홍 승 필 교수지도
박사학위 청구논문

클라우드 환경에서 안전한 OSMU (One-Source Multi-Use) 시스템의 설계 및 구현

2014

성신여자대학교 대학원
컴퓨터학과
김 재 중

클라우드 환경에서 안전한 OSMU (One-Source Multi-Use) 시스템의 설계 및 구현

홍 승 필 교수지도

이 논문을 박사학위논문으로 제출함

2013년 10월

성신여자대학교 대학원
컴퓨터학과
김 재 중

인 준 서

김재중의 박사학위 논문으로 인준함.

심사위원 _____인

심사위원 _____인

심사위원 _____인

심사위원 _____인

심사위원 _____인

성신여자대학교 대학원

목 차

표 목 차

그 림 목 차

논 문 개 요

다양한 무선단말기기를 통한 언제, 어디서나 인터넷을 접속할 수 있는 환경이 제공되면서 이미지, 오디오, 데이터, 비디오 등의 디지털 컨텐츠를 확보하고 가공하여 서로 다른 기기로 전송하는 서비스 역시 빠르게 확산되고 있다. 그러나 이러한 서비스는 스마트 폰, 스마트 패드 등의 N-screen 기반의 통합사용자 인증정책이나 방안이 미흡하고, 하나의 컨텐츠에 대하여 다양한 단말기기에서 안전하게 이용할 수 있는 멀티 사용 환경을 제공을 못하고 있다. 이를 해결하기 위해 본 논문은 클라우드 환경에 맞는 신뢰할 수 있는 통합사용자 인증 및 관리가 가능한 안전한 원소스 멀티유즈(Secure One-Source Multi-Use: SOSMU) 시스템을 제안하고자 한다.

설계된 SOSMU 시스템은 단말장치의 리소스나 성능을 고려하여 하나의 컨텐츠를 다양한 단말장치에서 재생할 수 있도록 하는 보안 및 인증기능이 적용된 시스템이다. SOSMU 시스템의 구성은 통합인증메커니즘(Consolidated Authentication Mechanism: CAM), 위험관리메커니즘(Risk Management Mechanism: RMM), 체계적인 정책 설정 및 관리 메커니즘(Policy Compliance Mechanism: PCM) 등으로 구성된다. 첫째, 통합인증 메커니즘(CAM)을 크리덴셜(인증서 등)에 대한 관리 및 사용 방법에 따라서 사용자가 가지고 있는 스마트기기를 이용한 통합인증모델(S-CAM)과 중앙 집중적인 크리덴셜 서버(Credential Server)를 이용한 통합인증모델(C-CAM)로 나누어 제시한다. 둘째, 위험관리 메커니즘(RMM)은 서비스별 사용자 인증

방법을 분석을 통하여 1등급부터 5등급까지의 사용자 인증 등급화 방안 모델(User Authentication Level Model)을 제시하여 각 응용서비스마다 위험평가를 통해 해당서비스에 적합한 사용자 인증의 선택 및 사용 방안을 제시한다. 셋째, 정책 컴플라이언스 메커니즘(PCM)은 정책엔진(Policy Engine)을 통하여 통합적인 정책관리를 수행하고 사용자 정책, 단말기기 정책, 컨텐츠 정책, 데이터 정책으로 나누어 정의한다.

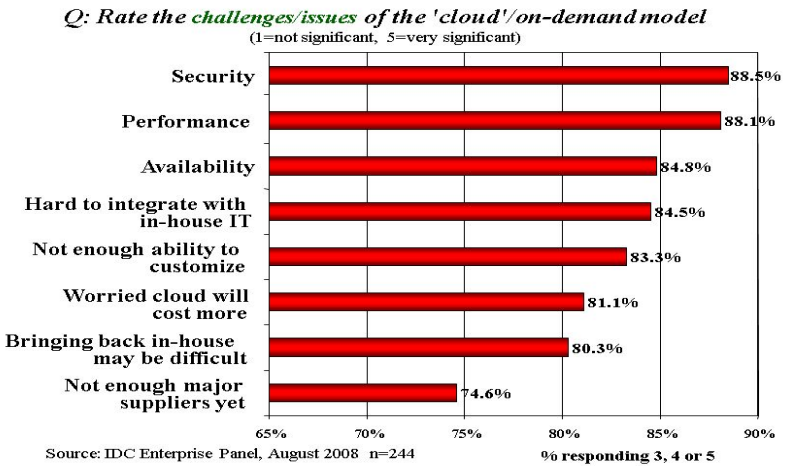
SOSMU 시스템은 사용자와 기기에 대한 통합인증 메커니즘, 사용자 인증등급모델이 적용된 위험관리 메커니즘, 체계적인 정책관리 메커니즘을 지원함으로써 컨텐츠에 대한 효율적인 원소스 멀티유즈 환경을 제공뿐만 아니라 다양한 모바일 기기에서 더 안전한 보안 및 개인정보보호를 제공한다.

Ⅰ. 서 론

1. 클라우딩 컴퓨팅 개요

클라우딩 컴퓨팅은 서비스 제공자의 상호작용이나 최소한의 관리 노력으로 빠르게 제공과 회수할 수 있는 변경 가능한 컴퓨터 자원들의 공유된 풀에 편리한 온 디맨드 네트워크 접근을 가능하게 하는 모델로 NIST(The National Institute of Standards and Technology)에서 정의되어 있다. [1]

인터넷 사용과 클라우딩 컴퓨팅 사용자의 증가가 계속되면서 보안 이슈관련 관심이 급격히 증가하고 있다. 특히 기존 컴퓨팅 환경에 비하여 모바일 장치를 사용하는 클라우드 환경에서 클라우드 컴퓨팅 서버에 저장된 정보를 해킹, 데이터 노출, 바이러스 등으로부터 안전하게 보호하기 위한 보안과 프라이버시 문제가 증가하고 있다. [2]



(그림 1) IT 클라우드 서비스의 이슈에 대한 비율

NIST는 공공 클라우드 컴퓨팅에서 보안과 프라이버시에 대한 가이드라인 (SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing)을 발행했다. 이 가이드라인은 보안에 대한 개요, 공공 클라우드 컴퓨팅에서의 프라이버시 문제들, 공공 클라우드 환경에서 기관의 아웃소싱 데이터, 응용서비스, 기반구조에 대한 인식 고려사항 등을 제공한다. [3]

잠재적인 클라우드 도입기관의 몇 가지 설문조사에서 보안과 개인정보보호가 클라우드를 도입시 최우선으로 고려되고 있다. [4]

클라우드 컴퓨팅은 많은 기존 기술과 가장 기본적인 컴퓨팅 접근의 혁명적인 발전으로 묘사되고 탄력적인 규모의 추가와 할당 활용모델을 사용하는 메커니즘과 인프라로부터 응용서비스와 정보를 분리하는 중요한 용어이다. 클라우드 적용을 위한 최대의 걸림돌은 규제준수, 불충분한 서비스 준수 계약, 공유 인프라, 데이터 저장 문제, 불분명 한 법적 의미 등의 요소에 대하여 사용자가 우려되는 보안과 개인정보보호 이슈이다. [5]

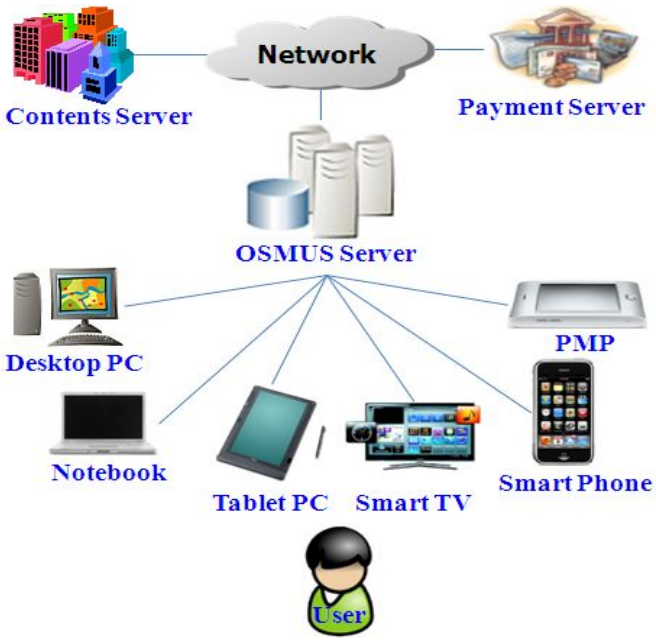
클라우딩 컴퓨팅 환경은 각 도메인은 서로 다른 보안, 개인정보보호, 그리고 신뢰 요구사항들, 잠재적으로 다양한 메커니즘, 인터페이스들을 적용할 수 있는 멀티도메인 환경이다. 이러한 도메인들은 개별적으로 사용가능한 서비스들 또는 다른 구조 또는 응용요소들을 표현할 수 있다. 서비스 중심의 구조는 서비스의 조합과 조화를 통하여 멀티도메인 정보와 같이 자연스럽게 촉진시키는 관련된 기술이다. [6]

2. OSMU 시스템(One-Source Multi-Use System) 개요

오늘날 인터넷이 널리 보급되고, 다양한 이동통신 기기들이 널리 보급되어 손쉽게 언제 어디서나 인터넷을 접속하여 다양한 서비스를 이용할 수 있는 환경이 조성되었다. 모바일 장비들을 이용하여 텍스트, 이미지, 오디오, 비디오 등의 디지털 컨텐츠[7]를 획득하고, 가공하고 서로 다른 기기로 전송하는 서비스 역시 빠르게 확산되고 있다. [8] 아날로그 방송형태에서 디지털방송형태로 변화함에 따라 인터넷과 디지털 방송을 이용한 웹 컨텐츠, 방송 컨텐츠가 기하급수적으로 증가하고 있고, 특히 정지화상, 동화상으로 이루어진 멀티미디어 컨텐츠들이 상당수를 차지하고 있다. 또한 멀티미디어 재상기능 또는 방송수신기능을 내장한 예를 들면, 스마트폰, 노트북, 타블릿 PC, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player) 등의 다양한 이동통신 기기들이 보급되어 이러한 이동통신 단말 기기들을 이용하여 멀티미디어 컨텐츠를 제공하는 서비스 역시 빠르게 확산되고 있다. 그러나 아직까지도 이동 통신 단말기 전용의 컨텐츠는 소수이고, 대부분의 컨텐츠들은 PC, DTV(Digital TV) 등의 유선 네트워크를 통해 접속하는 사용자에 집중되고 있는 실정이다. 따라서 PC 등의 유선 네트워크를 통하여 컨텐츠를 제공받은 사용자는 이동 통신 단말기를 PC에 연결하여 다운로드하거나, 이동 통신 단말기로 동일한 컨텐츠를 중복하여 다운받아야 하고, 다양한 이동 통신 단말기에서 컨텐츠를 재생할 수 없는 문제점이 있다. 또한, 컨텐츠를 다운받아도 이동 통신 단말기는 PC와 비교하여 취급 가능한 데이터 사이즈가 작고, 컬러 수, 해상도, 프로세서의 처리 능력 등의 성능

차이가 있고, 다양한 이동 통신 단말기 간에도 성능 차이가 존재하여 다양한 이동 통신 단말기에서 컨텐츠를 재생하는데 어려움이 있다. [9] 반면에 다양한 컨텐츠를 제공하는 컨텐츠 제공자(CP : Content Provider)는 아날로그 컨텐츠와 달리 복수번의 복제 후에도 원본과 같은 품질을 유지하는 디지털 컨텐츠의 특성으로 인하여, 무단으로 복제된 컨텐츠들이 급속히 전파될 수 있어 많은 비용을 투자한 컨텐츠 제작자들에게 막대한 재산적 손실을 입게 된다.

단말장치의 리소스나 성능을 고려하여 하나의 컨텐츠를 다양한 단말장치에서 재생할 수 있도록 하는 보안 및 인증기능이 적용된 One-Source Multi-Use(OSMU) 시스템의 개략적인 구성은 다음과 같다.



(그림 2) One-Source Multi-Use System

(표 1) OSMU 시스템 구성요소의 기능

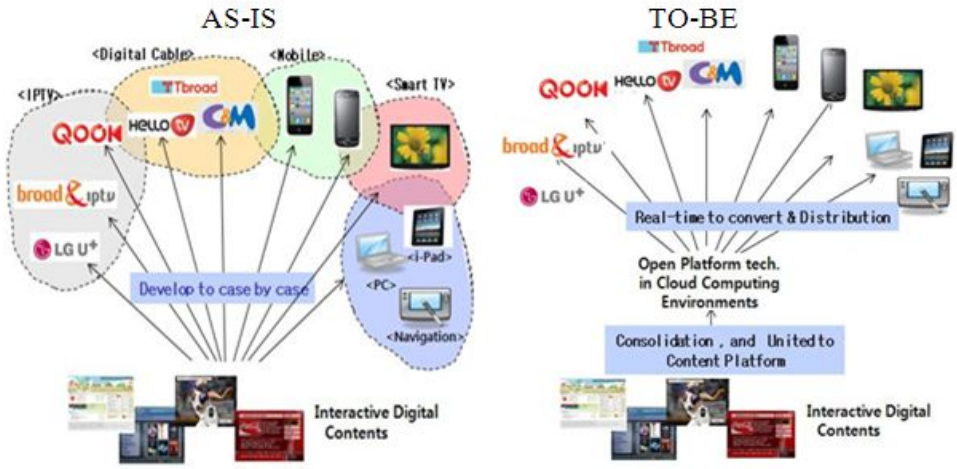
Item	Description
OSMUS Server	One-Source Multi-Use 기능과 사용자 통합인증을 담당하는 시스템
Contents Server	컨텐츠를 보관, 판매 등의 관리하는 시스템
Payment Server	컨텐츠에 대한 지불을 담당하는 시스템
Terminal Units	데스크탑 PC, 노트북, 스마트폰, 스마트 패드, 스마트 TV, 휴대용멀티미디어플레이어(PMP), 타블릿 PC 등의 각종 단말기기
USER	컨텐츠의 구매하여 사용하는 객체

디지털 컨버전스(Digital Convergence)[10]에서의 OSMU(One-Source Multi-Use)의 기본 개념은 다음과 같이 정의된다.

첫째는 스마트 TV, 모바일, PMP, 네비게이터, 스마트 패드, 디지털 케이블 등의 통합적인 결합을 의미한다. 둘째는 통합된 네트워크와 Window X, 안드로이드(Android), Apple(iOS) 등의 다른 모바일 플랫폼[11]을 통한 컨텐츠의 연결을 의미한다. 셋째는 모바일과 온라인 커뮤니케이션 툴과의 결합된 서비스들에 의한 향상된 컨버전스의 제공을 의미한다.

통신 정책의 전통적인 모델에서는 전략개발(법적 프레임웍)과 법정립(제정자)은 대부분 특정부분의 책임으로 되어 있었다. 그러나 통합미디어 관련 정책은 당연한 컨버전스 현상으로 여겨지고 결과적으로 과거 전통모델을 극복하고 정책결정에서 오래된 통신 매스미디어 이분법을 극복하기 위해 노력하고 있다. 개발 중인 전략 목표는

방송, 통신, 온라인서비스 등의 전자적인 것뿐만 아니라 우편, 편지 등의 비 전자적인 분야를 포함한 전체 통신 부문에서 달성하는 것이다.



(그림 3) 디지털 컨버전스를 위한 OSMU(One-Source Multi-Use)

제도적인 관점에서 보면 결합된 정치능력은 통합된 전략의 준비를 쉽게 한다. 클라우드 컴퓨팅 환경에서 디지털 미디어 융합을 가능하게 하는 OSMU 서비스를 제공하기 위해서는 보안과 프라이버시 문제를 고려해야 한다. 기관의 자산, 자원, 정보에 대한 보안과 위험은 다음과 같은 사항에 따라 달라진다.

- 분석되고 관리되어 지는 응용프로그램/정보/서비스들의 종류
- 서비스를 운영하는 인력과 안전한 상호연동 제공 방법
- 중앙 집중적인 보안과 프라이버시를 위한 통합적인 통제 방법
- 암호학적인 접근 및 정책 규칙의 사용
- 안전한 보안 관리를 설계하는 방법

3. 논문 구성

본 논문은 클라우드 환경에서 사용자가 디지털 컨텐츠에 대하여 편리하고 안전하게 사용할 수 있는 원소스 멀티유즈(SOSMU: Secure One-Source Multi-Use) 환경을 제공하는 시스템을 제안한다.

1장은 클라우드 컴퓨팅 환경과 디지털 컨버전스를 위한 OSMU 시스템을 소개한다. 2장은 기존 컨텐츠 관리기법, 각 서비스에서 사용되는 사용자 인증기법, 국내외 사용자 인증제도 현황, 크리덴셜 표준화 동향 등의 이론적 배경과 관련 연구 동향을 파악한다. 3장은 OSMU 환경의 문제점을 분석하여 안전한 OSMU 시스템 구현을 위한 요구사항을 분석한다. 4장은 SOSMU 시스템을 구현하기 위한 구체적인 구성요소와 메커니즘을 기술한다. SOSMU 시스템의 구성요소는 통합인증 메커니즘, 위험관리 메커니즘, 정책 컴플라이언스 메커니즘으로 구성된다. 통합인증메커니즘은 스마트기기를 이용한 통합인증방법과 크리덴셜 서버를 이용한 통합인증모델로 구성되고 각각의 아키텍처와 프로토콜 설계를 한다. 위험관리메커니즘은 각 서비스들의 사용자 인증방법을 분석하여 등급화하여 사용자 등급화 모델(User Authentication Level Model: UALM)을 정의한다. 5장은 설계된 SOSMU 시스템에 대한 프로토타입의 설계 및 구현으로 사용자 인증, 컨텐츠, 단말기기 등에 대한 정책 알고리즘, 화면설계, 데이터베이스 설계 등을 정의하여 프로토타입으로 구현한다. 6장은 구현된 SOSMU 시스템을 기존 모델과의 비교 분석을 통하여 안전성과 우수성을 검증한다. 마지막으로 제안된 SOSMU 시스템에 대한 기여부분과 향후 발전방향을 기술한다.

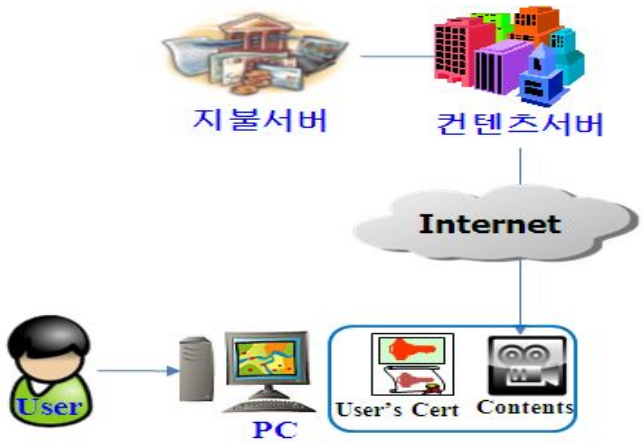
Ⅱ. 이론적 배경

OSMU 환경 구축을 위해 필요한 컨텐츠 관리 기법, 디바이스 인증 기법, 사용자 인증 기법, 크리덴셜 관리 기법에 대한 이론적 배경을 알아보고자 한다.

첫째, 컨텐츠 관리 기법(Traditional Content Management System: TCMS)은 현재 사용하고 있는 컨텐츠 관리 기술 및 현황을 파악한다. 둘째, 디바이스 인증 기법은 사용자가 사용하는 모바일 기기와 서버간의 인증 및 보안관련 현황을 파악한다. 셋째, 사용자 인증 기법은 포털, 전자상거래, 전자거래, 금융 서비스, 전자조달 등의 온라인 거래에서 사용되고 있는 다양한 사용자 인증기법의 현황을 파악하고 각 인증의 종류 및 특성을 조사한다. 넷째, 크리덴셜(Credential) 관리 기법은 사용자 인증을 위해서 사용하는 크리덴셜에 대하여 클라우드 환경 등 다양한 새로운 환경에 따라 안전하게 자신의 크리덴셜(Credentials)을 사용 가능하도록 현황 및 환경을 분석한다.

1. 컨텐츠 관리 기법

일반적으로 컨텐츠 관리 시스템은 디지털 방송 등에서 생성된 컨텐츠를 효율적으로 저장, 관리, 공급하기 위한 시스템으로 서비스된 컨텐츠에 대한 시청자의 반응을 수집하여 컨텐츠 데이터베이스(DB) 시스템으로 관리하고, 그 결과를 다양한 측정 기준으로 분석하여 추후 컨텐츠 제작에 대한 기초 자료로 활용한다.



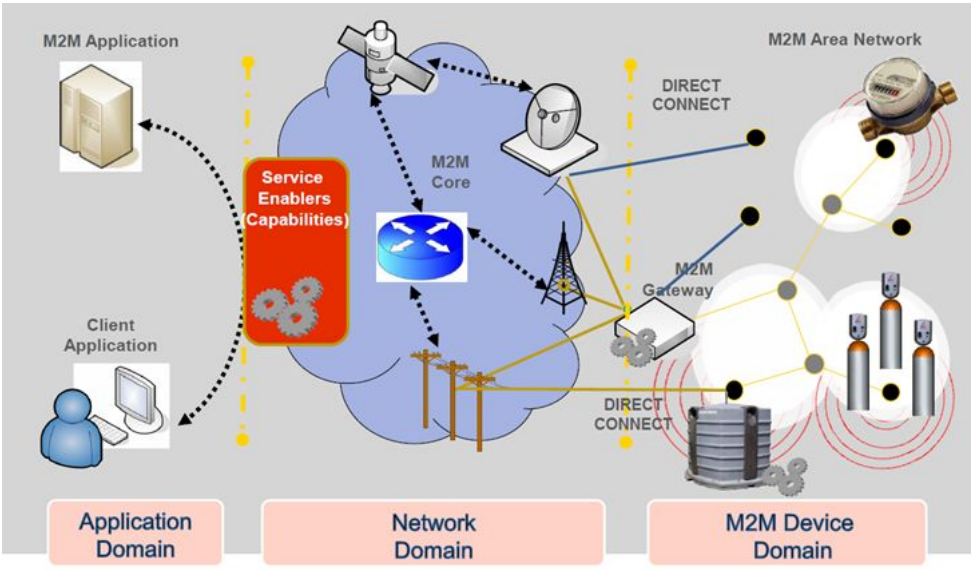
(그림 4) 컨텐츠 관리 시스템 구조

전형적인 컨텐츠 관리 시스템의 구조는 사용자가 자신의 PC, 노트북, 모바일 폰 등을 이용하여 각 컨텐츠 서버의 컨텐츠를 검색하여 구매하고자하는 컨텐츠를 선택하고 지불서버를 이용하여 비용을 지불한 후 이를 사용자의 단말기기에 다운받아 이를 사용하는 구조로 되어 있다. 컨텐츠를 구매하기 위한 사용자 인증의 경우 ID/Password 방식, 공인인증서 방식 등 사이트마다 상의하게 적용되고 인증등급 또한 사이트의 정책에 의존적으로 적용되어 상호연동이나 통합적인 인증을 제공하지 못하고 있다. 지불의 경우 특정금액 초과시 공인인증서를 통한 인증을 통하여 지불하도록 설정되어 있다. 다운받은 컨텐츠의 경우 각 컨텐츠 서버의 DRM(Digital Rights Management)이나 암호화 방식을 통하여 처리되어 다른 기기로 옮기는 방법이나 옮겨지더라도 사용할 수 없는 경우가 발생한다.

2. 디바이스 인증 기법

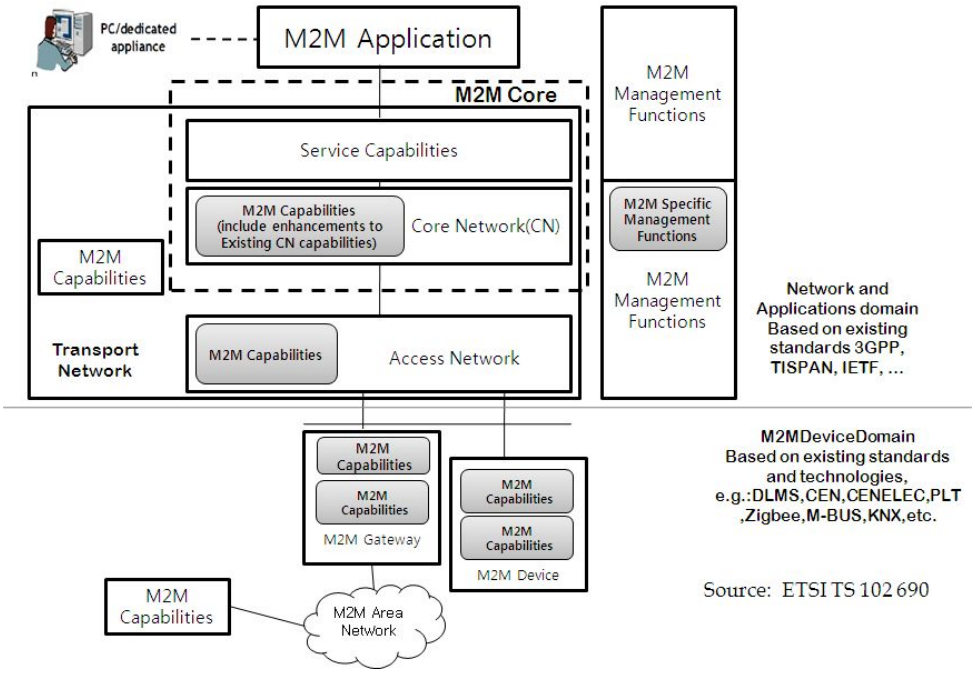
사용자들은 인터넷을 통하여 수많은 사이트로부터 다양한 서비스를 제공받는 편리한 환경이 제공되고 있다. 그러나 이러한 오픈된 환경에서 부적절한 계정과 다른 사용자의 불법적인 접속 등 사용자 인증에 관련하여 기관 또는 회사의 위험을 최소화하기 위해서는 서비스의 중요도에 따라서 적절하고 안전한 사용자 인증 방법이 적용되어야 한다. 최근 들어서는 사람에 대한 안전한 인증환경을 제공하는 공인인증체계를 바탕으로 하여 인증의 대상 또한 IPTV, 인터넷 전화, CCTV 등의 다양한 기기로 확장되어 가고 있다. 디바이스 인증은 네트워크에 참여하는 다양한 기기의 안전한 운영을 위하여 해당 기기를 식별하고 진위를 판단할 수 있는 신뢰된 인증방법을 말하며 특히 기기인증서 기반의 인증을 의미한다. 인터넷 환경은 광대역 통합망(BcN), u-센서네트워크(USN) 등 다양한 기술이 통합·연계되어 사람 및 기기를 모두 연결하는 네트워크 환경으로 진화하고 있다. 과거의 아날로그 신호기반의 휴대폰, TV, 전화기 등은 낮은 대역폭, 폐쇄된 네트워크 환경, 낮은 컴퓨팅 사양 이였으나 최근에 스마트폰, 스마트TV, 타블릿 PC 등의 스마트 기기 시대가 되면서 정보통신 기기에 대한 보안의 중요성이 증가하였다. [12]

M2M(Machine to Machine)의 정의(3GPP/ETSI)는 사람이 개입하지 않는(혹은 최소 개입) 상태에서 Machine/Device간에 일어나는 통신으로 음성/영상 통신 등과 같이 사람 간에 일어나는 통신과 PC를 통한 인터넷 검색 등을 제외한 모든 통신(Machine-to-Human, Human-to-Machine)을 의미한다. [13]



(그림 5) M2M 구성도 (출처: IoTWEEK 2012, NEC)

M2M 아키텍처는 M2M Device, M2M Area Network, M2M Gateways, M2M Communication Networks, M2M Applications (Server)로 구성된다. M2M Device는 디바이스 안에 포함된 데이터에 대하여 요청에 대한 응답이나 전송을 할 수 있는 기기이다. M2M Area Network은 M2M Device와 M2M Gateways간의 연결성을 제공한다. M2M Gateway는 M2M Device가 Communication Network과 상호 연결하거나 상호작용을 할 수 있도록 한다. M2M Communication Networks은 M2M Gateway(s)와 M2M application과 통신을 제공하고 Access Network, Transport Network, Core Network으로 나누어 질 수 있다. M2M Application은 다양한 응용서버스로 가는 데이터를 위한 미들웨어 계층이 포함하고 특정 비즈니스 처리 엔진에 의해서 사용된다.



