Journal of Korea Multimedia Society Vol. 9, No. 3, March 2006(pp. 342-352)

# 스마트 공간을 위한 참여 제어 시스템의 설계 및 구현

양종필[†], 심미선[††], 신 원[†††], 이경현[††††]


## 요 약

오늘날 컴퓨팅 환경은 유비쿼터스로 변화하고 있다. 유비쿼터스 컴퓨팅 환경은 사용자들이 언제 어디서나 컴퓨팅 자원에 접근할 수 있는 스마트 공간(Smart space)으로 실현될 것이다. 그러나 스마트 공간내의 자원들에게 사전에 신뢰받지 못한 상태의 사용자들이 안전하게 자원들에 접근하기 위해서는 사용자들과 자원들 사이에 안전한 신뢰 관계를 형성하기 위한 기법이 요구된다. 본 논문에서는 유비쿼터스 컴퓨팅 환경에서의 신뢰 관계 형성을 위하여 기존에 제안된 분산된 신뢰(Distributed trust) 기법의 "악의적 권한 위임"과 "위임 권한 취소"에 대한 보안 문제점을 지적하고, 보안성이 개선된 새로운 참여 제어 시스템을 제안한 후 이를 구현한다.


# Design and Implementation of Admission Control System in Smart Space

Jong-Phil Yang[†], Mi-Sun Shim[††], Weon Shin[†††], Kyung Hyune Rhee[††††]


## ABSTRACT

Nowadays, Computing environment is changing to ubiquitous. In such ubiquitous computing environments, entities expect to access resources and services at any time from anywhere. Therefore, the way how to establish trust relationship among previously unknown devices or resources is needed under such environments. In this paper, we firstly review a model to delegate the trust to communicating entities in ubiquitous environment and its security problems(e.g., malicious right-delegation and revocation of right-delegation). Then, we design a new model for secure delegation over communication entities which is based on two-party signature scheme, and implement it.


**Key words:** Trust Management(신뢰 관리), Authentication(인증), Ubiquitous Computing(유비쿼터스 컴퓨팅)

## 1. 서 론

오늘날의 컴퓨팅은 데스크탑에서 벗어나 개인 디지털 장치를 통해 주위에서 쉽게 접할 수 있는 유비쿼터스 환경으로 변화하고 있다. 유비쿼터스 환경의 가장 두드러진 특징은 사용자들이 언제 어디서나 컴퓨팅 자원에 접속할 수 있다는 것이다. 예를 들어, 한 사용자의 건물 안의 복도를 지나갈 때 자동으로 전등이 켜지거나, 건물 안의 어떤 방에 들어갔을 때 음악이 자동적으로 흘러나오는 것처럼 사용자에 대하여 컴퓨팅 자원이 능동적으로 대처하는 컴퓨팅 환경을 의미하며, 이와 같은 능동적인 제한된 공간을 스마트 공간(SmarkSpace)이라고 한다. 즉, 스마트 공간의 실현은 곧 유비쿼터스 컴퓨팅 환경의 실현이

※ 교신저자(Corresponding Author) : 이경현, 주소 : 부산광역시 남구 대연3동 599-1(608-739), 전화 : 051)620-6395, FAX : 051)626-4887, E-mail : khrhee@pknu.ac.kr
접수일 : 2005년 7월 18일, 완료일 : 2005년 10월 27일
[†] 준회원, 부경대학교 전자계산학과
(E-mail : bogus@itslab.csce.kyushu-u.ac.jp)
[††] 준회원, (주)정보보호기술
(E-mail : ssssblue@infosec.co.kr)
[†††] 정회원, 동명대학교 정보보호학과
(E-mail : shinweon@tit.ac.kr)
[††††] 종신회원, 부경대학교 전자계산학과
※본 이 논문은 2003학년도 부경대학교 기성회 학술연구비에 의하여 연구되었음.

될 수 있다는 것이다. 유비쿼터스 컴퓨팅 환경에서 사용자는 언제 어디서나 자원과 서비스에 접근하기를 원하지만, 사용자의 자원 접근에 대한 제어를 수행하고자 할 때, "사전에 신뢰하지 못한 상태의 자원이나 장치들 사이에서 서로간의 안전한 신뢰 관계를 어떻게 형성시킬 수 있는가?"라는 문제가 제기된다. 또한, D. Hutter 등은 [6]에서 유비쿼터스 컴퓨팅 환경을 위해서 새롭게 연구되어야할 다양한 보안 기술들 중에서 신뢰 관리(Trust management) 기술이 선결되어야 할 연구 분야로 소개하고 있다. 본 논문에서는 다양한 형태로 구체화되는 유비쿼터스 컴퓨팅 환경들 중에서 제한된 공간인 스마트 공간에서의 외부 사용자에 대한 신뢰 관계 형성을 성공적으로 수행할 수 있는 기술에 대해서 논하고자 한다.

본 논문에서는 기 제안된 분산된 신뢰(Distributed Trust) 기법에서 외부 사용자에 대한 신뢰 관계 형성을 위하여, "권한 위임"을 통한 참여 제어를 수행하는 방안을 살펴본다. 그리고, 분산된 신뢰 기법의 권한 위임을 통한 참여 제어 시에 발생할 수 있는 보안 위협을 지적한다. 또한, 이를 근간으로 mRSA(mediated RSA) [5]와 UCTPS(User Controllable Two Party Schnorr signature) [10]와 같은 양자간 전자서명 기법을 통하여, 외부 사용자로의 권한 위임에 대한 안전성이 개선된 새로운 참여 제어(Admission Control) 시스템을 설계 및 구현한다. 2장에서는 관련 연구로서 스마트 공간을 구현하기 위한 기존의 연구와 분산된 신뢰 기법을 소개한 후, 분산된 신뢰 기법에서의 권한 위임에 따른 참여 제어에서의 보안 이슈에 대해서 논한다. 3장에서 본 논문에서 제안하는 스마트 공간을 위한 새로운 참여 제어 시스템의 구조를 살펴본다. 그리고 4장에서는 제안 시스템의 구체적인 동작 프로토콜과 안전성에 대해 기술하며, 5장에서는 시스템 구현 및 성능 분석 결과를 소개한다. 마지막으로, 6장에서 결론을 맺는다.

