韓國컴퓨터情報學會 論文誌
第15卷 第5號, 2010. 5.

2010-15-5-3-5

디바이스 ID 기반의 하이브리드 PKI 공인 인증 보안 기법

손영환*, 최운수*, 김기현**, 최한나*, 이대윤*, 오충식***, 조용환*

Hybrid PKI Public Certificate Security Method Based on Device ID

Young-Hwan Son*, Woon-Soo Choi*, Ki-Hyun Kim**,
Han-Na Choi*, Dae-Yoon Lee*, Chung-Shick Oh***, Yong-Hwan Cho*

요 약

본 논문에서는 안전한 사용자 인증의 초석인 인증서의 원천지 무결성 보장과 함께 사용자의 편의성 향상을 위한 방안으로써, PKI 인증서 인증기법에 디바이스 ID에 기반한 하이브리드 공인 인증 기법을 제안하여 기존 하이브리드 PKI 공인인증서 인증기법에서의 사용자 편의성과 보안성을 향상시키고자 한다. 본 논문에서 제안하는 모델의 특징은 크게 다섯 가지로 설명할 수 있다. 첫째, 사용자 스스로 각각의 인증 상황 및 보안 수준에 맞는 정책을 선택할 수 있어 사용자의 편의성을 향상 시킬 수 있다. 둘째, 정책별 디바이스 ID의 해시 값인 DLDI Key(Device Location Dependence ID Key)의 비교를 통해 사용자 인증서의 원천지 무결성을 보장할 수 있다. 셋째, EOTP Key(Event of One Time Password Key)를 통해서 인증서를 암호화, 복호화 하는 키의 값을 매 인증 시도마다 변경시킴으로써 보안성을 향상 시킬 수 있다. 넷째, 인증서에 Index 값을 추가시켜 멀티 디바이스에 인증서의 저장이 가능하다. 다섯째, 보안 카드 등 인증서의 원천지 무결성 보장을 위한 추가적인 장치가 필요치 않아, 인증 처리 시간의 지연을 단축시킬 수 있으며 인증 서버의 연산 부하를 감소시킬 수 있다.

Abstract

In this study, the hybrid authorization quotation technique is based on the device ID for the integrity of the source region guarantee of user certificate, in order to improve the convenience and security for user in the hybrid PKI certificate Mechanism for authentication. The feature of the model in which it is presented from this paper is 5. First, because the user can select the policy himself in which it matches with each authentication situation and security level, the convenience can be improved. Second, the integrity of the source region of the user certificate can be guaranteed through the comparison of the DLDI Key, that is the hash-value of the device ID. Third, the security can be improved by continuously changing an encoding, and the value of the key in which it decodes through the EOTP Key. Fourth, the index value is added to a certificate, and the storage of a certificate is possible at the Multi-Device. Fifth, since the addi the inan aratus for the integrity of the source region guarantee of a certificate is not needed, the authentication process time can be reduced and the computational load of the certificate server can be reduced also.

▸ Keyword : 원천지 무결성(Integrity of the source region), 디바이스 ID(Device ID), 하이브리드 인증(Hybrid Certificate)

• 제1저자: 손영환 교신저자 : 조용환
• 투고일 : 2010. 02. 22, 심사일 : 2010. 03. 31, 게재확정일 : 2010. 04. 12.
* 충북대학교 전자정보대학 **에스지에이(주) *** 한국과학기술정보연구원
※ 이 논문은 2008년도 충북대학교 학술연구지원사업의 연구비지원에 의하여 연구되었음(This paper was supported by the research grant of the Chungbuk National University in 2008)

Ⅰ. 서 론

인터넷과 암호화, 사용자 인증 기법들은 서로 밀접하게 연관되어진 필수불가결의 조건들로써 현재 눈부신 발전을 거듭하고 있으며, 특히 사용자 인증은 유비쿼터스 시대의 초입에 들어선 현 사회 전반에서 중요한 화두로 떠오르고 있다. 안전한 사용자 인증을 위해 보다 강력한 보안 기능을 갖춘 물리적인 장치나 하드웨어, 소프트웨어적인 해결 방안들이 범람하고 있음에도 불구하고 안전한 사용자 인증이나, 인증 절차에 따른 사용자들의 불편함은 해결되지 못하고 있는 실정이다. 현재 사용자 인증 분야에서는 PKI 기반의 공인인증서를 이용한 인증 기법이 가장 많이 사용되어지고 있다. 그러나 PKI 기반의 공인인증서 인증 기법은 휴대용 저장 장치나 하드 디스크 드라이브에 저장된 공인인증서가 너무 쉽게 복사나 이동되어진다는 치명적인 단점이 있다. 또한 공인인증서의 인증 메커니즘 어디에서도 인증을 원하는 사용자가 현재 인증서의 진짜 소유주인지 확인하거나 보장하는 안전장치가 없어 인증서 자체에 대한 원천지 무결성이 보장되지 못하고 있다. 이에 PKI 공인인증서 인증기법에서는 원천지 무결성을 보장하기 위한 소유기반 인증기법의 일환으로 보안 토큰이나 보안 카드를 이용한 하이브리드 또는 다중 요소 인증 기법들을 복합적으로 사용하고 있다. 그러나 보안 토큰이나 보안 카드를 이용한 하이브리드 인증기법 역시 높은 하드웨어 발급 비용, 장치의 도난, 분실, 훼손에의 취약성 및 낮은 휴대성으로 인한 사용자의 불편 등의 단점이 있다. 또한, 추가적인 보안 카드의 연산 처리로 인한 전체적인 인증 처리 시간의 지연 및 인증 서버의 연산 부하 등 여러 가지 문제점들을 야기 시키고 있다. 따라서 본 논문에서는 안전한 사용자 인증의 초석인 인증서의 원천지 무결성 보장과 함께 사용자의 편의성 향상을 위한 방안으로써, 기존의 PKI 공인인증서 인증기법에 추가적으로 디바이스 ID에 기반한 하이브리드 공인 인증 기법을 제안하여 기존 PKI 공인인증서 인증기법에서의 사용자 편의성과 보안성을 향상시키고자 한다.

Ⅱ. 기존 사용자 인증 기법

1. 인증의 기본 요소

인증의 기본 요소는 지식기반 인증, 소유기반 인증, 존재기반 인증으로 분류되며 각각의 장·단점은 표 1과 같이 분석된다[1].

표 1. 인증 기본 요소의 장·단점 분석표
Table 1. Analysis table of basic factor of authentication

분류	장점	단점
지식 기반 인증	- 적은 비용 - 별도의 장치 필요 없음 - 사용하기 간편함	- 망각, 착각 - 추측 가능 - 높은 노출 빈도와 도용 가능성 - 해킹 공격에 취약
소유 기반 인증	- 안전한 하드웨어 성능에 기인하는 높은 보안성	- 특별한 장치 필요 - 높은 시스템 구축비용 - 분실, 도난, 훼손 - 장치 휴대에 따른 불편함
존재 기반 인증	- 위조, 변조 어려움 - 분실, 도난에 대한 안전성	- 높은 시스템 구축비용 - 프라이버시 문제 - 오류 인식 문제

표 1에서 분석한 바와 같이 모든 요소들은 각각의 문제점을 가지고 있기 때문에 보다 강력한 사용자 인증이 요구되는 경우에는 위에서 분류된 세 가지 인증 기법 중 두 가지 이상의 방법을 병합하여 보다 안전하게 사용자를 인증하는 다중 요소 인증(Multi-Factor Authentication) 또는 하이브리드(Hybrid) 인증 기법이 사용된다.