(그림 6) ETSI M2M Architecture

3. 사용자 인증 기법

인터넷의 발달함에 따라 많은 서비스를 인터넷을 통하여 쉽게 사용할 수 있게 되었다. 그러나 인터넷은 직접대면을 통한 상호작용이 아니기 때문에 중요한 자원에 접근하는 사용자에 대한 물리적인 검증방법을 제공하지 못하고 있다. 서비스에서 적법한 사용자를 확인하는 것이 중요한 이슈가 되고 있다. 다양한 해킹 기술이 발전함에 따라 아이디와 패스워드기반의 인증보다 더 강한 보안과 인증기술이 필요하게 되었고 최근에는 사용자의 생체인식 등 인간의 특성을 인식하는 방법들을 사용하는 인증방법이 증가하고 있다. [14] 타인사칭(Impersonation), 위조(Counterfeits), 크리덴셜(PINs, Passwords, ID Cards 등)에 대한 탈취나 변경, 피싱(Phishing) 등을 통하여 다른 사람의

신분을 획득, 오남용(Identity Theft)는 범죄가 세계적으로 증가하고 있다. 이런 신분사칭으로 인한 피해는 소비자의 신뢰성 감소 등 서비스 기관에 커다란 피해를 가져온다. 이를 방지하기 위하여 개인정보보호법, 정보통신망법 등 법적인 제도를 통하여 엄격한 신원 확인 및 보장을 지원하고 있다. 본고는 각 분야의 사용자 인증 방법을 분석하고 위험평가 절차를 정의하고 인증 방법은 등급화하여 지속적인 위험에 증가에 따른 효과적인 방안의 선택을 위한 가이드라인을 제공하고자 한다.

가. 사용자 인증의 종류

인증(Authentication)은 사용자가 정당한 사람인가을 확인하는 과정으로 아래의 요소를 이용하여 확인할 수 있다.

(표 2) 인증 종류

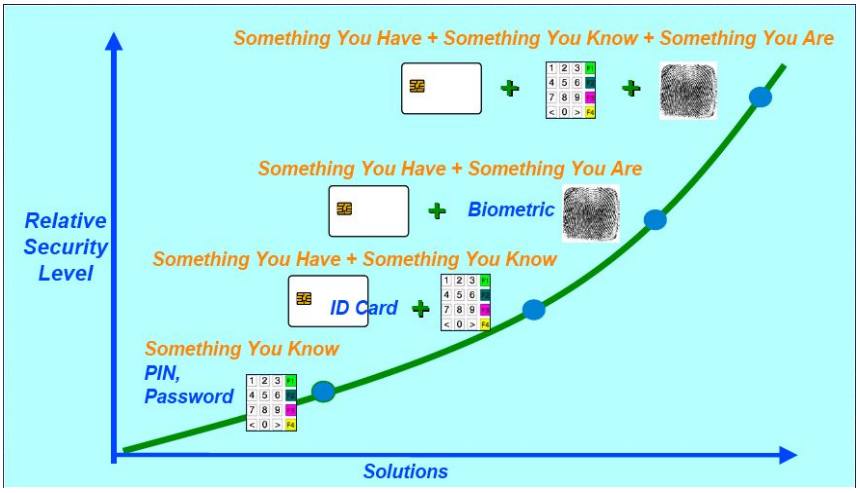
구 분	종 류
Proof-of-Knowledge (Something you know?)	비밀번호(Passwords), 핀(PIN), 엄마 이름(Mom's Name), 전화번호(Phone Number) 등
Proof-of-Possession (Something you have?)	스마트카드(Smart Cards), 보안토큰(Tokens), 운전면허증(Driver's License), 공인인증서(PKI Certificates) 등
Proof-of-Characteristics (Something you are?) -physiologically or behaviorally	지문(Fingerprints), 손금인식(Hand Geometry), 얼굴인식(Facial Image), 홍채인식(Iris), 망막인식(Retina), DNA, 음성인식(Voice), 서명패턴인식(Signature Patterns) 등

사용자 인증의 종류는 크게 단일인증(Single-Factor Authentication: SFA)과 다중인증(Multi-Factor Authentication: MFA)으로 구분된다.

단일인증은 주로 사용되는 것이 아이디와 패스워드이다. 아이디와

패스워드 조합의 경우 Malware Attack, Replay Attack, Offline Brute Force Attack, Key Logger Trojan, Dictionary Attack, Shoulder Surfing 등 많은 취약성이 발견되어 많은 기관들이 다중인증으로 옮겨가고 있고 또한 정부차원에서도 법/제도적으로 다중인증을 강제하는 경우가 증가하고 있다. [15]

다중인증은 단일인증 방법을 조합하여 사용자를 인증하는 방법으로 특히 중요한 고객정보의 접근이나 고위험의 금융거래 등에는 사용되어야 한다. [16] 인증방법의 강도는 얼마다 많은 인증을 사용하는가에 따라 판단할 수 있다. [17]



(그림 7) 보안레벨과 신원확인의 상관도 (출처: NIST Workshop: July 9, 2003)

나. 국내외 사용자 인증제도 및 현황

1) 사용자 인증제도 및 현황

가) 국내제도현황

정부는 아이핀(i-PIN)[18], 공인인증서[19] 등 여러 가지 제도를 만들어 의무화함으로써 사용자 인증을 강화하고 있다.

(표 3) 국내 법제도 현황

구 분	관련 법/제도	
정보통신기반보호법	주요기반보호시설 지정	국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무
정보통신망법	정보보호안전진단 의무화	주요정보통신서비스제공자(ISP), 집적정보통신시설사업자(IDC), 쇼핑몰 등 안전진단을 받아야함
	아이핀 의무화	포털, 게임, 전자상거래 등에서 회원가입시 적용하여야함
	보안서버 의무화	개인정보 및 인증정보 송수신시 이를 암호화해야 함
전자서명법	공인인증서 의무화	은행, 증권, 전자상거래, 전자정부 등에서 인증, 무결성, 부인방지를 필요한 서비스에 적용하여야함

나) 서비스별 사용자 인증 현황

실명인증, 휴대폰인증, 아이핀(i-PIN), 신용카드 지불(VISA 안심클릭, 인터넷 안심 지불(Internet Secure Payment: ISP), 공인인증서, 지문인증[20] 등의 다양한 사용자 인증방법이 인터넷 사용자들이 사용하고 있는 포털, 전자상거래, 금융기관(은행), 전자정부(조달청)에서 사용되고 있다. 사용자 인증현황은 (표 4)와 같이 다양한 분야에서 다양한 사용자 인증방법들이 사용되고 있다.

(표 4) 서비스별 사용자 인증현황

구분	기능		인증방법
Portal	로그인(Optional)		ID/PW, OTP
	회원가입		실명인증, 아이핀, 휴대폰인증
	아이디/비밀번호 찾기 (한 가지 선택)		재발급용 메일
			등록된 휴대폰
			휴대폰 본인확인
			범용공인인증서
			신분증 정보확인
			신용카드인증
전자 상거래	로그인		ID/PW, 공인인증서
	전자지불	실시간 계좌이체	계좌정보+공인인증서
		신용카드 결제	카드정보+공인인증서 - 안심클릭 - 안전결제서비스(ISP)
		휴대폰결제(소액)	휴대폰정보+주민번호
금융기관 (은행)	로그인		공인인증서, ID/PW
	계좌이체	1등급	공인인증서+OTP 발생기
			HSM 방식공인인증서+보안카드
			공인인증서+보안카드+2채널인증
		2등급	공인인증서+보안카드+SMS
		3등급	공인인증서+보안카드
전자정부 (조달청)	로그인		공인인증서
	전자입찰		공인인증서+지문보안토큰

다) 기능별 사용자 인증 절차

서비스기관에서 사용하고 있는 실명확인, 휴대폰 본인확인, 아이핀, 전자지불(신용카드인증), 공인인증서, 지문인증 등의 다양한 인증방법과 서비스 절차를 알아보고자 한다.

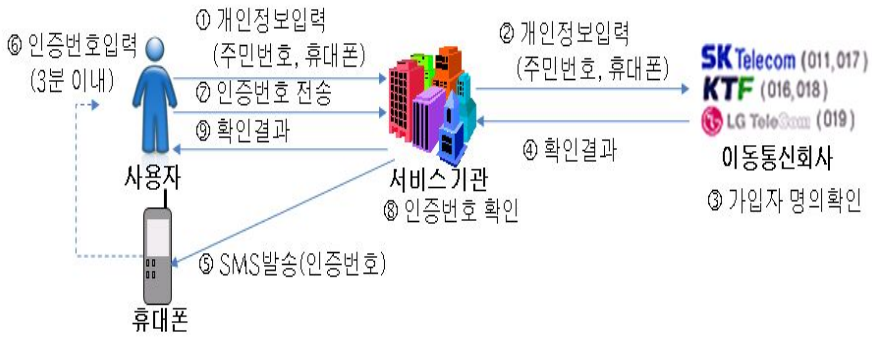
(1) 실명인증

사용자의 실명과 주민등록번호의 실제존재여부 및 일치여부를 확인하는 서비스로 실명확인기관인 신용평가기관이 보유하고 있는 실명DB를 사용한다. 인터넷이나 오프라인을 통하여 실명과 주민등록번호를 쉽게 얻을 수 있어 정확한 본인확인기능은 제공하지 못한다.

(그림 8) 실명인증 흐름도

(2) 휴대폰 본인확인

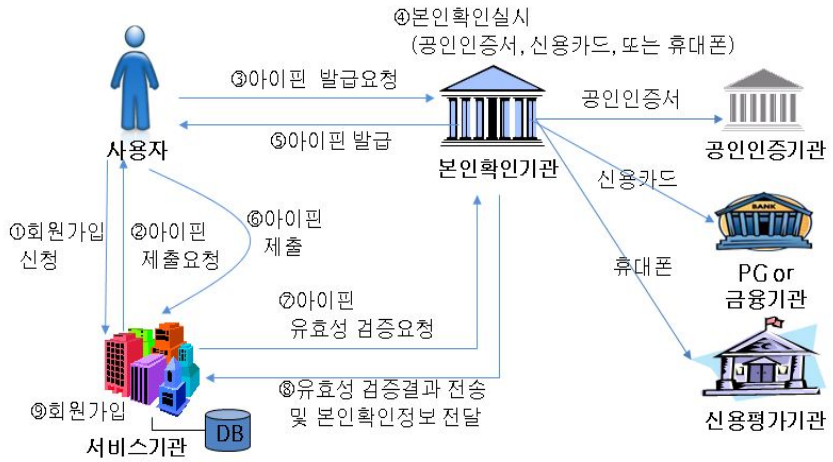
사용자가 입력한 주민등록번호, 휴대폰번호와 휴대폰 가입시에 등록한 사용자의 주민등록번호로 본인인증하고 SMS를 통하여 휴대폰의 소유여부를 확인하는 서비스이다. 휴대폰의 명의자와 소유자간의 상이로 발생하는 문제점에 대한 해결을 제공한다.



(그림 9) 휴대폰인증 흐름도

(3) 아이핀(i-PIN)

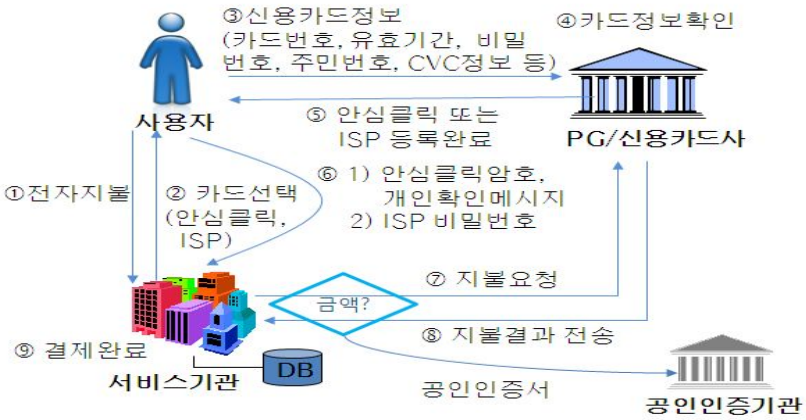
아이핀(Internet Personal Identification Number: i-PIN)은 대면확인이 어려운 인터넷에서 명의도용이 쉬운 주민등록번호를 대신하여 이용자에게 부여되는 인터넷 개인식별번호(ID)이다. i-PIN은 이용자가 인터넷 사이트 회원가입이나 성인인증 등을 위해 자신의 신원정보를 본인확인기관에 제공하고 본인확인 필요할 때마다 식별ID와 비밀번호를 입력하여 본인확인을 받는 방법으로 현재 4개 본인확인기관이 서비스를 제공하고 있다.



(그림 10) 아이핀 흐름도

(4) 신용카드 전자지불 인증

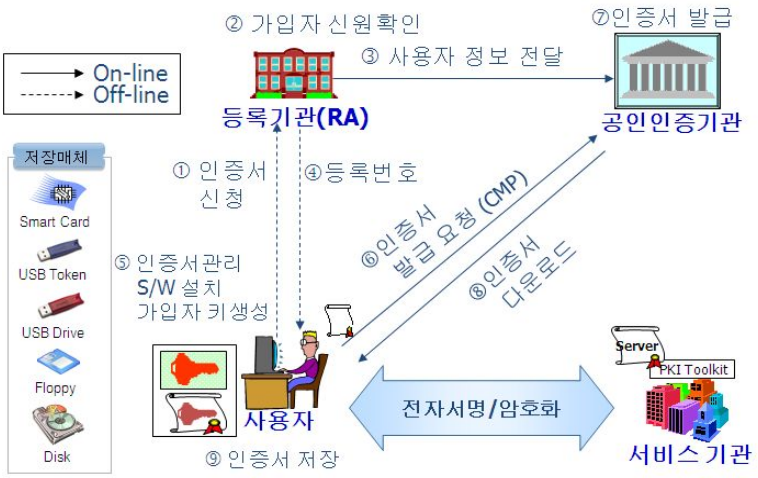
전자지불시 사용자의 카드번호/비밀번호 등을 입력함으로써 발생될 수 있는 개인정보 유출 및 카드도용 등의 문제점을 차단해 주는 지불수단으로, 비밀번호만으로 안전한 전자상거래를 할 수 있는 서비스로 카드종류에 따라 안심클릭과 인터넷안전결제서비스(ISP)가 있다.



(그림 11) 전자지불 흐름도

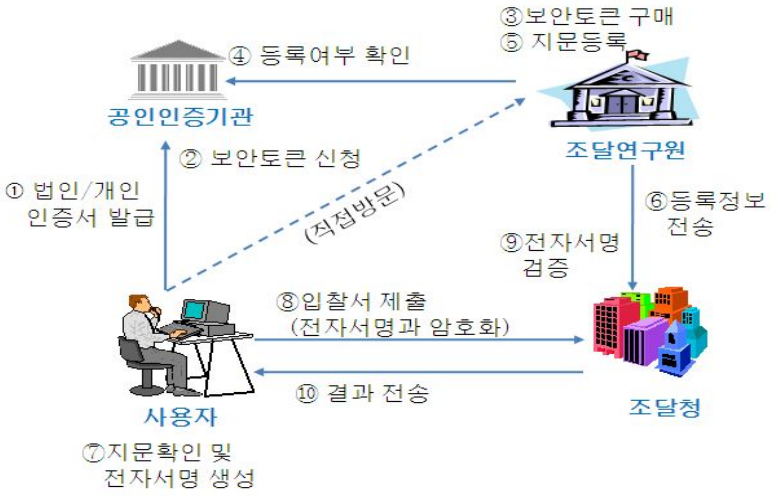
(5) 공인인증서

공인인증서는 대면확인을 통한 확실한 신원확인을 통하여 발급되는 인터넷 인감증명으로 전자거래 시 신원확인, 문서의 위/변조, 거래사실 증명 등의 효과를 얻을 수 있다.



(그림 12) 공인인증서 발급 흐름도

(6) 공인인증서 + 지문인증



(그림 13) 지문인증을 통한 전자입찰 절차

공인인증서와 사용자의 지문정보를 함께 저장하여 보다 안전하고 신뢰성 있는 환경을 제공하다. 조달청[20]에서 실제 입찰자의 신원을 확인하기 위해 지문정보를 이용하여 신원을 확인하는 것으로, 공인인증서 불법대여를 통한 불법전자입찰 차단 목적으로 도입하였다.

2) 해외현황

가) 미국(United States)

미국의 OMB 04-04(The Office of Management and Budget)[21]는 네 가지 단계의 사용자 신원 인증 보증레벨을 제시한다. 각각의 보증레벨은 사용자가 제시하는 크리덴셜(예, 비밀번호)의 보안 등급을 제시한다.

(표 5) Authentication Levels of Assurance(OMB 04-04)

레벨	설명
Level 1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier
Level 2	Confidence exists that the asserted identity is accurate; used frequently for self service applications
Level 3	High confidence in the asserted identity's accuracy; used to access restricted data
Level 4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data

NIST 800-63 전자적 인증 가이드라인(Electronic Authentication Guideline)[22]은 OMB 04-04에 정의된 각각의 보증레벨에 대한 기술적인 요구사항을 제공한다. 각 보증 레벨은 아래의 정리된 테이블처럼 신원확인방법(Identity Proofing), 토큰 요구사항, 그리고, 인증/확인 보호 메커니즘 등의 통제방안이 정의되어야 한다.

(표 6) Technical Requirements of NIST 800-63

레벨	Identity Proofing	Token (Secret)	Authentication Protection Mechanisms
1	Requires no identity proofing	Allows any type of token including a simple PIN	Little effort to protect session from off line attacks or eavesdropper is required.
2	Requires some identity proofing	Allows single-factor authentication. Passwords are the norm at this level	On-line guessing, replay and eavesdropping attacks are prevented using FIPS 140-2 approved cryptographic techniques.
3	Requires stringent identity	Multi-factor authentication, typically a password	On-line guessing, replay, eavesdropper, impersonation and man-in-the-middle attack

	proofing	or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) OTP device token	are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.
4	Requires in-person registration	Multi-factor authentication with a hardware crypto token.	On-line guessing, replay, eavesdropper, impersonation, man-in-the-middle, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security

나) 캐나다(Canada, Province of British Columbia (BC))

캐나다의 브리티쉬 콜롬비아(British Columbia) 주에서 다음과 같은 레벨로 전자적 크리덴셜과 인증 표준(The Electronic Credential and Authentication Standard[23]) 발표되었다.

(표 7) Authentication Levels of Assurance in Canada

Level		Description
1	Low	Credential validated or provision of shared secret/file knowledge is a match
2	Medium	Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret
3	High	Owner of multi-factor credential substantiated by

		successful log on or in person presentation(e.g. software certificate or OTP; multi-factor physical ID card)
4	Very High	Owner of hard multi-factor credential corroborated by successful log on or biometric match (e.g. PKI and/or high quality biometric)

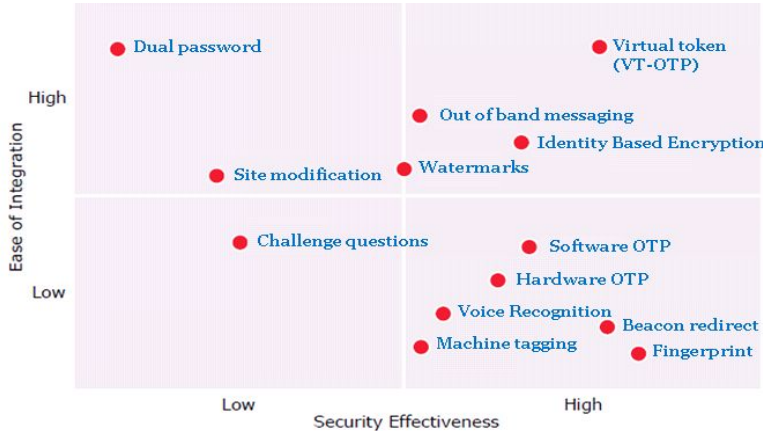
3) 사용자 인증의 종류 및 특성

국내외 서비스 현황조사를 통하여 사용하고 있는 사용자 인증방법을 특성에 따라 분리하면 (표 8)과 같다. [24]

(표 8) 사용자 인증 종류 구분

Authentication Factors: Something You _____				
Know	*Have*			*Are*
Text PIN	IP Address	공인인증서 (certificate)	Scratch-off/Bingo card	지문 Fingerprint
Visual PIN	Browser Type	신용카드 정보	Phone/PDA w/OTP	Hand Geometry
Text Password	Cookie	은행계좌 정보	OTP 발생기	얼굴인식 (Face)
Life Questions	Email Address	보안카드 (Grid card)	USB Device	홍채인식 (Iris)
SMS Message	Toolbar/Agent	휴대폰	Proximity/ Smartcard	망막인식 (Retina)
	신분증 정보	아이핀 (ID/PW)	보안토큰 (HSM)	

사용자 인증방법을 선택함에 있어서 중요한 기준인 안정성 (Security)과 사용성(Usability)에 따라 사용자 인증매체 분류하면 (그림 14)와 같다 .[25][26]



(그림 14) 안정성과 사용성의 상관도

4. 크리덴셜 관리 기법

응용서비스에 정보보호기술의 도입이 증가되면서 하나의 응용서비스에서 사용하던 암호학적 개인정보를 다른 응용서비스에서 사용하기를 원하는 암호학적 개인 정보의 이동성 요구가 점차적으로 증가되고 있다. 이러한 암호학적 개인정보를 통상 크리덴셜(Credentials)라 부른다. 크리덴셜은 한 개인이 사용하는 공개키 암호알고리즘으로 생성된 암호화된 개인키, 공인인증기관이 발행하는 공인인증서(Certificate), 그리고 신뢰하는 인증기관 체인 정보, 인가 정보 등을 포함하는 암호학적 정보의 총합이라고 할 수 있다. 크리덴셜을 이용할 가능성이 높은 장치는 데스크톱 컴퓨터(PC), 노트북, 태블릿 PC, 스마트패드, 스마트폰, 모바일 통신 기기 등이다. 이들 디바이스들 간에 한 디바이스에서 사용하던 크리덴셜를 다른 디바이스로 이동하고자 하는 요구가 증가하고 있다.

가. 크리덴셜 이동성 지원 표준화 동향

크리덴셜 이동성 지원 기술의 표준화는 RSA사에서 제정한 사실 표준인 PKCS (Public-Key Cryptography Standard)와 IETF (Internet Task Force Engineering) 보안영역의 SACRED(Securely Available CREDdentials) 작업반에서 수행되고 있다. 이를 요약하면 (표 9)과 같다.

(표 9) 크리덴셜즈 이동성 관련 국제 표준

기관	표준	제정시기	주요내용
RSA	PKCS#1 v2.1	2001.6	RSA 암호를 위한 공개키 및 서명 방법 정의
	PKCS#5 v2.0	1999.3	패스워드를 이용한 암호키를 생성하는 방법 기술
	PKCS#8 v1.2	1999.11	개인키를 암호화하여 저장하는 방법 기술
	PKCS#12 v1.0	1999.6	사용자 개인키, 인증서 등의 저장 및 이동을 위한 방법 정의
	PKCS#15 v1.1	2000.6	암호 토큰에 저장되는 암호학적 크리덴셜(개인키, 공개키, 인증서, 비밀키 등) 형태 기술
IETF	RFC 3157	2001.8	크리덴셜 이동성 지원을 위한 요구사항 정의
	RFC 3760	2004.4	크리덴셜 이동성 지원을 위한 프레임워크 및 프로토콜 프레임워크 정의
	RFC 3767	2004.6	XML을 이용한 크리덴셜 프로토콜 정의
	RFC 2945	2000.9	SRP 인증 및 키 교환 프로토콜
	RFC 2246	1999.1	종단간 TLS 프로토콜

PKCS 표준은 PKCS#12를 제외하면 대부분 크리덴셜에 대한 표현

형태를 정의하고 있다. PKCS#1에서는 현재 공개키 암호 알고리즘으로 가장 널리 활용되고 있는 RSA 암호 알고리즘의 개인키와 공개키 표현 방식을 정의하고 있다. PKCS#5에서는 이러한 암호 키를 패스워드를 사용하여 암호화하기 위한 기술적인 방법 및 절차를 제시하고 있다. PKCS#8에서는 개인키를 평문 형태로 표현하기 위한 방식과 개인키를 PKCS#5 방식을 이용한 암호화한 형태로 저장하는 방식을 제시하고 있다. 또한 PKCS#12에서는 PKCS#8 형태의 개인키, 인증서, 인증서 폐지목록, 또는 인증서 체인 등의 여러 가지 크리덴셜 정보를 평문 형태, 공개키 또는 패스워드를 이용하여 암호화하는 형태로 표현하는 방식을 제시하고 있다. PKCS#15에서는 PKCS#12에서 포함되지 않았던 암호 토큰(스마트카드 등)을 위한 인증서, 암호키, 개인키, 패스워드, 인가 정보 등의 아주 많은 크리덴셜 정보를 저장하기 위한 메시지 형태를 정의하고 있다

IETF의 SACRED 워킹 그룹은 디바이스간의 크리덴셜을 안전하게 전달하기 위한 프로토콜들에 대한 표준화 작업을 진행 중이다.

