通信情報保護學會誌
第 11 券 第 2 號, 2001. 4

PKI 제품의 적합성 시험

이 종 후*, 김 충 길*, 이 석 래**, 이 재 일**, 김 학 범**, 류 재 철*

요 약

PKI 정보보호 제품의 개발에 있어서 반드시 고려해야 하는 요소 가운데 하나는 PKI 정보보호 제품이 안전성, 신뢰성 등의 요구조건을 만족하며, 확장성 및 상호연동성을 갖도록 개발되었는지 확인하는 것이다. 만약 이와 같은 사항들이 만족되지 못한다면, 사용자는 PKI 정보보호 제품의 안전성 및 신뢰성을 의심할 수밖에 없다. 또한 다른 PKI 제품들과의 연동에 있어서 문제를 일으킬 수밖에 없으며, 이는 결과적으로 사용자에게 불이익을 가져다 주게 된다. 이러한 문제를 방지하기 위해서는 개발 단계에서부터 X.509 등 관련된 기술 표준을 정확하게 준수하여야 한다. 또한 표준 적합성 확인을 위해서 PKI 정보보호 제품이 표준에 따라 적합하게 구현되었는지 검증하는 절차가 필요하다. 즉, PKI 정보보호 제품의 표준 적합성 여부에 대한 검증을 전문적으로 수행할 수 있는 시험도구의 개발이 요구된다.

본 논문에서는 PKI 정보보호 제품의 표준 적합성 여부를 판단할 수 있는 시험 절차를 제시하고, 이에 따라 PKI 정보보호 제품에 대한 검증을 수행할 수 있는 시험도구를 구현하였다. 즉, PKI 정보보호 제품이 인증 서비스 제공을 위해 사용하는 X.509 등 인증 관련 기술이 표준을 준수하고, 이를 통해 PKI 제품 간의 상호운용성을 지원할 수 있는지 여부를 검증하려는 것이다.

Ⅰ. 서 론

범세계적인 정보통신망인 인터넷의 급속한 확산과 정보기술의 발전은 일상생활과 비즈니스 관행을 근본적으로 변화시키고 있다. 특히 현재 많은 사람의 관심이 대상이 되고있는 전자상거래는 새로운 문화현상의 하나로 자리잡아가고 있는 실정이다. 국경없는 무한 경쟁의 시대를 맞아 세계 각국은 이러한 현상에 국가적인 차원에서 대처하고 있다. 그 대표적인 예로 전자문서에 법적인 효력을 부여함으로써 전자상거래의 안전성 및 신뢰성을 제고하는 전자서명 관련 법규의 제정 및 이를 기술적으로 뒷받침하는 PKI 구축을 들 수 있다. 미국의 경우 1995년 유타주의 전자서명법을 시작으로 하여, 얼마전 연방정부 차원에서도 전자서명법이 제정된 바 있으며, 국가 PKI인 FPKI에 대한 지속적인 연구를 진행중이다. 또한 독일, 이탈리아, 말레이시아, 싱가폴 등의 국가도 이미 전자서명법을 제정하였으며, 덴마크, 영국, 핀란드, 일본 등에서도 전자서명법 제정 작업을 서두르고 있다. 이와 같이 성공적인 전자상거래 운영을 위해서 PKI를 비롯한 정보보호 기술에 대한 중요성이 강조되고 있는 가운데, 국내에서도 이미 전자거래기본법과 전자서명법이 시행되고 있다.

인증 서비스와 관련된 수요가 증가하고 관련 법규의 제정이 이루어짐에 따라 인증 업무 수행을 위한 인증기관의 운영 및 PKI 정보보호 제품의 개발 또한 활발하게 이루어질 것으로 기대된다. PKI 정보보호 제품의 개발에 있어서 반드시 고려해야 하는 요소 가운데 하나는 PKI 제품이 안전성, 신뢰성 등의 요구조건을 만족하며, 확장성 및 상호연동성을 갖도록 개발되었는지 확인하는 것이다. 만약 인증업무 수행을 위해 사용하는 기술들이 이와 같은 사항을 만족하지 못한다면, 사용자는 이러한 인증기관의 안전성 및 신뢰성을 의심할 수밖에 없다. 또한 이러한 PKI 제품은 등록기관, 저장소, 또는 다른 인증기관 등 PKI 구성요소들과의 연동에 있어서 문제를 일으킬 수밖에 없으며, 이는 결과적으로 사용자에게 불이익을 가져다 주게 된다.