2.1 기존의 인증 기법

2.1.1 HSM (Hardware Security Module)

HSM이란 키 노출의 위험으로부터 키를 안전하게 저장하기 위한 저장소를 제공하는 하드웨어로 CA 서버의 키, OCSP(Online Certificate Status Protocol : 온라인 인증서 상태 프로토콜) 서버의 키 등 중요한 키를 물리적으로 관리하기 위한 암호 키 관리 전용 하드웨어 장비를 말한다. HSM은 운영체제와의 독립적인 동작으로 키를 저장, 보호, 관리한다[2~3].

2.1.2 OTP (One Time Password)

OTP는 소프트웨어적으로 보안성을 높이는 기법이다. OTP는 전통적인 ID와 Password를 사용해 사용자를 인증하는 방식과는 달리 매 회 Transaction이 발생할 때 마다 매번 다른 Password를 입력하게 해 인증함으로써 지식기반 인증 기법의 단점인 높은 노출빈도와 추측가능성을 제거하는 기법이다[4~6]. OTP 인증 방식의 특징을 정리하여 아래의 표 2에 각각의 장·단점을 분석하였다[7].

표 2. OTP 인증 방식별 장·단점 분석표
Table 2. Analysis table of authentication techniques of OT

구 분	입력 값	장 점	단 점
질의-응답	- 인증 서버로 부터 전달 받은 임의의 난수	- 타 방식에 비해 구현이 간편함 - 서버와 사용자 간에 동기화 불필요	- 질의 값 입력에 따른 불편 - 동일 질의 값 반복 생성 방지장치 필요
시간 동기화	- 시간 값 자동 입력	- 서버의 질의 값을 입력할 필요 없어 사용이 간편함 - 호환성이 높음	- 서버와 사용자간 시간 동기화 필요 - 인증 실패시 재시도를 위해 대기 - 일정시간 내 입력하지 못하면 Password가 변경
이벤트 동기화	- OTP 인증 횟수 자동 입력	- 시간 동기화에 비해 적은 전력소모 - 시간 동기화 불필요	- 서버와 사용자간 인증 횟수 동기화 필요
시간-이벤트 조합	- 시간 - OTP 인증 횟수	- 시간 동기화에 비해 긴 시간간격을 유지 할 수 있음	- 같은 시간 간격 내 인증 횟수 동기화 장치 필요

2.1.3 PKI 공인인증서

PKI는 기본적으로 한 쌍의 Private Key와 Public Key를 사용하여 안전하고 은밀하게 데이터를 교환할 수 있게 한다. 서버 클라이언트 모델의 경우 서버를 A, 클라이언트를 B라 정의 한다면, 만약 B가 A에게 데이터를 송신하려 할 때, B가 자신의 Private Key로 데이터를 암호화 하여 송신하면 A는 B의 Public Key로 복호화 하여 데이터를 전달 받는 방식이다. 그러나 인터넷을 통한 비대면 방식의 데이터 전송에 있어서 PKI는 키 분배라는 핵심 문제에서 Public Key의 위·변조 등 여러 가지 문제점을 야기 시킬 수 있기 때문에 Public Key의 무결성을 보장하기 위한 방안으로 Public Key와 그 소유자를 신뢰할 수 있는 인증기관(CA : Certification Authority)이 비밀 키로 서명한 공인인증서(Certificate) 방식을 사용한다.

현재 PKI 인증서 시스템은 사용자의 Public Key의 안전성과 신뢰성을 보장하여 공표하는 방법을 제공함으로써, 안전이 보장되지 않은 인터넷과 같은 비대면 사용자들 사이의 정보 교환이나 데이터 전송에 있어서 신원확인, 데이터 무결성(Data Integrity), 부인 방지(Non-repudiation) 등을 위한 방안으로 각광받고 있다[8]. 하지만 PKI 인증 매커니즘 중 어떠한 Application이나 CA 어디에도 사용자 인증서의 원천지 무결성을 확인하지 않고 있어, 이를 보장할 수 없다. 인증을 득하려는 사용자가 실제 인증서의 소유주인지 확인하기 위한 방안이 없어, 이에 대한 대응책으로 하이브리드 PKI 공인 인증 기법으로 PKI 인증서에 보안토큰(HSM)과 보안카드(OTP)를 혼합하여 인증하는 방식이 사용되고 있는 실정이다[9,10].

2.2 기존 인증 기법의 장·단점 분석

인증 기본 요소들의 단점을 보완 하기위해 현재 여러 기법들을 사용하고 있지만, 이 역시 많은 문제점들을 가지고 있다. 표 3은 현재 사용 중인 주요 인증 기법들의 장점과 단점을 비교 분석한 결과이다.

표 3. 기존 인증 기법의 장·단점 분석표
Table 3. Analysis table of existing authentication Techniques

분류	장점	단점
HSM	- 서버의 취약점으로부터 키 보호 - 안전한 키 관리 기능 제공 - 물리적 접근 권한 제어 - 서버의 암호연산 부하 감소 - 키의 원천지 무결성 입증 가능	- 장치의 도난, 분실, 훼손에 취약 - 낮은 재사용성 - 장치의 생산, 제조, 발급시의 키 노출 위험성
OTP	- 다른 보안기법과의 높은 호환성 - 해킹에 대한 강한 보안성 - 여러 기관의 공용 사용 가능	- 서버의 높은 암호연산 부하 - 서버와 사용자간의 동기화 필요 - 질의 값 입력의 불편함 - 시간, 횟수 동기화에 따른 불편함 - 원천지 무결성 입증 불가
PKI 인증서	- 데이터 무결성, 부인방지 기능 - 다른 보안기법과의 높은 호환성 - 여러 기관의 공용 사용 가능 - 안전한 키 관리 기능 제공	- 인증서의 높은 노출 위험성 - 인증서의 도용 가능성 - CA서버의 암호 연산 부하 - 원천지 무결성 입증 불가

III. 디바이스ID 기반의 하이브리드 공인 인증 모델

본 논문에서 제안하는 DbHC 모델(Device-based Hybrid Certificate)은 기존에 가장 많이 사용되어지고 있는 인증기법인 HSM과 OTP, PKI 인증서 인증 방법의 특징들을 모아 장점을 극대화 시키고, 단점을 최소화한 하이브리드 공인 인증 보안 기법이다. DbHC 모델의 특징은 PKI 인증서 인증 방식을 토대로 HSM의 단점인 높은 장치 의존성과 낮은 하드

웨어의 유연성을 제거하기 위해 각각의 인증 정책에 따라 지정된 장치의 디바이스 ID와 IP 주소를 하이브리드 암호화하는 방식으로 설계함으로써 HSM의 단점들을 보완하였다. 또한, OTP Event 동기화방식을 이용하여 생성된 EOTP Key(Event of One Time Password Key)를 매 인증 시 마다 갱신해 인증서를 암호화·복호화 함으로써 OTP의 장점인 강력한 보안성을 유지하도록 설계하였다.