정의된 크리덴셜 지원방식은 서버방식과 직접전달방식이 있다. 서버방식은 중앙에 하나의 크리덴셜 서버를 두고, 각 사용자들이 초기에 등록 시 각 사용자의 크리덴셜을 서버에 등록해 두었다가, 필요시에 인터넷의 임의의 위치에서 이 서버와 연결하여 크리덴셜을 다운받아 사용토록 하는 방식이고, 직접전달방식은 각 장치 간에 직접 연결하여 크리덴셜을 직접 주고받는 방식이다. 두 가지 방식은 크리덴셜 서버와 디바이스 간에 상호동작을 위하여 필요한 간접 전달 프로토콜과 디바이스간에 크리덴셜를 직접 전달하기 위한 직접 전달 프로토콜이 정의되고 있다.

SACRED 워킹그룹의 국제표준 목록은 다음과 같다.

첫째, RFC 3157(Requirements)는 크리덴셜의 안전한 이동성을 위한 프레임웍과 이러한 목적을 달성하기 위한 프로토콜들을 제공한다. [27] 둘째, RFC 3760(Credential Server Framework)은 추상적인 프로토콜 프레임웍을 제공함으로써 RFC 3157에 나열된 크리덴셜의 안전한 교환을 위한 프로토콜들의 요구사항들이 기술되어 있다. [28] 셋째, RFC 3767(Protocol)은 사용자가 지역적으로 신뢰된 소프트웨어가 설치된 워크스테이션을 사용하여 크리덴셜 서버로부터 암호학적 크리덴셜들을 얻을 수 있는 프로토콜을 기술하고 있다. [29]

1) RFC 3157(Requirements)

RFC 3157에서는 크리덴셜 이동성을 제공하기 위한 다음과 같이 다섯 가지의 요구사항을 정의하고 있다. 첫 번째 요구사항은 서버 방식과 직접 전달 방식의 두 가지 이동성 프레임워크를 모두 지원해야 한다는 프레임워크 관련 요구사항이고, 두 번째 요구사항은 사용자 인증에 관한 것으로, 사용자 인증을 위하여 사용되어야 할 인증방식이 기술의 발전에 따라 향후 나타날 수 있는 새로운 인증방식을 용이하게 수용할 수 있도록 구성되어야 한다는 사용자 인증 관련 요구사항이며, 세 번째 요구사항은 전달 프로토콜이 구체적인 크리덴셜 형태와 독립적으로 수행되어야 한다는 크리덴셜 형태 독립성에 관한 요구사항이다. 네 번째 요구사항은 프로토콜이 하부 전송 프로토콜(TCP 또는 BEEP 프로토콜을 모두 사용 가능해야 함)에 독립적이여 한다는 전송 프로토콜 독립에 대한 요구사항이다. 다섯 번째 요구사항은 프로토콜과 관련되는

요구사항으로, 크리덴셜이 임의의 노드에서 평문 형태로 존재하지 않도록 SAC(Securely Available Credentials) 프로토콜이 구성되어야 한다는 등의 여러 사항을 규정한 일반 요구사항, 크리덴셜의 다운로드와 업로드가 보장되도록 해야 한다는 등의 여러 사항을 규정한 크리덴셜 서버 방식에 한정된 요구사항, 크리덴셜 수신자가 크리덴셜 송신자를 인증할 수 있어야 한다는 등을 규정한 직접 전달 방식에 한정된 요구사항으로 다시 세분될 수 있다.

2) RFC 3760(Credential Server Framework)

RFC 3760에서는 크리덴셜 서버 방식의 프레임웍을 제시하고 있다. 이를 위한 네트워크 구성 요소는 크리덴셜 서버에 저장하고 조회하는 사용자(User), 사용자 인증 후에 암호학적으로 안전하게 크리덴셜를 전달하는 기능을 수행하는 크리덴셜 서버, 그리고 크리덴셜 서버와 사용자가 자신의 크리덴셜을 암호학적으로 안정하게 저장하기 위한 크리덴셜 저장소(Repository) 등이다. 여기서는 크리덴셜 업로드 절차, 크리덴셜 다운로드 절차, 크리덴셜 삭제 절차, 크리덴셜 관리 절차 등을 고차원으로 설계하였다. 또한 사용자에 대한 서버 인증과 서버에 대한 사용자 인증이 요구되고, 사용자에게 크리덴셜을 안전하기 전달하기 위하여 강력한 패스워드 인증 프로토콜의 부산물로 얻어지는 세션키를 사용자와 서버가 패스워드 인증 과정에서 공유해야 하고, 하나 이상의 크리덴셜을 협상된 세션키로 암호학적으로 안전하게 보호되어야 한다는 요구사항을 요구했으며, 이를 위하여 강한 패스워드 인증 방식(Secure Password Authentication Protocol)과 TLS(Transport Layer Protocol)라는 두 가지 기존 프로토콜을

이용하도록 권고하고 있다.

3) RFC 3767(Protocol)

RFC3767은 SAC 프로토콜에 관하여 규정하고 있으며, 사용자가 특별히 사용자 관련별도 구성 설정 없이 크리덴셜 서버로부터 자국에 신뢰성 있는 소프트웨어를 설치한 워크스테이션을 이용하여 암호학적 크리덴셜를 다운받기 위한 프로토콜을 기술하고 있다. SAC 프로토콜의 패이로드(Payload)는 XML 형식으로 표현된다. 각 사용자는 별도의 계정을 서버에 두며, SAC 프로토콜은 계정 관리 프로토콜(Account Management Protocol)과 실시간 동작 프로토콜(Run-time Protocol)로 크게 구성된다. 계정 관리 프로토콜은 다시 사용자가 계정 정보 생성에 필요한 정보를 서버에게 요구하는 정보 요구(Information Request), 사용자가 인증 후에 서버에 새로운 계정을 만드는 계정 생성(Create Account), 상호 인증(서버 인증 및 사용자 인증) 후에 기 설정되어 있는 계정을 삭제하기 위한 계정 삭제(Remove Account), 상호 인증을 완료한 후에 인증과 관련된 서버에 저장되어 있는 정보를 변경하기 위한 계정 변경(Modify Account) 등으로 구성된다. 실시간 동작 프로토콜은 다시 상호인증 후에 크리덴셜 서버에 저장하기 위한 크리덴셜 업로드(Credential Upload), 상호 인증 후에 하나 이상의 크리덴셜을 서버로부터 다운받기 위한 크리덴셜 다운로드(Credential Download), 상호 인증 후에 서버에 저장되어 있는 하나 이상의 크리덴셜을 제거하기 위한 크리덴셜 제거(Credential Delete) 절차 등으로 구성되어 있다. 서버에 저장되어 있는 크리덴셜 구성은 특정 크리덴셜을 확인하기 위한

크리덴셜 선택자 필드, PKCS#15 크리덴셜을 저장하기 위한 XML로 표현되는 패이로드, 최종 변경일, 수명 등을 포함하고 있다. 또한 사용자 인증과 서버 인증을 위한 프로토콜로 강력한 패스워드 기반 인증 프로토콜과 TLS(Transport Layer Security) 프로토콜을 이용할 것을 권고하고 있다. 패스워드 기반 인증 프로토콜은 패스워드를 기반으로 상호 인증을 제공하며, 인증 프로토콜의 부산물로 크리덴셜을 안전하게 다운받는데 필요한 세션 키를 추가로 얻을 수 있는 프로토콜이다.

5. 관련 연구 동향

가. 클라우드 컴퓨팅 기술

클라우드 컴퓨팅과 연관된 보안기술은 명확히 정립되지 않았으나 클라우드 컴퓨팅이 기존 IT 기술 연장성상에 있으므로 기존 보안기술을 적용할 수 있다. 다음 표는 '클라우드 보안 위협요소와 기술 동향 분석(보안공학연구논문지, 2014.4)'에 기술된 클라우드 컴퓨팅 구성요소와 각 요소에 해당되는 보안기술이다. [30]

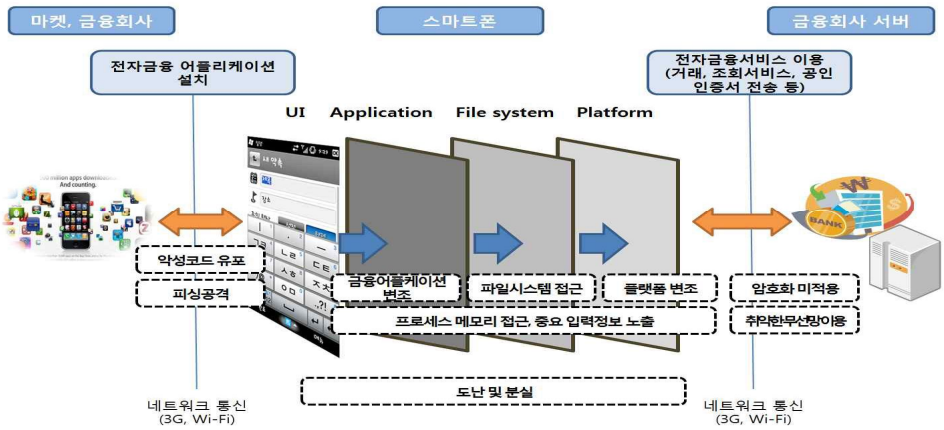
(표 10) Cloud Computing Components and Security Technologies

구분	보안관련 영역
플랫폼	▪ 접근제어: DAC, MAC, RBAC ▪ 사용자인증: ID 및 Password, PKI, Multi-factor, SAML(Security Assertion Markup Language), I-PIN, IAM(Identity and Access Management)
데이터 및 스토리지	▪ 검색 가능 암호시스템: 기존의 암호 기술과 같이 기밀성을 보장하면서 특정 키워드의 정보를 검색할 수 있도록 고안된 기술 ▪ PPDM(Privacy Preserving Data Mining): 데이터

	소유자의 프라이버시를 침해하지 않으면 서 유용한 정보를 추출해내는 기술 ▪ 기밀성: 체크섬(Checksum), 해싱(Hashing), PKI(Public Key Infrastructure) 등 ▪ 태깅(Tagging): 데이터태깅의 줄임말로 물리적으로 동일한 공간에 위치한 데이터에 부가정보를 추가하여 각 데이터 간 접근제어를 가능하게 하는 작업
네트워크	▪ 암호화 프로토콜의 사용: SSL, IPSec ▪ 보안장치: Application Firewall, Anti-DDOS, IDS(Intrusion Detection System), IPS(Intrusion Prevention System), ACL(Access Control List), SIEM(Security Information and Event Management), VPN(Virtual Public Network)
단말	▪ TPM(Trusted Platform Module), CryptoCell, SafeXcel IP, Virtualization Security, Renewable Security

나. 스마트폰 관련 연구 동향

스마트폰 기반의 전자금융거래를 시도할 때 발생 가능한 보안위협을 도식화한 것이다.



(그림 15) 스마트폰의 보안위협 분류 (출처: 금융부문 스마트폰 보안가이드)

스마트폰의 보안위협으로는 악성코드 유포, 피싱 공격, 어플리케이션 및 플랫폼 변조 증의 주요 입력정보 노출, 변조, 루핑 등이 가능하다. [31] 이러한 스마트폰 보안위협을 해결하기 위해서 '국내외 스마트폰 보안 표준화 동향 및 추진전략(TTA, 2010)'에서 기술된 스마트폰 보안기술(표 11)처럼 다양한 보안기술을 사용하고 있다. [32]

(표 11) 스마트폰 보안기술

구분	보안 기술
단말기 영역	▪ 어플리케이션 코드의 난독화 기술적용 ▪ 데이터의 암호화 ▪ 도난 및 분실방지 솔루션 ▪ 정기적인 업데이트 ▪ 안티바이러스
네트워크 영역	▪ 데이터 암호화 ▪ 방화벽, VPN ▪ 디바이스 인증
서비스 영역	▪ 스마트폰 안티바이러스 기술 ▪ 첨부파일 필터링 ▪ 스팸 메일 필터링 ▪ 불법 AP 및 인터넷 사용 방지
PC, 메모리 영역	▪ 스마트폰 안티바이러스 기술 ▪ 보안저장 장치 ▪ 개인정보 유출방지 솔루션 ▪ AD-HOC을 통한 접근통제
어플리케이션 스토어 영역	▪ 전자서명 기술을 이용한 코드서명 기술
GPS 영역	▪ 위치정보 보호

다. 전자인증 연구 동향

1) 금융감독원 인증수단 안정성 기술평가기준

금융감독원은 2011년 1월 31일 개최된 인증방법평가위원회에서 인증수단 안정성 기술평가기준을 제정하였다. 평가기준은 크게 인증방법의 기술적 요건과 보안등급, 보안요구사항(표 12)으로 나누어진다. 보안등급은 전자금융거래에 대하여 가장 낮은 보안등급인 보안 3등급에서 가장 높은 보안 1등급까지 총 세 등급으로 나누어져 있다. [33]

(표 12) 등급별 보안요구사항

등급	보안요구사항
3등급	▪ 비밀번호 추측방지, 파싱 및 파밍 방지 ▪ 유출 및 노출 방지, 위조 및 변조 방지 ▪ 거래내역 무결성 확인정보에 대한 검증 ▪ 금융기관에 저장된 거래내역에 대한 안전한 보관대책 수립 ▪ 인증수단의 등록, 발급, 배포, 폐기 등에 대한 안전한 관리적 요건 수립 ▪ 안전성이 검증된 암호 알고리즘 및 암호키 길이 사용 ▪ 암호키 관리를 위한 물리저그 관리적 절차 마련 ▪ 인증관련 기록의 보존 및 변경에 대한 보호대책 제공 ▪ 인증 장애시 대응 방안 제공
2등급	▪ 3등급 보안 요구사항을 모두 만족 ▪ 인증정보 재사용 방지, 인증정보 생성값 유출 방지 ▪ 중간자 공격 대응 ▪ 세션 가로채기 방지, 거래사실 부인 방지 ▪ 부인방지 확인정보에 대한 합리적인 검증 ▪ 사용자의 부인방지 정보가 사용자에 속한 유일한 정보임에 대한 합리적인 검증 ▪ 부인방지정보는 거래여부에 대해 유일하게 증명 ▪ 부인방지 정보에 대한 위변조 여부 확인
1등급	▪ 2등급 보안 요구사항을 모두 만족 ▪ 인증수단의 비밀정보의 물리적 유출 방지

2) NIST의 전자인증 가이드라인

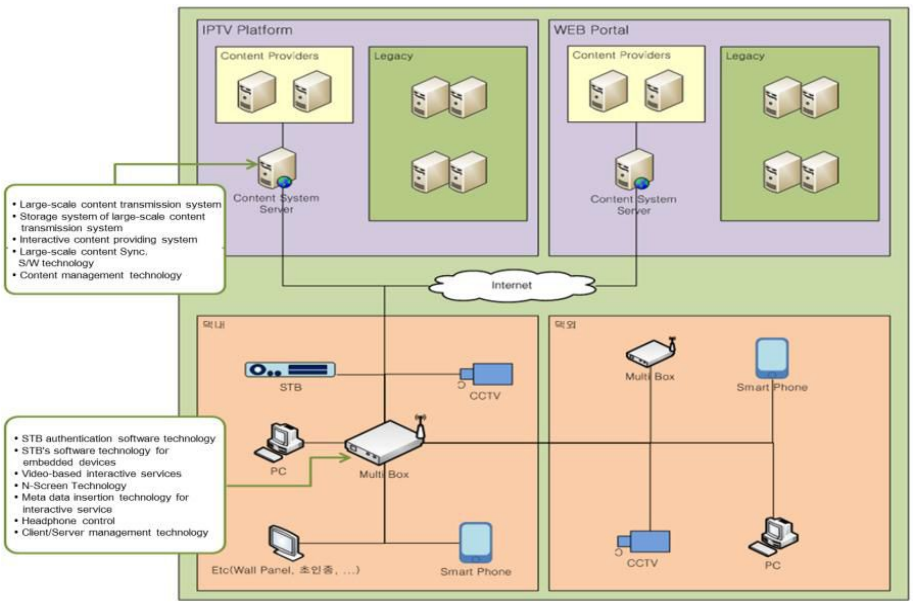
NIST에서 전자인증가이드라인을 배포하였고 이 문서는 등록 및 발행, 토큰, 토큰과 크리덴셜 관리 등 인증프레임워크별 위협 및 보증레벨을 정의하고 있다. [22]

(표 13) 레벨별 기술요구사항

단계	기술요구사항 또는 특성
레벨1	▪ 엄격한 신분증명이 요구되지 않으며 동일한 사용자가 보호된 정보나 작업에 접근을 보장 ▪ 패스워드에 함호학적 기법을 요구하지 않음 ▪ 오랫동안 사용된 인증 비밀값이 노출 가능성 존재
레벨2	▪ 한 가지 인증수산을 이용해 증명가능 ▪ 도청, 재사용, 온라인 추측 공격 방어 가능 ▪ 오랫동안 사용한 인증 비밀값이 외부 유출 불가 ▪ NIST에서 승인된 암호기술 사용
레벌3	▪ CSP를 통한 신분증명을 요구에 대해 사용자 신분증명 정보를 제공 ▪ 인증토큰 유출을 막을 수 있는 암호 매커니즘 요구 ▪ 인증시 암호프로토콜을 통해 비밀키나 인회용 패스워드의 소유여부 증명을 기반 ▪ 멀티펙터 인증수단을 이용한 사용자 인증을 요구 ▪ 모든 동작에서 NIST에서 승인한 암호기술 사용
레벌4	▪ 하드웨어 기반 암호토큰만을 사용해야하며 중요데어터 전송시에도 인증필요 ▪ 모든 참여자와 중요데이터 전송에 대한 강력한 암호학적 인증을 요구 ▪ 악성코드로부터 비밀정보 보호 필요 ▪ 도청, 재사용, 온라인추측, 검증자 위조, 중간자 공격 및 세션 가로채기 등의 공격에 대해 안전해야함 ▪ NIST에서 승인된 강력한 암호기술을 모두 동작에 사용

라. 스마트 디바이스를 위한 OSMU 관리 연구

“Study on the OSMU(One-Source Multi-Use) Management for Smart Devices(International Journal of Smart Home, Vol. 7, No. 1, January, 2013)”의 논문에서는 다양한 스마트 기기(Smart Phone, CCTV, PC, IPTV 등)에서 멀티박스를 사용하는 통합관리모델 구조를 통하여 디지털 컨텐츠를 배포 및 관리를 제공하여 하나의 컨텐츠에 대하여 다양한 스마트기기에서 사용할 수 있는 구조를 제공한다. 이 시스템은 대용량 컨텐츠 전송 시스템, 켄텐츠 전송 클라이언트, 웹서버, 컨텐츠 관리서버, IPTV와 웹을 통하여 컨텐츠를 제공하는 것으로 구성된다. [34]



(그림 16) 통합 컨텐츠 관리모델 구조

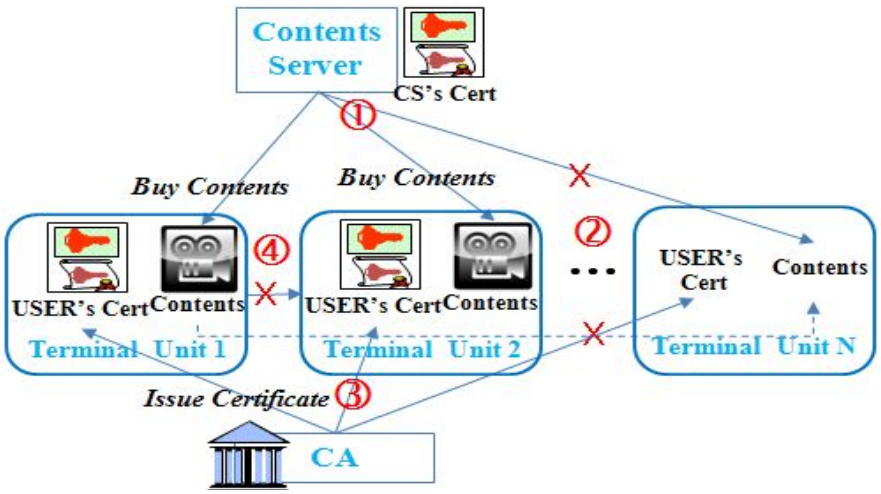
(출처: Study on the OSMU(One-Source Multi-Use) Management for Smart Devices)

Ⅲ. OSMU 환경내의 문제점

OSMU 환경에서 사용되는 컨텐츠 관리 기법, M2M 보안, 사용자 인증 기법, 크리덴셜 관리 기법 등의 한계 및 문제점 분석을 통하여 클라우팅 컴퓨팅 환경에 알맞은 SOSMU(Secure One-Source Multi-Use) 시스템의 요구사항을 도출하고자 한다.

1. 컨텐츠 관리시스템의 문제점

현재의 컨텐츠 관리시스템에 대한 분석을 통하여 안전하고 다양한 단말기기에서 사용 가능한 모델을 제안하고자 한다. 현재 사용하고 있는 관리시스템의 문제점은 아래와 같다.



(그림 17) 현재 컨텐츠 관리 모델의 문제점

첫째, 동일한 컨텐츠에 대하여도 단말기기가 상의한 경우 서로 다른 DRM을 적용하고 있어 다시 구매하여야 한다. 둘째, 컨텐츠 서버나

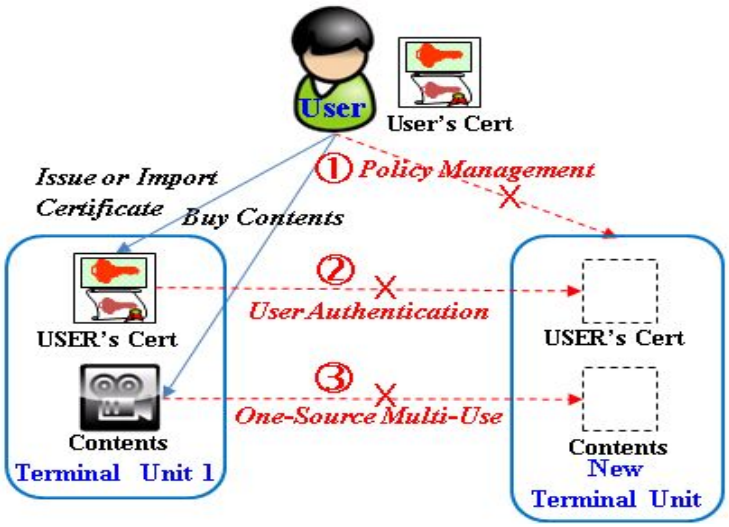
인증기관(CA)가 다양한 신규 단말기기나 다양한 운영체계 지원 등의 지원이 어려워서 통합적인 사용자 인증방안이 존재하지 않는다. 셋째, 단말기기에서 사용자 인증을 위해 중복적인 인증서의 발급 또는 복사로 인한 인증서 관리 및 노출의 문제점 발생 가능하다. 넷째, 단말기기간의 컨텐츠에 대한 이동 및 공유가 어렵고, 만약 공유하더라도 단말기기들의 사양차이로 인해 컨텐츠의 재생의 최적화된 환경이 어렵다.

이런 한계 분석을 통하여 다음과 같은 요구사항을 도출하였다.

첫째, 사용자 인증, 컨텐츠 관리, 새로운 모바일 기기, 사용자 정보에 대한 보안정책 등에 대한 통합적인 정책관리를 제공되어야 한다.

둘째, 신규 단말기기에 대한 경우에 다양한 환경이나 새로운 운영체계 에서의 사용자 인증 방안을 제공이 제공되어야 한다.

셋째, 단말기기 간의 컨텐츠에 대한 이동 및 공유가 편리해야 하고 단말기기들 간의 차이의 맞게 컨텐츠의 최적화된 지원이 필요하다.

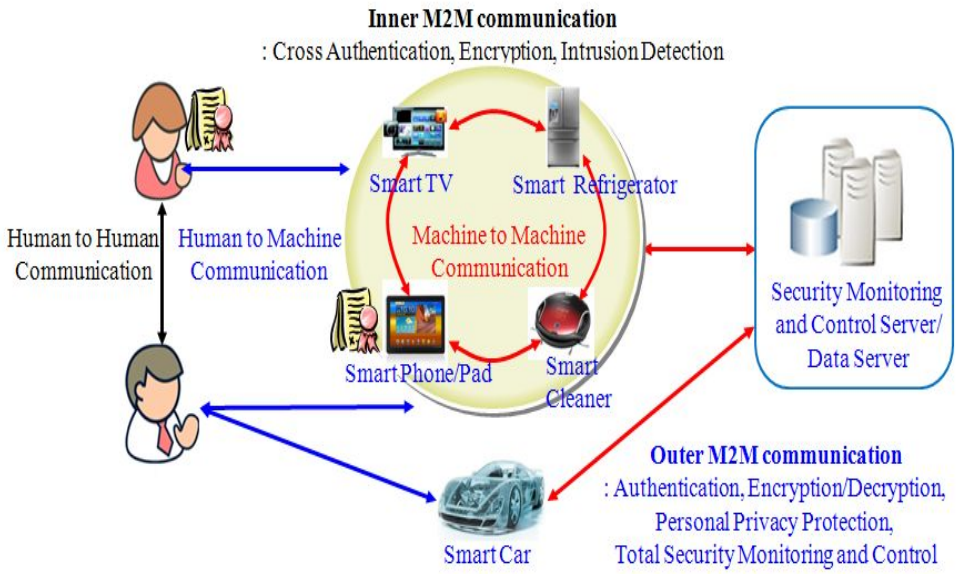


(그림 18) 컨텐츠 관리 시스템의 요구사항

위와 같은 한계를 극복하기 위해 통합된 정책관리방법과 동일한 컨텐츠에 대하여 다양한 단말기기에서 이용할 수 있는 환경 구축 필요하고 다양한 기기와 다양한 운영체계를 가진 신규 단말기기 들에 대하여 손쉽게 지원 가능한 N-screen 기반의 통합 사용자 인증방법의 필요성이 대두되었다.