* 충남대학교 정보통신공학부 (jcryou@home.cnu.ac.kr)
** 한국정보보호센터

이러한 문제를 방지하기 위해서는 개발 단계에서부터 X.509 등 관련된 기술 표준을 정확하게 준수하여야 한다. 특히 국내에서는 전자서명법의 시행과 함께 공인인증기관 지정제도가 실시됨에 따라 공인인증기관 신청자에 대한 평가가 실시되고 있다. 평가의 정확성과 신뢰성을 높이기 위해서는 평가시 신청자의 PKI 제품이 위에서 언급한 인증기술을 표준에 따라 적합하게 사용하였는지 시험하는 절차가 필요하다. 이를 위해서는 시험을 전문적으로 수행할 수 있는 시험도구의 개발이 요구된다.

이에 본 논문에서는 PKI 정보보호 제품의 표준 적합성 만족 여부를 판단할 수 있는 시험절차를 제시하고, 시험도구를 구현하였다. 즉, PKI 정보보호 제품이 인증 서비스 제공을 위해 사용하는 X.509 등 인증 관련 기술이 국제 및 국내 표준을 준수하고, 이를 통해 상호운용성을 지원할 수 있는지 여부를 검증하려는 것이다. 이 때 인증 관련 기술은 사실상의 국제표준으로 받아들여지고 있는 IETF (Internet Engineering Task Force) pkix (Public Key Infrastructure X.509)를 기반으로 한다.

본 논문의 2장에서는 미국방성 PKI와 외부 인증기관과의 연동을 위해 실시하고 있는 인증서 적합성 테스트에 대해서 살펴본다. 3장에서는 PKI 정보보호 제품의 적합성 시험 절차에 대해서 살펴보고, 4장에서 시험도구의 구현 내용에 대해서 알아본다. 마지막으로 5장에서 결론을 맺는다.

II. IECA X.509 인증서 적합성 테스트

1. 테스트 개요

자체적인 PKI 구축에 대한 연구를 지속적으로 수행해 오고 있는 미국방성(DOD: Department of Defense)의 X.509 인증서 정책은 인트라넷 및 인터넷 통신에 있어서 전자서명 및 암호화 등의 보안기술을 이용하는 데 필요한 공개키 인증서의 생성 및 관리 정책을 정의하고 있다. DOD는 DOD PKI 내에서 민간 인증기관의 활동을 허용하고 있다. 즉 외부 인증기관 (ECA: External Certificate Authority)으로 하여금 DOD PKI 내에서 사용되는 인증서 발급 업무를 수행할 수 있도록 하고있다[1].

외부 인증기관의 수용을 위해 가장 먼저 해결해야 할 것은 상호운용성의 문제이다. 즉 외부의 인증기관과 DOD PKI의 연동이 올바르게 이루어져야 하는 것이다. 이와 관련된 작업은 DOD 내 JITC (Joint Interoperability Test Command)에서 주관하고 있는데, JITC에서는 ECA가 표준을 준수하는지 여부를 결정하기 위해서 ECA가 생성하는 SSL 클라이언트 인증서, 전자우편 인증서, 서버 인증서 등에 대한 테스트를 수행한다[2].

테스트는 아리조나주 Fort Huachuca에 위치한 JITC PKI 연구소에서 이루어진다. 테스트 대상자는 테스트용 샘플 인증서를 제출해야 한다. 테스트에 소요되는 시간은 5일이 넘지 않으며, 테스트는 DOD의 가장 최신 인증서 표준 프로파일에 기준하여 이루어진다.

이 테스트의 목적은 IECA가 다음과 같은 능력을 갖추었는지 평가하는 것이다.

- X.509 v3 인증서 생성 능력
- DOD PKI 중급 X.509 인증서 표준 프로파일 지원 능력
- 사용자 SSL 인증서 지원 능력
- 사용자 전자우편 인증서 지원 능력
- 서버 인증서 지원 능력

JITC는 평가대상자들이 제출한 샘플 인증서를 분석하여 이들이 필요한 테스트 기준을 준수하는지를 평가한다. 평가에 소요되는 시간은 1일 가량 될 것으로 예상하고 있다. 그러나 샘플 인증서의 전달 방법, 인증서 생성에 필요한 정보의 JITC 생성 여부, 인증서 생성에 사용된 암호 알고리즘에 대한 테스트 여부 등 테스트의 자세한 사항은 아직 공개되지 않은 상태이다.

2. 테스트 기준

평가대상자들은 평가에 앞서서 JITC에서 배포하는 질문에 응답함으로서 인증기관을 운용하는데 필요한 지식과 경험을 보유하고 있음을 증명해야 한다. 실제 테스트는 DOD PKI 중급 X.509 버전3 인증서 표준 프로파일의 준수 여부를 확인하는 것으로 이루어진다. 테스트를 위해서 평가대상자는 다음과 같은 사항을 만족시켜야 한다.