그림 1은 DbHC 모델의 시스템 구성도이다. 그림 1에 모듈의 경계선이 점선으로 표현되어 있는 것들은, 기존의 PKI 인증 구조의 전체 시스템 구성에 추가 되거나 변경된 DbHC의 주요 모듈을 나타낸다. 표 4는 DbHC 모델에 사용된 주요 모듈들의 기능 명세이다.

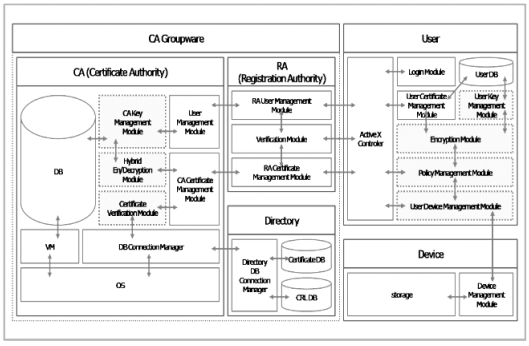


그림 1. DbHC 모델 시스템 구성도
fig. 1. System constitution of DbHC model

표 4. DbHC 모델의 주요 모듈 명세
Table 4. Specification of primary modules of DbHC Model

User	
Policy Management Module	- 인증서 인증 정책 관련 관리 및 처리
User Device Management Module	- 정책별 디바이스 ID, IP 주소 추출
Encryption Module	- DLDI Key 생성 - DLDI Key 검증을 통한 1차 인증 과정 처리
User Key Management Module	- 정책별 디바이스 ID, IP 주소 관리 - DLDI Key 관리 - User의 OTP Event Value 관리

CA Groupware	
CA Key Management Module	- CA의 OTP Event Value 관리 - User의 Private Key 생성 및 관리
Hybrid En/Decryption Module	- EOTP Key 생성 - EOTP Key를 통한 2차 인증 과정 처리
Certificate Verification Module	- 인증서 유효성 검사를 통한 3차 인증 과정 처리 - 사용자의 멀티 디바이스 관련 처리

3.1 정책별 인증 방법

DbHC 모델은 사용자의 요구에 맞추어 3개의 Level로 구성된 정책을 선택하여 적용하게 함으로써 사용자의 필요에 맞는 보안 수준을 설정하게 해 각각의 사용자와 인증 상황에 맞는 보안 수준을 제공할 수 있게 설계하였으며, 사용자의 편의성 향상을 위해 CA Groupware와 User ActiveX Controller와의 연동으로 각 정책별 DLDI Key(Device Location Dependence ID)를 관리·갱신함으로써 인증방법 변경에 따른 불편을 사용자가 느낄 수 없다는 장점을 가지고 있다. 그리고 멀티 디바이스(Multi Device)를 지원할 수 있게 설계하여 기존의 PKI 기반 인증서 인증 기법처럼 다중 저장장치에 인증서를 저장, 보관이 가능하도록 DbHC 모델을 설계하였다. 표 5는 DbHC 모델의 정책에 따른 인증 방법이다.

표 5. DbHC 모델의 인증서 인증 정책
Table 5. Certificate authentication policy of DbHC Model

인증 정책	필요 디바이스 ID	인증 범위	특징
Level 1	USB Device ID or HDD Device ID	단일 디바이스 내의 인증서	- 기존방식과 동일한 인증기법 - 인증서의 원천지 무결성 보장에 의한 보안성 향상 - 보안카드 불필요 - 이동성/휴대성/편리성 증가
Level 2	USB Device ID or HDD Device ID + IP Address	같은 Class의 IP대역 내에서 접속한 Clie-nt의 디바이스 내의 인증서	- IP 주소의 Class에 대한 인증으로 보안성 향상 - 같은 Class 내에서만 인증 가능 - 외부에서의 접속으로 인증 불가
Level 3	USB Device ID or HDD Device ID + CPU Device ID	특정 Client에 연결된 디바이스 내의 인증서	- 특정 Client에서의 접속만 인증하므로 보안성 대폭 강화 - 다른 Client에서의 인증 불가 - 휴대용장치 분실/도난에 안전

3.2 인증 정책별 알고리즘

DbHC 모델의 인증 정책별 알고리즘은 다음과 같다. 우선 보안 등급이 가장 낮은 Level 1 인증 정책은 기존의 PKI 인증서 인증 방식과 유사하게 동작한다.

Level 2 인증 정책은 Level 1 인증 정책에서 인증서 발급 당시에 선택된 디바이스 ID에 추가로 사용자가 현재 사용 중인 Client의 IP 주소나, 사용자가 직접 입력한 IP 주소의 Class 대역을 비교하여 인증하는 정책이다.

Level 3 인증 정책은 제안하는 모델의 인증 정책 중 가장 보안성이 높은 방법으로 인증서가 저장된 장치의 디바이스 ID와 현재 사용 중인 Client의 CPU 디바이스 ID를 해시하여 만들어진 DLDI Key를 통해 인증하는 인증 정책이다. 그림 2는 DLDI 키를 생성하는 과정을 도식화 한 것이다.

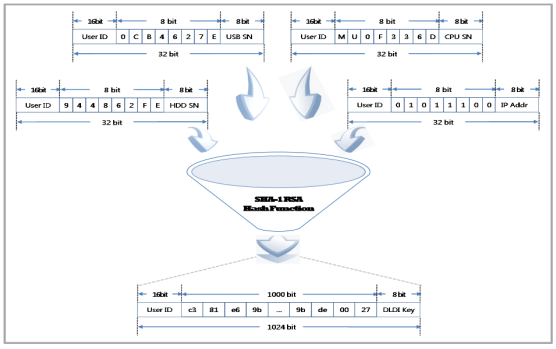


그림 2. DLDI Key 생성 과정
fig. 2. DLDI Key creating process

그림 2의 DLDI Key 생성 과정을 살펴보면, User ActiveX Controller는 각각 8 bit로 구성된 디바이스 ID나 IP 주소를 가져와 16 bit의 User ID와 8 bit의 Extension bit와 결합하여 각각 32 bit로 이루어진 Seed Key를 생성한다. 이렇게 생성된 Seed Key들을 사용자가 선택한 인증 정책에 맞게 SHA-1 RSA 해시 알고리즘으로 해시하여 만들어진 1 kbit의 해시 값과 함께 User ID 16bit와 8 bit의 Extension bit를 더해 1024 bit로 이루어진 DLDI Key를 생성한다.

사용자가 Level 3 인증 정책을 선택하면 현재 접속 중인 특정한 Client에서의 접속만을 허가하고, 등록되지 않은 여타 Client에서의 인증은 모두 불허하므로 인증서 저장 장치의 도난이나 분실에 대한 보안성이 대폭 강화 된다. 그림 3은 DbHC 모델의 인증서 저장장치 선택과 인증 정책의 처리 알고리즘을 나타낸다.