2. M2M(Machine to Machine) 보안의 문제점

스마트기기의 인증에 대한 표준화, 공통된 보안 감시 및 통제 서비스, 인간중심의 개인정보보호, 다양한 스마트기기 간의 M2M (Machine to Machine)[35] 보안 등의 보안문제는 스마트기기 기반의 사회의 통신모델에서는 발생된다. [36]



(그림 19) 스마트기기 기간의 사회에서의 통신 모델

첫째는 다양한 종류의 새로운 스마트기기에 대한 디바이스인증 표준은 부재와 오픈 마켓에서의 인터넷 뱅킹 등과 같은 안전한 모바일 상거래와 금융서비스를 위한 표준화된 보안기술의 부재이다. 이러한 문제를 해결하기 위해서 통신환경, 스마트기기, 서비스들에서 사용하는 다양한 보안기술의 효과적인 관리를 위한 공개된 보안 플랫폼 기술의 표준이 필요하다.

둘째는, 새로운 형식의 사이버 테러리즘의 등장이 모든 스마트기기에 대한 해킹이 가능하기 때문에 악성코드의 배포, 악성 프로그램의 설치가 가능하다. 이러한 문제를 해결하기 위해서는 지능적이고 정교한 네트워크 인프라를 위한 보안 정책과 기술개발이 필요하다.

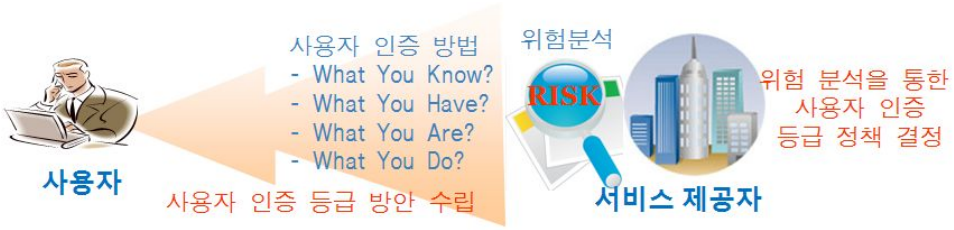
셋째는, M2M 통신에 참여하는 스마트기기 들에 저장된 개인정보의 노출이나 불법적인 획득에 의해 개인 생활이 위협을 받고 있다. 이를 해결하기 위한 스마트기기에 저장되는 개인정보에 대한 보호 대책 수립이 필요하다. [37]

넷째는, 스마트기기간의 상이한 인증방법 사용되고 기기간의 통신에서 중요한 데이터에 대하여 암호화 되지 않아 노출위험이 증가하고 있다. 이를 해결하기 위해서 스마트기기간의 통합적인 사용자 인증, 데이터 암호화, 복호화가 M2M 통신에서 요구되어 진다.

마지막으로 스마트기기, 네트워크, 서비스 등에 각 부분에 대한 전체적인 보안을 고려한 인프라가 구축이 요구되어 진다. 이를 해결하기 위해서 스마트기기, 네트워크, 서비스 등 모든 영역에서 스마트기기에의 통합보안 인프라의 구축이 요구된다. [38][39]

3. 사용자 인증 방법의 문제점

서비스 별 사용자 인증 방안의 분석을 통하여 사용자 인증 방법에서의 문제점 및 요구사항을 제시하고자 한다.



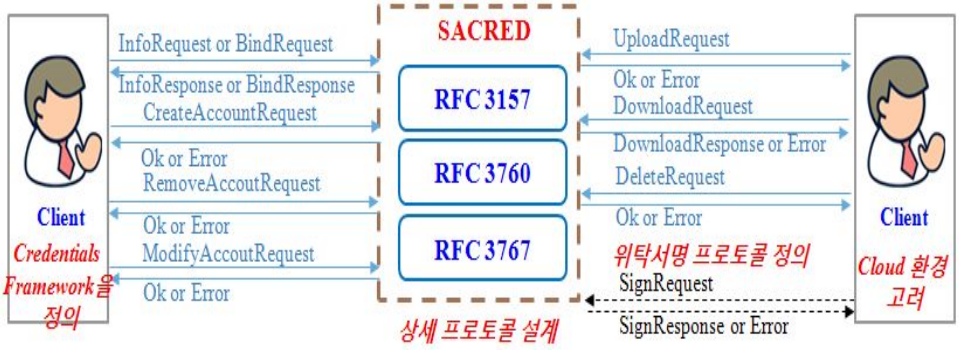
(그림 20) 사용자 인증 방법의 요구사항

첫째, 다양한 사용자 인증의 종류와 특성에 따라 사용자 등급화가 되어 있지 않아서 다양한 서비스에 사용자 인증 적용시 기준 점의 수립이 어렵다. 이를 위해 사용자의 인증의 종류와 특성에 분석하여 단계별 사용자 인증 등급화 방안 수립 필요하다.

둘째, 서비스 사이트 별 특성에 따른 사용자 등급의 결정 방법 수립이 수립되지 않아 일관되지 않는 사용자 인증 정책 적용으로 취약성이 존재한다. 이를 해결하기 위해서 서비스, 거래종류 및 현황파악, 거래량 범위, 고객홍보, 고객 구분, 거래의 영향 등을 통한 위험평가를 통한 서비스별 사용자 인증 방법 선택을 위한 절차 및 기준을 제공이 필요하다.

4. 크리덴셜 환경(SACRED)에서의 문제점

현재의 SACRED 표준의 바탕으로 분석한 문제점 및 요구사항은 다음과 같다.



(그림 21) 크리덴셜 환경의 요구사항

첫째, Securely Available Credential에 대한 프레임웍, 프로토콜에 대한 요구사항은 정의 되어 있으나 구체적인 구현을 위한 가이드는 제공하지 못하고 있다. 이를 해결하기 위해 클라우드 환경을 고려한 상세 프로토콜을 설계 등의 효율적인 개발 방안 제시가 필요하다.

둘째, SACRED은 크리덴셜에 대한 업로드(Upload)와 다운로드(Download) 프로토콜은 정의되어 있지만 클라우드 환경에서의 크리덴셜 이용을 위한 사용자가 업로드한 크리덴셜을 이용한 위탁 서명 프로토콜은 정의되어 있지 않다. 이러한 한계를 해결하기 위하여 SACRED에 정의된 프레임웍과 프로토콜의 요구사항을 충족하는 크리덴셜 프레임웍을 정의하고 크리덴셜 프로토콜을 구체적으로 설계하고 ASN.1(Abstract Syntax Notation) 기반으로 정의하고 클라우드 환경에 맞는 키 로밍(Key Roaming) 및 위탁서명 (Proxy Signature) 프로토콜을 정의가 필요하다.

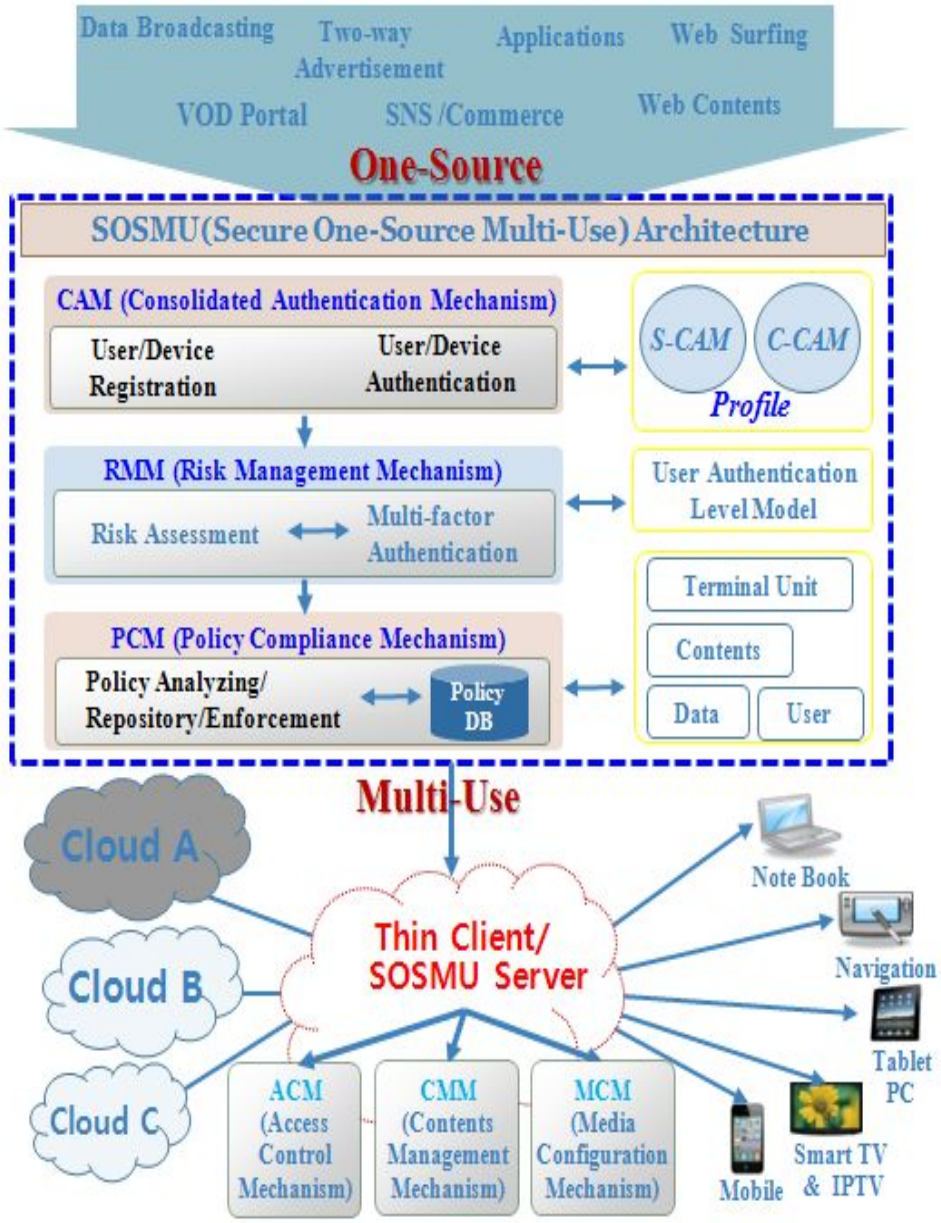
Ⅳ. SOSMU(Secure One-Source Multi-Use) 시스템

1. SOSMU 아키텍쳐

가. SOMUS 시스템 구조

제안된 SOSMU 시스템은 통합사용자 인증을 제공하는 통합인증 메커니즘(CAM: Consolidated Authentication Mechanism), 위험에 따른 사용자 인증방법을 선택할 수 있도록 지원하는 위험관리 메커니즘(RMM: Risk Management Mechanism), 체계적인 정책 설정 및 관리를 지원하는 정책 컴플라이언스 메커니즘(PCM: Policy Compliance Mechanism)로 구성된다. 추가적으로 요구되는 컨텐츠에 대한 관리를 담당하는 컨텐츠 관리 메커니즘(CMM: Content Management Mechanism), 사용자, 기기의 접근 권한을 관리하는 권한관리 메커니즘(ACM: Access Control Mechanism), 미디어 형상관리를 제공하는 미디어 관리 메커니즘(MCM: Media Configuration Mechanism)은 자세히 다루지 않는다.

CAM 모듈은 클라우드 컴퓨팅 환경에서 One-Source Multi-Use 시스템을 위한 보안 기술을 사용하여 사용자, 디바이스, 컨텐츠에 대한 통합적인 인증을 보장한다. PCM 모듈은 각 모듈 간의 상호연동 도중에 체계적인 정책관리와 OSMU 시스템의 통제를 담당한다. CMM 모듈은 현재의 컨텐츠와 미디어 정보를 관리하고 유무선 네트워크 구조에서 컨텐츠의 송신, 수신, 다운로드 등의 운영방법의 관리를 담당한다. ACM 모듈은 PCM 모듈로 부터의 관련된 보안과 프라이버시 정책들에 대한 수행 및 접근제어의 역할을 담당한다. [40][41][42]



(그림 22) SOSMU Architecture

나. 컨텐츠 구매 및 관리 절차 흐름

SOSMU 시스템은 사용자(User)와 단말기기(Terminal Unit)를 등록하고 컨텐츠에 대한 선택 및 구매하여 컨텐츠를 해당 기기에서 디스플레이를 수행하는 기본기능과 이미 다운받은 컨텐츠에 대하여 다양한 다른 기기에 변환 및 이동하여 사용하는 기능을 제공한다.

첫째, SOSMU 시스템에 사용자와 단말기기(Terminal Unit)들을 등록한다. 그리고 디지털 컨텐츠를 선택하여 구매를 한다. 구매된 컨텐츠는 서로 운영체계를 가진 여러 가지 단말기기에서 사용가능하도록 등록된 단말기기에 맞게 컨텐츠를 변환하여 다운로드한다.

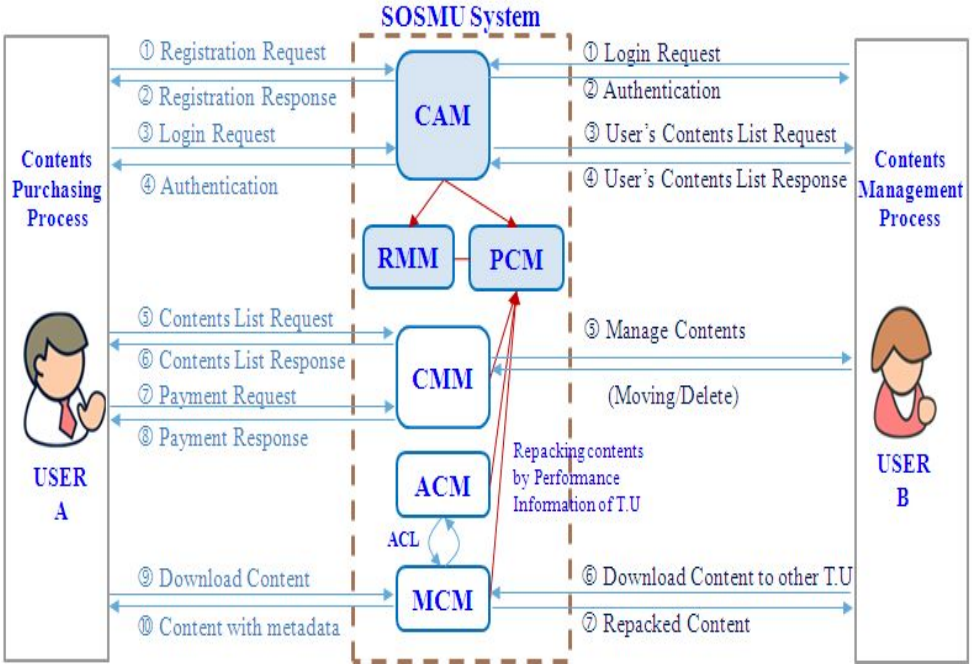
컨텐츠를 구매하고 관리하는 두 가지 절차는 다음과 같다.

1) 사용자 A : 컨텐츠의 구매 절차

SOSMU 시스템에 사용자 정보를 등록하고 사용하고자 하는 단말기기를 등록한다. 사용자는 등록된 단말기를 이용하여 단말기기 자체에 저장된 인증서나 크리덴셜 서버에 저장된 인증서를 이용하여 로그인을 수행한다. 사용자는 컨텐츠 목록으로부터 컨텐츠를 선택하고 이에 대한 지불을 하고 선택한 컨텐츠를 다운로드 받아 설치하고 이를 단말기기에서 사용한다.

2) 사용자 B :컨텐츠 관리 절차

사용자는 등록된 단말기기로 SOSMU 시스템에 로그인을 수행한다. 사용자는 구매한 컨텐츠의 목록을 확인 가능하다. 사용자가 구매한 컨텐츠를 다른 단말기기로 옮길 수 있다. 만약 컨텐츠가 다른 단말기기로 옮겨질 경우 선택된 단말기기의 정보에 따라서 컨텐츠는 해당 단말기기에 맞게 재 변환되어 설치된다.



(그림 23) SOSMU 시스템 흐름도

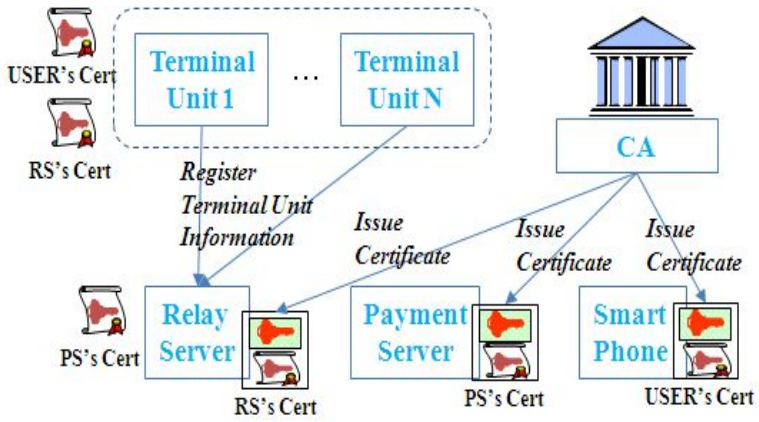
다. SOSMU 시스템 워크플로어

(표 14) Notations and Abbreviation

기호	설명	기호	설명
TU	Terminal Unit	OS	SOSMU Server
CS	Content Server	PG	Payment Server
SSN	사용자 주민번호	Key	암복호화용 세션키
USER	사용자	SN	단말기기 일련번호
R1	랜덤넘버1	R2	랜덤넘버2
H()	Hash Function	=?	비교함수
S()	서명생성	V()	서명 검증
E()	암호화	D()	복호화

SOSMU 시스템을 사용하기 위해서는 각 객체간의 초기설정단계를

통하여 인증서 발급 및 사용자가 소유하고 있는 단말기기에 대한 등록을 수행한다.



(그림 24) 초기 설정 절차

다음단계로 초기설정이 완료된 후는 실제 사용자가 단말기기를 이용하여 컨텐츠를 구매하여 해당 단말기에서 사용하는 단계이다.

① 단말장치는 중계서버에 단말장치 정보(Terminal Unit Information) 및 사용자 정보(User Identification Information)를 전달하고 중계서버는 기 가입된 사용자인지 및 상기 단말장치가 기 등록된 단말인지 여부를 인증하여 등록된 단말장치 및 기 가입된 사용자라는 조건으로 단말장치 연동 승인한다.

② 중계서버는 단말장치로부터 컨텐츠 목록정보 요청을 수신하고 컨텐츠 서버로 컨텐츠 목록 정보를 요청하여 받아 이를 단말장치에게 전달한다.

③ 단말장치는 전달받은 컨텐츠 목록에서 컨텐츠를 선택하여 암호화하여 중계서버로 전송한다. 중계서버는 암호화된 컨텐츠를 지정하는 정보(Contents Information)를 복호화하고 지정된 컨텐츠의 지불정보를

암호화하여 단말장치에 전송한다. 단말장치는 암호화된 지불정보를 복호화하고 결제정보를 입력하여 결제서버에 지불을 수행한다.

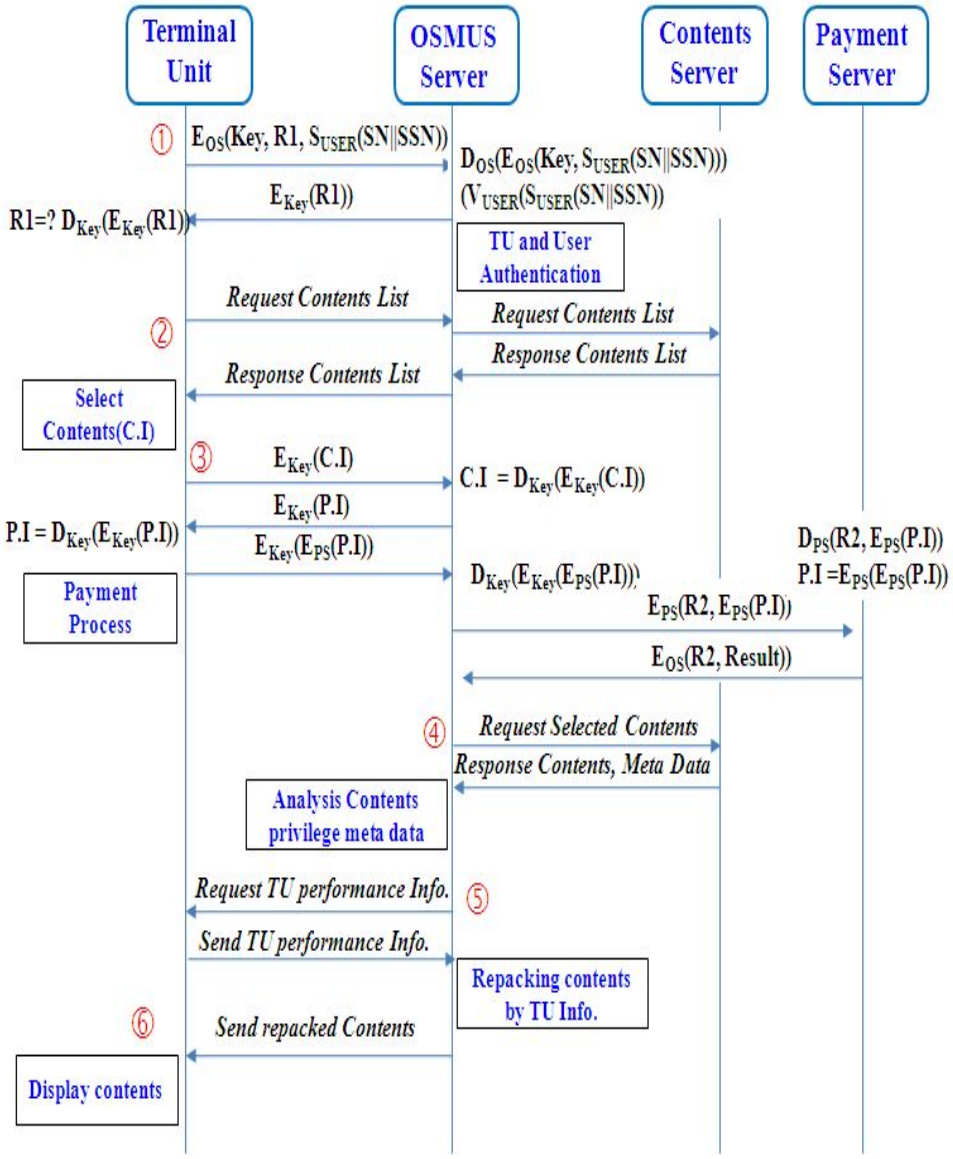
④ 지불이 완료되면 중계서버는 지정된 컨텐츠를 컨텐츠 서버로부터 수신하고, 수신된 컨텐츠에 패키징된 권한 메타데이터(Meta Data)를 분석한다.

⑤ 중계서버는 상기 단말장치의 성능정보를 획득하여 성능정보를 고려한 컨텐츠의 영상을 이미지화 한다.

⑥ 중계서버는 이미지화된 컨텐츠의 영상을 단말장치에 송신하고 단말장치는 이을 재생하고 재생된 이미지를 화면에 출력한다.

(표 15) Definition of Acronym

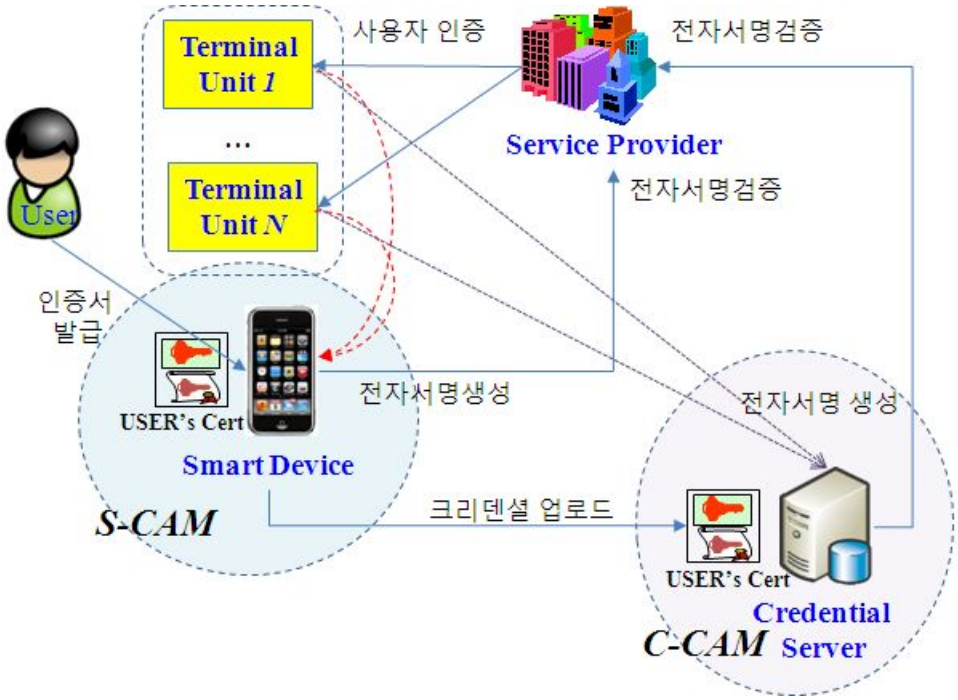
구분	설명
단말기기 정보 (T.I: Terminal Unit Information)	기기일련번호(Electronic Serial Number), 모바일 식별 번호, 전화번호, MAC 주소, 제품일련번호 등,
사용자 인증 정보 (U.I: User Identification Information	주민등록번호(Social Security Number), ID/Password, 인증서(Certificate), 지문(Fingerprint), 망막(Retina), 홍채(Iris) 등
컨텐츠 정보 (C.I: Content Information)	컨텐츠 이름, 컨텐츠 ID, 가격, 저작권자, 생산자(Provider)와 배포자(Distributor) 정보 등
지불정보 (P.I: Payment Information)	지불방법 및 정보(신용카드, 계좌이체, 휴대폰 결제 등), 지불자 정보 등
컨텐츠 메타정보 (M.D: Content Meta data)	구분(Category), 사용자, 단말기기, 권한정보(읽기, 쓰기, 수정, 삭제), 유효기간, 카운터, 사용기간, 복사 횟수 등
단말기기 성능정보 (T.P: Performance Information)	데이터 송수신 속도, 해상도, 컬러 수, 프로세스 종류, 이미지 타입, 비디오 가속기능(Video Accelerator) 등



(그림 25) SOSMU 시스템 동작 시나리오

2. 통합 인증 메커니즘(CAM: Consolidated Authentication Mechanism) [43]

통합 사용자 인증 모델을 크리덴셜(인증서 등)에 대한 관리 및 사용 방법에 따라서 사용자가 가지고 있는 스마트기기(Smart Device)를 이용한 통합인증모델(S-CAM: Consolidated Authentication Model using Smart Device)과 중앙 집중적인 크리덴셜 서버(Credential Server)를 이용한 통합인증모델(C-CAM: Consolidated Authentication Model using Credential Server)로 나누어 제시한다.