## 2. 관련 연구

### 2.1 분산된 신뢰 (Distributed Trust) 기법

지금까지 스마트 공간의 실현을 위하여, 인터렉티브 워크스페이스 프로젝트(Interactive Workspace Project) [7]와 닌자 프로젝트(Ninja Project) [14]등과 같은 프로젝트들이 진행되었다. 스텐포드 대학의 인터렉티브 워크스페이스 프로젝트는 무선 LAN을 통하여 대형 디스플레이 장치, 노트북 그리고 PDA 등과 같은 이기종 장치들 사이의 통신을 위한 하드웨어/소프트웨어 테스트 배드를 개발하였다. 또한, 닌자 프로젝트는 버클리 대학에서 진행되었던 것으로, 개인용 컴퓨터, 이동 전화기 그리고 PDA와 같은 이기종 장치를 연결시키기 위한 연구이다. 전체 기반 구조에 일종의 인공 지능을 추가하여, 동일 컨텐츠를 특정 장치에 맞도록 자동으로 번안이 가능하도록 고안되었다. L. Kagal 등은 인텔리전트 서비스들로 구성된 스마트 공간을 실현하기 위하여 Centaurus 시스템을 제안하였다 [12]. Centaurus 시스템의 목적은 이기종인 다수의 장치들이 다양한 형태의 서비스들을 사용 가능하도록 하는 일관된 기반구조(Uniform Infrastructure)를 제공하기 위한 기술로서, 적외선 또는 무선 LAN과 같은 근거리 무선 통신을 통하여, 이동 장치의 사용자들이 스마트 공간내의 인텔리전트 서비스들에게 접근하는 환경을 고려하고 있다. 또한, Centaurus 시스템에서의 인증, 접근제어 및 권한 위임과 같은 다양한 보안 요구사항을 만족시키기 위하여, 새로운 시스템인 Vigil [11]을 제안하였다. Vigil 시스템을 구성하는 6개의 주요 구성 요소와 기능은 아래와 같다.

- 서비스 관리자(Service Manager) : Vigil에서의 스마트 공간은 하나 이상의 서비스 관리자에 의해서 제어된다. 사용자들과 서비스들은 서비스 관리자에 등록하며, 서비스 관리자는 그 둘 사이의 서비스 제공을 위한 중재를 수행한다.
- 통신 관리자(Communication Manager) : 서비스 관리자와 스마트 공간내의 통신 개체들 사이의 통신을 통로를 제공함으로써, 사용되는 통신 프로토콜의 추상화 및 번역을 수행한다.
- 인증서 관리자(Certificate Manager) : Vigil내의 통신 개체들을 위한 X.509 인증서를 발행 및 인증서 유효성 검증을 위한 질의에 대한 응답을 수행한다. 인증서 유효성 검증을 위한 응답은 기존의 Online Certificate Status Protocol(OCSP)나 Certificate Revocation List(CRL)을 사용한다.
- 역할 할당 관리자(Role Assignment Manager)

: Vigil내의 알려진 통신 개체들에 대한 역할 리스트와 역할 할당을 위한 규칙 집합을 유지 관리한다. 스마트 공간내의 역할 할당을 위하여 다른 개체로부터의 요청에 응답을 한다.

- 보안 에이전트(Security Agent) : 스마트 공간내의 신뢰(trust)를 관리한다. 사용자에게 수여된 새로운 접근 권한들과 취소된 권한들에 대한 정보를 수집 관리하며, 현재 그 사용자가 소유한 권한들에 대한 추론을 수행한다.
- 클라이언트(Client) : 사용자와 서비스를 의미한다.

Vigil에서는 인증, 접근제어 및 권한 위임과 같은 다양한 보안 요구사항을 만족하기 위하여 "분산된 신뢰(Distributed Trust)" 기법을 통해서 해답을 찾고자 하였다. 분산된 신뢰 기법은 시스템을 위한 보안 정책(Security policy), 스마트 공간을 위한 신임장(Credential) 발행 및 검증, 외부 사용자에 대한 신뢰의 위임(Delegation), 권한들에 대한 취소 및 접근 권한에 대한 판단 등과 같은 다양한 보안 메커니즘을 포함하고 있다. 특히, 본 논문에서는 분산된 신뢰 기법에서 외부 사용자에게 신뢰를 위임하기 위한 보안 메커니즘을 논하고자 한다. 유비쿼터스 컴퓨팅 환경을 고려하면, 외부 사용자들은 스마트 공간내의 어떠한 역할(Role)이 사전에 정의되어 있지 않기 때문에, 그 역할에 따른 접근 권한(Access right)들을 설정하기 위한 규칙(Rule)을 새로이 정립할 필요가 있다. 즉, 스마트 공간에 대한 외부 사용자들에 대한 접근 제어를 위하여, 외부 사용자의 X.509 인증서의 검증을 통해서는 "스마트 공간내의 특정 서비스에 대한 사용 권한"을 결정하기가 어렵다. 따라서 분산된 신뢰 기법에서는 스마트 공간내의 특정 인가된 사용자가 자신의 권한과 기간의 범위 내에서 외부 사용자를 위하여 서비스 사용 권한을 위임함으로써, 외부 사용자에 대한 접근 제어를 수행하고 있다.

어떤 사용자가 자신이 사전에 소유한 권한을 타인에게 위임할 경우 그 행위를 위임(delegation)이라 하며, 전자를 위임자(delegator)라고 하며, 후자를 위임 수혜자(delegatee)라고 한다. 만약 어떤 사용자가 특정 서비스에 대한 접근 권한을 가지거나 인가된 사용자로부터 그 권한을 위임 받았을 경우, 그 사용자는 대상 서비스에 대한 접근을 할 수 있게 된다. 이와 같은 방법은 기존에 잘 알려진 Simple Public Key Infrastructure(SPKI)와 Pretty Good Privacy(PGP)와 같이 신뢰를 위임할 수 있는 보안 모델과 유사한 형태를 가지고 있으나, 위임 수혜자가 얻은 위임 정보에 대한 스마트 공간 내의 접근 제어는 시스템 보안 정책을 추가적으로 고려하여 이루어진다. 특히, 외부 사용자와 같이 스마트 공간을 위하여 사전에 어떠한 권한도 없는 경우, 접근 제어를 위하여 "위임자의 권한", "위임 수혜자가 위임자로부터 부여 받은 위임 정보"와 "보안 정책"을 모두 고려하여 접근 제어를 수행하고 있다. 따라서, 위임자가 스마트 공간에서 탈퇴 또는 전임으로 인한 권한의 취소 발생은, 위임 수혜자의 위임 정보가 비록 현재 유효할 지라도 즉시적으로 취소가 된다. (그림 1)은 스마트 공간의 한 형태인 스마트 오피스에서의 위임 정보를 생성하기 위한 시나리오를 보여주고 있다. 본 논문에서는 접근 제어를 위한 보안 정책(Security policy)에 대한 상세한 기술은 생략한다.