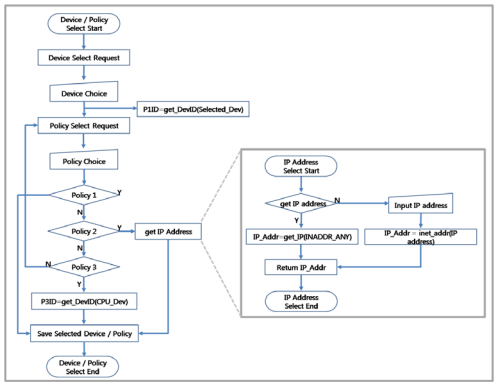


그림 3. DbHC의 인증서 저장장치 선택과 인증 정책 선택 처리 순서도
fig. 3. Certificate storage selection of DbHc and Flowchart of authentication policy selecting process

3.3 전체 인증 처리 과정

User ActiveX Controller는 정책 관리 모듈을 통해 인증서가 저장될 때 사용자가 선택했던 정책을 확인하여 선택된 정책의 Level에 따라 달리 설정되어 있던 각 장치별 디바이스 ID나 IP 주소를 가져와서 해시해 DLDI Key를 만들고, 인증서가 발급될 때 저장되었던 DLDI Key와 비교를 해 인증서의 원천지 무결성을 가장 먼저 확인한다. 원천지 무결성이 입증되지 않으면 User ActiveX Controller는 사용자의 인증서가 불법 복제나 도난, 유출 된 것으로 가정하고 미인증 처리를 한다.

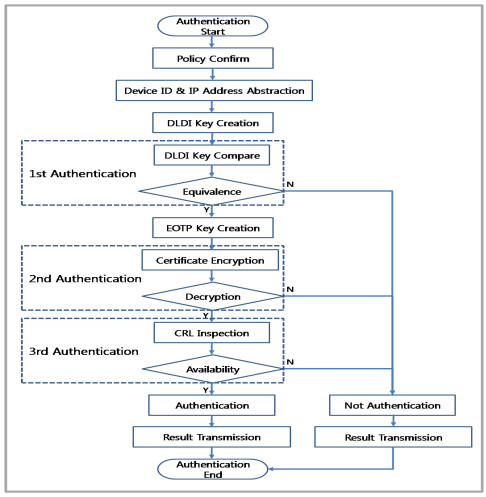


그림 4. DbHC 모델의 전체 인증 처리 과정 순서도
fig. 4. Flowchart of overall authentication process of DbHC Model

그림 4에 도식화된 DbHC 모델의 전체 인증 처리 알고리즘을 보면, 가장 먼저 1차 인증으로 사용자의 ActiveX Controller가 인증서가 저장될 때 선택되었던 정책에 포함된 장치들의 디바이스 ID나 IP 주소를 추출하여 DLDI Key를 생성한다. 인증서가 발급될 때 만들어진 DLDI Key와 비교하여 1차 인증을 하여 인증서의 원천지 무결성을 확인한다.

2차 인증은 CA에서 사용자가 가지고 있는 EOTP Key로 암호화 된 인증서가 CA가 소유한 EOTP Key로 복호화 되는지의 여부로 사용자의 인증서가 맞는지를 판별한다. 마지막 3차 인증 과정으로 Directory에 저장된 CRL 목록을 확인하여 인증서의 유효성 검사를 하여 총 3차의 인증 과정을 거친다. 만약 위의 3단계의 검증 과정 중 하나라도 만족시키지 못하면 사용자의 인증서는 유효하지 않음으로 판단되고 CRL에 등록되어 사용자에게 인증서를 재발급하는 과정을 거치게 된다. 그림 5는 DbHC 모델의 3차 인증과정인 인증서 유효성 검사의 세부 절차이다.

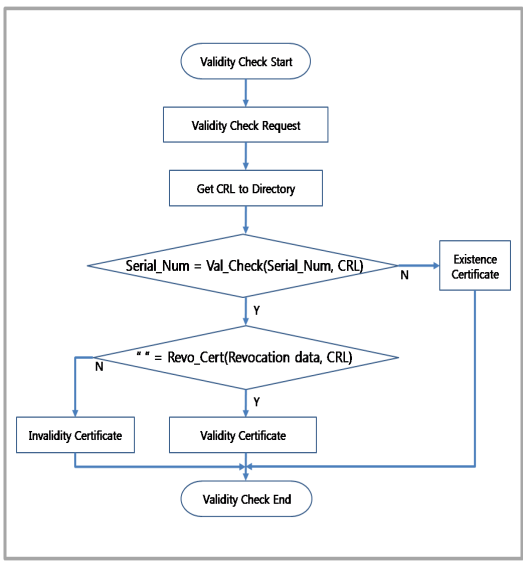


그림 5. 인증서 유효성 검사 과정 순서도
fig. 5. Flowchart of certificate validation

3.4 미인증 처리

사용자가 인증을 시도 하였을 때 ActiveX Controller는 제일 먼저 1차 인증으로 인증서 발급 당시의 DLDI Key와 인증 시도 시의 DLDI Key를 비교하게 된다. 이때, DLDI Key가 서로 상이하면 2차 인증 단계로 진행되지 못하고 그림 6의 DLDI Key 검증 과정 미인증 처리 순서도와 같이 미인증 처리를 하게 된다.

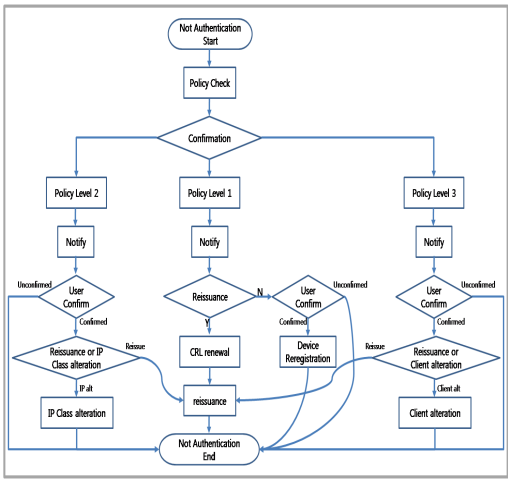


그림 6. DLDI Key 검증 과정 미인증 처리 순서도
fig. 6. Processing flowchart of unauthenticated case in DLDI Key validation

DbHC 모델에서는 1차 인증 과정인 DLDI Key 검증 과정을 통과하면 2차 인증 과정인 EOTP Key를 통한 인증서 복호화 과정이 실행된다. EOTP Key 복호화 과정의 미인증 경우는 표 6의 EOTP Key 복호화 과정의 미인증 경우 분석표에 분석한 바와 같이 크게 3가지로 분류된다.

표 6. EOTP Key 복호화 과정의 미인증 경우 분석표
Table 6. Analysis table of unauthenticated case in EOTP Key decryption

Case	Dangerousness	Counterplan
인증서 오류	highest	- 인증서 재발급
Private Key 오류	highest	- Private Key 재발급
OTP Event Value 동기화 오류	middle	- OTP Event Value 동기화 및 초기화

첫 번째와 두 번째 경우는 인증서나 Private Key의 오류로 인한 EOTP Key가 잘 못 생성된 경우이다. 이러한 경우는 PKI 인증서 인증 방식에서 발생할 수 있는 가장 위험성이 높은 경우이다. 이 경우 DbHC 모델에서는 사용자 확인 후, CA에서의 인증서 재발급이나 Private Key의 재발급으로만 해결할 수 있다. 세 번째는 OTP Event Value의 동기화 오류로 불법적인 사용자의 인증 시도나 CA와 User ActiveX Controller사이의 OTP Event Value 동기화 오류로 발생된다. 이러한 경우는 중간 수준의 위험성으로 분류되며 CA와

User ActiveX Controller의 OTP Event Value 동기화 및 초기화로 해결된다.