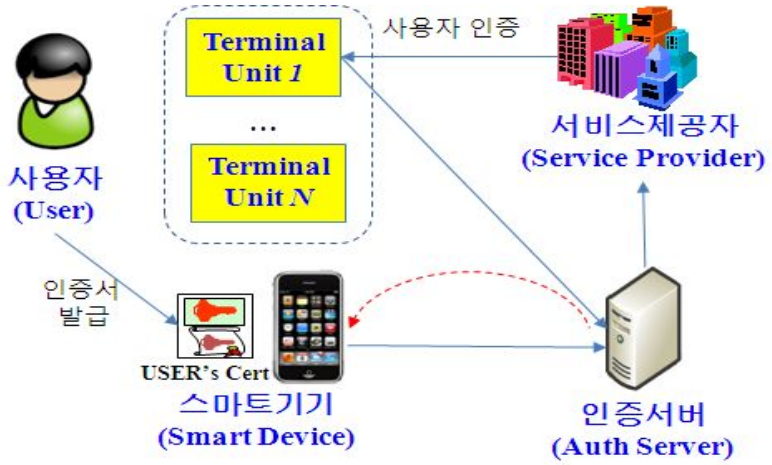


(그림 26) 통합 사용자 인증 모델

가. 스마트기기를 이용한 통합인증모델(S-CAM)

1) 개요

스마트기기를 이용한 통합인증모델은 사용자가 다양한 단말기기에서 동일한 사용자 인증방법을 사용하기 위하여 스마트기기 한곳에 인증서를 발급하여 보관하고 다른 단말기기 사용시 사용자 인증을 요구할 경우 인증서가 보관되어 있는 스마트기기를 통하여 인증을 수행하는 모델이다.



(그림 27) S-CAM 구성요소

2) 구성요소 및 절차

S-CAM의 구성요소 및 각 구성요소별 기능은 다음과 같다.

(표 16) S-CAM 구성요소의 기능

구분	설명
사용자 (User)	다양한 스마트기기와 단말기기를 이용하여 서비스를 이용하는 객체
스마트 기기 (SD: Smart Device)	스마트폰, 스마트 패드 등으로 사용자의 인증서를 발급, 관리하는 단말기기

인증서버 (AS: Auth Server)	사용자와 단말기기 간의 중간에서 사용자 및 기기에 대한 통합인증을 담당하는 시스템
단말기기 (Terminal Units)	Desktop PC, Notebook, Smart Phone, Smart TV, Tablet PC, PMP 등의 각종 단말기기
서비스제공자 (SP: Service Provider)	사용자를 위해서 다양한 단말기기를 통하여 서비스를 이용할 수 있도록 제공하는 공급자

다음은 S-CAM 프로토콜 절차 및 적용방법이다.

첫째, 사용자(User) 자신의 단말기기(Terminal Unit)로 서비스 제공자(Service Provider)에게 서비스를 요청한다. 둘째, 서비스제공자는 세션키(sk1)을 생성하고 서명할 데이터를 암호화하여 인증서버(Auth Server)에 전송한다. 셋째, 인증서버는 인증코드(auth_code)을 생성하여 서비스제공자에게 전송한다. 넷째, 서비스제공자는 사용자에게 안전한 보안채널을 통하여 인증코드를 전달한다. 다섯째, 사용자는 스마트기기의 응용프로그램을 이용하여 인증코드를 입력하고 인증서버에 전달한다. 인증서버는 입력된 인증코드와 서버의 인증코드와 비교하여 맞는 경우 인증서버는 스마트기기에 사용자의 전자서명을 요청한다. 여섯째, 사용자는 스마트기기에 저장된 인증서를 이용하여 전자서명 요청정보를 복호화하고 전자서명을 생성한다. 일곱째, 스마트기기는 서명된 데이터를 공유된 세션키(sk1)으로 암호화하여 인증서버로 전송한다. 여덟째, 인증서버는 인증기관의 인증서 폐지목록(CRL: Certificate Revocation List) [44]이나 실시간

인증서 상태조회 서비스(OCSP: Online Certificate Status Protocol) [45]를 통하여 사용자의 인증서의 유효성을 검증한다. 검증이 성공하면 인증서버는 암호화된 서명정보를 서비스 제공자에게 전달한다. 아홉째, 서비스제공자는 암호화된 서명정보를 복호화하고 전자서명을 검증한다. 만약 서명검증이 성공한다면 사용자에게 서비스를 제공한다.

3) 상세프로토콜

제안된 S-CAM은 스마트 기기(Smart Devices)에 저장된 사용자 인증서를 이용하여 다양하고 새로운 사용자 모바일 단말에서 N-screen 기반의 사용자 인증을 수행할 있도록 하는 모델이다. 크롭북(Chromebook) 등 별도의 플러그인(Plug-in)이나 엑티브엑스(ActiveX)등의 소프트웨어를 설치 없이 웹 브라우저만으로 사용자 인증이 가능한 구조이다. 전자서명정보의 안전한 전달을 위하여 서비스 제공자(Service Provider)과 스마트 기기간의 단대단(End-to-End) 암호화를 통해 인증서버(Auth Server)가 전자서명정보를 볼 수 없도록 설계하였다.

다음은 S-CAM 프로토콜의 상세 절차 및 적용방법이다.

① User: 서비스 요청

② SP: 전자서명할 데이터를 암호화

$$sk1 = E_{USER}(K1),\ encData = E_{K1}(Data),$$

$$Data = Name||SSN||sign\_msg$$

③ SP → AS: 서비스 기관코드(SP_code), 세션키(sk1),
서비스제공자 인증서(SP_cert), 암호화된 데이터(encData) 전송

④ AS: 인증코드 생성

⑤ AS → SP : 인증코드 전송

⑥ SP → TU : 인증코드 전송

⑦ SD : 스마트폰 어플을 이용하여 인증코드 입력

⑧ SD → AS : 사용자가 입력한 인증코드 전송

⑨ AS : 사용자가 입력한 인증코드의 일치여부를 확인하고
전자서명 요청

⑩ AS → SD : 세션키(sk1), 암호화된 데이터(encData),
서비스제공자 인증서(SP_cert) 전송

⑪ SD : 사용자의 개인키를 이용하여 암호화된 데이터를 복호화

$K1 = D_{USER}(E_{USER}(K1))$, $Data = D_{K1}(E_{K1}(Data))$

사용자의 개인키를 이용하여 전자서명을 수행함

$signedData = S_{USER}(sign\_msg)$,

$encSignData = E_{K1}(signedData)$

⑫ SD → AS : 사용자 인증서(User_cert), 암호화된 전자서명값
(encSignData)을 전송

⑬ AS : 인증기관의 CRL이나 OCSP를 이용하여 사용자 인증서를
검증함

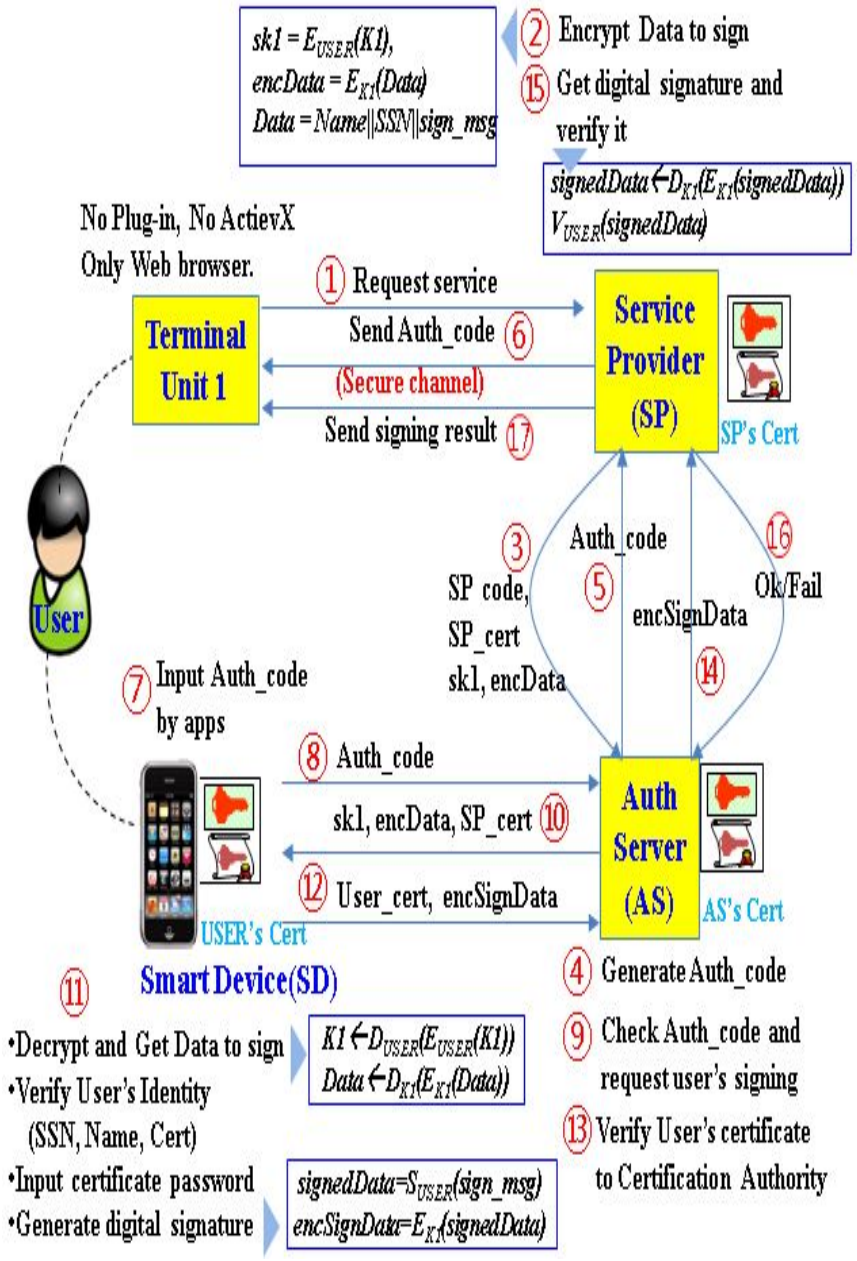
⑭ AS → SP : 암호화된 전자서명 값(encSignData)을 전송

⑮ SP : 암호화된 전자서명 정보를 복호화하고 전자서명을 검증함

$signedDataD_{K1}(E_{K1}(signedData))$, $V_{USER}(signedData)$

⑯ SP → AS : 검증 결과를 전송함

⑰ AS → TU : 전자서명 결과를 전송함

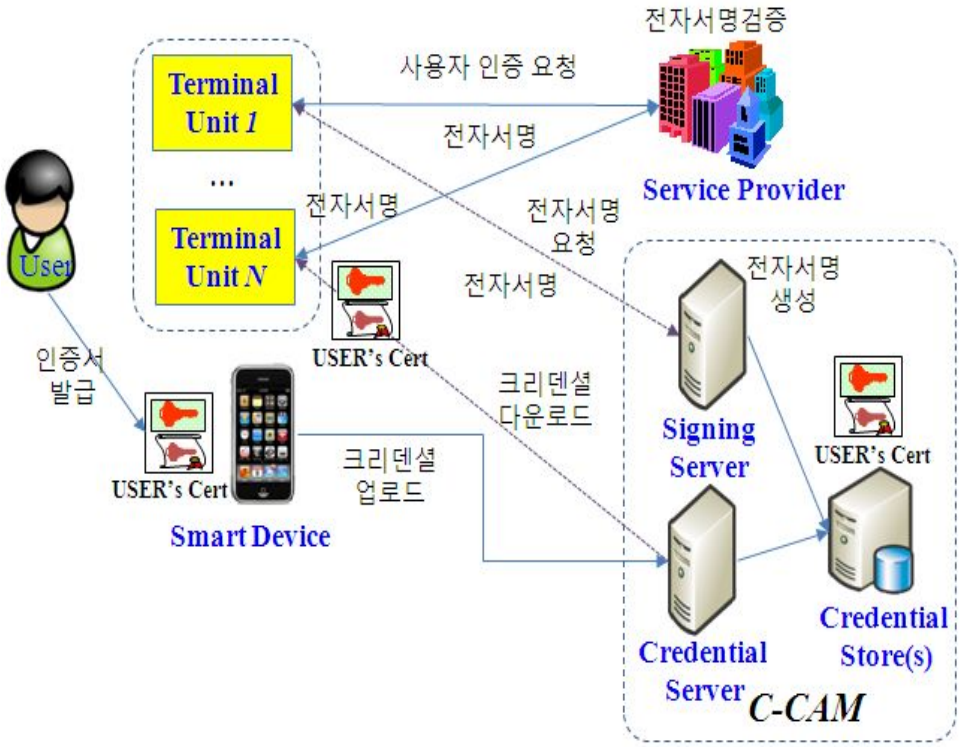


(그림 28) S-CAM 프로토콜 구조

나. 크리덴셜 서버를 이용한 통합인증모델(C-CAM)

1) 개요

크리덴셜 서버를 이용한 통합인증 모델은 사용자가 관리하는 크리덴셜을 중앙 집중적으로 관리하여 이를 필요로 하는 다양한 단말기기(Terminal Unit)에서 업로드되어 있는 크리덴셜을 다운로드하여 사용자 인증에 사용하거나 크리덴셜이 존재하지 않는 단말기기에서는 서명서버(Signing Server)를 이용하여 대신 전자서명을 생성하여 사용자 인증을 할 수 있는 구조이다.



(그림 29) C-CAM 구성요소

2) 구성요소 및 절차

프레임웍에 참여하는 사용자(User), 크리덴셜 서버(Credential Server), 크리덴셜 저장소, 서명서버(Signing Server)는 다음과 같은 역할을 수행한다.

(표 17) C-CAM 구성요소의 기능

구분	설명
사용자 (User)	PC, 스마트 패드(Smart Pad), 스마트폰(Smart Phone) 등의 다양한 기기를 통하여 크리덴셜 서버로부터 크리덴셜을 업로드하거나 다운로드하고 서명서버로부터 전자서명(digital signature)을 수행하는 주체(entity)
크리덴셜 서버 (CS: Credential Server)	사용자의 요구에 따라서 암호화된 크리덴셜을 다운로드하거나 업로드 하는 기능을 제공
크리덴셜 저장소 (Credential Store(s))	암호화된 크리덴셜을 안전하고 보관하는 저장소 역할을 수행
서명서버 (SS: Signing Server)	사용자의 요청에 의해 사용자 인증을 한 후 대신 전자서명을 생성하는 기능 수행
단말기기 (Terminal Units)	Desktop PC, Notebook, Smart Phone, Smart TV, Tablet PC, PMP 등의 각종 단말기기
서비스제공자 (SP: Service Provider)	사용자를 위해서 다양한 단말기기를 통하여 서비스를 이용할 수 있도록 제공하는 공급자

3) 프로토콜 구성

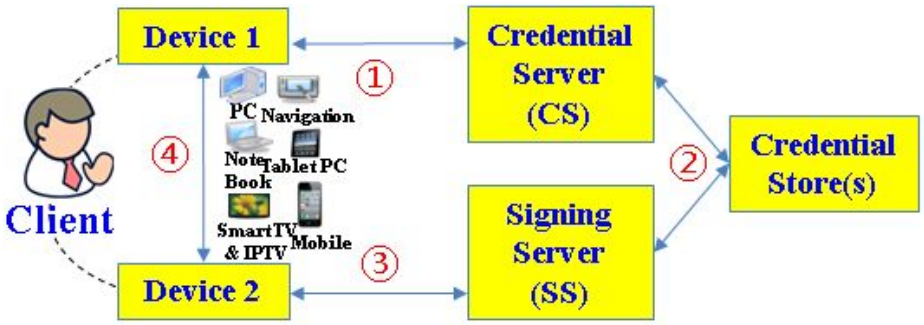
각 객체 간에 사용되는 프로토콜의 종류는 다음과 같다.

① Protocol 1: 사용자와 크리덴셜 서버의 간의 인증을 하고 크리덴셜 서버로부터 사용자의 크리덴셜을 업로드 또는 다운로드하는 프로토콜

② Protocol 2: 크리덴셜 서버에 의해서 사용자의 크리덴셜 정보를 저장하거나 가져오는데 사용되는 프로토콜

③ Protocol 3: 서명서버를 이용하여 사용자의 전자서명을 생성하는 프로토콜

④ Protocol 4: 하나의 기기에서 다른 기기로 크리덴셜을 직접 전송하기 위해 사용되는 프로토콜



(그림 30) 프로토콜 구성

4) 시스템 워크플로어

시스템 사용 흐름도를 설명하기 위해 사용자가 PC, 스마트폰, 태블릿 PC를 가지고 있고 사용자의 PC에 인증기관으로부터 크리덴셜(공인인증서 등) 발급 받아 저장하였다고 가정한다. 사용자는 다음과 같이 스마트폰, 스마트 패드 등의 다양한 단말기기를 이용하여 인터넷으로 제공되는 다양한 서비스를 C-CAM 기반의 사용자 인증을

통하여 자유롭게 이용할 수 있다.

다음은 사용자가 C-CAM을 이용한 다양한 시나리오이다.

① PC → C-CAM: Create Account (Register PC)

② PC → C-CAM: Upload Credential(s)

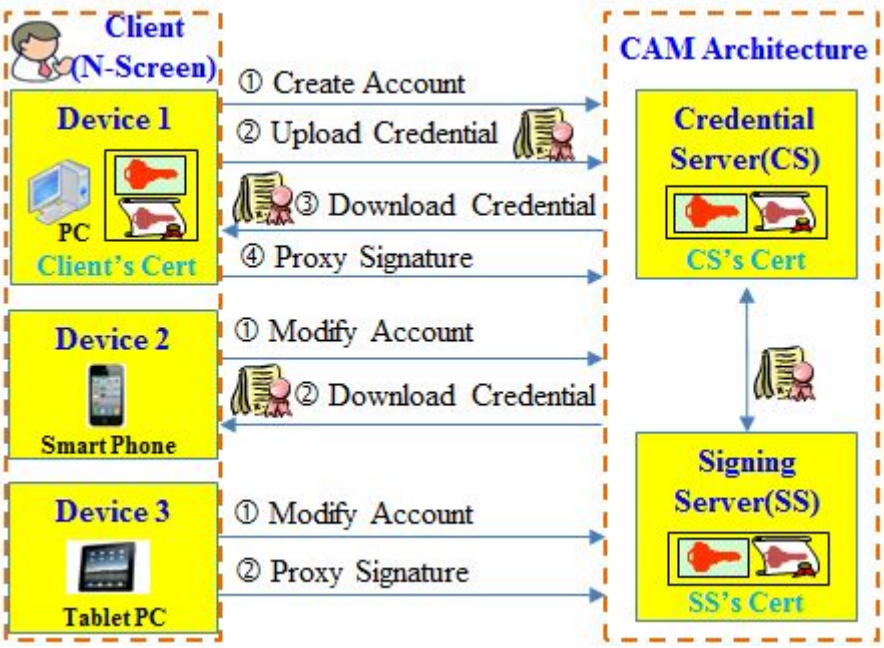
③ 스마트폰 → C-CAM: Modify Account (Register 스마트폰)

④ 스마트폰 → C-CAM: Download Credential(s)

⑤ 태블릿 PC → C-CAM: Modify Account (Register 태블릿PC)

⑥ 태블릿 PC → C-CAM: Proxy Signature Generation

⑦ PC → C-CAM: Download Credential(s)



(그림 31) 시스템 워크플로어

5) 안전한 크리덴셜 설계(Secure Credentials Design)

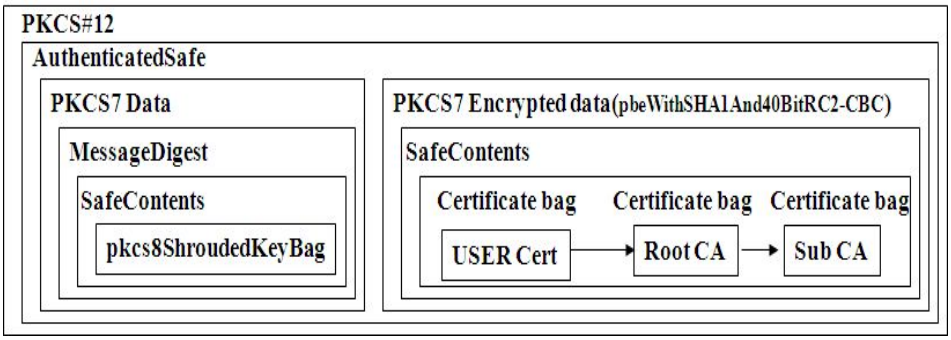
크리덴셜(Credential)은 객체의 신원확인을 위한 정보 또는 객체가 안전하게 통신을 도와 줄 수 있는 정보를 말한다. 크리덴셜은 개인키(Private Keys), 인증서 체인(Trust Roots), 티켓(Tickets), 또는 개개인의 보안환경(PSE: Personal Security Environment)에서의 중요부분 등이 포함된다[RFC2510]. 크리덴셜을 표현하기 위한 PKCS#12[46], PKCS#15[47] 등과 같은 여러 가지 표준 양식이 존재한다. 안전한 크리덴셜(Secure Credentials)은 안전한 암호학적 방법으로 보호되는 하나 또는 그 이상의 크리덴셜의 집합을 의미한다.

(표 18) 크리덴셜 프로파일

Field	F	Description
Version	M	Version
CredentialSelector	M	Credential identifier such as Name and ID
PayLoad	M	Form of credential such as PKCS#12 or PKCS#15
LastModified	M	Time of last modified
TimeToLive	O	The number of seconds the downloaded credential is to be unable
ProcessInfo	O	Information that server is intended to process
UserInfo	O	Information that User is intended to process

* M: Mandatory, O: Optional

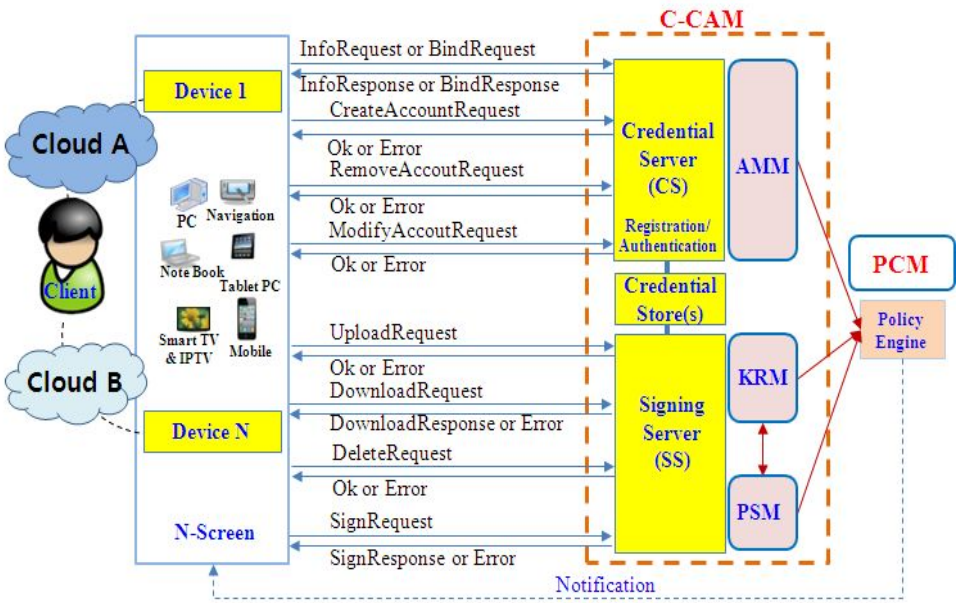
크리덴셜의 Payload에 PKCS#12 형식을 사용할 경우 암호화된 개인키, 인증서, 인증서 체인을 다음과 같은 형식으로 저장한다.



(그림 32) PKCS#12 Format

6) 프로토콜 프레임웍(Protocol Framework)

C-CAM은 계정관리 모듈(AMM: Account Management Module), 크리덴셜 로밍 모듈(CRM: Credential Roaming Module), 대리 서명 모듈(PSM: Proxy Signature Module)로 구성된다.



(그림 33) 프로토콜 프레임웍

프로토콜 설계에 사용되는 함수(Notations) 및 약어(Abbreviation)는 다음과 같다.