"컴퓨터 수리기사(A)는 스마트 오피스의 파트너 회사의 근무자이다. 하지만, 스마트 오피스 내의 보안 관리자는 A의 신원을 알지 못하기 때문에, A는 기본적으로 스마트 오피스내의 서비스 이용에 대한 접근이 거부된다. 따라서, A는 스마트 오피스내의 매니저 중 누군가에게 자원이나 서비스를 이용할 수 있는 권한에 대한 위임을 요청한다. A의 요청을 수신한 매니저(B)는 A를 위한 위임자가 된며, B는 위임 수혜자가 된다. 만약, 보안 정책에 의해서 B가 자신이 신뢰하는 이에게 자원에 대한 접근 권한을 위임할 수 있는 권한을 가질 경우, B는 A에게 자원과 서비스 접근 권한에 대한 위임 정보를 자신의 개인키로 전자서명하여 발급하고, 이를 보안 에이전트에게 통보한다. 보안 에이전트는 위임자의 역할과 위임자가 권한을 위임할 수 있는가를 검사한다. 또한, 위임 정보가

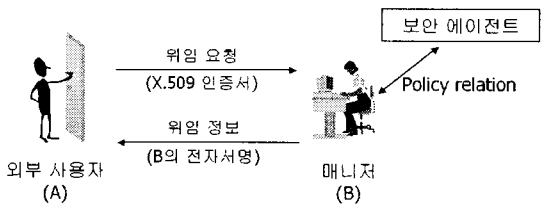


그림 1. 분산된 신뢰 기법에서의 위임 정보 생성

보안 정책에 부합되는가를 검사한다. 결국, A는 수신한 위임 정보 내에 서술된 권한의 범위 안에서 보안 에이전트의 인가를 받을 수 있으므로, 스마트 오피스의 자원과 서비스에 접근이 가능하게 된다. 물론, 위임 정보에 대한 유효기간(아주 짧은 기간)이 만료된다면 자원에 대한 A의 접근은 즉시 거부된다."

만약 위임자가 자신이 외부 사용자에게 위임했던 권한을 유효기간 이전에 취소하고자 할 경우, 그 위임자는 보안 에이전트에게 위임 취소를 요청하는 메시지를 전송한다. 보안 에이전트는 위임 수혜자의 권한을 즉시 취소시킨다. 따라서 외부 사용자가 어떤 서비스를 사용하기 위하여 서비스 관리자를 접근하면, 그 서비스 관리자는 보안 에이전트에게 외부 사용자가 소유한 위임 정보의 유효성에 대하여 질의한다. 그러면, 보안 관리자는 그 외부 사용자의 위임은 취소되었음을 서비스 관리자에게 통보를 할 것이므로, 외부 사용자는 더 이상 서비스에 대한 접근을 할 수 없게 된다.

하지만, 위의 스마트 오피스 시나리오는 "위임자가 악의적으로 외부 사용자(위임 수혜자)와 공모를 할 경우, 스마트 오피스 내의 보안 정책에 합당한 오용된 권한의 위임"이 발생할 수 있다. 즉, 외부 사용자(A)와 공모를 한 매니저(B)는 자신이 소유한 개인키로서 자신이 위임할 수 있는 권한 범위 내에서 아무런 제약 없이, A를 위한 위임 정보를 생성할 수 있으며, 생성된 위임 정보는 보안 에이전트의 보안 정책에 대한 검사를 아무런 문제없이 쉽게 통과할 수 있을 것이다. 또한, 이러한 경우에 "악의적 B로부터 위임할 수 있는 권리를 즉시적으로 취소"를 위한 방법이 요구된다. 참고 문헌 [11,12]에서는 악의적인 권한 위임에 대한 보안 위협에 대한 소개와 그에 따른 해결 방안에 대한 기술적인 내용은 포함되어 있지 않다. 다만, Vigil의 6개의 주요 구성 요소들의 기능에 따라서 추론할 수 있는 해결책은 악의적 위임 발생시에 인증서 관리자가 악의적 매니저에 대한 서명 능력 취소를 위하여, 인증서 취소 정보를 OCSP나 CRL 등과 같은 방법으로 해당 스마트 오피스 내의 보안 에이전트에게 취소 사실을 통보한다. 그러면, 악의적 매니저에 대한 권한 위임 및 매니저의 스마트 공간 내의 서비스들로의 접근은 보안 에이전트에 의해서 차단될 수 있다. D. Boneh 등은 Semi-Trusted Mediator(SEM)이라는 온라인 기관을 통하여, 기존의 OCSP나 CRL보다 더욱 빠른 인증서 취소가 가능한 메커니즘을 소개하였다 [5]. 이러한 빠른 인증서 취소는 RSA 전자서명의 변형인 mediated RSA (mRSA)와 같은 양자간 전자 서명을 통하여 가능하게 된다.

본 논문에서는 "공모를 통한 악의적 권한 위임 발생"과 "악의적 위임자의 빠른 위임 능력 취소"와 같은 보안 이슈를 해결하기 위해서, 양자간 서명 기법을 통하여 위임자의 서명 권한을 효율적으로 제어함으로써, "악의적 위임자의 권한 위임을 위한 전자 서명 수행의 방지" 및 "악의적 위임자의 서명 능력에 대한 빠른 취소"를 위한 방안을 모색하고자 한다. 따라서 새로이 설계되는 권한 위임을 위한 시스템은 아래와 같은 요구사항을 만족시켜야 한다.

- 매니저는 단독으로 외부 사용자에게 위임 정보를 발행하지 못해야 한다.
- 악의적인 매니저에 대한 즉시적인 위임 권한에 대한 취소가 가능해야 한다.
- 외부 사용자는 해당 스마트 오피스를 위한 새로운 신원(identity)이나 역할(role) 생성에 대한 부담 없이, 자원과 서비스에 접근이 가능해야 한다.