- 인증서는 전자적 매체 또는 마그네틱 미디어를 통해서 ASCII base 64 인코딩되어 전달되어

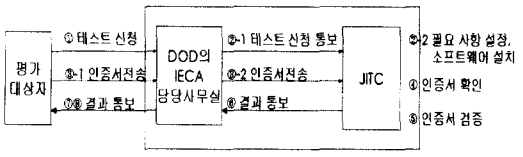
야 한다.
- 평가되는 인증서는 최소한 SSL 인증서 10개와 전자우편 인증서 10개로 이루어져야 한다.

테스트 과정에서는 다음과 같은 인증서 정보가 기록된다.

- Version
- Serial Number
- Issuer's Signature Algorithm
- Issuer's Distinguished Name
- Validity Period
- Subject Distinguished Name
- Subject Public Key Information
- Issuer Unique Identifier
- Subject Unique Identifier
- Issuer's Signature
- Extensions
  - Authority Key Identifier
  - Subject Key Identifier
  - Key Usage
  - Extended Key Usage
  - Private Key Usage Period
  - Certificate Policies
  - Policy Mapping
  - Subject Alternate Name
  - Issuer Alternate Name
  - Subject Directory Attributes
  - Basic Constraints
  - Name Constraints
  - Policy Constraints
  - CRL Distribution
  - 위에서 언급되지 않은 기타 확장필드

3. 테스트 절차

테스트는 그림 1과 같은 절차를 통해 이루어진다.



〔그림 1〕 IECA X.509 인증서 적합성 테스트 절차

① 테스트 신청인은 IECA 담당 사무실에 테스트를 신청하고 테스트 시작 날짜 등을 협의한다. 테스트 날짜는 최소한 1주일 전에 결정되어야 한다.
② JITC는 관계자들과 테스트 일정을 협의하고, 테스트를 위해 필요한 사항을 설정하며, 필요한 소프트웨어를 설치한다.
③ 테스트 신청인은 샘플 인증서를 담당 사무실로 전송한다. 담당 사무실에서는 이를 제출 시간과 함께 JITC에 전송한다.
④ JITC는 다음 사항을 확인한다.
- 테스트용 인증서가 올바르게 인코딩되었는지 여부.
- 10개의 SSL용 인증서와 10개의 전자우편용 인증서가 제출되었는지 여부
⑤ JITC는 제출된 인증서를 디코딩하고 이 것을 DOD PKI 중급 X.509 v3 인증서 표준 프로파일과 비교한다.
⑥ 테스트가 완료된 후, JITC는 담당 사무실에 결과를 통보한다.
⑦ 테스트에서 모든 요구사항을 만족하지 못하는 경우, 테스트 신청인에게 불일치되는 항목을 통보하고, 테스트 신청인은 이를 수정하여 다시 테스트를 받는다.
⑧ 테스트 신청인이 수정하지 못하는 오류가 발생한 경우, 테스트를 통과하지 못한 것으로 하며, 테스트가 종료된다.

테스트가 수행되는 동안 JITC는 테스트 항목별 로그 데이터를 시간순으로 기록한다. 이 때, 테스트 수행자와 테스트에 소요된 시간이 함께 기록된다. 만약 테스트가 연기되는 경우에는 그 사유가 기록되어야 한다. 테스트에 사용된 인증서 등의 정보는 JITC에 의해서 12개월 동안 보관되며, 12개월이 지난 후에 모든 정보는 파괴된다.

Ⅲ. 적합성 시험 절차 및 시험도구 설계

1. 개 요

본 장에서는 시험도구에 의한 PKI 정보보호 제품의 적합성 시험절차에 대해 기술하고, 시험도구의 설계 내용에 대해서 살펴본다. 시험의 목표는 인증서비스를 제공하기 위해 사용되는 인증기술의 표준

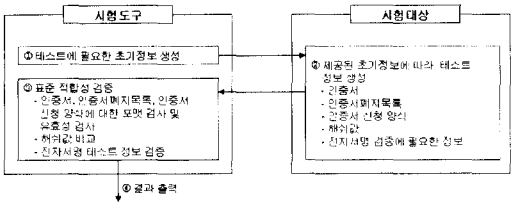
적합성을 검증하는 것으로, 다음과 같은 항목에 대해서 PKI 정보보호 제품의 적합성을 검증한다.

- X.509 V3 인증서
- X.509 V2 인증서폐지목록
- 인증서 신청 양식

위와 같은 항목의 검증은 다음과 같은 사실상의 국제표준에 기반해서 이루어진다.

- 인증서 및 인증서 폐지목록:Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)[3]
- 인증서 신청 양식:PKCS#10 Certification Request Syntax Standard[4]

이 때, 시험 대상은 사용자 인증서를 발급할 수 있는 능력을 갖춘 PKI 정보보호 제품이며, 전체적인 시험 절차는 그림 2와 같다.



〔그림 2〕 시험 절차

① 시험도구는 시험에 필요한 여러 가지 정보들을 생성한다. 이 초기정보에는 다음과 같은 것들이 포함된다.