(표 19) Notations and Abbreviation

기호	설명	기호	설명
ID	Identification Number	KDF2	키 도출 함수 (Key Derivation Function 2) [48]
SN	Serial Number	RC,RS	랜덤값(Random Number)
C	크리덴셜 (Credential)	SC	암호화된 크리덴셜 (Secure Credential)
SD	Signed Data	TIME	서명시간
PV	Password Verifier	K	Key for SC
H()	해쉬함수(Hash)	=?	비교(Compare with)
S()	서명함수(Sign)	V()	검증 함수(Verify)
E()	암호화(Encryption)	D()	복호화(Decryption)

C-CAM에서 사용되는 프로토콜의 구성 및 상세 기능은 다음과 같다. 프로토콜은 초기화 및 키 교환 운용, 계정 관리 운용, 크리덴셜 로밍 운용, 대리서명 운용으로 구성된다.

가) 초기화 및 키 교환 운용(Initialization And Key Sharing Operations)

(1) BindRequest/BindResponse Protocol

사용자(User)가 인증서(Certificate)를 가지고 있는 경우 사용자가 자신의 개인키로 전자서명(Digital Signature)하여 서버에 전달하면 서버는 이를 검증(Verify)하고 세션키(Session Key: RS)를 생성하여 사용자의 인증서로 암호화하여 전달하여 상호간의 인증 및 키 교환(Key Exchange)을 한다.

①: User: I=H(ID), N=H(SN), SD=S_{User_key}(I|N|TIME)

②: User → CS: BindRequest(SD, User_Cert)

③: *CS: I|N|TIME= $V_{User\_cert}(SD)$, ERS=$E_{User\_cert}(RS)$*

④: *CS → User: BindResponse(ERS, CS_cert)*

⑤: *User: RS=$D_{User\_key}(ERS)$*

(2) InfoReqeust/InfoResponse Protocol

사용자(User)가 인증서가 없는 경우 SSL/TLS[49]나 DH Key Exchange[50]를 통하여 보안채널(Secure Channel)을 형성한 후 서버는 세션키(Session Key: RS)와 인증서를 전달한다.

①: *User → CS: InfoRequest*

②: *CS → User: InfoResponse(RS, CS_cert)*

나) 계정 관리 운용(Account Management Operations)

(1) 계정생성프로토콜(Create Account Protocol)

사용자(User)가 C-CAM에 가입할 때 크리덴셜 서버(Credential Server)는 사용자의 고유한 정보(Unique ID)의 해쉬 값과 사용자가 사용하는 PC, 스마트 패드(Smart Pad), 스마트폰(Smart Phone) 등의 기기의 고유정보인 일련번호(Serial Number)나 MAC Address 등의 해쉬 값을 등록한다.

①: *User → CS: BindRequest(SD, User_Cert)*

②: *CS → User: BindResponse(ERS, CS_cert)*

③: *User: <u>ERC</u>=$E_{RS}(RC)$, I=H(ID), N=H(SN),*
K=KDF2(I, PW), PV=H(H(ID, K)),
HI=H(I|PV|RS|RC|N), <u>EI</u>=E_{RC}(I|PV|HI|N)

④: *User → CS: CreateAccountRequest(ERC, EI)*

⑤: *CS: RC=D_{RS}(ERC)),I|PV|HI|SN=D_{RC}(EI),*
HI'=H(I|PV|RS|RC|SN, I|PV|HI|SN=?I|PV|HI'|SN

⑥: *CS → User: CreateAccountResponse(Ok or Error)*

(2) 계정 수정 또는 삭제 프로토콜(Modify Account Protocol and Remove Account Protocol)

사용자(User)가 새로운 기기정보를 등록하거나 등록된 기기정보를 수정할 수 있다. 사용자가 더 이상 계정을 사용하지 않을 경우 등록된 계정을 삭제할 수 있다

①: *User → CS: BindRequest(SD, User_Cert)*

②: *CS → User: BindResponse(ERS, CS_cert)*

③: *User: ERC=E_{RS}(RC), I=H(ID), N=H(SN),*
K=KDF2(I, PW), PV'=H(ID, K),
HI=H(I|PV'|RS|RC|N), EI=E_{RC}(I|PV'|HI|N)

④: *User → CS: {Modify,Remove}AccountRequest*
(ERC,EI)

⑤: *CS: RC=D_{RS}(ERC)), I|PV'|HI|N=D_{RC}(EI),*
HI'=H(I|PV'|RS|RC|N),
I|H(PV')|HI|N=?I|PV|HI'|N

⑥: *CS → User: {Modify, Remove}AccountResponse*
(Ok or Error)

다) 크리덴셜 로밍 운용(Credential Roaming Operations)

(1) 크리덴셜 업로드 프로토콜(Credential Upload Protocol)

사용자가 크리덴셜들을 크리덴셜 서버에 업로드하는 절차는 다음과 같다.

①② 사용자와 크리덴셜 서버가 상호인증 및 키 교환(RS)을 수행한다. ③④ 사용자는 크리덴셜을 암호화 및 복호화에 사용될 암호키(K)를 생성하여 크리덴셜을 암호화(SC: Secured Credential) 한다. 사용자는 자신의 세션키(RC)를 생성하고 서버로 보낼 데이터를 암호화한다. 또한, 사용자 세션키(RC)는 상호 공유된 키(RS)로 암호화한다. 크리덴셜 서버로 데이터를 전송한다. ⑤⑥ 크리덴셜 서버는 상호 공유된 키(RS)로 암호화된 세션키(ERS)를 복호화 하고, HI의 무결성을 검증한다. 크리덴셜 서버는 키 쉐어링 기법(Key Sharing Method) 등의 안전한 방법으로 크리덴셜 저장소(Credential Store(s))에 패스워드 검증자(Password Verifier)와 암호화된 크리덴셜(SC)을 저장한다.

①: User → CS: BindRequest(SD, User_Cert)

②: CS → User: BindResponse(ERS, CS_cert)

③: User: ERC=E_{RS}(RC),I=H(ID), N=H(SN),

K=KDF2(I, PW), PV=H(H(ID, K)), SC=E_K(C),

HI=H(I|PV|SC|RS|RC|N),

EI=E_{RC}(I|PV|SC|HI|N)

④: User → CS: UploadRequest(ERC, EI)

⑤: CS: RC=D_{RS}(ERC), I|PV|SC|HI|N=D_{RC}(EI),

HI'=H(I|PV|SC|RS|RC|N),

$I|PV|SC|HI|N=?I|PV|SC|HI'|N$

⑥: *CS → User: UploadResponse(Ok or Error)*

(2) 크리덴셜 서버로부터 크리덴셜 다운로드 프로토콜(Credential Download Protocol From Credential Server)

다양한 환경에서 크리덴셜을 사용하기 위하여 크리덴셜 서버에서 크리덴셜을 다운로드 받는 절차는 아래와 같다.

①② 사용자는 다운로드 받을 단말기기를 선택하고 크리덴셜 서버와 보안채널을 통하여 키 교환(RS)을 수행한다. ③ 사용자는 패스워드 검증자(PV')를 생성하고 자신의 세션키(RC)를 생성하여 보내질 데이터를 암호화 하고 자신의 세션키는 기 교환한 공유키(RS)로 암호화한다. ④사용자는 크리덴셜 서버에 데이터를 전송한다. ⑤⑥ 크리덴셜 서버는 공유된 키(RS)로 암호화된 사용자 세션키(RC)를 복호화하고 사용자 세션키로 EI를 복호화 하여 HI를 검증하고 패스워드 검증자(PV')와 저장되어 있는 패스워드 검증자(PV)의 일치여부를 확인한다. 만약 모든 검증 절차가 완료되면 크리덴셜 서버는 크리덴셜 저장소에 저장된 암호화된 사용자의 크리덴셜(SC)을 가져온다. 그리고 사용자의 세션키로 암호화된 크리덴셜을 암호화한다. ⑦ 사용자는 사용자 세션키(RC)로 암호화된 크리덴셜을 복호화하고 다시 암호화된 크리덴셜을 크리덴셜 복호화 키(K)를 이용하여 크리덴셜 정보를 얻는다.

①: *User → CS: InfoRequest*

②: *CS → User: InfoResponse(RS, CS_cert)*

③: *User: ERC=E_{RS}(RC), I=H(ID), N=H(SN),*

$K=KDF2(I, PW)$, $PV' = H(ID, K)$,

$HI=H(I|PV'|RS|RC|N)$, $\underline{EI}=E_{RC}(I|PV'|HI|N)$

④: *User* → *CS: DownloadRequest(ERC, EI)*

⑤: *CS:* $RC = D_{RS}(ERC)$, $I|PV'|HI|N=D_{RC}(EI)$,

$HI'=H(I|PV|RS|RC|N)$,

$I|H(PV')|HI|N=?\ I|PV|HI'|N$, $\underline{ESC}=E_{RC}(SC)$

⑥: *CS* → *User: DownloadResponse(ESC)*

⑦: *User:* $SC=D_{RC}(ESC)$, $C = D_K(SC)$

(3) 직접 솔루션에 의한 크리덴셜 다운로드 프로토콜(Credential Download Protocol From Direct Solutions)

서로 다른 디바이스 간에서 크리덴셜을 전달하는 방법은 현재 대부분의 웹 브라우저에서 지원하는 PKCS#12 방식을 사용한다. 크리덴셜은 개인키의 비밀번호와 PKCS#12의 비밀번호에 의하여 이중으로 보호된다.

①: *Device 1: PKCS#12Export*

(data or file(.pfx or *.p12))*

②: *Device1* → *Device 2: Transfer PKCS#12 data*

③: *Device 2: PKCS#12Import*

(data or file(.pfx or *.p12))*

라) 대리서명운용(Proxy Signature Operations)

(1) 대리서명프로토콜(Proxy Signature [51] Protocol)

사용자가 서명서버(Signing Server)를 이용하여 대리서명하는 프로토콜은 아래와 같다.

①② 서명서버(Signing Server)와 크리덴셜간에 인증서를 이용하여 상호인증을 수행하고 키(RS) 교환을 수행한다. ③④ 사용자는 안전한 채널을 통하여 서명서버와 키(RS) 교환을 수행한다. ⑤⑥ 사용자는 ID, PW를 입력하고 사용하는 디바이스의 일련번호(SN)을 추출한다. 입력된 정보를 가지고 크리덴셜 암복호화 키(K), 비밀번호 검증자(PV)를 생성한다. 전자서명 하고자 하는 원문(M)에 대한 해쉬 값(D)을 생성한다. ⑦⑧⑨⑩ 서명서버는 전달받은 데이터를 공유된 세션키(RS)를 이용하여 복호화 한 후 암호화된 크리덴셜(SC)을 얻기 위하여 크리덴셜 서버와 크리덴션 다운로드 프로토콜을 수행한다. ⑪⑫ 서명서버는 암호화된 크리데셜(Secured Credential)을 얻은 후 사용자가 보내준 키를 이용하여 크리덴셜을 얻고 이를 이용하여 전자서명(SD)을 생성한다. 전자서명을 생성 후 크리덴셜 정보, 각종 키 정보(K)등 관련 정보는 모두 삭제하여야 한다. ⑬ 사용자는 전송 받은 전자서명 정보(SD)에 대하여 검증을 수행한다.

①: SS → CS: BindRequest(SD, SS_cert)

②: CS → SS: BindResponse(ERS, CS_cert)

③: User → SS: InfoRequest

④: SS → User: InfoResponse(RS, SS_cert)

⑤: User: ERC=E_{RS}(RC), I=H(ID), N=H(SN),

$K=KDF2(I,\ PW),\ PV'=H(ID,\ K),\ \underline{D}=H(M),$

$HI=H(I|PV'|D|RS|RC|N),EI=E_{RC}(I|PV'|HI|N),$

$\underline{ED}=E_{RS}(ERC|EI),\underline{EK}=E_{RS}(K)$

⑥: $User \rightarrow SS:\ SignRequest\ (ED,\ D,\ EK,\ ERC)$

⑦: $SS:\ ERC|EI=D_{RS}(ED)$

⑧: $SS \rightarrow CS:\ DownloadRequest(ERC,\ EI)$

⑨: $CS:\ RC=D_{RS}(ERC),\ I|PV'|HI|N=D_{RC}(EI),$

$HI'=H(I|PV|RS|RC|N),$

$I|H(PV')|HI|N=?I|PV|HI'|N,\ \underline{ESC}=E_{RC}(SC)$

⑩: $CS \rightarrow SS:\ DownloadResponse(ESC)$

⑪: $SS:\ RC=D_{RS}(ERC),$

$SC=D_{RC}(ESC),K=D_{RS}(EK),C=D_K(SC),\underline{SD}=S_{User\_key}(D)$

⑫: $SS \rightarrow User:\ SignResponse(SD)$

⑬: $User:\ D=H(M),\ D'=V_{User\_cert}(SD),D=?D'$

3. 위험 관리 메커니즘(RMM: Risk Management Mechanism)

서비스별 사용자 인증 방법을 분석하여 1등급부터 5등급까지의 인증의 등급 분류 방안(User Authentication Level Model)을 제시하고 각 서비스마다 해당 사용자 인증의 선택 및 사용 방안을 제시하고자 한다. [52]

가. 사용자 인증의 등급분류

1) 1 등급(본인확인 정보: 중)

(표 20) 1등급 인증 등급

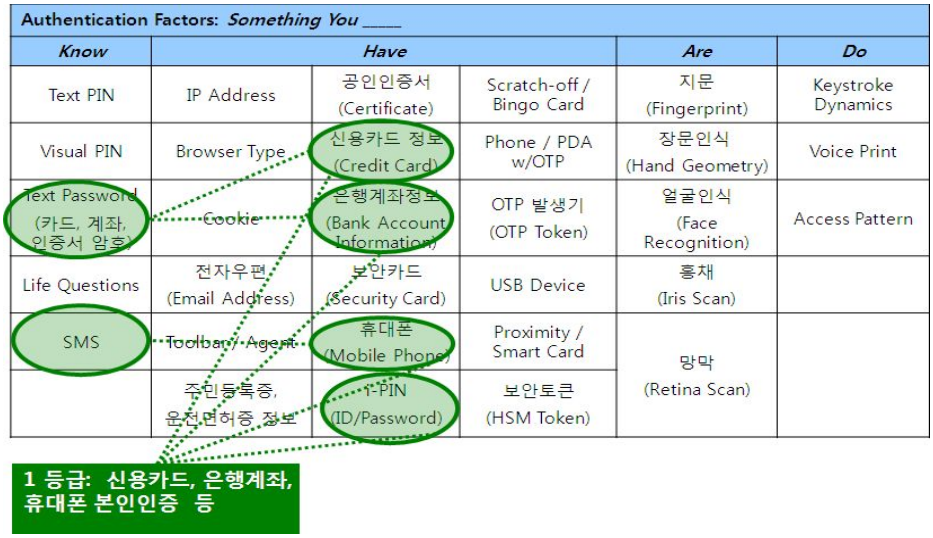
등급	번호	종류
1등급	①	신용카드 정보(주민번호, 카드번호, 유효기간, CVC 번호) + 카드비밀번호
	②	은행계좌 정보(실명, 주민번호, 계좌번호, 은행명) + 계좌비밀번호
	③	휴대폰 본인확인(주민번호, 휴대폰번호) + SMS 인증
	④	아이핀(신용카드, 은행계좌 본인인증)

① 신용카드 발급 및 전달 과정에서 신원확인 없이 전달되는 경우가 있음

② 신용카드, 계좌정보 입력시에는 키보드 보안과 보안채널은 반드시 적용되어야함

③ 휴대폰 소유주의 주민번호와 입력된 주민번호의 일치여부를 판단하고 SMS(Short Message Service)을 이용하여 인증을 하지만 기존의 SMS의 문제는 그대로 남아 있음

④ 신용카드와 은행계좌정보를 통하여 아이핀을 발급받아 아이디와 비밀번호로 본인확인을 수행할 경우에 해당되며 키보드 보안과 보안채널은 적용되어야함



(그림 34) 1등급 인증방법 예시

2) 2 등급(본인확인 정도: 상 (Soft Token + Password))

(표 21) 2등급 인증 등급

등급	번호	종류
2등급	①	공인인증서 + 인증서 암호
	②	아이핀(공인인증서 본인인증)

① 대면확인에 준하는 방식을 통한 신원확인을 수행하고 발급한 인증서의 경우 확실한 온라인 본인확인 수단을 제공함

- 공인인증서 암호의 경우 8자리 이상 대문자, 소문자, 숫자 1개 이상을 사용하고 입력시 키보드 보안의 적용을 권고함

② 공인인증서 본인확인을 통해 발급된 아이핀이 해당되며 키보드 보안과 보안채널은 적용되어야함

(그림 35) 2등급 인증방법 예시

3) 3 등급(본인확인 정도: 상 (Hard Token + Password))

(표 22) 3등급 인증 등급

등급	번호	종류
3등급	①	공인인증서 + 인증서 암호 + 보안카드
	②	공인인증서 + 인증서 암호 + 보안카드 + 휴대폰 SMS
	③	공인인증서 + 인증서 암호 + 휴대폰(저장장소)
	④	공인인증서 + 인증서 암호 + 보안토큰 + PIN

① 보안카드는 대면확인을 통하여 지급된 코드표로 분실되거나 스캔된 이미지 보관시 문제가 될 수 있음

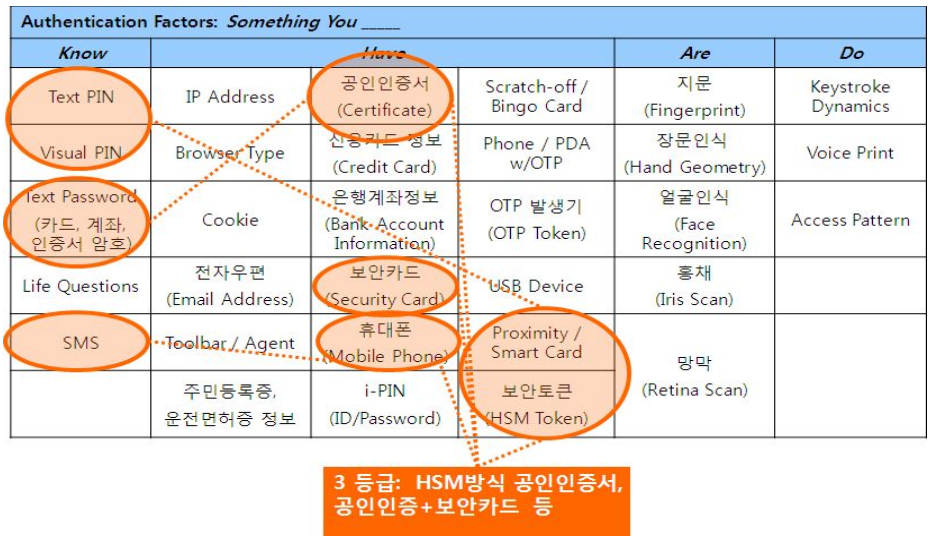
② 휴대폰 SMS을 통하여 거래내역을 전송하여 부정 사용시 이를 확인할 수 있도록 함

③ 인증서의 저장장소로 언제든지 휴대가 가능한 모바일 단말기를 사용

할 수 있으며 인증서 정보가 유/무선 환경에서 전달이 될 경우 안전한 방법을 사용하여야 함 (KISA의 기술규격을 준수하여야 함)

④ 보안토큰은 PIN 번호에 의해 보호되고 자유롭게 휴대가 가능하고 공인인증서를 저장 및 관리하기 위해서는 한국인터넷진흥원(KISA)로부터 인증심사를 통과하여야 함

- 사용자의 PC상에 불법적인 프로그램에 의한 공인인증서의 불법적인 취득을 방지하기 위하여 보안토큰을 사용을 권고하고 있고 보안토큰의 경우 개인키가 토큰 밖으로 나오지 않음



(그림 36) 3등급 인증방법 예시

* HSM : 공인인증서 복사방지를 위해 사용하는 보안성이 강화된 스마트카드, USB(Universal Serial Bus) 저장장치

4) 4 등급(본인확인 정도: 상)

(표 23) 4등급 인증 등급

등급	번호	종류
4등급	①	공인인증서 + 인증서 암호 + 보안카드 + 보안토큰 + PIN
	②	공인인증서 + 인증서 암호 + OTP발생기
	③	공인인증서 + 인증서 암호 + 보안카드 + 2 channel 인증

① 보안토큰에 공인인증서를 저장하여 보호하고 추가적으로 보안카드 이용하는 방안으로 물리적으로 안전한 보관이 필요함

② 공인인증서와 함께 보안카드보다 안전한 OTP발생기를 이용하는 방안으로 OTP 발생기에 대한 구매비용이 소요됨

③ 2 channel 인증은 두개의 서로 다른 통신경로(예, 인터넷과 전화, 전화와 FAX)를 이용하여 본인을 인증하는 방식

(그림 37) 4등급 인증방법 예시

5) 5 등급(본인확인 정도: 상 (Hard Token + Biometric))

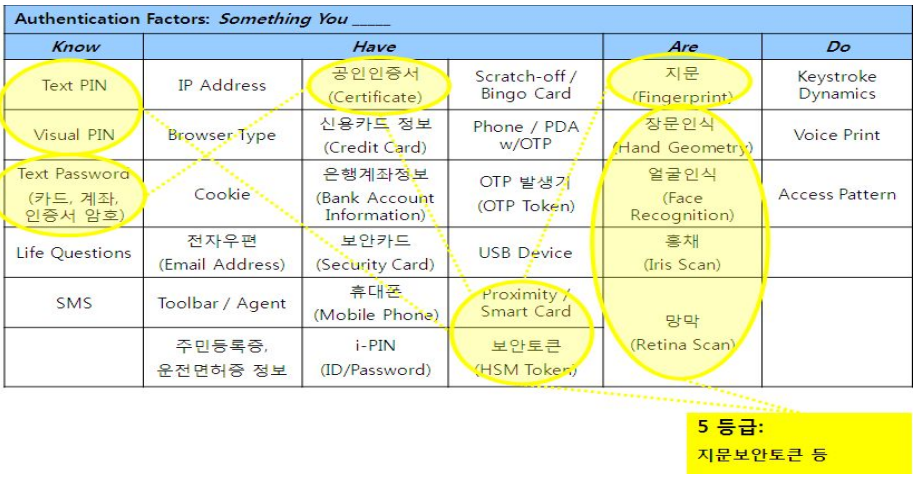
(표 24) 5등급 인증 등급

등급	번호	종류
5등급	①	공인인증서 + 인증서 암호 + 지문 + 보안토큰 + PIN
	②	공인인증서 + 지문(+인증서 암호) + 보안토큰 + PIN
	③	공인인증서 + 인증서 암호 + 보안토큰 + PIN + 생체인증

① 보안토큰에 공인인증서와 지문을 보관하고 PIN과 인증서 암호를 통하여 인증하는 방식

② 보안토큰에 공인인증서와 지문을 보관하고 보안토큰의 접근은 PIN인증을 통하고 인증서 암호를 지문인증으로 대체하여 사용의 편리성을 제공하는 방법

③ 보안토큰에 공인인증서를 보관하고 PIN과 인증서 암호를 통해 접근하고 사용자가 가지는 생체정보(장문인식, 홍채, 얼굴, 망막 등)을 이용하여 인증하는 방식



(그림 38) 5등급 인증방법 예시

나. 사용자 인증의 선택 및 사용방안

사용자 인증 방법의 선택을 위한 절차는 다음과 같다. [53]

① 응용서비스에서 사용되는 거래종류, 위험수준, 사용자 인증방법, 부가적인 보안방법에 대한 조사를 수행한다.

② 사용자 인증관련 위협(Threats), 취약점(Vulnerabilities)에 대해 파악한다.

③ 각 거래에 미치는 영향을 평가하고 위험빈도를 순위화 한다.

④ 제안된 인증 등급 방안을 이용하여 적용방안을 선택한다.

⑤ 사용자 인증을 적용한 후 해당 위험이 제거되었는지를 테스트를 수행한다.

⑥ 지속적이고 주기적으로 위험평가 및 관리를 수행한다.

(표 25) 위험평가(Risk Assessment) 방법

평가 항목	상세설명
서비스 설명	고객, 고객의 종류, 데이터 흐름 등의 전반적인 개요
거래종류 및 현황파악	개개인의 거래의 종류에 따라 다양한 위험수준을 파악하는 것(예, 거래종류, 위험수준(상, 중, 하), 인증방법, 추가적인 보안방법 등 포함)
거래량 범위	추가적 인증이 필요한 거래의 종류 및 범위에 대한 확인
고객 홍보	서비스를 이용하는 고객에 대하여 위험을 대처하기 위한 교육 및 정보를 제공하는가를 확인 (비밀번호 관리정책, 거래의 주기적인 확인 등)
고객 구분	서비스를 이용한 고객별 올바른 인증정책을 사용하고 있는지를 확인
거래의 영향	하루에 고위험의 거래가 얼마나 많은가? 만약 다중인증을 적용시 고객서비스에 대한 영향평가 수행

4. 정책 컴플라이언스 메커니즘(PCM: Policy Compliance Mechanism)

SOSMU 시스템에서 PCM모듈의 정책엔진(Policy Engine)을 통하여 통합적인 정책관리를 수행한다.

(표 26) 정책 종류(Policy Classification)

No	Entity	Policy Item
1	사용자(User)	인증 등급(Authentication Level)
		인증 방법(Authentication Method)
		사용자 인증 정보(User Identification Information)
2	단말기기 (Terminal Unit)	기기인증(Device Authentication)
		단말기기 종류(Type of Terminal Unit)
		단말기기 성능(Device performance)
3	컨텐츠 (Contents)	컨텐츠 종류(Content Type)
		지불방법(Payment Method)
		메타데이터(Meta Data)
4	데이터(Data)	데이터 등급(Data Level)
		암호화 필드(Encryption Field)
		암호화 방법(Encryption Method)

가. 사용자 정책(User Policy)

사용자 인증은 사용자 인증 등급모델(UALS: User Authentication Level Model)[52]에서 정의하는 사용자 인증 등급을 사용한다.

(표 27) 사용자 인증 정책(User Authentication Policy)

Policy Item	Examples
인증 등급(Authentication Level)	Level1 ~ Level5
인증 방법 (Authentication Method)	Certificate, Certificate+Mobile phone, Certificate+Biometric etc.
사용자 인증 정보 (U.I: User Identification Information)	Social Security Number, ID/Password, Certificate, Fingerprint, Retina, Iris etc

나. 단말기기 정책(Terminal Unit Policy)

단말기기의 인증의 경우 기기(Device)의 맥주소(MAC Address), 기기 일련번호(Serial Number) 등이 포함된 기기 인증서(Device Certificate)를 이용하여 인증을 수행한다.