본 논문에서는 기 제안된 분산된 신뢰 기법에서 위임 정보의 생성 절차에 대한 안전한 방안만을 모색한다. 즉, 분산된 신뢰 기법에서의 권한 및 위임을 위한 보안 정책은 본 논문의 연구 범위를 벗어난다. 따라서 본 연구는 기존의 분산된 신뢰 방안에서의 위임 정보의 보다 안전하게 생성시킴으로써, 외부 사용자의 "참여 제어"를 성공적으로 수행하기 위한 새로운 시스템의 설계 및 구현을 목적으로 한다.

### 2.2 양자간 서명 기법(Two-party signature scheme)

본 논문에서는 제안 시스템의 구체화를 위하여, 소인수분해 문제에 기반한 mRSA(mediated RSA) 기법[5]과 이산대수 문제에 기반한 UCTPS(User Controllable Two Party Schnorr signature) 기법[10]을 암호학적 도구로 사용한다. 위의 두 기법들은 전자 서명을 수행하기 위해서, 개인키를 두 부분으로 나누어서 각 부분을 양자간이 나누어 소유하게 된다. 따라서 유효한 전자 서명문을 생성하기 위하여 양자

서로 간의 전자서명 연산을 위한 협력이 요구되기 때문에, 어느 한쪽이라도 단독으로 유효한 전자 서명문을 생성할 수 없다.

## 3. 참여 제어 시스템의 구조

(그림 2)는 본 논문에서 제안하는 시스템에서 외부 사용자에게 위임 정보를 발행하기 위한 절차를 보여주고 있다. 제안 시스템에서의 시스템 구성요소와 전제조건은 아래와 같다.

- $FU$ : 외부 사용자. Certification Authority (CA)로부터 발급받은 X.509 인증서와 키 쌍을 소유한다. 스마트 오피스 내의 자원을 접근하기 위해서, 멤버에게 참여(즉, 권한 위임)을 요청한다.
- $SM$ : 스마트 오피스 내의 보안 관리자(Security Manager). Vigil의 보안 에이전트의 기능을 수행하며, 스마트 오피스 내의 각 멤버의 개인키에 대한 부분 정보를 소유한다. 따라서 각 멤버와 협력하여 외부 사용자에게 발행할 위임 정보를 생성한다. 악의적인 멤버의 단독적인 위임 행위를 방지하는 역할을 수행하며, 악의적 멤버에 대한 전자 서명 지원을 수행하지 않음으로써, 악의적 멤버에 의한 위임 행위를 즉시적으로 취소 가능하다. [5]의 SEM과 같이 $SM$은 공격자로부터 침해를 당하지 않는 한 악의적인 행위를 하지 않음을 가정한다.
- $M_i$ : 스마트 오피스 내의 $i$번째 멤버. 각 멤버의 개인키는 두 부분으로 나뉘어져 한 부분은 멤버가 소유하고, 다른 부분은 $SM$이 소유한다. 외부 사용자로부터 참여 요청을 받을 때 위임자 역할을 하게 되며, CA로부터 발급받은 X.509 인증서를 소유한다.
- $AC_{FU}$ : 참여 신임장(Admission Credential). 제안 시스템에서의 권한 위임 정보로서, 스마트 오피스 내의 자원에 대한 접근 권한 및 유효 기간이 명시되어 있다. $FU$는 $AC_{FU}$를 통하여 스마트 오피스 내의 자원에 대한 제한된 접근이 가능하다.

$FU$로부터 위임 요청을 받은 $M_i$는 보안 정책에 따라서 $AC_{FU}$를 위한 권한 정보를 구성하고, $SM$과 협력하여 그에 대한 전자 서명을 수행하여, 최종적으로 $FU$를 위한 $AC_{FU}$를 발행한다. $FU$는 획득한 $AC_{FU}$ 내의 권한과 유효 기간에 따라 스마트 오피스 내의 자원 및 서비스에 접근할 수 있다. 본 논문에서는 스마트 오피스 내의 보안 정책과 각 멤버들이 소유한 구체적인 권한의 설정 및 운용에 대한 규칙들은 이미 정의가 되어 있다고 가정한다.

## 4. 참여 신임장의 발행

본 논문에서 제안되는 참여 제어 시스템의 시스템 초기화 및 참여 신임장 발행을 위한 통신 개체간의 메시지 전달은 인증된 형태로 이루어짐을 가정한다. 제안되는 참여 신임장 발행 프로토콜은 적용되는 암

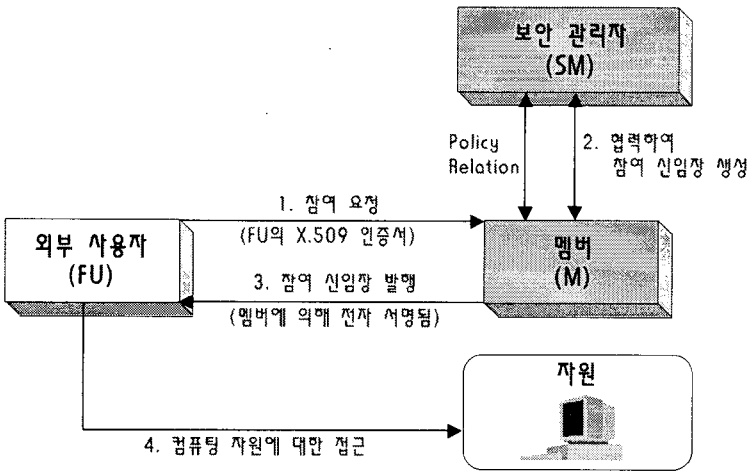


그림 2. 제안 시스템의 위임 정보 발행

호학적 도구에 따라 다음과 같이 분류된다.

- TYPE-I : 암호학적 도구로 mRSA를 사용
- TYPE-II : 암호학적 도구로 UCTPS를 사용

### 4.1 초기화 프로토콜

시스템을 초기화하기 위해 2.1절의 신뢰 기관인 인증서 관리자(Certificate Manager : CM)는 멤버 $M_i$를 위하여 아래의 과정을 수행한다. 본 논문에서는 RSA와 Schnorr 전자 서명 기법의 키 생성 규칙에 대한 소개는 생략한다 [1,4].