인증서 유효성 검증 과정의 미인증 경우 분석표를 보면 3차 인증 과정에서는 크게 해당 인증서가 없는 경우와 유효기간의 만료일자 도래, 그리고 기타 유효하지 않은 인증서로의 인증으로 나뉜다. 인증을 득하려는 해당 인증서가 없거나 유효기간이 만료된 인증서의 경우 위험성은 중간 수준이며, 이 경우는 인증서의 재발급으로 처리가 된다. 마지막으로 기타 유효하지 않은 인증서로의 인증은 사용자 확인 후 인증서를 재발급 함으로써 인증서 유효성 검증 과정의 미인증 처리를 완료하게 된다. 인증서의 유효성 검증 과정의 미인증 처리를 끝으로 DbHC 모델의 전체 인증 처리 과정에 관련 된 미인증 처리는 모두 완료된다.

IV. 실험 및 결과 분석

본 장에서는 본 논문에서 제안하는 모델의 실험 및 결과를 분석하기 위하여 제안 모델의 시뮬레이션 환경을 기술하고, DbHC 모델의 모듈 구성도와 모듈 관계도를 명세한다. 또한 제안 모델의 성능을 검증하기 위한 시뮬레이션으로 인증서 발급과정과 인증서 인증과정으로 나누어 실험한다. 그리고 DbHC 모델의 미인증 처리 정상 동작 실험을 하고, 타 방식과의 처리 시간 비교를 위한 제안 모델의 각 정책별 인증 완료시간을 측정한다. 마지막으로 HSM, OTP 방식과의 성능 비교를 끝으로 실험 및 결과 분석을 마친다.

4.1 시뮬레이션 환경

본 논문에서 제안한 DbHC 모델은 Visual Studio 6.0의 Visual C++ 6.0으로 구현하였고, 웹 환경 하에서 동작하도록 구현되어 CA Groupware인 RA, Directory 등 웹서버는 Windows Server 2003 Web Edition의 IIS 6.0을 사용하였다. 시뮬레이션 환경은 표 7의 시뮬레이션 환경과 같다.

표 7. 시뮬레이션 환경
Table 7. Simulation environment

구분		사양 및 버전
Software	OS	- Windows XP Pro.
	DBMS	- MySQL v5.0
	CA Application	- Windows Server 2003
	Web Server	- IIS 6.0
	Development Tool	- Visual Studio 6.0
	Development Language	- Visual C++ 6.0
Hard-ware	Client	CPU: AMD Athlon 64 X2 6200+
		RAM: 1GB X 2
		HDD: 500GB
	CA	CPU: Intel Core2 Duo E6750
		RAM: 1GB X 2
		HDD: 400GB
	RA	CPU: Intel Core2 Duo E6750
		RAM: 1GB X 2
		HDD: 400GB
	Directory	CPU: Intel Dual-Core E5200
		RAM: 512MB X 2
		HDD: 350GB

4.2 제안 모델 성능 검증 시뮬레이션

본 절에서는 3장에서 제안한 DbHC 모델이 정상적으로 동작하는지 실제 시뮬레이션 하여 성능을 검증할 것이다. 먼저 인증서가 정상적으로 발급되는지 확인한 후, 제안한 모델을 통해 발급된 인증서가 정상 인증 되는지 확인할 것이다. 또한 미인증 경우를 만들어 제안한 모델이 정확히 미인증 처리를 하는지 시뮬레이션 할 것이다.

4.2.1 DbHC 모델 정상 동작 실험

(1) 인증서 발급 과정 실험 : DbHC 모델에서 사용자가 인증서 발급을 요청하면 CA는 User Active X Controller에게 발급될 인증서가 저장될 위치를 선택할 것을 요청한다. 그림 7은 인증서가 저장될 장치를 선택하는 과정과 장치 선택 과정에서 사용자의 USB 드라이브를 선택했을 경우의 디바이스 ID 추출 결과이다.

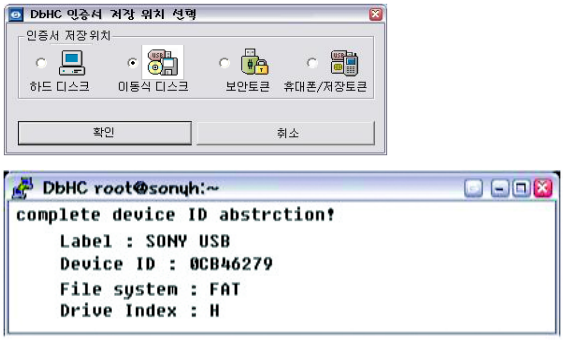


그림 7. 인증서 저장 위치 선택과 선택된 디바이스의 ID 추출 화면
fig. 7. Certificate storage selection and Extracted ID from selected device

인증서가 저장될 장치의 디바이스 ID 추출이 완료되면 CA는 User Active X Controller에게 인증서 인증 정책을 선택할 것을 요청한다. 그림 8은 DbHC 모델의 인증서 인증 정책 중 Level 2 정책을 선택했을 경우와 Level 2 정책의 인증에 필요한 IP 주소를 사용자가 직접 입력하는 화면이다.

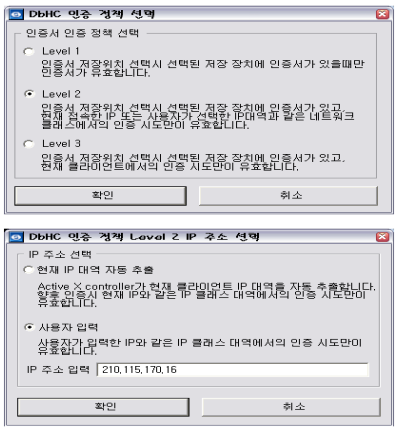


그림 8. 인증서 인증 정책 선택과 IP 주소 사용자 입력 화면
fig. 8. Selection window for certificate authentication policy and Input window for IP address user

DbHC 모델에서 인증서 인증 정책을 선택하면 User Active X Controller는 선택된 정책별로 필요한 디바이스 ID와 IP 주소를 추출하게 된다. 그림 9는 선택된 정책별 디바이스 ID 또는 IP 주소의 추출 결과이다.

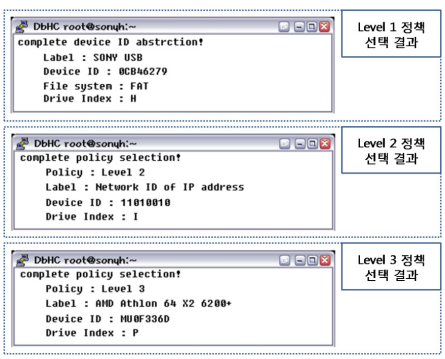


그림 9. 정책별 선택 결과와 디바이스 ID 추출 결과
fig. 9. device ID extraction results of policy selections

정책 선택과 디바이스 ID 혹은 IP 주소의 추출이 완료 되면, 선택된 정책에 따라 추출된 디바이스 ID와 IP 주소를 이용해 DLDI Key를 만든다. CA에서는 Private Key와 인증서를 생성해 Directory에 인증서와 CRL을 등록한다.

Directory의 DB에 사용자의 인증서와 CRL이 등록되면 등록 결과를 CA에 전송하고 CA에서는 생성된 Private Key와 인증서를 사용자에게 발급하고, 이를 사용자가 선택된 디바이스에 저장함으로써 인증서 발급과정이 완료된다. 그림 10은 User의 Client와 CA의 인증서 발급 처리 결과 화면이다.