(표 28) 단말기기 정책(Terminal Unit Policy)

Policy Item	Examples
등록된 단말기기 목록 (Registed Terminal Unit List)	User's Terminal Units (Smart Phone, Tablet PC, Notebook, PC 등)
단말기 인증사용여부 (Use of the Device Certificate)	Yes or No
단말기기 정보(T.I: Terminal Unit Information)	Electronic Serial Number, Mobile Identification Number, Phone Number, MAC Address, Product ID 등
단말기기 성능 정보 (T.P: Performance Information)	Data Receiving Speed, Display Resolution, Color Depth, Processor, Image Type, Video Accelerator

다. 컨텐츠 정책(Content Policy)

컨텐츠의 경우 컨텐츠의 종류에 따라서 연령별 사용 가능여부를 확인하고 컨텐츠의 금액에 따른 신용카드(Credit Card), 계좌이체(Money Transfer) 등의 지불방법에 대한 정책 설정, 컨텐츠별로 부여되는 권한, 재행 횟수 등의 정보가 포함된 메타데이터(Meta Data)를 통한 확인이 포함된다.

(표 29) 컨텐츠 정책(Content Policy)

Policy Item	Examples
Contents Information (C.I)	Contents Name, Contents ID, Content Type, Price, Copywriter, A Provider and A Distributor, 등
Payment Information (P.I)	Payment Method and Data (Credit Card, Money Transfer, Mobile Payment 등), Payer Information 등
Contents Metadata (M.D)	Category, User, Terminal Unit, Permission Data(Read, Write, Update, Delete), Validity, Counter, Duration, Copy Count 등

라. 데이터 정책(Data Policy)

SOSMU 시스템에서 사용되는 데이터에 대한 중요도 (High, Medium, Low)를 설정하고 민감한 데이터(Sensitive Data)의 경우 안전한 암호 알고리즘을 이용하여 암호화하도록 정책을 설정한다.

(표 30) 데이터 정책(Data Policy)

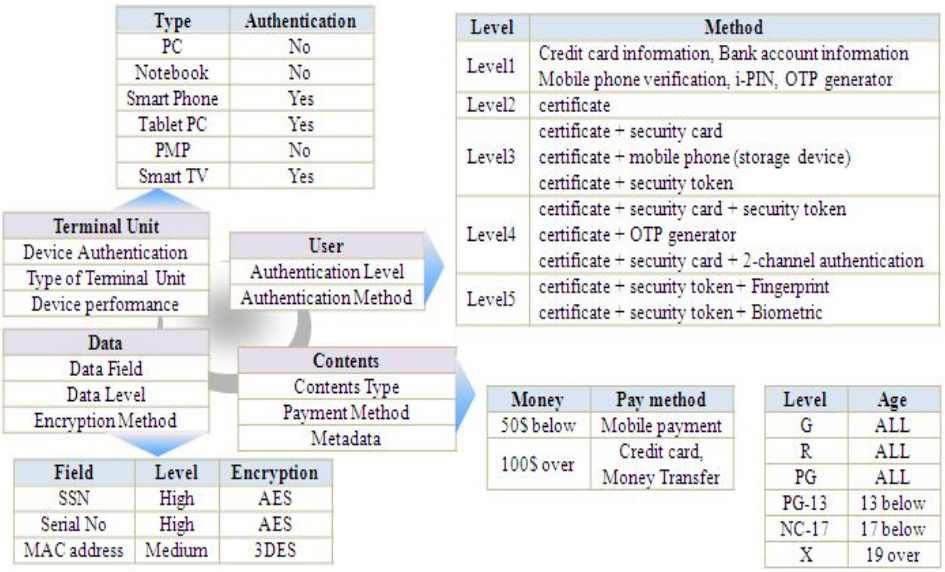
Policy Item	Examples	
데이터 (Data)	등급(Level)	상(High), 중(Medium), 하(Low)
	암호화 필드 (Field)	사용자 정보 필드(User Information), 지불 정보 필드(Payment Information) 등
	암호화 방법 (Method)	AES (Advanced Encryption Standard), 3DES 등

Ⅴ. 시스템 설계 및 구현

1. 정책 알고리즘(Policy Algorithm Design)

가. 정책 알고리듬 설계

아래의 그림은 OSMU 시스템을 위한 사용자, 단말기기, 컨텐츠, 데이터의 정책 항목에 대한 상세한 정책 구성 예시이다.



(그림 39) 정책 알고리즘 예시

나. 정책 알고리즘 구성

SOSMU 시스템을 구현하기 위해 사용자 정책(User Policy), 단말기기 정책(Terminal Unit Policy), 컨텐츠 정책(Content Policy), 데이터 정책(Data Policy)에 대한 알고리즘의 정의하고자 한다.

1) 사용자 정책 알고리즘(User Policy Algorithm)

(표 31) 사용자 정책 알고리즘

Algorithm 1: User/Device Access Decision

Input: A subject and a selected Terminal Unit Information

Output: A boolean variable, *decision*

```
1 /* If decision = true, access will be granted otherwise no
  access*/
2 decision = false;
3 if UserAuth(Authentication_Level, Authentication_Method,
   User_Info)= true then
4    if UseDeviceCert = yes then
5        foreach Registed_TerminalUnit_List do
6            if Selected_TerminalUnit_Info then
7                if DevicAuth(Device_Certificate,
  TerminalUnit_Info) then
8                    decision = true;
9 return decision;
```

2) 단말기기 정책 알고리즘(Terminal Unit Policy Algorithm)

(표 32) 단말기기 정책 알고리즘

Algorithm 2: Get Terminal Unit Performance Information

Input: Terminal Unit Information

Output: Performance Information

```
1 Performance_Info = GetTUPerformanceInfo(TerminalUnit_Info);
2 if Performance_Info = NULL then
3        return "Not Supported";
4 else
5        return Performance_Info;
```

3) 컨텐츠 정책 알고리즘(Content Policy Algorithm)

(표 33) 컨텐츠 정책 알고리즘

Algorithm 3: Content Level Decision

Input: User Information and Content Information.

Output: A boolean variable, *decision*

```
1 /* If decision = true, contents will be accessed otherwise no access
     Content Level: G, PG, PG-13,R,NC-17,X */
2 decision = ContentLevel(Content_Type,User_Info);
3 return decision;
```

(표 34) 메타데이터 정책 알고리즘

Algorithm 4: Check Content Metadata Policy

Input: A Content Information, Terminal Unit Information, Metadata

Output: A boolean variable, *decision*

```
1 /* If decision = true, contents will be processed
                        otherwise no process */
2 decision = CheckMetadata(Content_info,
                        TerminalUnit_Info, Metadata);
3 return decision;
```

4) 데이터 정책 알고리즘(Data Policy Algorithm)

(표 35) 데이터 정책 알고리즘

Algorithm 5: Data Level Decision

Input: Data Field.

Output: Data Level, Data Encryption Algorithm

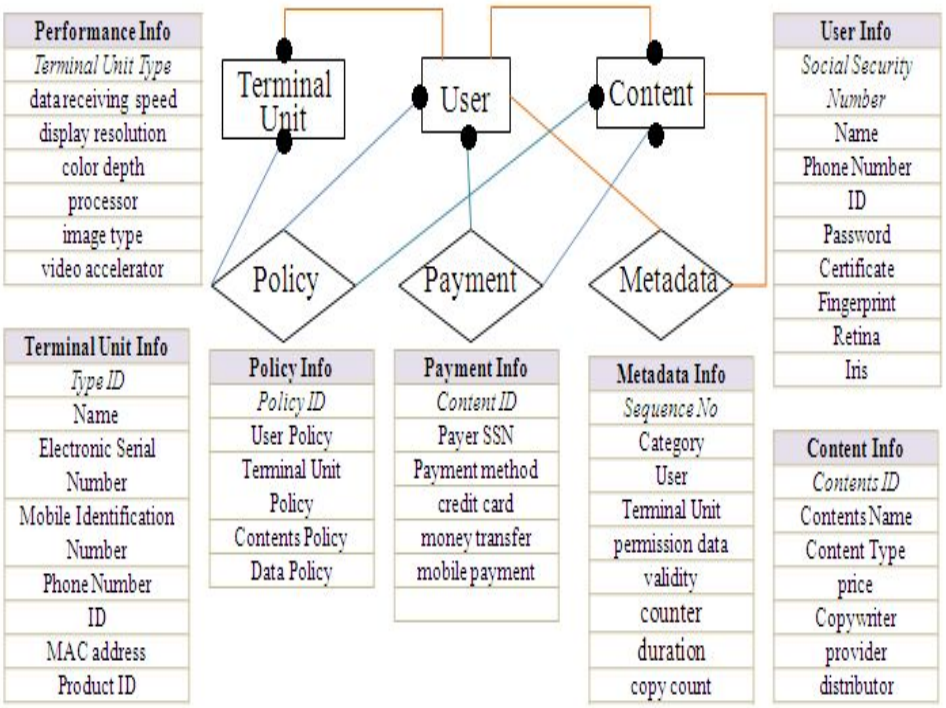
```
1 /* Data_Level: High, Medium, Low */
2 Encrypt_Algorithm= NULL; /* No Encryption */
3 Data_Level ß DataLevel(Data_Field);
4 Encrypt_Algorithmß GetEncryptAlgo(Data_Level);
5 return (Data_Level, Encrypt_Algorithm);
```

2. OSMU 시스템 설계

가. 데이터베이스 설계

체계적인 정책 관리를 제공하는 정책준수모듈(PCM)을 구현하고 기정의된 정책 알고리즘을 반영한 OSMU 시스템의 데이터베이스 스키마 구조는 다음과 같다.

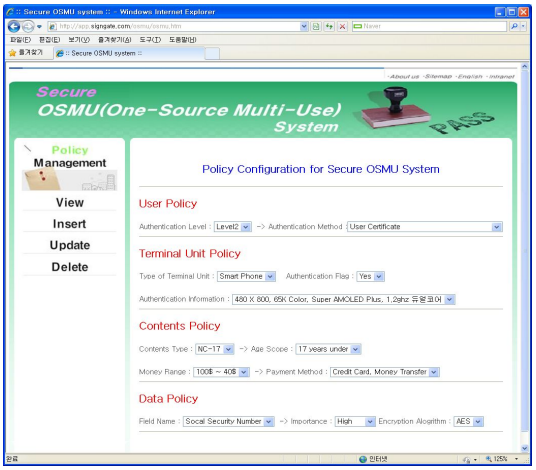
정의된 테이블은 성능정보(Performance Info), 단말기 정보 (Terminal Unit Info), 정책정보(Policy Info), 지불정보(Payment Info), 메타정보(Metadata Info), 사용자정보(User Info), 컨텐츠정보 (Content Info)이다.



(그림 40) PCM 데이터베이스 스키마

나. 화면 설계

다음은 OSMU 시스템에서의 정책 조회 화면, 정책 설정 화면 예시이다.



(그림 41) 정책 조회 화면

(그림 42) 정책 설정 화면

3. 스마트기기를 이용한 통합인증(S-CAM)

가. 구현

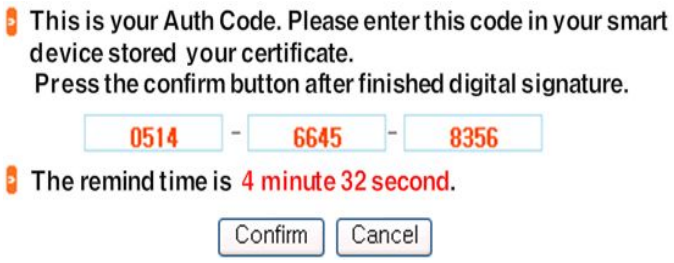
스마트 기기를 이용한 통합인증의 구현은 JSP, JAVA, iOS 용 개발 툴킷을 사용하였다.

다음 시나리오는 사용자의 스마트폰에 사용자의 인증서가 저장되어 있고 PC를 이용하여 응용서비스의 이용시 서비스기관(SP: Service Provider)이 사용자 인증을 요구할 경우 스마트폰에 저장된 인증서를 통하여 전자서명을 수행하여 사용자 인증을 수행하는 것이다.

다음은 스마트기기를 이용한 통합인증(S-CAM)의 프로토타입에 대한 이용 절차 예시이다.

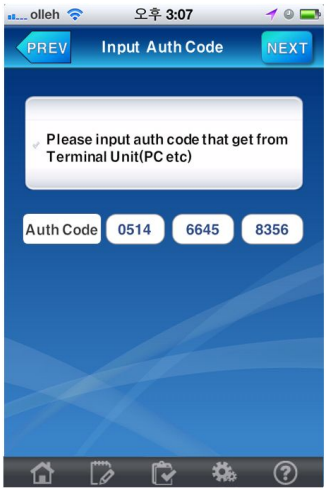
① PC : 사용자 로그인(전자서명 요구)

② 서버(AS) → PC : 사용자의 PC에서 인증코드 생성하기



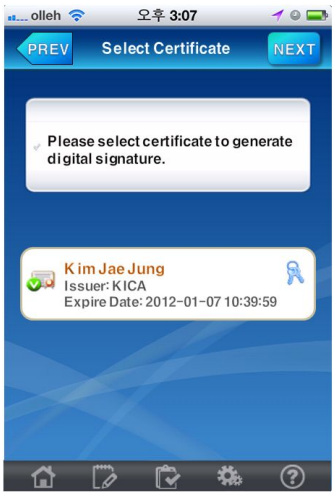
(그림 43) 인증코드를 생성하는 화면

③ Smart Phone : 인증코드 입력



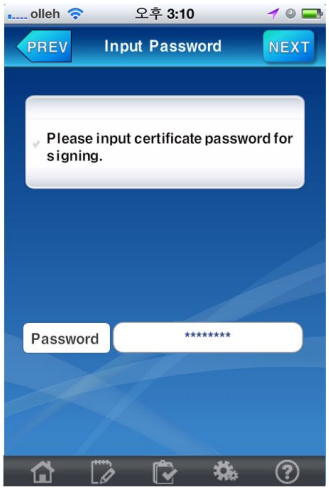
(그림 44) 스마트폰에
인증코드 입력 화면

④ Smart Phone : 사용자 인증서 선택



(그림 45) 사용자 인증서
선택 화면

⑤ Smart Phone: 인증서 암호 입력 및 전자서명 생성



(그림 46) 인증서 암호 입력 화면

⑥ Smart Phone → AS, AS → SP : 전자서명 검증

⑦ SP → PC : 로그인 성공

4. 크리덴셜 서버를 이용한 통합인증(C-CAM)

가. 크리덴셜 프로파일(Credential Profile)

크리덴셜을 구현을 위한 ASN.1 구조 정의는 다음과 같다.

(표 36) 크리덴셜 ASN.1 정의

```
Credential ::= SEQUENCE {
        version          [0] EXPLICIT Version DEFAULT v1,
        selector          Selector,
        payLoad           Payload,
        lastModified      GeneralizedTime,
        timeToLive         [1] IMPLICIT    TimeToLive OPTIONAL,
        processInfo        [2] IMPLICIT    ProcessInfo OPTIONAL,
```

```
        UserInfo            [3] IMPLICIT    UserInfo OPTIONAL
}
Credentials     ::= SEQUENCE SIZE (1..MAX) OF Credential
SecuredCredentials     ::= OCTET STRING
```

나. 프로파일 교환(Profile Exchange)

C-CAM에서 사용자와 서버 간에 교환되는 프로토콜의 메시지 형식은 다음과 같다.

(표 37) 프로토콜의 성공과 실패시 메시지 형식

요청 프로토콜	성공	실패
InfoRequest	InfoResponse	error
BindRequest	BindResponse	error
CreateAccountRequest	ok	error
RemoveAccountRequest	ok	error
ModifyAccountRequest	ok	error
DownloadRequest	DownloadResponse	error
UploadRequest	ok	error
DeleteRequest	ok	error
SignRequest	SignResponse	error

다. 구현(Implementation)

크리덴셜 서버를 이용한 통합인증(C-CAM)의 프로토타입은 서버의 경우 JSP, JAVA를 이용하고 사용자의 경우 iPhone 개발 툴을 이용하여 구현하였다. [54] 다음의 화면은 iPhone의 어플리케이션을 이용하여 계정을 생성하고 서버에 저장된 사용자 크리덴셜을 이용하여 전자서명을 수행하는 예시이다.

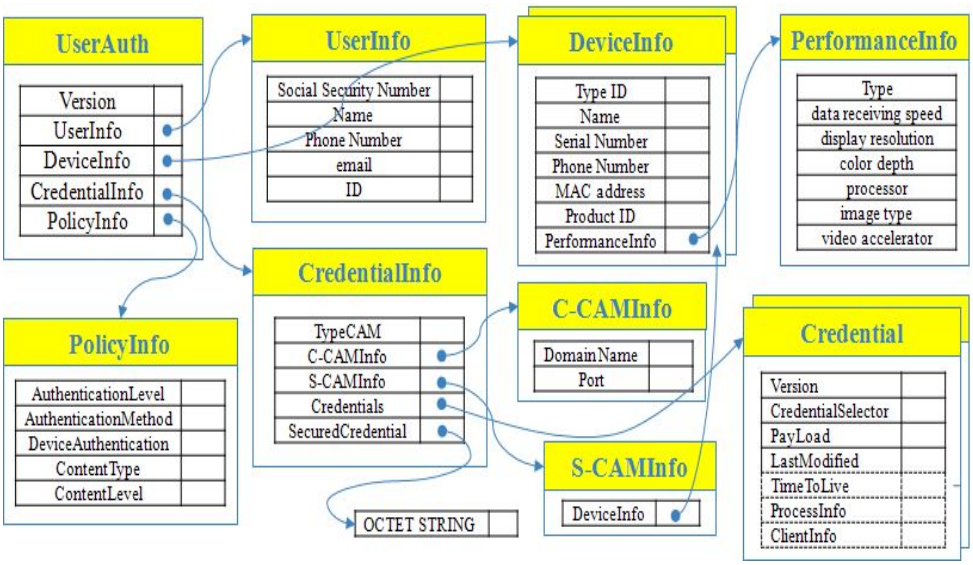
(그림 47) 아이폰(iOS) 사용자 화면 예시

5. 통합인증을 위한 사용자 프로파일(User Information Profiling) [55]

가. CAM 프로파일(CAM Profile)

C-CAM과 S-CAM을 위하여 ASN.1 구조를 사용하여 사용자 인증 프로파일을 정의하고자 한다. 이 프로파일은 사용자 정보(User Information), 스마트기기 정보(Smart Device Information), 크리덴셜 정보(Credential Information), 정책정보(Policy Information)으로 구성된다. 사용자 정보는 주민등록번호, 이름, 전자우편, 전화번호 등의

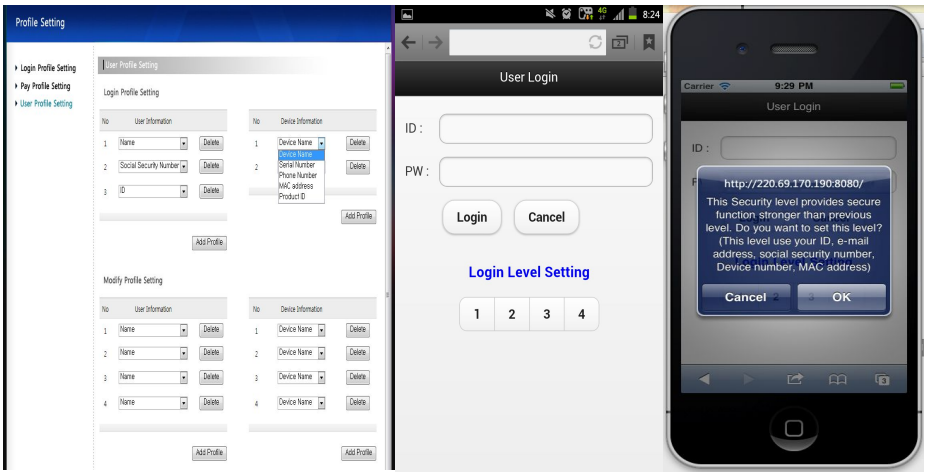
기본정보를 포함한다. 스마트기기 정보는 디바이스 타입, 이름, 일련번호, 전화번소 MAC 주소, 제품ID, 성능정보를 포함한다. 크리덴셜 정보는 CAM 타입, C-CAM 정보, S-CAM 정보, 크리덴셜, 암호화된 크리덴셜로 구성된다. 정책정보는 사용자 인증 수준, 사용자 인증방법, 디바이스 인증 방법, 컨텐츠 종류 및 레벨 정보 등이 포함된다.



(그림 48) CAM 사용자 프로파일 정의

나. 구현(Implementation)

첫 번째 화면은 사용자와 장치 인증을 위해서 사용자 정책을 설정하는 화면이고 시스템 관리자는 서비스의 종류에 따라서 다양한 인증레벨을 설정가능하다. 두 번째 화면은 사용자가 로그인 수준을 설정하고, 세 번째 화면은 사용자가 설정한 로그인 수준에 대하여 시스템이 안내하여 주는 화면이다.



(그림 49) CAM 사용자 프로파일 화면 예시

6. 시뮬레이션(Simulation)

가. 시뮬레이션(Simulation) 환경

통합 인증 메커니즘(CAM)과 기존 PKI(Public Key Infrastructure)와의 차이점에 대하여 다음과 같은 시뮬레이션 플랫폼과 인증서를 통하여 증명하고자 한다.

(표 38) 시뮬레이션 환경(Simulation Environments)

구분	Description
플랫폼 (Platform)	PC (Intel dual core, 3.2GHz), Smart Phone (iPhone 4), UNIX (SUN Fire V240 1.5GHz*2ea)
인증서 (Certificate)	User certificate, Device certificate: RSA 2048bit / SHA256

각 플랫폼에 대하여 RSA 서명과 검증 시간을 측정하였다.

(표 39) 각 플랫폼 별 RSA 서명 및 검증 결과

종류	서명(Sign)	검증(Verify)
UNIX	0.6 ms	21 ms
PC	8 ms	400 ms
Smart Phone	16 ms	800 ms

C-CAM과 PKI간의 차이점은 다음과 같다. CAM 구조의 경우 사용자 기기는 서명서버(Signing Server)에 대리서명을 요청하고 서비스 제공자는 대리서명을 검증하는 구조로 서버에서 전자서명을 생성하기 때문에 PC나 스마트폰에서 생성하는 경우보다 빠르다. 또한 사용자 인증방법의 경우에도 CAM의 경우 중앙 집중적 정책관리를 통한 통합인증을 제공함으로써 효율적이고 빠른 서비스 제공이 가능하다.

(표 40) 각 플랫폼 별 환경 비교

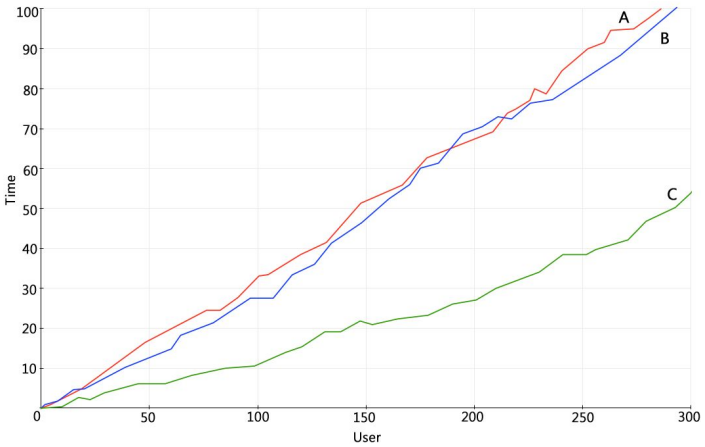
구분	PKI	CAM
사용자 인증 (User Authentication)	Slow (PC, Smart Phone)	Fast (UNIX)
인증방법 (Authentication Method)	각 서비스마다 다르게 적용됨	중앙 집중적인 정책에 따라 인증방법의 관리

나. 시뮬레이션(Simulation) 결과

시뮬레이션 조건의 경우, A는 PC에서 스마트폰에 저장된 인증서를 통하여 전자서명을 제공하고 통합인증 프로파일을 통하여 인증을 수행하는 시나리오이고 B는 A와 동일 조건이나 통합인증 프로파일이 적용되지 않은 시나리오이고 C의 경우 PC에 저장된 인증서를 통하여 전자서명을 제공하는 시나리오이다.

서비스 응답시간에 대한 시뮬레이션 결과는 다음과 같다.

그래프 A는 사용자 프로파일을 적용하여 통합 사용자 인증을 수행한 응답시간이고, 그래프 B는 일반적인 통합인증을 적용한 응답시간이고, 그래프 C는 통합인증을 수행하지 않은 경우의 응답시간이다.



(그림 50) CAM 사용자 프로파일 시뮬레이션 결과

결과에서처럼 그래프 C가 저장된 인증서를 사용하기 때문에 가장 빠른 응답시간을 제공하고 있고 그래프 A와 B는 거의 비슷한 결과가 나오고 있다. A와 B의 경우 사용자가 PC와 스마트폰에 개입되어야 하고 무선 환경에 중계서버를 통하여 전송하여 주어야 하기 때문에 C의 경우 보다 다소 많은 시간이 소요되는 것으로 나타나지만 실제 서비스에 적용에 문제없는 결과를 보여주고 있다. 결론적으로 A나 B와 같이 통합 사용자 인증을 사용할 경우 사용자, 단말기기, 컨텐츠에 대하여 통합인증을 제공함으로써 다양한 새로운 스마트 기기와 다양한 환경에 쉽게 적용 가능하다.

Ⅵ. 보안성 분석 및 검증

제안된 모델과 기존모델과의 비교를 통하여 기존 문제점의 해결됨을 증명하고자 한다.

1. 사용자 인증 등급화 모델 [56]

사용자 인증 등급화 모델에 정의된 사용자 인증 등급에 대하여 등급별 허용 토큰 형식, 등급별 방어책, 등급별 인증 프로토콜 형식, 등급별 추가적인 요구되는 속성 등 NIST SP 800-63의 기술적 요구사항을 근간으로 아래와 같이 검증하고자 한다.