**(Step 1)** CM은 스마트 오피스 내의 각 $M_i$를 위한 키 쌍을 생성한다.

- TYPE-I : CM은 RSA의 키 생성 규칙에 따라 $M_i$에 대한 개인키$(d_{M_i}, N_{M_i})$와 공개키$(e_{M_i}, N_{M_i})$를 생성한다.
- TYPE-II : CM은 Schnorr 서명 기법의 키 생성 규칙에 따라 $M_i$에 대한 개인키$x_{M_i}$와 공개키 $y_{M_i} = g^{x_{M_i}} \bmod p$를 생성하며, 스마트 오피스 내에 $p$, $q$, $g$를 공개한다. 여기서, $q$는 $p-1$을 나누는 소수.

**(Step 2)** CM은 $M_i$의 개인키를 두 부분으로 나누어, 각 부분을 안전하게 $M_i$와 $SM$에게 보낸다.

- TYPE-I : CM은 $d_{M_i} = d_{1..M_i} + d_{2..M_i} \bmod \phi(N_{M_i})$를 만족하는 $d_{1..M_i}$과 $d_{2..M_i}$을 구한 후, $d_{1..M_i}$을 $M_i$에게, $d_{2..M_i}$을 $SM$에게 안전하게 전송한다.
- TYPE-II : CM은 랜덤한 수 $\delta_{M_i}$를 생성하고 $SK_{M_i} = x_{M_i} + \delta_{M_i} \bmod q$를 계산한 후, $M_i$에게 $\delta_{M_i}$를 보내고, $SM$에게 $SK_{M_i}$를 안전하게 전송한다.

**(Step 3)** CM은 $M_i$에게 대응되는 X.509 인증서를 발행한다.

위의 프로토콜은 스마트 오피스 내의 멤버의 수만큼 실행된다.

### 4.2 참여 신임장 발행 프로토콜

$FU$가 스마트 오피스내의 자원에 접근하기 위하여, 참여 신임장 $AC_{FU}$를 발행 받기 위해서 아래의 절차가 수행된다. (그림 3)은 mRSA가 암호학적 도구로 사용될 때인 TYPE-I에서의 프로토콜을 보여주고 있으며, (그림 4)는 UCTPS가 암호학적 도구로 사용될 때인 TYPE-II에서의 프로토콜을 보여주고 있다.

**(Step 1) 참여 요청**

$FU$는 자신이 접속 가능한 임의의 멤버 $M_i$에게 참여 요청을 하기 위하여, 자신의 X.509 인증서와 인증서 내의 공개키에 대응되는 개인키로서 서명된 챌린지(Challenge)를 $M_i$에게 전송한다. 챌린지를 구성하는 파라메터는 스마트 오피스 내의 보안 정책에 따라서 다양한 형태로 구성될 수 있다.

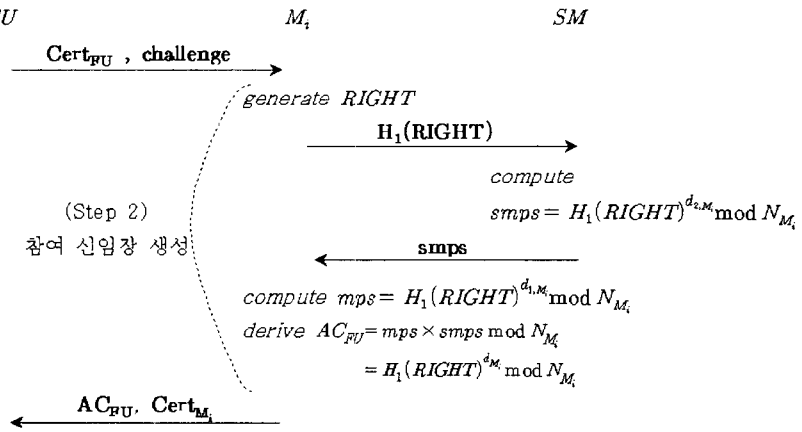


그림 3. 참여 신임장(Admission Credential) 발행 프로토콜 (CASE-1)
$Cert_{FU}$ : $FU$의 X.509 인증서, $Cert_{M_i}$ : $M_i$의 X.509 인증서,
challenge : $FU$의 전자 서명문, $H_1(\cdot)$ : PKCS#1 또는 OAEP 패딩

**(Step 2) 참여 신임장 생성**

$M_i$가 $FU$의 참여 요청을 수령한 후, $M_i$가 자신이 속한 스마트 오피스내의 자원에 대한 접근 권한을 위임할 수 있는 권한을 소유한다면, 수신한 참여 요청 내에 포함된 $FU$의 X.509인증서와 서명된 챌린지에 대한 유효성을 검증한다. 검증 결과가 옳다면 $M_i$는 보안 정책과 자신의 위임 권한 한도 내에서 $FU$를 위한 권한 정보($RIGHT$)를 구성한 후, $M_i$는 참여 신임장을 생성하기 위하여, (그림 3)과 (그림 4)와 같이 $SM$과 협력하여 $AC_{FU}$을 생성한다. 여기서, $SM$은 수신한 $RIGHT$가 보안 정책 및 $M_i$의 위임 권한에 부합되는지를 판단하여, 유효할 경우에만 $smps$를 계산하여 $M_i$에게 돌려준다.

**(Step 3) 참여 신임장 발행**

$M_i$는 참여 요청을 송신한 $FU$에게 $AC_{FU}$와 $M_i$의 X.509 인증서를 전달한다. $FU$는 $M_i$의 인증서를 검증한 후, $M_i$의 공개키를 이용하여 $AC_{FU}$를 검증하게 된다. 모든 검증이 성공적이면, $FU$는 획득한 $AC_{FU}$내의 접근 권한과 유효 기간의 범위 내에서 스마트 오피스의 자원 및 서비스를 서비스 관리자를 통하여 접근이 가능하게 된다.

### 4.3 제안 시스템의 고찰

제안 방안은 다음과 같은 속성을 만족시킨다.

■ **즉시적인 위임 취소** : 제안 시스템은 $SM$이 $M_i$의 위임 권한을 파기하고 싶은 경우, $SM$은 단지 $M_i$의 개인키의 일부를 이용한 전자서명 연산을 수행하지 않음으로써 $M_i$의 위임 능력을 쉽게 취소 할 수 있다.

