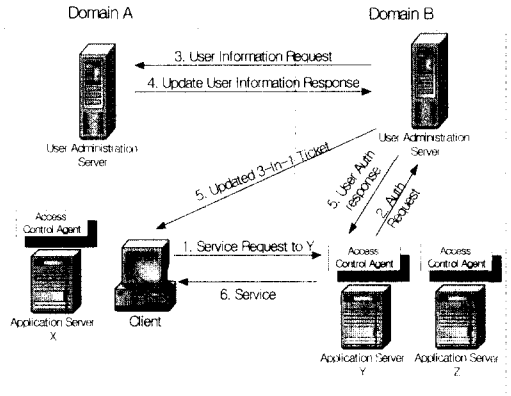
4.1 도메인간 사용자 관리 서버의 상호 인증

도메인간의 상호 인증은 각 도메인의 사용자 관리 서버가 상호 연동 과정을 통해 공통의 비밀키를 유지하는 것을 기반으로 성립된다. 아래의 과정은 도메인간의 사용자 관리 서버의 상호 인증을 통한 사용자의 단일 인증 기능을 통해 신뢰 도메인 사이에서 응용 서비스를 제공받는 과정이다.

[가정]

사용자는 도메인 A의 사용자 관리 서버로부터 서비스 티켓을 발급 받았다.

1) 사용자는 도메인 B의 응용 서버 Y에 도메인 A의 사용자 관리 서버가 발급한 3-In-1 서비스 티켓을 가지고 서비스를 요청한다.
2) 응용 서버 Y는 자신이 속한 도메인 B의 사용자 관리 서버에게 사용자의 인증을 요청한다.
3) 도메인 B의 사용자 관리 서버는 사용자의 도메인 A로부터 발급 받은 3-In-1 서비스 티켓에서 도메인간 사용자 관리 서버의 비밀키로 암호화된 사용자 인증 정보를 얻어내고 도메인 A의 사용자 관리 서버의 서명 값을 검증한 후 서비스를 요청한 사용자의 정보의 변경 여부를 도메인 A의 사용자 관리 서버에 확인한다.
4) 도메인 A의 사용자 관리 서버는 사용자 정보가 변경되었을 경우 관련 사용자 정보를 보내준다.
5) 도메인 B의 사용자 관리 서버는 응용 서버 Y에 대한 사용자의 권한을 부여하고 사용자에게는 갱신된 서비스 티켓을 그리고 응용 서버에게 관련 사용자 정보를 보낸다.
6) 사용자는 위와 같은 과정을 통해 도메인 A에서와 같이 도메인 B에서 응용 서비스를 받게 된다.



〔그림 3〕 도메인 간 상호 인증 과정(프로토콜 2. 참조)