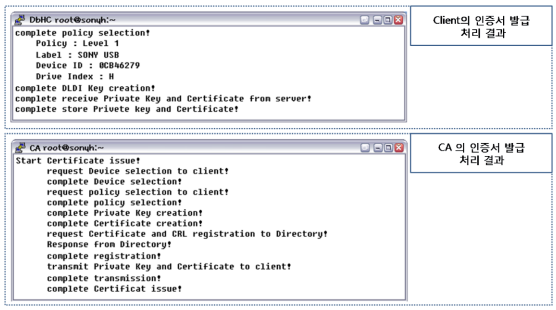


그림 10. Client와 CA의 인증서 발급 처리 결과 화면
fig. 10. Result of certificate granting process between Client and CA

(2) 인증서 인증 과정 실험 : 인증서 인증 과정은 4.2.1절의 실험 1에서 발급된 인증서를 통해 DbHC 모델이 사용자 인증서를 정상 인증 처리를 하는지 시뮬레이션 하였다. 그림 11은 Client와 CA의 사용자 인증서 처리 결과화면이다.

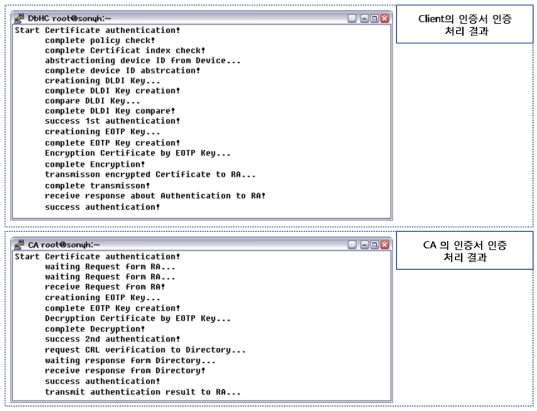


그림 11. Client와 CA의 인증서 인증 처리 결과 화면
fig. 11. Result of authentication process between Client and CA

4.2.2 DbHC 모델 미인증 처리 정상 동작 실험

미인증 처리 정상 동작 실험은 제안한 DbHC 모델의 미인증 처리 경우인 DLDI Key 검증과정과 인증서 유효성 검사 과정의 미인증 경우를 만들어 제안한 모델이 정상적으로 미인증 처리가 진행되는지 시뮬레이션 하였다.

(1) DLDI Key 검증을 통한 인증서 원천지 무결성 보장 실험

인증서 원천지 무결성 보장 실험은 4.2.1절의 실험 1에서 발급된 인증서를 인증서가 발급될 때 선택된 장치가 아닌 다른 장치에 옮겨 인증을 시도하여, 제안하는 모델에서 인증서의 원천지 무결성이 보장되는지의 결과를 시뮬레이션 하였다. 또한 인증서 인증 정책을 Level 3로 했을 경우 선택된 Client가 아닌 다른 Client에서의 인증을 시도하여 인증서의 원천지 무결성이 보장되는지의 결과를 시뮬레이션 하였다. 그림 12는 DLDI Key 비교를 통한 원천지 무결성 보장 실험의 결과 화면이다.

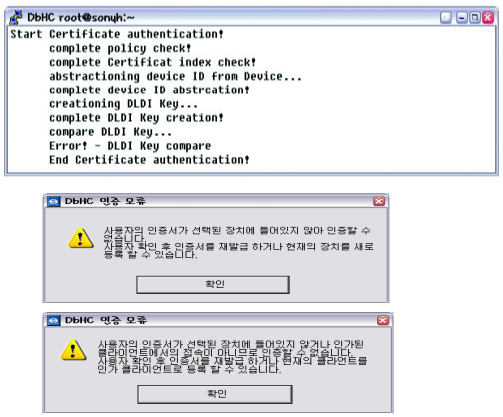


그림 12. DLDI Key 비교를 통한 원천지 무결성 보장 실험 결과
fig. 12. Result of origin integrity test via comparing DLDI Keys

(2) 인증서 유효성 검증 과정의 미인증 처리 실험

유효성 검증 과정의 미인증 처리 실험은 DbHC 모델에서 유효기간이 만료된 인증서로의 인증 시도를 통한 인증서 유효성 검증과정에서의 미인증 처리를 시뮬레이션 하였다. 그림 13은 인증서 유효성 검증과정의 미인증 경우 처리 결과 화면이다.

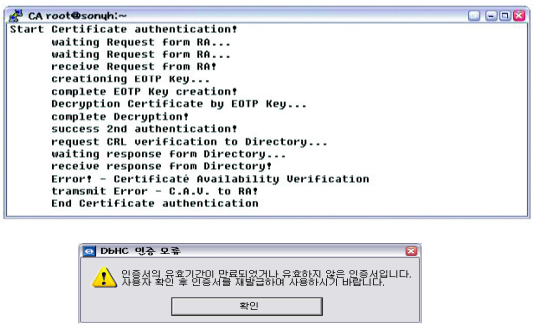


그림 13. 인증서 유효성 검증과정의 미인증 경우 처리 결과 화면
fig. 13. Processing result of unauthenticated case in certificate validation

4.2.3 DbHC 모델의 각 정책별 인증 완료 시간 측정 실험

타 방식과의 인증 시간 비교를 위해 우선적으로 DbHC 모델의 각 정책별 인증 소요시간을 측정 해 보았다. 그림 14은 DbHC 모델의 각 정책별 인증 소요시간을 측정하기 위한 프로그램의 소스코드와 측정된 결과화면이다.

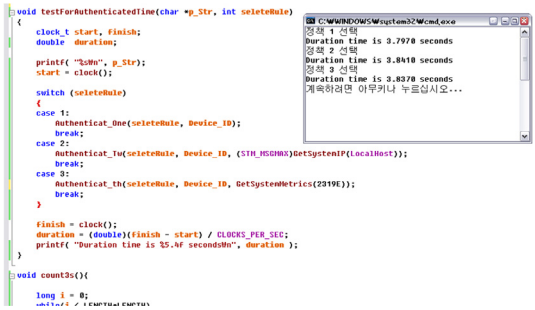


그림 14. 정책별 인증 소요시간 측정 프로그램과 결과 화면
fig. 14. Turnaround time testing software of policies and Test result

그림 14의 정책별 인증 소요시간 측정 프로그램과 결과 화면을 보면, Level 2 정책이 IP 주소 추출과정에서의 Network ID Class 분석 시간 소요 등의 원인 때문에 3.841초로 가장 높게 측정되었다. 본 실험을 5회 반복하여 각 정책별 평균 인증 소요시간 측정 결과 DbHC 모델의 인증 완료까지의 평균 소요 시간은 3.825초로 측정 되었다.

4.3 기존 방식과의 인증 완료 시간 비교 실험

본 절에서는 제안하는 모델과 기존 방식과의 성능을 비교하기 위해 첫 번째로 HSM과 DbHC 모델, 두 번째로 OTP와 DbHC 모델과의 각각의 인증 과정별 인증 시간을 비교 해 본다.