■ **공모에 대한 안전성** : 멤버와 보안 관리자가 협력하여 외부 사용자를 위한 참여 신임장을 발행하며, 보안 관리자는 참여 신임장 발행 이전에 항상 외부 사용자에게 위임되는 권한 정보에 대한 검사를 수행한다. 따라서 스마트 오피스내의 멤버와 외부 사용자로부터의 공모 공격에 의한 침해를 최소화할 수 있다.

■ **개인키의 강력한 보호** : $M_i$의 개인키를 두 장소로 나누어 배치시킴으로서 제안 시스템은 양자간 서명 기법을 사용하도록 구성했다. 그로 인해 $M_i$의

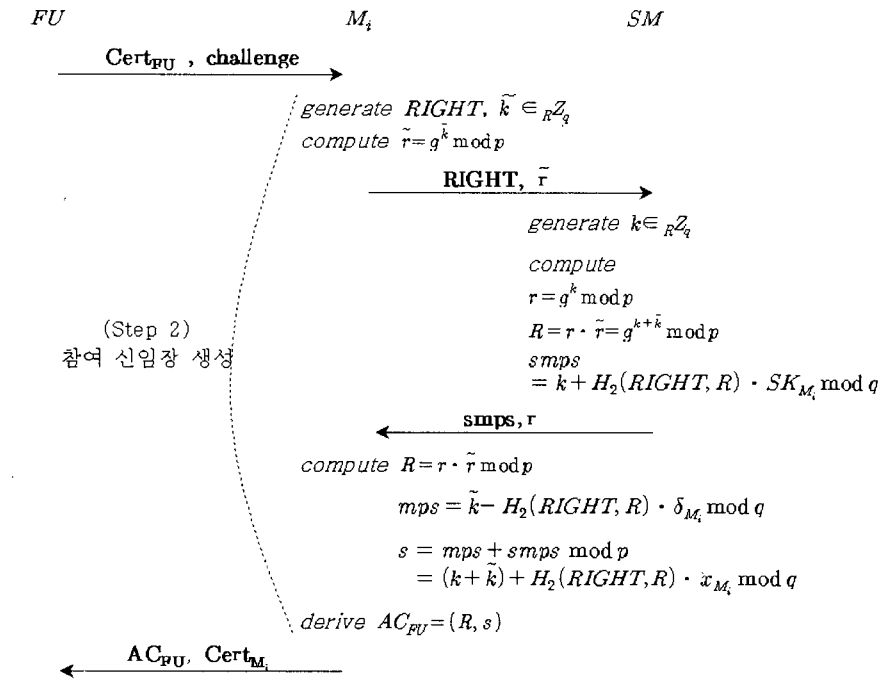


그림 4. 참여 신임장(Admission Credential) 발행 프로토콜 (CASE-2)
$H_i(\cdot)$ : 암호학적 일방향 해쉬 함수

개인키를 알아내려는 공격자는 $M_i$ 뿐만 아니라 $SM$까지 동시에 공격을 성공시켜야 하는 어려움이 존재한다.

■ **새로운 신원과 역할 생성의 불필요** : $FU$는 해당 스마트 오피스를 위하여 새로운 신원이나 역할을 생성할 필요 없이 참여 신임장 내의 권한과 유효기간 내에 자원에게 접근이 가능하다.

### 4.4 보안 관리자(Security Manager)에 대한 보안성 강화

본 논문에서 제안된 참여 제어 시스템은 스마트 오피스 내의 멤버들의 서명 능력을 양자간 전자 서명 기법을 통하여 제한하고 있다. 그로 인하여, 보안 관리자는 멤버들의 개인키의 부분키들을 멤버들의 수만큼 소유하게 됨으로써, 악의적인 공격자의 주요 공격 대상이 될 수 있다. 또한, 보안 관리자가 시스템 결함 등의 이유로 4.2절의 참여 신임장 발행 프로토콜을 수행할 수 없을 경우, 외부 사용자들은 스마트 오피스 내의 참여가 불가능하게 된다.

보안 관리자의 단일 실패(single failure)로 인한 시스템의 동작 불능에 대한 강건성을 위하여, 보안 관리자를 임계 암호 시스템(Threshold cryptosystem)을 통한 분산된 서버 시스템으로 구성하는 방안을 고려할 수 있다. 즉, $n$개의 서버들로 구성된 분산 시스템이 보안 관리자로서 동작하게 되며, 보안 관리자가 보관하고 있는 각 멤버의 개인키의 부분키를 $n$개의 서버들에게 비밀 분산(Secret sharing)을 통하여 안전하게 분배 시킨다 [2]. 4.2절의 참여 신임장 발행 프로토콜에서 보안 관리자가 $smps$를 생성하기 위해서, $(n,t)$-임계 암호 시스템을 통하여, $n$개의 서버들 중에서 $t$개 $(n \geq 2t-1)$의 서버들만 참여하여도 $smps$를 성공적으로 계산할 수 있다. 하지만, 보안 관리자를 분산된 형태로 구현할 경우, 시스템의 강건성에 대한 이득은 전체적인 성능 감소를 수반하게 된다. 또한, 보안 정책에 따른 각 서버들의 참여 신임장 발행에 대한 결정(decision)의 일관성(consistency)을 보장하기 위해서, 시스템 운영에 대한 복잡도 또한 증대되는 단점을 가지게 된다. TYPE-I의 경우 mRSA와 [8]에서 소개된 Threshold RSA의 결합을 통하여 분산 시스템을 구성할 수 있을 것이며, TYPE-II의 경우 UCTPS와 [13]에서 소개된 Threshold Schnorr의 결합을 통하여 분산 시스템을 구성할 수 있다. 비록 [8]의 Threshold RSA의 경우 [15]에서 반복적인 능동적 비밀 분산(Proactive secret sharing) 수행에 따른 취약성이 발견되었으나, 본 논문에서 능동적 비밀 분산에 대한 안전성을 고려하는 것은 본 논문의 주요 연구 범위를 너무 벗어난다.