- 테스트에 필요한 인증서 개수
- 테스트에 필요한 인증서폐지목록 개수
- 테스트에 필요한 인증서 신청양식 개수
- 해쉬 알고리즘의 구현 검증에 사용되는 임의의 메시지
- 전자서명 알고리즘 구현 검증에 사용되는 임의의 소수, 파라미터, 공개키 쌍 등

② 시험도구로부터 검증에 필요한 초기정보를 제공받은 시험대상은 이를 이용하여 다음과 같은 정보를 생성한다.

- 사용자 인증서, 인증기관의 인증서
- 인증서폐지목록
- 인증서 신청양식
- 임의의 메시지로부터 생성한 해쉬값
- 전자서명 알고리즘 구현 검증에 사용되는 정보(파라미터, 공개키쌍, 전자서명 유효성 확인 결과 등)

③ 시험대상으로부터 필요한 정보를 받은 뒤, 시험도구에서는 이에 대한 표준 적합성 검증을 실시한다. 이는 인증서, 인증서폐지목록, 인증서 신청양식의 포맷의 표준 준수 여부 확인하고 각각의 유효성 확인을 수행하는 것으로 이루어진다.

④ 시험이 완료되면 시험도구는 이에 대한 결과를 출력한다. 이 때 결과는 성공/실패로 표현된다.

2. 항목별 시험 절차

시험도구는 인증서, 인증서폐지목록, 인증서 신청양식을 읽어서 표준에 따른 정확한 포맷인지 확인하고, 그 내용을 보여준다. 또한 인증서 등에 대한 유효성 검사를 수행하는데, 이는 전자서명 확인, 데이터 무결성 확인, 유효기간 확인 등으로 구성된다.

2.1 인증서 포맷 검증

X.509 인증서 포맷에 대한 검증에서는 X.509 버전3 형식의 인증서를 읽어서 표준에 따른 포맷인지 여부를 테스트한다. 이 테스트는 크게 기본 필드에 대한 테스트와 확장필드에 대한 테스트로 구분할 수 있다. 기본 필드에 대한 테스트에서는 다음과 같은 X.509 인증서의 기본 필드가 모두 구현되었는지 여부를 테스트한다.

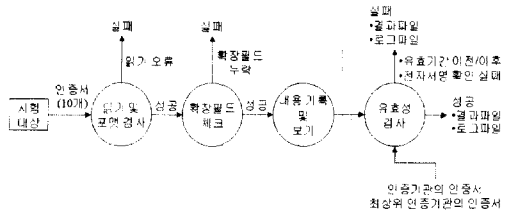
- 버전
- 일련번호
- 발행기관의 서명 알고리즘
- 발행기관의 DN
- 유효기간
- 인증서 소유주의 DN
- 인증서 소유주의 공개키 정보
- 발행기관의 유일 식별자
- 인증서 소유주의 유일 식별자
- 발행기관의 서명

확장필드에 대한 테스트에서는 다음과 같은 14개의 표준 확장필드에 대해서 테스트한다. 확장필드는 인증기관의 인증 정책에 따라 사용될 수도 있고, 사용되지 않을 수도 있기 때문에 사용된 확장필드에 대해서만 테스트한다. 그러나 시험을 수행하는 기관의 정책에 의해서 반드시 구현해야 하는 확장필드가 구현되었는지 여부를 테스트할 수 있다.

- 인증기관 키 식별자
- 인증서 소유주 키 식별자
- 키 용도
- 비밀키 사용 기간
- 인증서 정책
- 정책 매핑
- 인증서 소유주 대체 이름
- 발행기관 대체 이름
- 인증서 소유주 디렉토리 속성
- 기본 제약
- 이름 제약
- 정책 제약
- 확장 키 용도 필드
- 인증서폐지목록 배포점

2.1.1 X.509 버전3 인증서 기본 필드 테스트

이 테스트에서는 X.509 버전3 인증서의 기본 필드 부분이 표준에 따라 적합하게 구현되었는지 테스트한다. 테스트 절차는 그림 3과 같다.



〔그림 3〕 인증서 테스트

① 시험도구는 시험대상에게 필요한 인증서의 개수를 지정하여 자신의 로그 파일에 기록하고, 시험대상에게 알린다. 테스트에 필요한 인증서는 직접적인 시험 대상이 되는 인증기관에서 발행한 10개의 사용자 인증서와 인증서의 유효성 검사를 위해 필요한 인증기관의 인증서 및 최상위 인증기관의 인증서이다.

② 개수를 전달받은 시험대상은 개수만큼 사용자 인증서를 생성하여 시험도구에게 전달한다.

③ 인증서를 전달 받은 시험도구는 각각의 인증서를 읽어서 포맷이 올바른지 확인한다.