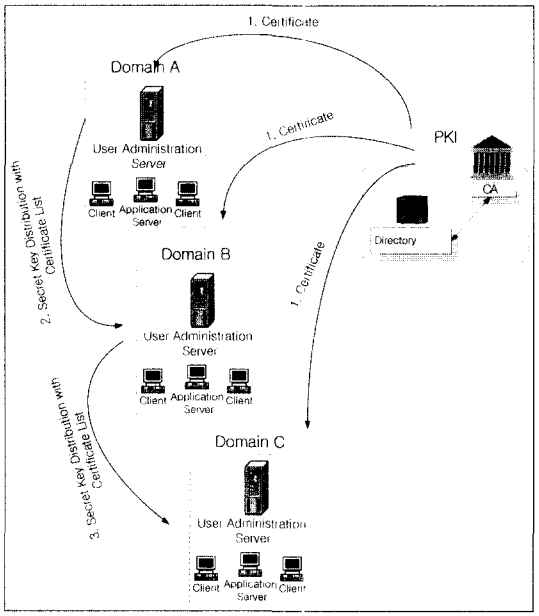
4.2 PKI 기반 상호 연동 체계

도메인간의 상호 연동을 위해서는 도메인간에 상호 신뢰 관계가 필요하며 이러한 신뢰 관계가 성립한 후에 상호 간 공통의 비밀키를 유지함으로써 상호 인증이 가능하게 된다. 따라서 본 논문에서 제안하는 다중 도메인간 상호 인증이 가능한 단일 인증 시스템에서는 현재 널리 사용되고 있는 PKI를 기반으로 한 전자 인증 체계를 사용하여 도메인간의 상호 연동을 가능하게 한다. 즉 각 도메인의 사용자 관리 서버들은 신뢰 할 수 있는 공인 인증기관에서 발급 받은 인증서를 사용하여 서로 간에 인증서 검증을 통한 신뢰 관계를 유지한다. 결국 인증서 검증을 통한 신뢰 관계의 구축은 검증된 인증서들을 계속하여 리스트 구조로 유지함으로써 같은 비밀키를 공유하며 상호 인증을 허용하는 도메인들을 나타내주고 신뢰성을 보증해주는 수단이 된다. 다음은 〔그림 4〕의 상호 연동 과정 설명이다.

[가정]

도메인 A가 주 도메인이라고 가정(본 예에서는 단일 계층의 단순한 구조로 설명)

1) 도메인 A, B, C의 사용자 관리 서버가 CA로부터 인증서를 발급 받는다.
2) 도메인 A의 사용자 관리 서버는 도메인 B의 사용자 관리 서버에게 상호 인증에 필요한 비밀키와 그 서명 값을 함께 암호화하여 자신의 인증서와 함께 보낸다.
3) 도메인 B의 사용자 관리 서버는 도메인 A의 사용자 관리 서버가 보낸 인증서를 검증하고 도메인 A의 사용자 관리 서버 공개키로 비밀키의 서명 값을 비교하여 비밀키의 정당성을 확인한다. 그 후 자신의 인증서를 검증된 신뢰 관계를 나타내는 인증서 리스트에 포함하여 도메인 C의 사용자 관리 서버에 암호화 된 비밀키와 함께 보낸다.



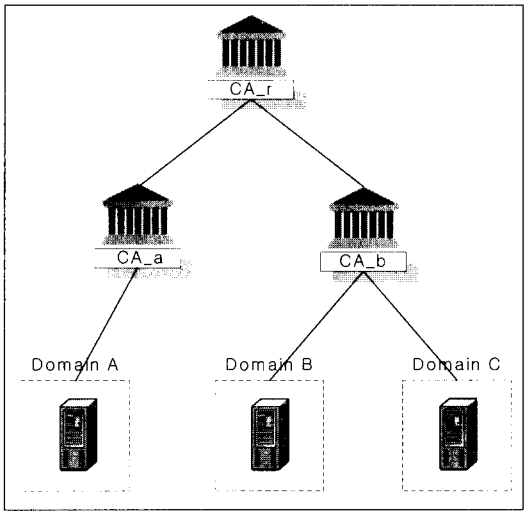
〔그림 4〕 도메인 간 상호 연동 과정(프로토콜 3. 참조)

상호 연동이 필요한 도메인에 위와 같은 과정을 반복하여 신뢰 관계를 생성하는 가운데 비밀키를 공유한다. 따라서 도메인 간 직접적인 인증 과정이 없을지라도 자신의 상위 및 인접 도메인의 PKI 기반 상호 인증 체계를 통해 신뢰하는 인증서 리스트에 속한 모든 도메인을 신뢰할 수 있다. 또한 신뢰 관계에 속한 도메인이 많을 경우에도 PKI 기반 계층적 인증 체계를 통해 신뢰 관계 관리의 효율성을 가져 올 수 있다.