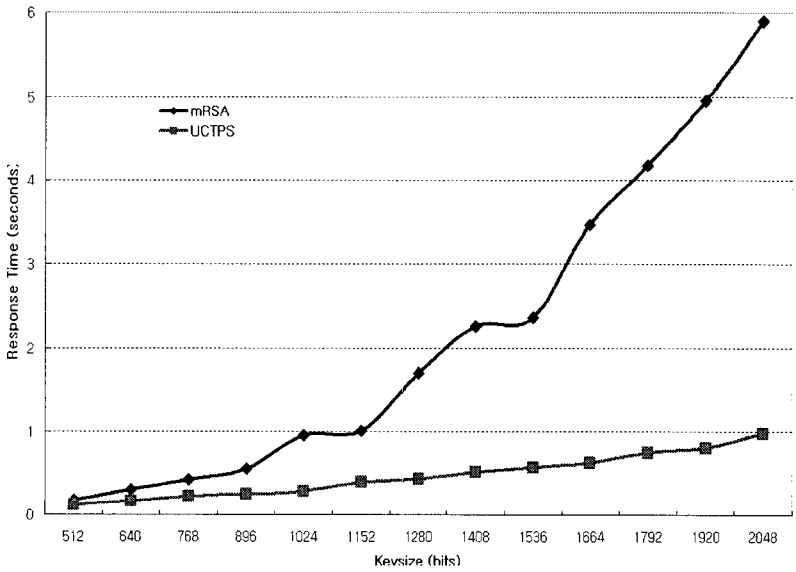


그림 5. Keysize변화에 따른 응답시간(Pentium IV 1.5GHz)

## 5. 시스템 구현 결과

본 논문에서 제안된 참여 제어 시스템을 구현하기 위해서 Java 언어를 사용하였으며, Schnorr 전자 서명 기법의 키 생성을 위해서 Bouncy Castle package를 사용하였다 [3,9]. 특히, Schnorr 전자 서명 기법의 키 생성을 위한 $p$와 $q$ 값에 대한 비트 크기는 DSS (Digital Signature Standard)를 따랐다. 제안 시스템에서 사용된 암호학적 도구인 mRSA와 UCTPS를 통하여, 외부 사용자가 참여 신임장을 획득하는데 소요되는 응답시간은 (그림 5)와 같다. mRSA의 경우 keysize가 증가할수록 UCTPS에 비하여 응답 시간이 상대적으로 급격히 증가함을 보이나, 현재 일반적으로 많이 사용되는 1024-bits의 키 사이즈에서는 수용할 만한 성능을 보이고 있다.

(그림 6)은 제안되는 참여 제어 시스템의 구현에서 사용된 참여 신임장(Admission Credential)을 Abstract Syntax Notation One (ASN.1)으로 표현한 것이며, (그림 7)에서 (그림 9)는 제안된 참여 제어 시스템의 GUI(Graphic User Interface)를 보여주고 있다.

외부 사용자는 (그림 7)-①로서 스마트 오피스내의 멤버에게 참여 요청을 수행하며, 멤버는 (그림 8)-②를 통하여 외부 사용자의 X.509 인증서 정보를 확

```
Credential ::= SEQUENCE {
  AdmissionCredential                   AdmsCredential,
  signatureAlgorithm                    AlgorithmIdentifier,
  signatureValue                        BIT STRING,
  hashAlgorithm                         AlgorithmIdentifier,
  hashValue                             OCTET STRING }

AdmsCredential ::= SEQUENCE {
  serialNumber                          INTEGER,
  issuer                                Name,
  subjectrPublicKeyInfo                 SubjectrPublicKeyInfo,
  validity                              Validity,
  accessRight                           SET OF RightValue,
  signature                             AlgorithmIdentifier,
  hash                                  AlgorithmIdentifier }

AlgorithmIdentifier ::= OBJECT IDENTIFIER

SubjectrPublicKeyInfo ::= SEQUENCE {
  algorithm                             AlgorithmIdentifier,
  sujectPublicKey                       BIT STRING }

Validity ::= SEQUENCE {
  notBefore                             UTCTime,
  notAfter                              UTCTime }

RightValue ::= SEQUENCE {
  serviceName                           UTF8String,
  serviceCode                           INTEGER }

Name ::= CHOICE { RDNSequence }

RDNSequence ::= SEQUENCE OF RDN

RDN ::= SET OF AttributeTypeValue

AttributeTypeValue ::= SEQUENCE {
  type                                  AttributeType,
  value                                 AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
  utf8String                            UTF8String }
```

그림 6. 참여 신임장을 위한 ASN.1 Notation

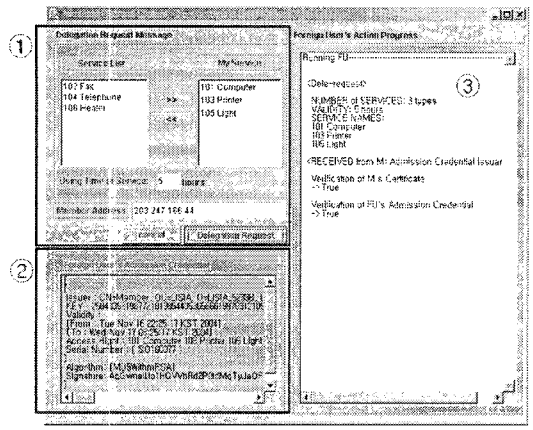

그림 7. 외부 사용자의 Action Frame

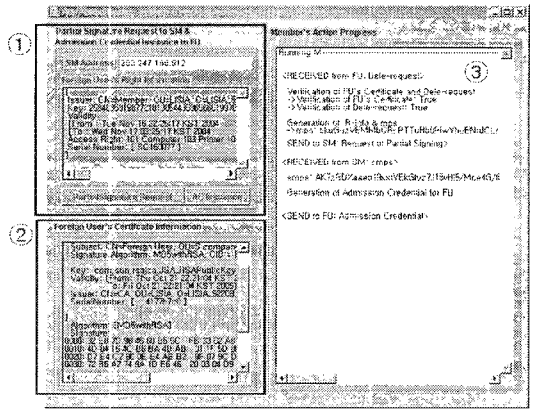

그림 8. 멤버의 Action Frame

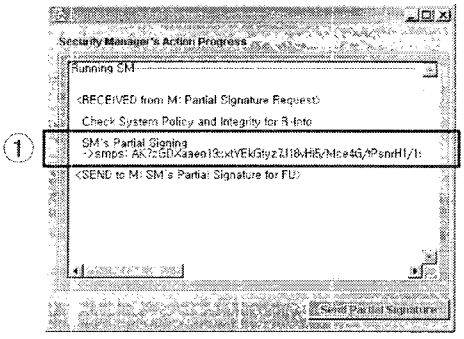

그림 9. 보안 관리자의 Action Frame

인 가능하다. 멤버는 (그림 8)-①로서 외부 사용자를 위한 권한 정보를 생성하고, 보안 관리자에게 부분 서명을 요청한다. 보안 관리자는 (그림 9)-①과 같이 부분 서명을 생성하여, 멤버에게 전송한다. 멤버는 수신한 부분 서명을 통하여, 외부 사용자를 위한 참여 신임장을 생성한다. 생성한 참여 신임장은 외부 사용자에게 전달되며, (그림 7)-②를 통해서 외부 사용자는 획득한 참여 신임장을 확인할 수 있다. 또한, (그림 7)-③ , (그림 8)-③과 (그림 9)를 통하여, 4.2절에서 소개된 참여 신임장 발행 프로토콜의 실질적인 진행과정을 확인할 수 있다.