2.1.2 X.509 버전3 인증서 확장필드 테스트

이 테스트는 기본 필드에 대한 테스트와 동시에 진행된다. X.509 버전3 확장필드가 표준에 따라 구현되었는지 테스트하며, 특히 검증을 수행하는 측에서 지정하는 확장필드가 구현되었는지 테스트한다. 테스트 절차는 다음과 같다.

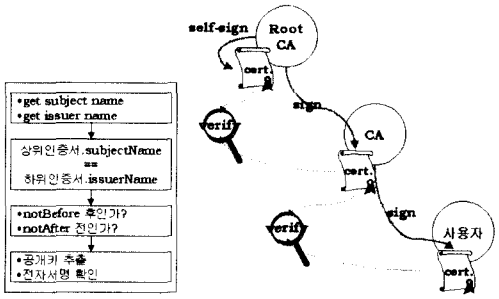
① 그림 3에서 기본 필드에 대한 포맷 테스트가 완료된후, 검증 수행자는 14개의 표준 확장필드 가운데 인증기관이 반드시 구현해야하는 필드를 지정한다.

② 시험도구는 인증서를 읽어서 표준 확장필드가 적절하게 구현되었는지 확인한다. 이 때 각 확장필드의 critical 여부를 체크한다.

③ 시험도구는 사용자가 입력한 반드시 필요한 확장필드가 모두 구현되었는지 테스트한다.

2.3 인증서 유효성 검사

그림 3에서와 같이 인증서의 기본 필드와 확장필드에 대한 포맷 검사와 필요한 확장필드의 구현 여부를 확인한 후에는 인증서에 대한 유효성 검사를 실시한다. 이때는 그림 4와 같이 전자서명이 올바른지, 유효기간이 지나지 않았는지를 테스트하고, 데이터 무결성을 테스트한다. 인증서의 유효성 검사를 위해서는 사용자의 인증서 뿐만 아니라 사용자의 인증서를 발행한 인증기관의 인증서와 최상위 인증기관의 인증서가 추가적으로 필요하다.

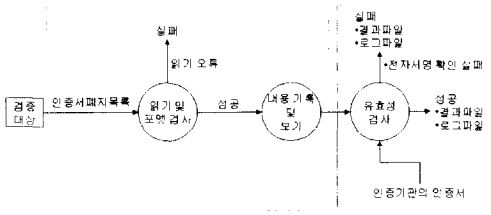


〔그림 4〕 인증서의 유효성 검사

2.3 인증서폐지목록 포맷 검증

이 테스트는 X.509 버전2 인증서폐지목록이 표준에 따라 적합하게 구현되었는지 테스트하며, 테스트 절차는 인증서 포맷에 대한 테스트 절차와 마찬가지로 인증서폐지목록의 포맷을 확인하고, 유효성 검사를 하는 것으로 이루어진다. 인증서폐지목록은 다음과 같은 구조로 이루어지며, 인증서폐지목록 테스트 절차는 그림 5와 같다.

- 기본 필드
  - 버전
  - 전자서명
  - 발행기관명
  - This Update
  - Next Update
  - 취소된 인증서
- 확장필드
  - 기관 키 식별자
  - 발행기관 대체 이름
  - 인증서폐지목록 번호
  - 델타 인증서폐지목록 지시자
  - 발행 배포점
- 인증서폐지목록 엔트리 확장필드
  - 이유 코드
  - 보류 코드
  - 무효일
  - 인증서 발행기관

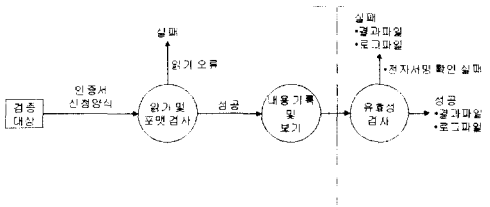


〔그림 5〕 인증서폐지목록 검증

2.4 인증서 신청 양식 검증

이 테스트는 인증서 신청 양식이 PKCS#10에 따라 적합하게 구현되었는지 확인한다. 인증서 신청 양식은 다음과 같은 구조로 이루어지며, 검증 절차는 그림 6과 같이 인증서와 인증서폐지목록에 대한 검증 절차와 유사하다.

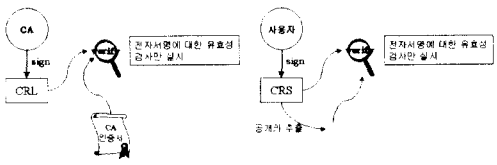
```
CertificationRequest::= SEQUENCE
{
  certificationRequestInfo
     CertificationRequestInfo,
  signatureAlgorithm
     SignatureAlgorithmIdentifier,
  signature
     Signature
}

CertificationRequestInfo::=SEQUENCE
{
  Version       Version,
  subject       Name,
  subjectPublicKeyInfo
     SubjectPublicKeyInfo,
  attributes [0] IMPLICIT Attributes
}
```