V. 제안 시스템의 기능 검증

5.1 상호 연동 기능

도메인간 상호 인증의 기반이 되는 상호 연동은 PKI 기반 구조의 인증 체계를 통하여 도메인간 사용자 관리 서버들이 신뢰 관계를 구축하는 것이다. 각 도메인의 사용자 관리 서버들은 비밀키를 공유하기 위해서 공개키를 사용한 키 분배 방법을 사용한다. 이때 비밀키를 분배하는 주체에 대한 인증은 비밀키



〔그림 5〕 공개키 기반 구조의 상호 연동

를 보내온 메시지에 포함된 인증서의 발급 경로를 검증하여 공인 인증기관이 인증 하는 범위까지의 인증 경로가 타당한지를 확인함으로써 이루어진다. 이렇게 비밀키를 보내온 도메인의 검증된 인증서는 계속해서 리스트 구조로 연결되어 여러 도메인 사이의 신뢰성을 보장해주며 또한 신뢰 관계를 나타내는 하나의 수단이 된다. 결국 이러한 검증된 인증서 리스트는 서로 신뢰하는 도메인들간에 비밀키를 공유하는 기반이 되고 여러 도메인들 간의 연동을 가능하게 한다. 다음의 과정은 〔그림 5〕의 PKI를 기반으로 하는 상호 연동 과정에 대한 설명이다.

1) 도메인 A와 도메인 B사이의 공개키 이용 비밀키 분배와 인증서 검증 과정

Domain A -> Domain B :
E_{b_pub}[mk, $Sign_{a\_pri}$(mk)] || Admin_A_Cert
(도메인 A에서 비밀키를 도메인 B에 보낸다.)

Domain B :
Verify(CA_A_Cert)
=$Verify_{ca\_r\_pub}$($Sign_{ca\_r\_pri}$(ca_a_pub))
Verify(Admin_A_Cert)
=$Verify_{ca\_a\_pub}$($Sign_{ca\_a\_pri}$(a_pub))
D_{b_pri}(Encrypted Secret key)
=D_{b_pri}[E_{b_pub}[mk, $Sign_{a\_pri}$(mk)]]
Verify(Sign value of Secret key)
=$Verify_{a\_pub}$($Sign_{a\_pri}$(mk))

2) 도메인 B와 도메인 C사이의 공개키 이용 비밀키 분배와 인증서 검증 과정

Domain B -> Domain C :
E_{b_pub}[mk, $Sign_{a\_pri}$(mk)] || Admin_A_Cert ||
Admin_B_Cert

(도메인 B에서 비밀키를 도메인 C에 보낸다. 이때 암호화된 메시지 뒷부분의 연결된 인증서 리스트가 검증된 후에 자신이 알고있는 신뢰하는 리스트가 된다.)

Domain C :
Verify(CA_B_Cert)
=$Verify_{ca\_r\_pub}$($Sign_{ca\_r\_pri}$(ca_b_pub))
Verify(Admin_B_Cert)
=$Verify_{ca\_b\_pub}$($Sign_{ca\_b\_pri}$(b_pub))
Dc_pri(Encrypted Secret key)
=D_{c_pri}[E_{c_pub}[mk, $Sign_{b\_pri}$(mk)]]
Verify(Sign value of Secret key)
=$Verify_{b\_pub}$($Sign_{b\_pri}$(mk))