(표 41) 등급별 허용 토큰 형식(Token Type)

Token Type	Level				
	1	2	3	4	5
Bio-Hard Crypto Token	√	√	√	√	√
Hard Crypto Token	√	√	√	√	
One-time Password Device	√	√			
Soft Crypto Token	√	√			
Passwords & PINs	√				

(표 42) 등급별 요구되는 방어책(Required Protections)

Protect against	Level				
	1	2	3	4	5
On-line Guessing	√	√	√	√	√
Replay	√	√	√	√	√
Eavesdropper		√	√	√	√
Verifier Impersonation			√	√	√
Man-in-the-middle			√	√	√
Session Hijacking				√	√
Signer Impersonation					√

(표 43) 등급별 인증 프로토콜 형식(Authentication Protocol Types)

Protect against	Level				
	1	2	3	4	5
Private Key PoP	√	√	√	√	√
Symmetric Key PoP	√	√	√	√	√
Tunneled or Zero Knowledge Password	√				
Challenge-response Password	√				

(표 44) 등급별 추가적으로 요구되는 속성(Additional Required Properties)

Protect against	Level				
	1	2	3	4	5
Shared secrets not revealed to third parties by verifiers or CSPs		√	√	√	√
Multi-factor authentication	√	√	√	√	√
Sensitive Data Transfer Authenticated		√	√	√	√

사용자 인증 방법에 대한 안정성 검증방법은 OWASP(The Open Web Application Security Project)에서 제공하는 다중인증의 테스트 방법(Testing Multiple Factors Authentication (OWASP-AT-009) [57])을 통하여 제시된 등급에 대한 안전성을 검증을 하고자 한다.

OWASP에서 정의된 5개(T1-T5)의 테스트 항목을 가지고 제안된 사용자 인증 방법에 적용하여 테스트를 수행한다.

(표 45) OWASP 테스트 항목

구분	취약성 설명
T1	Credential Theft(Phishing, Eavesdropping, MITM)
T2	Weak Credentials(Credentials Password guessing and Password Brute Forcing Attacks)
T3	세션 기반의 공격들(Session Riding, Session Fixation)
T4	트로이젠(Trojan)과 악성코드(Malware) 공격 들
T5	비밀번호 재사용(다른 목적 및 운영에서의 같은 비밀번호 사용)

2. 크리덴셜 서버 기반의 통합인증(C-CAM) [58]

본 논문은 제안한 크리덴셜 서버기반의 통합인증모델이 기존에 존재하는 사용자 인증모델에서 문제가 되었던 부분을 해결하면서 프레임웍 요구사항, 프로토콜 요구사항, 개인정보보호 요구사항 등을 만족하는 모델임을 증명하고자 한다.

C-CAM은 다음과 같이 프레임웍 요구사항(Framework Requirements)을 만족한다.

(표 46) 프레임웍 요구사항(Framework Requirements)

항목	설명	C-CAM
F1	프레임웍은 크리덴셜 서버 방식과 직접 솔루션 방식을 제공하여야 한다.	O
F2	크리덴셜 서버 방식과 직접 솔루션방식은 가능하면 동일한 기술을 사용하여야 한다.	O
F3	프레임웍은 다양한 사용자 인증 방안을 제공하기 위한 프로토콜을 허용하여야 한다.	O
F4	비록 프로토콜 상대방이 처리할지 않더라고, 실제 크리덴셜의 타입이나 형식에 대한 상세는 프로토콜 상에서 숨겨져야 한다. 프로토콜은 다른	O

	크리덴셜 타입이나 포맷의 내부 구조에 의존하지 말아야 한다.	
F5	프레임웍은 다른 전송방법을 허용해야 한다.	O

C-CAM은 다음과 같이 프로토콜 요구사항을 만족한다.

(표 47) 프로토콜 요구사항(Protocol Requirements)

번호	설명	C-CAM
G1	크리덴셜를 기기에 넣고 빼고 전송방법을 지원하여야 한다.	O
G2	크리덴셜은 프로토콜 상에서 사용자의 기기 등에서 안전한 방법으로 전달되어야 한다.	O
G3	프로토콜은 여러 가지 방법으로 모든 전송된 크리덴셜의 인증이 보장하여야 한다.	O
G4	프로토콜은 대칭키 알고리즘, 공개키 알고리즘, 해쉬 알고리즘, MAC 알고리즘 등의 암호알고리즘을 지원하여야 한다.	O
G5	프로토콜은 다양한 크리덴셜 타입들과 형식등의 사용을 허용해야한다.	O
G6	기본적으로 하나 이상의 지원하는 크리덴셜 형식은 정의되어야 한다.	O
G7	기본적으로 제공하는 하나 이상의 사용자 인증방안이 정의 되어야 한다.	O
G8	프로토콜은 사용자가 크리덴셜들 중에서 선택 가능하도록 크리덴셜에 대한 구분라벨정보를 크리덴셜 외부에서 부여하는 것이 허용할 수 있다.	O
G9	UTF8처럼 국제 메시지(I18N)를 지원해야한다.	O
G10	프로토콜이 사용자의 익명성 등의 프라이시 보호기능을 제공하는 것을 권고한다.	O
G11	전달된 크리덴셜은 사용 제한 정보를 넣은 수 있다. 예를 들어 “time to live”는 다운로드된 크리덴셜에 대한 최대 사용 한도를 정의하는 값이다.	O

C-CAM은 다음과 같이 개인정보보호 요구사항을 만족한다.

(표 48) 개인정보보호 요구사항(Privacy Protection Requirements)

생명주기	설명	C-CAM
수집	사용자 동의를 통하여 수집되는 정보에 대한 용도와 범위를 표시한다.	O
저장	저장되는 개인정보는 암호화되어 저장된다.	O
이용	사용자가 해당 크리덴셜을 이용시 등록된 전화번호나 전자우편을 통하여 통지를 전달한다.	O
전송	Protocol 상에서 개인정보는 전송시 반드시 보안채널이나 암호화하여 전달한다.	O
파기	가입자가 더 이상 계정을 사용하지 않을 경우 고객정보를 파기하고 서비스이용을 해지한다.	O

C-CAM과 기존 사용자 인증모델과의 비교자료는 다음과 같다.

(표 49) 기존모델과 C-CAM과의 비교표

조건	기존모델	C-CAM
프레임웍 요구조건 (Framework Requirements)	△	O
프로토콜 요구조건 (Protocol Requirements)	△	O
개인정보보호 요구사항 (Privacy Protection Requirements)	△	O
대리서명 (Proxy Signature)	X	O

O: Provided △: Partially Provided X: Not Provided

3. SOSMU 시스템

클라우딩 컴퓨팅 환경에 알맞은 안전한 SOSMU 시스템과 기존 컨텐츠 관리 시스템(TCMS)과의 비교를 통하여 안전성을 검증하고자 한다. SOSMU 시스템은 하나의 컨텐츠에 대한 멀티 사용 기능, 신규 단말장치에 대한 추가가 용이, 사용자 단말기의 통합관리 기능, N-Screen 기반의 사용자 인증 기능, 사용자, 단말기기, 컨텐츠, 데이터에 대한 통합 정책 관리 기능 등의 보안 기능을 제공한다.

본고는 SOSMU 시스템은 컨텐츠 관리시스템의 문제점, 기기 및 사용자 인증의 문제점, 크리덴셜 환경에서의 문제점을 해결하여 클라우드 환경에 맞는 안전한 One-Source Multi-Use 환경을 제공한다.

(표 50) SOSMU와 TCMS의 비교표

Item	TCMS	SOSMU
하나의 컨텐츠에 대한 Multi-Use 기능	X	O
신규단말장치에 대한 추가지원 기능	X	O
사용자 단말장치 통합관리 기능	X	O
N-screen 기반의 사용자 인증 기능	X	O
인증서를 이용한 사용자 인증 기능	△	O
통합 개인정보보호 정책	X	O
단말장치 성능에 따른 최적화된 재생	X	O
컨텐츠 권한관리 기능	△	O
통합 사용자 인증 제공	X	O
사용자, 단말기기, 컨텐츠, 데이터에 대한 통합 정책 관리	△	O

O: Provided △: Partially Provided X: Not Provided

Ⅶ. 결론 및 향후 연구

본 논문은 클라우드 환경에 맞는 안전한 원소스 멀티유즈 시스템(Secure One-Source Multi-Use System)을 설계 및 구현하기 위해서 기존의 컨텐츠 관리 기법의 문제점과 요구사항을 분석하였고, 사용자 인증 등급화를 위하여 국내 다양한 인터넷서비스에서의 사용자 인증방법의 분석하였고 미국, 캐나다 등의 해외사례를 분석하였고, 크리덴셜 관리 기법에서 안전하게 사용가능한 크리덴셜(SACRED)의 국내외 표준 현황 분석을 통한 문제점과 요구사항을 도출하였다.

SOSMU 시스템은 단말장치의 리소스나 성능을 고려하여 하나의 컨텐츠를 다양한 단말장치에서 재생할 수 있도록 하는 보안 및 인증기능이 적용된 시스템이다. SOSMU 시스템은 통합인증모듈(CAM), 위험관리모듈(RMM), 체계적인 정책 설정 및 관리 모듈(PCM), 컨텐츠 관리 모듈(CMM), 사용자, 기기의 접근제어 모듈(ACM) 등으로 구성된다. 통합 사용자 인증 모델(CAM)을 크리덴셜(인증서 등)에 대한 관리 및 사용 방법에 따라서 사용자가 가지고 있는 스마트기기를 이용한 통합인증모델(S-CAM: Consolidated Authentication Model using Smart Device)과 중앙 집중적인 크리덴셜 서버(Credential Server)를 이용한 통합인증모델(C-CAM: Consolidated Authentication Model using Credential Server)로 나누어 제시하였다. 위험관리 메커니즘(RMM)은 서비스별 사용자 인증 방법을 분석을 통하여 1등급부터 5등급까지의 사용자 인증 등급화 방안 모델(User

Authentication Level Model)을 제시하여 각 응용서비스 마다 위험평가를 통해 해당서비스에 적합한 사용자 인증의 선택 및 사용 방안을 제시하였다. 정책 컴플라이언스 메커니즘(PCM)은 정책엔진(Policy Engine)을 통하여 통합적인 정책관리를 수행하고 사용자 정책, 단말기기 정책, 컨텐츠 정책, 데이터 정책으로 나누어 정의하였다.

이렇게 정의된 SOSMU 시스템에 대하여 프로토타입팅 형식의 구현을 위하여 정책 알고리즘을 정의하고 데이터베이스 설계, 화면 설계하고, 스마트기기를 이용한 통합인증(S-CAM)과 크리덴셜 서버를 이용한 통합인증(C-CAM)를 구현하였다.

구현된 SOSMU 시스템의 보안성 분석 및 검증을 통하여 제안된 사용자 인증 등급화 모델의 안전성을 분석하였고 SOSMU 아키텍처와 기존 컨텐츠 관리 시스템과의 비교를 통하여 사용자 통합인증, 체계적인 정책 관리 등의 보안성이 향상되었고, 통합인증모델에 대하여 프레임웍 요구사항, 프로토콜 요구사항, 개인정보보호 요구사항에 대하여 충족함을 검증을 하였다.

제안된 SOSMU 시스템을 통하여 다음과 같은 기여점(Contribution)을 제공한다.

첫째는 제안된 SOSMU 시스템은 컨텐츠의 사용자 인증, 컨텐츠 선택 및 구매, 단말 환경에 컨텐츠의 변환의 절차에 따른 안전하고 신뢰성 있는 컨텐츠 유통모델을 설계하였다. 하나의 컨텐츠를 단말장치의 리소스나 성능을 고려하여 다양한 단말장치에서 재생될 수 있도록 함으로써 컨텐츠의 구매비용을 줄일 수 있고, 다양한

단말장치에서 컨텐츠를 볼 수 있도록 하여 사용자의 요구를 충족한다. 컨텐츠를 지정하는 정보 및 지불정보를 암호화하여 개인정보가 유출되어 사생활이 침해되는 것을 방지하고 수신된 컨텐츠에 대한 권한을 제어할 수 있어 컨텐츠의 불법복제나 무한의 재생을 방지하여 컨텐츠의 저작권의 보호를 할 수 있다. 다양한 단말장치에 대하여 스마트폰 등의 스마트기기 기반의 클라우딩 환경 맞는 통합 사용자 인증모델을 제공하여 손쉽게 다양한 단말기기나 운영체계의 지원이 가능하다.

둘째는 제안된 통합 사용자인증 모델은 어떠한 환경에서도 사용 가능하도록 스마트기기를 이용한 통합인증모델(S-CAM)과 크리덴셜 서버를 이용한 통합인증모델(C-CAM)을 동시에 제안하였다.

스마트기기를 이용한 통합인증모델(S-CAM)은 플러그인이나 엑티브엑스(ActiveX)와 같은 부가적인 소프트웨어의 설치 없이 다양한 모바일 기기에서 N-스크린 기반의 통합 사용자 인증을 제공한다. 웹 브라우저를 지원하는 새로운 스마트기기에 대하여서는 손쉽게 적용이 가능하다.

크리덴셜 서버를 이용한 통합인증모델(C-CAM)의 경우는 SACRED에 정의된 프레임웍과 프로토콜의 요구사항을 충족하는 크리덴셜 프레임웍과 프로토콜을 XML기반 대신 ASN.1 기반으로 정의하였다. 기존 프로토콜을 기반으로 추가적인 키 로밍(Key Roaming) 및 위탁서명 (Proxy Signature) 프로토콜을 정의하여 클라우딩 환경에 알맞은 통합 사용자 방안을 제공하였다.

셋째는 현재 인터넷 기반의 다양한 서비스 분석을 통하여 서로 다른

많은 종류의 인증방법을 분석하여 사용자 등급화 방안을 제시하였다. 제안된 등급화 방안을 통하여 인터넷 기반의 제품과 서비스를 제공하는 많은 기관들에 고객들을 인증하기 위한 신뢰성 있고 안전한 방법을 제공하였다. 또한 서비스에 맞는 등급을 선택하기 위하여 서비스와 관련된 리스크의 종류 및 등급을 파악하고 주기적인 위험분석을 수행하여 보안성(Security), 사용의 편리성(Usability), 이동성(Portability), 확장성(Upgradeability) 등을 고려한 적절한 인증서 방안을 선택할 수 있도록 하였다.

향후 연구 방향은 제안된 모델에 대한 구체적인 설계 및 구현 진행하고 새로운 장치나 환경에 확장 가능성에 대한 연구를 진행하고자 한다. 또한 원소스 멀티유즈(OSMU: One-Source Multi-Use) 환경에서 멀티소스 멀티유즈 (MSMU: Multi-Source Multi-Use) 환경으로의 확장부분에 대한 연구도 지속적으로 추진하고자 한다.

참 고 문 헌

[1] Peter Mell, Timothy Grance, “The NIST Definition of Cloud Computing (Draft)”, NIST, January 2011.

[2] Wei Yi-ling, "Recommended Industries for Foreign Investment－Cloud Computing Industry", ITRI IEK Report, 2010.

[3] Wayne Jansen, Timothy Grance, “Guidelines on Security and Privacy in Public Cloud Computing”, Draft NIST Special Publication, January 2011.

[4] P.J. Bruening and B.C. Treacy, “Cloud Computing: Privacy Security Challenges,” Bureau of Nat’l Affairs, 2009.

[5] Wayne A. Jansen, NIST, “Cloud Hooks: Security and Privacy Issues in Cloud Computing”, the 44th Hawaii International Conference on System Sciences, 2011.

[6] Takabi, H. Joshi, J.B.D. Ahn, G, “Security and Privacy Challenges in Cloud Computing Environments”, IEEE, October 2010.

[7] [Definition] Wikipedia, Definition of Digital Contents.

[8] JaeJung Kim, SengPhil Hong, “One-Source Multi-Use System having Function of Consolidated User Authentication”, YES-ICUC 2011, 2011.

[9] Lee Badger et al., "DRAFT Cloud Computing Synopsis and Recommendations", NIST Special Publication p800-146, 2011.

[10] Hyunmi Jang, Sengphil Hong, Kyongjin Kim and Jae-Jung Kim,

"Applied Method for One Source Multi Use (OSMU) in the Broadcasting Communication Convergence Environment", Communications in Computer and Information Science, 2011.

[11] Jonghong Jeon, ETRI, "Future of Mobile Platform", Korea Mobile Web2.0 Forum, 2009.

[12] KISA, "정보통신기기 대상 기기인증서비스 적용방안", 2011.

[13] ETSI, "Machine-to-Machine communications(M2M); Functional architecture", ETSI TS 102 690 V1.1.1, October, 2011.

[14] Dale Vile, Freeform Dynamic, "User convenience versus system security", 2006.

[15] Roger Elrod, "Two-factor Authentication", East Carolina University, July 2005.

[16] Smart Card Alliance (Randy Vanderhoof), "Smart Card Technology Roadmap for secure ID applications", 2003.

[17] Tim Hastings, "Multi-factor Authentication and the Cloud", 2010.

[18] Korea Internet Security Agency, "Introduction of i-PIN (http://i-pin.kisa.or.kr)", 2010.

[19] Accredited Certificate: www.rootca.or.kr.

[20] Public Procurement Service: www.g2b.go.kr.

[21] OMB M-04-04, "E-Authentication Guidance for Federal agencies", December 2003.

[22] NIST Special Publication 800-63, "Electronic Authentication Guideline", April 2006.

[23] Ministry of Citizens' Services, "Electronic Credential and Authentication Standard", April 2010.

[24] Bret Hartman, "From Identity Management to Authentication: Technology Evolution to Meet Cyber Threats", ITAA IdentEvent, 2008.

[25] Karim Zerhouni, "Multifactor Authentication: A Brief Selection Guide", October 2007.

[26] Christina Braz, Jean-Marc Robert, "Security and Usability: The case of the user authentication methods", 2006.

[27] IETF RFC 3157, "Securely Available Credentials-Requirements", August 2001.

[28] IETF RFC 3760, "Securely Available Credentials-Credential Server Framework", April 2004.

[29] IETF RFC 3767, "Securely Available Credentials-Securely Available Credentials Protocol", June 2004.

[30] 정성재, 배유미, "클라우드 보안 위협요소와 기술 동향 분석", 보안공학연구논문지, 제 10권 제 2호, 2013.

[31] 금융보안연구원, "금융분야 스마트폰 보안가이드", 2012.

[32] 염흥열, 장기헌, "국내외 스마트폰 보안 표준화 동향 및 추진전략", TTA Journal No.132. 59, 2010.

[33] 금융감독원, "금융감독원 인증수단 안정성 기술평가기준", 2011.

[34] H Jang, S Hong, "Study on the OSMU (One-Source Multi-Use) Management for Smart Devices", International Journal of Smart

Home, 2013.

[35] Jae Young Ahn, Jae-gu Song, Dae-Joon Hwang and Seoksoo Kim, “Trends in M2M Application Services Based on a Smart Phone”, Communications in Computer and Information Science, Volume 117, p50-56, 2010.

[36] 장현미, 김유진, 김재중, 홍승필, “IPTV환경내의 Set-Top Box를 이용한 주요정보보호 아키텍처 설계 방안”, 한국인터넷정보학회, June 2010.

[37] 정지희, 김재중, 홍승필, “개인정보 관리 정책 기술 분석 및 개발 방안”, 한국인터넷정보학회, October 2009.

[38] Kyong-jin Kim, Hyun-mi Jang, Yu-jin Shin, Saeromi Yang, Seng-phil Hong and Jaejung Kim, “Constructing the Trusted Information Sharing Architecture in Cloud Computing Environments”, KSII The first International Conference on Internet (ICONI) 2011, December 2011.

[39] 장현미, 김경진, 신유진, 양새로미, 이연우, 김재중, 홍승필, “N-Screen환경 내 금융 프레임워크 개발 방안 연구”, 한국인터넷정보학회, November 2011.

[40] 김재중, 홍승필, “통합 사용자인증을 통한 One-Source Multi-Use 시스템”, 한국인터넷정보학회, June 2011.

[41] Jaejung Kim and Seng-phil Hong, “Secure OSMU (One-Source Multi-Use) Architecture in Cloud Computing Environments”, International Information Institute, Vol.16, No.6(B), p4117-4132, June

2013.

[42] Hyunmi Jang, Sengphil Hong, Kyongjin Kim and Jae-Jung Kim, “Applied Method for One Source Multi Use (OSMU) in the Broadcasting Communication Convergence Environment”, Future Information Technology Communications in Computer and Information Science, Volume 185, Part 5, p224-229, 2011.

[43] Jaejung Kim, Sengphil Hong and Jaehyoun Kim, “One-Source Multi-Use System having Function of Consolidated User Authentication”, JCICT & The first Yellow Sea International Conference on Ubiquitous Computing (YES-ICUC) 2011, August 2011.

[44] IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008.

[45] IETF RFC 2560, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”, June 1999.

[46] RSA Lab. “PKCS #12 v1.0: Personal Information Exchange Syntax”, June 1999.

[47] RSA Lab. “PKCS #15 v1.1: Cryptographic Token Information Syntax Standard”, June 2000.

[48] ITEF RFC 6070, “PKCS #5: Password-Based Key Derivation Function 2 (PBKDF2)”, January 2011.

[49] ITEF RFC 5246, “The Transport Layer Security (TLS) Protocol Version 1.2”, August 2008.

[50] ITEF RFC 2631, “Diffie-Hellman Key Agreement Method”, June 1999.

[51] Constantin Popescu, “A Secure Proxy Signature Scheme with Delegation by Warrant, Studies in Informatics and Control”, Vol. 20, No. 4, December 2011.

[52] 김재중, 유동영, 홍승필, “인터넷 환경에서의 사용자 인증에 대한 등급화 방안”, 한국인터넷정보학회, p797-802, June 2010.

[53] Fidelity National Information Services, “Multi-Factor Authentication Risk Assessment”, 2006.

[54] Mark Sinkinson, “The Complete iPhone Development Toolbox”, March 2010.

[55] Jae-jung Kim, Seng-phil Hong, Yu-jin Shin, Hyun-mi Jang and Jaehyoun Kim, “Design of user information profiling for consolidated authentication in N-Screen environment”, International Journal of Security and Its Applications, Vol. 6, No. 4, p215-221, October 2012.

[56] JaeJung Kim, SengPhil Hong, “A Method of Risk Assessment for Multi-Factor Authentication”, Journal of Information Processing Systems (JIPS), p187-198, March 2011.

[57] OWASP foundation, “OWASP Testing Guide”, v3.0, p140-143, 2008.

[58] Jaejung Kim, Seng-phil Hong, Bong Gyou Lee and Joon Suk Hwang, “Securely Available Credentials Framework in Cloud Computing Environments”, International Information Institute Vol.16, No.3(B), p3171-3176, March 2013.

ABSTRACT

Design and Implementation of Secure OSMU(One-Source Multi-Use) System in Cloud Computing Environments

Jaejung Kim
Dept. of Computer Science
The Graduate School
SungShin University

As the access of Internet has been widely expanding, digital contents transmit service is increasing in popularity enabling a range of mobile devices to acquire, process and transmit various digital contents such as images, audio data, and videos. However, the current content services are not able to provide one-source multi-use environment due to the absence of systematic policy management and consolidated user authentication method. That is, without N-screen based user authentication method, users of smart phone or smart pad are not allowed to operate the same content within different mobile devices. In order to solve this problem, there needs to be N-screen based consolidated authentication mechanism for user authentication by designing and implementing secure OSMU architecture so that one content is applicable to various mobile

devices.

The designed SOSMU system provides security and authentication features that one content can be played in a variety of terminal units by considering the performance and resources of it. The components of secure OSMU system consist of consolidated authentication mechanism(CAM), risk management mechanism (RMM), policy compliance mechanism(PCM), and so on. Consolidated authentication mechanism is divided into consolidated authentication model using smart devices of users (S-CAM) and consolidated authentication model using centralized credential service(C-CAM). Risk management mechanism is designed user authentication level model(UALM) from 1 level to 5 level and proposed how to select user authentication methods and how to evaluate them with risk assessment procedure. Policy engine of PCM in SOSMU system provides systematic policy management. Each entity such as User, Terminal Unit, Contents, and Data defined policy items in order to control and manage security.

We designed and implemented the SOSMU architecture with N-screen based consolidated authentication mechanism, risk management mechanism and policy compliance mechanism in cloud computing environments, which not only provides more flexible Multi-Use environment but also leads to safer privacy protection and security in operating various mobile communication devices and systems of smart phone and smart pad.

감사의 글

회사를 다니면서 늦게 시작한 공부를 무사히 졸업할 수 있도록 도와주신 모든 분들에게 깊은 감사드립니다.

먼저 귀한 시간을 내어 박사논문 검토와 지도편달을 아끼지 않으신 변 혜원 교수님, 김 태훈 교수님, 강 성민 교수님, 설 순욱 교수님께 감사드립니다.

오랜 인연으로 뜻 밖의 만남으로 포기할 수 있었던 긴 학업의 길을 끝까지 이끌어 주신 존경하는 지도교수님인 홍 승필 교수님께 머리 숙여 다시 한번 감사드립니다. 주말마다 논문을 쓰느라 힘들 때도 있었지만 지금 생각해보면 회사 때문에 힘들어 포기할 수도 있었던 목표를 항상 상기시켜주시고 목표를 향해 한 걸음 할 걸음 가까이 갈수 있는 밑거름 이였음을 깨달았습니다. 또한 여대라는 특수한 환경에서 학교생활을 하는데 많은 도움을 준 IS LAB실에 있는 선후배분들도 감사드립니다.

다음으로 지금까지 저를 잘 길러주신 부모님, 언제나 곁에서 이해해주고 믿고 뒷받침해준 사랑스런 아내 경아, 논문 쓴다고 놀아주지 않아도 불평 없이 따라준 믿음직한 우리아들 선호, 바쁜 와중에도 논문 영작 작업에 많은 도움을 준 현동이 아빠, 엄마 등 여기까지 올 수 있도록 이끌어 주고 격려해준 모든 분에게 감사의 말을 전합니다,

마지막으로 10 여 년 동안 PKI 한 분야에 대하여 전문가가 될 수 있도록 만들어 주고 회사를 다니면서도 학업을 지속할 수 있도록 배려해준 한국정보인증 임직원, 선후배들에게 감사드립니다.

2014년 1월

김 재중