## 6. 결 론

본 논문에서는 스마트 오피스에서 외부 사용자의 참여를 위하여, "분산된 신뢰" 기법의 권한 위임 방안에 대한 두 가지 보안 문제점들을 소개하였다. 또한, 보안 문제점들을 해결하기 위하여 새로운 보안 요구사항을 도출하고, 이를 만족하는 새로운 참여 제어 시스템을 설계 및 구현하였다. 제안된 시스템은 "즉시적인 위임 취소", "공모에 대한 안전성", "개인키의 강력한 보호" 와 "새로운 신원과 역할 생성 불필요" 와 같은 속성들을 만족시킴으로써, 유비쿼터스 컴퓨팅 환경에서 특수 그룹으로의 참여 제어를 위해 적절히 활용 가능할 것이다.

## 참 고 문 헌


[1] Alfred J. Menezes, Paul C. van Ocrshot, and Scoot A. Vanstone, *Handbook of Applied Cryptography*, CRC press, 1997.

[2] A. Shamir, "How to Share a Secret," *Communications of the ACM*, Vol. 22, pp. 612-613, 1979.

[3] Bouncy Castle 1.24, *http://www.bouncycastle.org*, 2005. 6.

[4] Douglas R. Stinson, *Cryptography: Theory and Practice - Second edition*, Chapman & Hall, CRC press, 2002.

[5] D. Boneh, G. Tsudik, and G. M. Wong, "A method for fast revocation of public key certificates and security capabilities," *10th USENIX Security Symposium*, pp. 297-308, 2001.

[6] D. Hutter, W. Stephan, and M. Ullmann, "Security and Privacy in Pervasive Comput-

ing : State of the Art and Future Directions," *Security in Pervasive Computing*, LNCS 2802, pp. 285-289, 2004.

[7] George Candea and Armando Fox, "Using Dynamic Mediation to Integrate COTS Entities in a Ubiquitous Computing Environment," *Second International Symposium on Handheld and Ubiquitous Computing* 2000, pp. 216-226, 2000.

[8] H. Luo and S. Lu, *Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks*, Technical Report TR-200030, Dept. of Computer Science, UCLA, 2000.

[9] J. Garms and D. Somerfield, *Professional Java Security*, Wrox Press Ltd., 2001.

[10] J.P. Yang, S.U. Shin, and K.H. Rhee, "A Simplified Approach to User Controllable Threshold Signatures," *2004 IEEE International Conference in e-Commerce Technology*, p. 273-280, 2004.

[11] L. Kagal, J. Undercoffer, R. Pench, A. Joshi, T. Finin, and Y. Yesha, *Vigil: Providing Trust for Enhanced Security in Pervasive Systems*, Technical Report, University of Maryland, Baltimore County, 2002.

[12] L. Kagal, T. Finin, and A. joshi, "Moving from Security to Distributed Trust in Ubiquitous Computing Environments," *IEEE Computer*, 2001.

[13] R.Gennaro, S.Jarecki, H. Krawczyk, and T. Rabin, "Revisiting the Distributed Key Generation for Discrete-Log Based Cryptosystems", *RSA Security 2003*, 2003.

[14] Steven D. Gribble et al. "The Ninjar architecture for robust Internet-scale systems and services," *Computer Networks*, Vol. 35, pp. 473-497, 2001.

[15] S. Jarecki, N. Saxena, and J. H. Yi, "An Attack on the Proactive RSA Signature Scheme in the URSA Ad-Hoc Network Access Control Protocol," *ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 1-9, 2004.

**양 종 필**

1999년 2월 부경대학교 전자계산학과 (이학사)
2001년 2월 부경대학교 대학원 전자계산학과 (이학석사)
2005년 8월 부경대학교 대학원 전자계산학과 (이학박사)
2005년~현재 일본 큐슈대학교 전기정보공학과 객원연구원
관심분야 : 유비쿼터스 컴퓨팅 보안, 비밀 분산, 공개키 기반 구조, 익명성

**심 미 선**

2003년 2월 부경대학교 전자컴퓨터정보통신공학부 (공학사)
2005년 2월 부경대학교 정보보호학과 (공학석사)
2005년~현재 ㈜정보보호기술 연구소 연구원
관심분야 : 암호 프로토콜, 비밀 분산, 시스템 보안 기술

**신 원**

1996년 2월 부경대학교 전자계산학과 (이학사)
1998년 2월 부경대학교 대학원 전자계산학과 (이학석사)
2001년 8월 부경대학교 대학원 전자계산학과 (이학박사)
2002년 3월~2005년 1월 : (주)안철수연구소 선임연구원
2005년 3월~현재 동명정보대학교 정보보호학과 전임강사
관심분야 : 소프트웨어 보안, 악성코드 대응, 이동에이전트 보안, 암호학 응용

**이 경 현**

1982년 경북대학교 수학교육과 (이학사)
1985년 한국과학기술원 응용수학과 (이학석사)
1992년 한국과학기술원 수학과 (이학박사)
1982년~1993년 3월 : 한국전자통신연구소 선임연구원
1995년 7월~1996년 8월 Univ. of Adelaide, 방문교수
2001년 7월~2002년 8월 Univ. of California, Irvine 교환교수
2002년 8월~2003년 7월 국제간 정부기구 CPSC, Manila, Philippines, 교학부장
1993년 3월 현재 부경대학교 전자컴퓨터정보통신 공학부 교수
관심분야 : 암호이론, 멀티미디어 정보보호, 네트워크 보안, 암호프로토콜 응용