5.2 상호 인증 기능

본 논문의 도메인간 상호 인증 기능을 검증하기 위하여 사용자는 자신이 속한 도메인(도메인 A)에서 발급 받은 3-In-1 서비스 티켓을 사용해 다른 도메인(도메인 B)에 있는 응용 서비스를 요청한다고 가정하자. 이때 도메인 B에 속한 응용 서버는 사용자의 서비스 요청에 대하여 사용자 관리 서버(도메인 B)에 사용자 인증을 요청한다. 이때 맨 먼저 3-In-1 서비스 티켓에서 서비스 티켓에 포함되어 있는 서비스 티켓을 발급한 사용자 관리 서버의 인증서가 자신이 신뢰하는 인증서 리스트에 포함되어 있는지를 확인한다. 확인 과정이 끝나고 서비스 티켓을 발급한 사용자 관리 서버의 도메인(도메인 A)이 신뢰 관계에 있는 도메인이라면, 도메인간 사용자 관리 서버의 비밀키로 암호화되어 있는 사용자 인증 정보를 복호화 하고, 사용자 관리 서버(도메인 A)의 개인키로 서명되어 있는 사용자 인증 정보의 서명 값을 3-In-1 서비스 티켓에 있는 인증서의 공개키(도메인 A의 사용자 관리 서버의 공개키)로 검증하여 자신의 도메인에 속한 사용자가 아닐지라도 부가적인 사용자 등록 과정 없이 도메인간 신뢰 관계에 의

하여 도메인 상호간에 인증이 성립 할 수 있다. 이러한 도메인간 상호 인증 기능은 각 도메인의 사용자 관리 서버가 상호 연동 과정에서 신뢰 관계를 바탕으로 유일한 비밀키를 공유함으로써 성립된다. 결국 앞서 검증된 도메인간의 상호 연동에서 PKI를 기반으로 구축된 신뢰 관계는 도메인간의 상호 인증을 성립시켜주는 바탕이 된다. 다음의 과정은 도메인간 상호 인증 과정에서 사용되는 비밀키와 서명 값 검증 과정이다.

1) 3-In-1 서비스 티켓에서 사용자 정보 복호화

D_{mk}(user authentication information)
$=D_{mk}(E_{mk}[m, Sign_{a\_pri}(m)])$
(여기서 mk는 도메인간 사용자 관리 서버의 비밀키)

2) 3-In-1 서비스 티켓에서 서명 값 검증

Verify(Admin_A_Cert)
$=Verify_{ca\_pub}(Sign_{ca\_pri}(a\_pub))$

Verify(UAI sign value)
$=D_{a\_pub}(Sign_{a\_pri}(m))$
(여기서 a_pub는 도메인 A의 사용자 관리 서버의 인증서에 얻어낸 공개키)
* UAI=User Authentication Information

5.3 단일 인증 기능

응용 서버에 서비스를 요구하는 사용자에 대한 단일 인증은 도메인 내의 사용자 관리 서버에서 이루어진다. 이때 사용자 관리 서버에서 인증이 성공하는 경우 사용자 인증 정보를 포함하는 3-In-1 서비스 티켓이 사용자에게 발급된다. 이때 3-In-1 서비스 티켓의 사용자 인증 정보와 사용자 인증 정보에 대한 사용자 관리 서버의 서명 값은 도메인간 사용자 관리 서버들의 비밀키로 암호화되어 있다. 3-In-1 서비스 티켓을 가지고 있는 사용자가 새로운 응용 서버에서 서비스를 요청하는 경우 응용 서버는 이 3-In-1 서비스 티켓을 사용자 관리 서버에게 넘겨주고 사용자 관리 서버는 자신의 비밀키로 암호화되어 있는 사용자 인증 정보를 복호화 한다. 복호화한 사용자 인증 정보와 사용자 인증 정보의 서명 값을 비교함으로써 3-In-1 서비스 티켓을 가지고 있는 사용자에 대한 인증이 이루어지며 이러한 과정에서 사용되는 사용자 관리 서버의 비밀키와 서명 값의 검증을 통해 사용자에게는 부가적인 인증 정보 요청이 없는 단일 인증 기능이 제공된다. 단일 인증에 사용되는 비밀키와 전자 서명 기법의 정당성은 PKI를 기반으로 다중 도메인간에 상호 연동을 통한 신뢰 관계를 구축함으로써 보장된다. 다음의 과정은 비밀키와 전자 서명을 통해 단일 인증 기능이 수행되는 과정에 대한 검증 과정이다.