4.3.1 HSM 방식과의 인증 과정별 인증 완료 시간 비교

먼저 HSM과 DbHC 모델간의 인증 과정별 인증 시간을 비교하여 제안 모델의 성능을 검증하여 보았다. 그림 15는 HSM 방식과 제안 모델의 인증 과정별 인증 시간을 각각 5회 실험하여 각각의 평균을 비교한 데이터와 그래프이다.

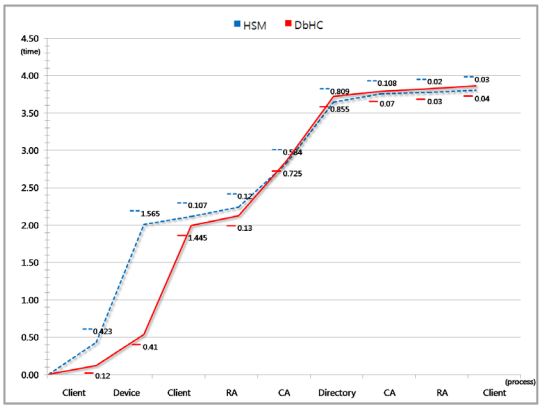


그림 15. HSM 방식과의 인증 과정별 인증 시간 비교 그래프
fig 15. Comparison graph for turnaround time of HSM and DbHC

그림 15의 그래프를 보면 HSM은 모듈 자체의 내부 연산의 영향으로 Client와 Device 부분에서 연산에 많은 시간 소요가 있었고, DbHC 모델에서는 모듈 내부 연산보다는 Client에서의 연산과 네트워크 환경의 영향에 의한 지연이 있었다. 인증 완료까지의 총 소요 시간은 두 방식이 비슷한 성능을 보였으나, HSM이 평균 3.766초의 인증 완료 시간을 소요하여 DbHC 모델의 평균 소요 시간인 3.825초 보다 평균 0.059초 높은 속도를 보였다.

4.3.2 OTP 방식과의 인증 과정별 인증 완료 시간 비교

두 번째로 DbHC 모델과 OTP와의 인증 과정별 인증 시간을 비교하여 제안 모델의 성능을 검증하여 보았다. 본 실험에서는 OTP 인증의 Password입력을 사용자 입력이 아닌 파일 입력으로 환경 설정 하였고[11], 제안 모델과 OTP 인증 모두 각각 5회 실험하여 각각의 평균을 비교하였다. 그림 16은 OTP 방식과 제안 모델의 인증 과정별 인증 시간의 평균을 비교한 데이터와 그래프이다.

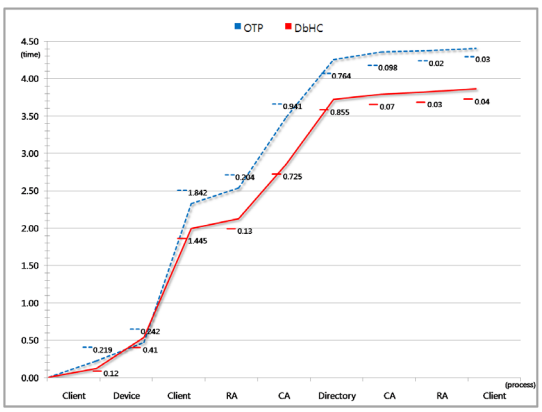


그림 16. OTP 방식과 인증 과정별 인증 시간 비교 그래프
fig 16. Comparison graph for turnaround time of OTP and DbHC

OTP 방식은 Device 처리 부분에서의 처리 시간이 짧은 반면 Password 입력을 위한 파일입력을 위한 Client부분에서의 처리 시간이 높게 나타났다. 전체 인증 완료 시간을 비교해 보면 제안 모델이 평균 4.360초를 소요한 OTP 방식보다 평균 0.535초 더 빠른 인증 처리 시간을 보였다.

4.4. 기존 방식과의 데이터 전송량 비교 실험

본 절에서는 기존 방식과 DbHC 모델의 데이터 전송량을 비교하여 제안 모델의 성능을 검증하였다. 본 실험에서 DbHC 모델은 보안성이 가장 높은 Level 3 정책을 적용하였고, 기존의 인증 방식 또한 보안성이 가장 높은 HSM과 OTP 혼용 방식을 적용하여 각 인증 과정별 데이터 전송량을 측정하였다. 그림 17은 기존 방식과의 데이터 전송량 비교 실험이다.

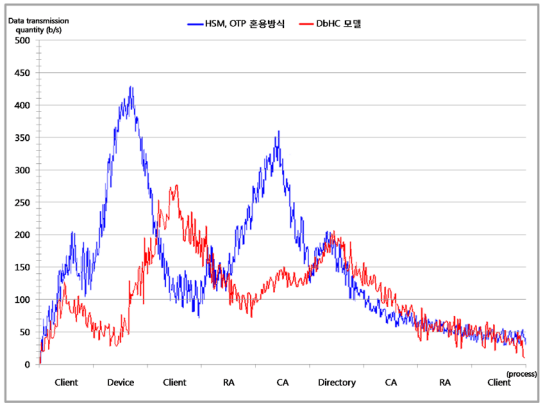


그림 17. HSM, OTP 혼용 방식과 데이터 전송량 비교 실험
fig 17. Data transmission rate comparing test between DbHC and hybrid of HSM and OTP

그림 17을 보면 제안 모델은 Client 부분에서의 DLDI Key 비교 등의 처리 과정 때문에 데이터 전송량이 가장 많게 나타났다. 반면 기존방식에서는 Device 부분에서의 HSM 모듈 처리연산과 CA 부분에서 OTP Password 처리 연산 때문에 데이터의 전송량이 폭발적으로 증가함을 볼 수 있다. 이는 서버의 연산 부하와 네트워크 지연을 유발할 수 있으나, 제안 모델에서는 Client 부분에서의 많은 연산처리로 CA 부분에서의 과다한 데이터 전송에 의한 연산 부하 및 네트워크 지연을 방지할 수 있다.

4.5. 인증서 원천지 무결성 보장 실험

이번 실험은 HSM 장치와 DbHC 모델에서의 인증서 원천지 무결성 보장 능력을 비교하여 보았다. HSM방식과 제안

모델의 인증서 저장 디바이스가 도난 또는 유출되었을 상황을 가정하여 두 방식이 원천지 무결성을 보장하는지 실험하였다. OTP 방식과의 인증서 원천지 무결성 보장 실험은 OTP 방식 자체가 인증서의 원천지 무결성을 보장할 수 없기 때문에 그에 대한 안전장치로 보안카드라는 OTP 방식을 도입한 것이고, 보안카드의 단점은 2.3절에서 분석하였으므로 OTP 방식과의 인증서 원천지 무결성 보장 실험은 무의미하여 실험하지 않았다. 본 실험은 발급된 인증서가 각각 HSM 장치와 인증정책이 Level 3 인 DbHC 모델의 사용자 USB 드라이브에 저장되어 있고, 각각의 장치가 도난 또는 유출되었음을 가정하였다. ID와 Password같은 지식기반 인증요소 또한 유출이나 해커에 의해 유추될 수 있음을 가정하고 실험하였다. 그림 18은 HSM 장치의 원천지 무결성 보장 실험 결과이다.