〔그림 6〕 인증서신청양식 검증

2.5 인증서폐지목록 및 인증서 신청 양식에 대한 유효성 검사

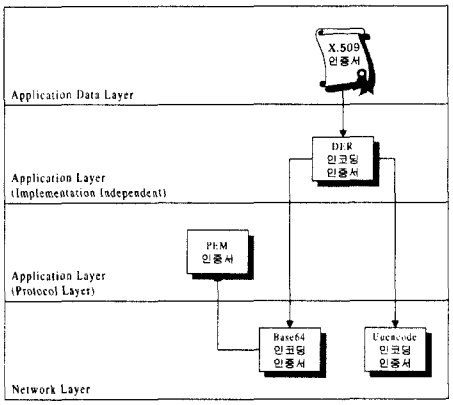
그림 5와 그림 6에서와 같이 인증서폐지목록 및 인증서 신청 양식에 대한 포맷 검사를 실시한 후에는 유효성 검사를 실시한다. 이는 그림 7에서와 같이 전자서명에 대한 확인 작업만을 수행한다. 이 때 인증서폐지목록의 유효성 검사를 위해서는 인증서폐지목록을 발행한 인증기관의 인증서가 필요하며, 인증서신청양식의 유효성 검사를 위해서는 사용자의 공개키를 인증서신청양식으로부터 추출하여야 한다.



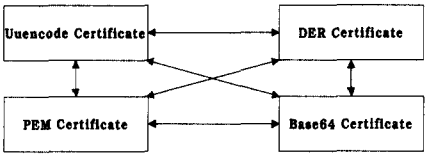
〔그림 7〕 인증서폐지목록 및 인증서신청양식 유효성 검사

2.6 인증서 변환

시험도구에서는 인증서 및 인증서폐지목록, 인증서 신청양식에 대한 검증 기능 외에 추가적으로 인증서 변환 기능을 제공한다. 이는 인증서의 DER, uuencode, base64, PEM 인코딩의 교차 변환 기능을 통해 인증서를 다양하게 활용하기 위함이다. 인증서의 인코딩 규칙은 그림 8과 같으며, 시험도구에서 제공하는 인코딩 변환 기능은 그림 9와 같이 4가지 인코딩 가운데 어떤 인코딩 방식에서도 다른 모든 인코딩 방식으로 변환할 수 있도록 한다.

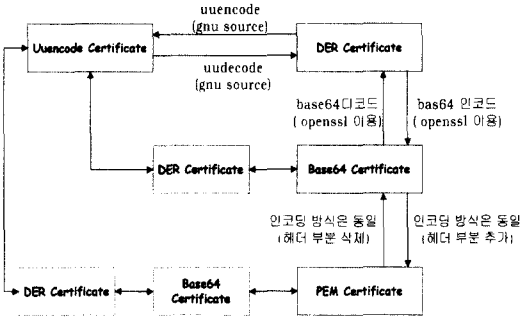


〔그림 8〕 인증서의 인코딩 규칙



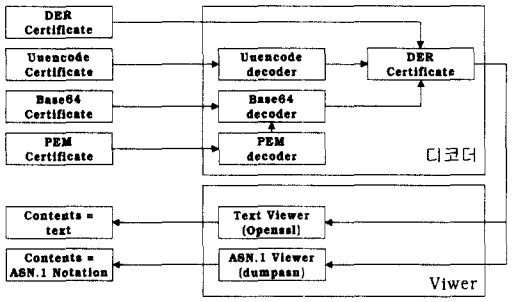
〔그림 9〕 인코딩 변환 기능

시험도구는 4가지 종류의 인코딩 가운데 하나로 인코딩 된 인증서를 입력 받아 이를 사용자가 지정한 방식으로 인코딩하여 출력한다. 변환 절차는 그림 10과 같다. 이 때, 인증서의 기본 인코딩 방식은 DER이기 때문에 DER를 기본으로 하여 다른 인코딩 방식으로의 변환이 이루어진다. 즉 DER와 uuencode 및 base64 인코딩 간의 직접 변환이 가능하며, PEM 인코딩은 base64 인코딩에서 헤더 부분만을 추가한 것이기 때문에 직접 변환이 가능하다. 그리고 base64 인코딩과 uuencode, PEM 인코딩과 uuencode 간의 변환은 일단 DER 인코딩을 거친 후에 이루어진다.



〔그림 10〕 인증서 인코딩 변환 절차

인증서 변환 기능에서는 인증서의 내용을 텍스트 형태나 ASN.1 형식으로 보여주는 기능을 함께 제공한다. 인증서의 내용을 보기 위해 시험도구는 그림 11과 같이 여러 가지 방식으로 인코딩된 인증서를 DER 인코딩으로 변환한 뒤, 이를 사용자의 선택에 따라 텍스트 또는 ASN.1 형식으로 출력한다.