1) 사용자 인증 후 발급 받은 3-In-1 서비스티켓

$Ticket=E_{mk}[m, Signa\_pri(m)] \,||\, App1 \,||$
Admin_A_Cert
$(m=[TSN, TVT, PUP, IDI],$
$App1=E_{ka}[PUP, User\_ACI])$

2) 사용자 관리 서버의 3-In-1 서비스티켓 복호화

Dmk(user authentication information)
$=D_{mk}(E_{mk}[\ m, Sign_{a\_pri}(m)\ ])$

3) 사용자 관리 서버의 서명 값 검증
Verify(UAI sign value)
$=D_{a\_pub}(Sign_{a\_pri}(m))$
* UAI=User Authentication Information

VI. 결 론

본 논문에서는 인터넷 기술의 발달과 함께 인트라넷 및 익스트라넷 환경의 정보 공유 과정에서 발생하는 보안 요구 사항을 충족시키는 방안으로서 다중 도메인 환경에서 상호 인증이 가능한 단일 인증 시스템 모델을 제안하였다.

제안한 단일 인증 시스템은 인트라넷 환경에서 여러 응용 서비스에 대한 단일 인증 기능은 물론이고 사용자 시스템의 투명성 제공, 중앙 집중적인 사용자 관리와 권한 부여 그리고 분산화 된 권한 속성 조절을 통해 기존의 SESAME나 Kerberos와 같은 분산 환경에서의 인증 시스템들[11,12,14,20]에 비하여 각 응용 시스템마다의 독립적인 보안성, 효율성 그리고 편리성이 강화되었다. 또한 다중 도메인 환경에서 도메인간 상호 인증을 위해 PKI 기반 신뢰 관계를 이용하여 여러 도메인들을 상호 연동 하였다.

따라서 다중 도메인 환경에서 상호 연동되어 있는 각 도메인의 사용자 관리 서버들이 비밀키를 공유함으로써 도메인간 상호 인증이 가능하다.

향후에는 단일 인증 시스템의 감사 기록 관리와 도메인 간 상호 인증에서 사용되는 키 관리, 스마트 카드 및 하드웨어 토큰 등[10]을 사용한 3-In-1 서비스 티켓의 보안에 대한 연구가 필요하다.

참 고 문 헌

[1] Harold F. Tipton, *Information Security Management*, 4th Edition, Auerbach publications USA, pp. 27~44.

[2] Richard Au, "Towards a New Authorization Paradime for Extranets", *in Proceeding of information security and privacy*, ACISP 2000, 2000.06.

[3] Ashley P., Practical Intranet Security, Kluwer Academic Publishers.

[4] Barry, "Extranet Security : What happens if your partner turns against you?", Computer Security Institute, 2000.

[5] Richard Power, "Intranet Security", Computer Security Institute, 2000.

[6] J.Hursti, "Single Sign-On", *in Proceeding of Helsinke Univ of Technology*, Seminar on Netwokr Security, 1997.

[7] T.Tervoi, "Single Sign-On Solutions in a Mixed Computing Environment", *in Proceeding of Helsinke Univ of Technology*, Seminar on Netwokr Security, 1998.

[8] Camilloi, "Unified Single Sign-On", *in Proceeding of Helsinke Univ of Technology*, Seminar on Netwokr Security, 1998

[9] Anonymous, *Single Sign-On Deployment Guide*, Netscape, Inc.,1997, http://developer.netscape.com/docs/manuals/security/SSO.

[10] Anonymous, *PKCS #11: Cryptographic Token Interface Standard* - Version 2.01, RSA, 1997, http://www.rsa.com/rsalabs/pubs/PKCS.

[11] Anonymous, Kerberos: *The Network Authentication Protocol*, Massachusetts Institute of Technology, 1998, http://web.mit.edu/kerberos.

[12] William Stallings, "Cryptography and Network Security", Prentice-Hall, pp. 324~340, 1999.