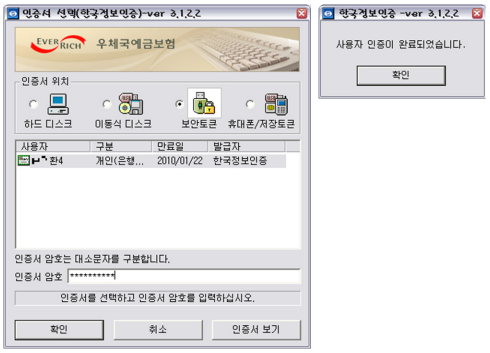


그림 18. HSM 장치의 원천지 무결성 보장 실험 결과
fig 18. Origin integrity test result of HSM device

HSM 장치의 보안성은 전적으로 하드웨어의 보안 능력에 의존하게 설계되어 있어 장치 내부의 인증서를 보호하는데 효과적이고 안정성이 높다. 하지만 장치 자체의 도난이나 분실에는 취약성을 보인다. 본 실험에서 HSM 장치는 인증서의 원천지 무결성을 보장하지 못하고 인증에 성공함을 볼 수 있다. 반면 그림 19는 DbHC 모델의 원천지 무결성 보장 실험이다.

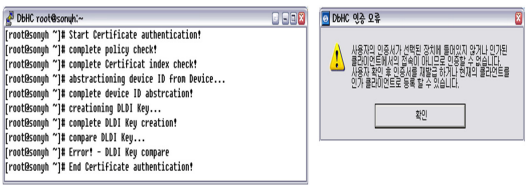


그림 19. DbHC 모델의 원천지 무결성 보장 실험 결과
fig 19. Origin integrity test result of DbHC device

그림 19의 실험 결과를 보면 DbHC 모델에서는 DLDI Key 비교를 통한 1차 검증에 의한 인증서의 원천지 무결성 보장을 통해 인증에 실패하게 함으로써 인증의 요소 중 가장 유출 가능성이 높은 Password 입력 인증 단계로의 진입조차 필요가 없어 보안성이 향상됨을 알 수 있다. 표 8은 HSM과 DbHC의 인증서 원천지 무결성 보장 실험 결과 표이다.

표 8. HSM과 DbHC의 인증서 원천지 무결성 보장 실험 결과 표
Table 8. Result table of Origin integrity test of HSM and DbHC

	원천지 무결성 검증	패스워드 입력 검증	공개키 복호화	인증서 유효성 검증	인증 성공
HSM	Don't try	success	success	success	success
DbHC	fail				

Ⅳ. 결론

본 논문에서는 디바이스 ID에 기반한 하이브리드 공인 인증 기법인 DbHC 모델을 제안하였다. OTP Event 동기화 기법을 이용한 보안성 향상과 사용자 선택에 의한 정책별 디바이스 ID와 IP 주소를 통한 인증서의 원천지 무결성 보장, 그리고 멀티 디바이스 지원에 의한 사용자 편의성 향상에 대한 연구를 수행하였다. 인증서 발급, 인증서 인증, 미인증 처리 등을 통한 제안 모델 정상 동작 시뮬레이션과 기존 인증 기법들과의 비교 실험 결과 사용자의 인증 환경에 따른 각각의 정책 설정과 기존 인증기법의

단점 보완 등으로 사용자의 편의성 향상과 원천지 무결성이 보장되었음을 보였다. 또한 HSM과 OTP 방식과의 비교 실험을 통한 성능 측정으로 처리 속도와 데이터 전송량에서 효율적이며, 서버에서의 연산 부하를 감소시킬 수 있고 안정적임을 검증하였다. 향후 연구 과제로는 키 검증 과정 및 인증 과정 그리고 연산 과정 등에서의 처리 속도 향상과 데이터 전송량 감소 및 효율적인 키 생성・관리・폐기 기법에 대한 연구가 추가적으로 필요하다.

참고문헌

[1] A. Mwnezes, P. Van Oorschot and S. Vanstone, "*Handbook of applied cryptography*," CRC Prss,

Inc, 1997.
〔2〕 노창현, "*GPKI 공인인증서의 보안토큰(HSM)적용 정책 연구*," 창원대학교 대학원 석사 학위 논문, 2009.6.
〔3〕 이성만, "*통합 OTP 인증센터 개선 방안*," 건국대학교 정보통신 대학원 석사학위 논문, 2008.6.
〔4〕 Mitchell, C.J., Chen, L., "Comments on the S/key User Authentication Scheme," ACM Operating Systems Review. Vol. 30. No. 4. 2002.
〔5〕 Yeh, T.C., Shen, H.Y., Hwang, j.j, "A Secure One-time Password Authentication Scheme Using Smart Cards," IEICE Trans. Commun. Vol. E85-B. No.11. Nov. 2002.
〔6〕 최동현, 김승주, 원동호, "일회용 패스워드(OTP : One-Time Password) 기술 분석 및 표준화 동향," 정보보호학회지, 제17권 제3호, pp. 12-17, 2007년 6월.
〔7〕 금융보안연구원, "OTP 통합인증센터에서 수용 가능한 인증방식," 주간정보 Vol. 1 제1권 제1호 창간지, 2007년 1월.
〔8〕 National Security Agency, "Technical Interoperability Profile for the Bridge Certification Authority (BCA) Interoperability DemOIStration Phase 2," prepared by A&N Associates, 2001.
〔9〕 Andre Arnes and Svein J. Knapskog, "Selecting Revocation SolutiOIS for PKI," Proceedings of The Fifth Nordic Workshop On secure IT system (NORDSEC), 2000.
〔10〕 양형규, 최종호, "안전한 하이브리드 인증 메시지 프로토콜," 제12권 제4호, 77-85쪽, 2007년 9월.
〔11〕 "OTP 솔루션", *http://www.datanet.co.kr*, NETWORK TIME 2006.10.

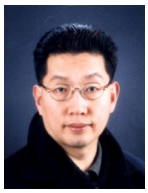
저 자 소 개

손 영 환
2010 : 충북대학교 공학석사
관심분야 : 유비쿼터스컴퓨팅, 정보보안 멀티미디어통신

최 운 수
2007 : 충북대학교 공학석사
2009 : 충북대학교 컴퓨터공학과 박사수료
관심분야 : 유비쿼터스컴퓨팅, 정보보안 멀티미디어통신

김 기 현
2010 - 현재 : 에스지에이(주) R&D사업부분 사장
2010 : 충북대학교 컴퓨터공학과 박사수료
관심분야: 시스템보안, 네트워크보안, 보안관제, 암호

최 한 나
2009 : 충북대학교 컴퓨터공학과 박사수료
2006 - 현재 : 우송대학교 컴퓨터공학과 겸임교수
관심분야 : 유비쿼터스, 디지털 음향, 게임사운드디자인



이 대 윤
2009 : 충북대학교 컴퓨터공학과 박사수료
1985 : 미국, NYIT Graduate School, Computer Graphics Dept.
관심분야 : 디지털방송, 유비쿼터스, 3D Animation

오 충 식
2004 : 충북대학교 전자계산학과 이학석사
2009 : 충북대학교 컴퓨터공학과 박사 수료
2005 - 현재 : 한국과학기술정보연구원 책임기술원
관심분야 : 정보보호, 유비쿼터스

조 용 환
1982 - 현재 : 충북대학교 전자정보대학 교수
현재 : (사)한국엔터테인먼트산업학회 수석부회장
1989 : 고려대학교 이학박사
관심분야 : U-healthcare, 유비쿼터스컴퓨팅, 멀티미디어통신