〔그림 11〕 텍스트 또는 ASN.1 형식으로 인증서 내용 보기

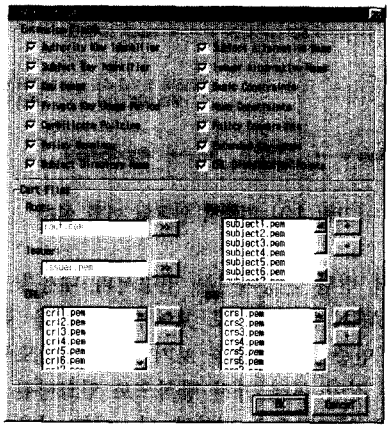
Ⅳ. 시험도구 구현

PKI 정보보호 제품 적합성 시험의 목적은 PKI 제품이 생성한 인증서 등의 포맷이 표준을 준수하였는지 확인하는 것이다. 즉 시험도구에서는 인증서 등의 포맷에 대해서만 표준 준수 여부를 확인하고, 그 내용에 대해서는 확인하지 않는다. 예를 들어 인증서 서브젝트 구별자의 유일성 여부를 확인하는 것과 같은 기능은 시험도구에서 제공하지 않는다. 따라서 시험도구는 표준에 따라 생성된 인증서, 인증서폐지목록, 인증서 신청양식을 읽어서 사용자에게 보여줄 수 있도록 구현되었으며, 시험도구를 통해 읽을 수 없는 경우에는 표준에 따라 생성된 양식이 아닌 것으로 간주하여 오류 메시지를 발생한다.

본 장에서는 시험도구의 구현 내용을 제공 기능을

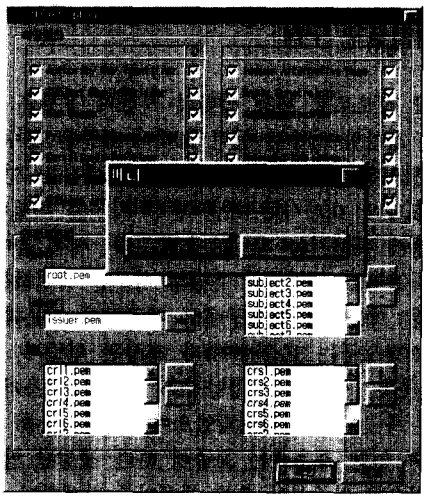
중심으로 살펴본다.

1. X.509 인증서 검증

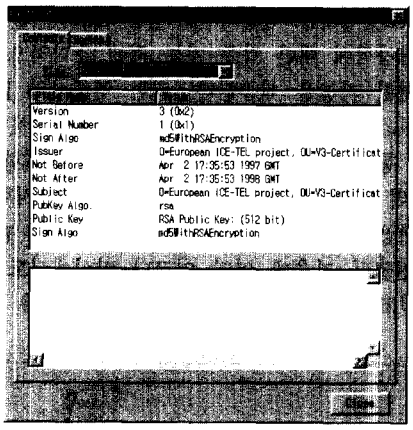


〔그림 12〕 인증서 검증 설정

그림 12는 X.509 인증서 및 인증서폐지목록, 인증서신청양식을 시험하기 위한 초기 설정화면이다. 화면 상단에서는 검증할 확장필드를 설정하며, 하단에서는 검증을 위해 필요한 최상위 인증기관의 인증서, 사용자 인증서 등을 설정한다. 표준을 준수하지 않은 인증서일 경우에는 시험도구에서 읽을 수 없으므로 올바른 인증서가 아님을 알리는 메시지를 발생한다(그림 13). 표준을 준수한 올바른 인증서일 경우에는 그림 14의 윈도우를 통해서 인증서의 내용을 볼 수 있다. 이 때 각 필드를 출력하여 그 내용과 확장필드의 criticality를 확인할 수 있다.



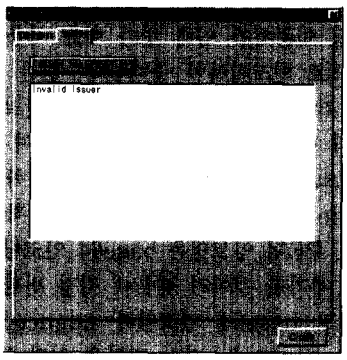
〔그림 13〕 잘못된 인증서에 대한 오류 메시지



〔그림 14〕 인증서 내용 보기

올바른 인증서일 경우에는 그림 13에서 Verify 탭을 클릭하여 인증서의 유효성 여부를 확인할 수 있다. 그림 15는 유효성 검사를 실시한 후의 화면이다. 이 경우에는 검증 대상이 되는 인증서를 발행한 인증기관의 인증서와 최상위 인증기관의 인증서가 추가적으로 필요하다. 만약 유효성 검사에 실패할 경우에는 오류 메시지와 함께 실패 이유가 출력된다. 실패 이유로는 다음과 같은 것들이 있다.