[13] Trickey, *F. Single Sign-On: Fantasy or Reality?* CSI Advisory Council, 1997, 〈http://www.gocsi.com/sso_ft.htm〉

[14] Mark Vandenwauver, 1995, *SESAME V3*. http://www.esat.kuleuven.ac.be/cosic/sesame3_2.html

[15] Securant, *Securant SSO*, OpenInfra, http://www.openinfra.com/report/sso.

[16] Anonymous, *Single Sign On white paper*, Systems Approach Corporation, 1999, http://1canada.com/sso.htm

[17] Philp Carden, "The New Face of Single Sign-On", Network Computing, March 22, 1999.

[18] Scott Oaks, Java Security, O'REILLY, pp. 196~322, 1999.02.

[19] Paul Johns, Signing and Marking ActiveX Controls, Microsoft Corporation, 1996.

[20] 이정현 외, "분산 환경에서의 정보보호 서버 : SESAME", 정보보호학회, 정보보호학회 학회지, Vol. 7, No. 4, 1997.12.

[21] 김동규 외, "브로커 및 에이전트 기반의 통합 단일 인증 시스템", *한국정보과학회*, 춘계종합학술대회 논문집, pp. 829~831, 2001

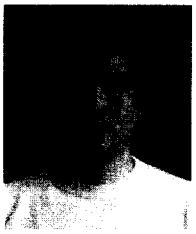
[22] 손태식, 김동규 외, "단일 인증 시스템의 인증 기법과 인증 모델 분석", 정보보호학회, 정보보호학회 학회지, Vol. 11, No. 4, 2001.08.

〈著者紹介〉

손 태 식 (Tae-Shik Sohn)
2000년 : 아주대학교 정보 및 컴퓨터 공학부 졸업(학사)
2000년~현재 : 아주대학교 정보통신전문대학원 석사과정
〈관심분야〉 네트워크 보안, 인터넷 프로토콜 보안, 자바/리눅스 보안

서 정 택 (Jung-Taek Seo)
1999년 : 충주대학교 컴퓨터공학과 졸업(학사)
2001년 : 아주대학교 대학원 컴퓨터공학과 졸업(석사)
2000년 11월~현재 : 국가보안기술연구소 연구원
〈관심분야〉 정보전, 시스템 및 네트워크 보안, 시스템 평가

윤 혁 중 (Hyouk-Jung Yoon)
1998년 : 아주대학교 컴퓨터공학과 졸업(학사)
2000년 : 아주대학교 대학원 컴퓨터공학과 졸업(석사)
1999년 12월~2000년 7월 : 한국정보보호센터 연구원
2000년 8월~현재 : 국가보안기술연구소 연구원
〈관심분야〉 네트워크 정보보호, 시스템 정보보호



이 철 원 (Cheol-Won Lee)
1987년 : 충남대학교 수학과 졸업(학사)
1989년 : 중앙대학교 대학원 전자계산학과(석사)
1989년~1996년 : 한국전자통신연구원 선임연구원
1996년~2000년 : 한국정보보호센터 선임연구원/통신모델링 과제책임자
2000년~현재 : ETRI 부설 국가보안기술연구소 팀장
〈관심분야〉 컴퓨터 및 네트워크 보안, 정보통신 기반보호, 정보보호시스템 평가기준

김 동 규 (Dong-Kyoo Kim)
1973년 : 서울대학교 공과대학 응용수학과 졸업(학사)
1979년 : 서울대학교 자연과학대학원 전자계산학과 졸업(석사)
1984년 : 미국 Kansas State University 전자계산학과 졸업(박사)
1986년~IEEE : 802.4,802.6,802.10 Working Group Member, Asiacrypt '96 조직위원회 위원장, 건설교통부 항공교통관제소 신항공 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국통신정보보호학회 부회장 역임
1979년~현재 아주대학교 정보 및 컴퓨터공학부 교수
〈관심분야〉 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링