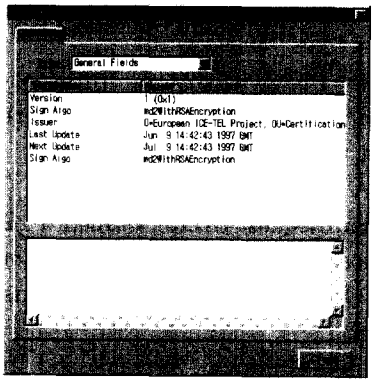
- 인증서의 유효기간 만기(또는 유효기간 이전)
- 인증서를 발행한 인증기관 인증서의 유효기간 만기(또는 유효기간 이전)
- 인증서를 발행한 인증기관의 인증서가 아님
- 인증서의 전자서명을 확인할 수 없음
- 인증기관 인증서의 전자서명을 확인할 수 없음



〔그림 15〕 인증서 유효성 확인

3. 인증서폐지목록 검증

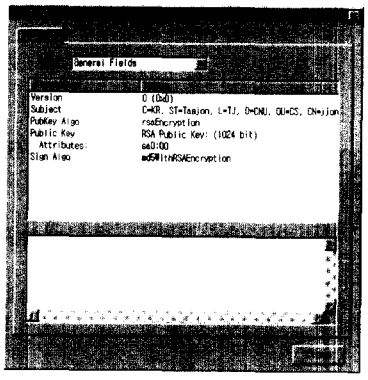
인증서폐지목록에 대한 시험은 인증서에 대한 시험과 마찬가지로 인증서폐지목록이 표준을 준수하지 않은 경우에는 시험도구에서 오류 메시지를 출력한다. 또한 인증서폐지목록이 표준을 준수한 올바른 인증서일 경우에는 그림 16과 같이 내용을 볼 수 있으며, 인증서와 마찬가지로 각 필드를 클릭하여 그 내용을 확인할 수 있다. 그리고 인증서와 마찬가지로 유효성 검사를 실시할 수 있다.



〔그림 16〕 인증서폐지목록 내용 보기

4. 인증서신청양식 검증

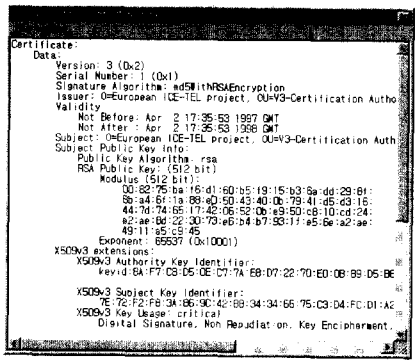
인증서신청양식이 표준을 준수하지 않은 경우에는 시험도구에서 오류 메시지를 출력한다. 또한 인증서신청양식이 표준을 준수한 올바른 인증서일 경우에는 그림 17과 같이 내용을 볼 수 있으며, 인증서와 마찬가지로 각 필드를 클릭하여 그 내용을 확인할 수 있다. 그리고 인증서와 마찬가지로 유효성 검사를 실시할 수 있다.



〔그림 17〕 인증서 신청양식 보기

5. 인증서 인코딩 변환

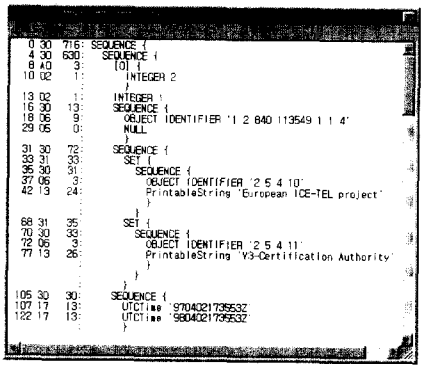
시험도구는 어떤 방식으로 인코딩된 인증서이던간에 확장자에 의해서 인코딩 방식을 인식하여 그 내용을 텍스트 형식으로 보여준다. 그림 18에서 시험도구는 DER로 인코딩된 인증서를 읽어 그 내용을 텍스트 형식으로 보여준다.



〔그림 18〕 DER 인코딩된 인증서 보기

인코딩 방식을 변환하기 위해서는 File-Save As 메뉴를 이용하여 파일 이름을 지정하면, 시험도구에서 인코딩 방식을 변환하여 파일로 저장한다.

또한 텍스트 형식의 인증서를 ASN.1 형식으로 볼 수 있다. 그림 19는 그림 18의 인증서를 ASN.1 형식으로 본 화면이다.



〔그림 19〕 ASN.1 형식으로 인증서 보기

ASN.1 형식으로 변환은 DER에 기초한다. 즉

PEM, base64, uuencode 등으로 인코딩된 인증서를 ASN.1 형식으로 보기 위해서는 일단 이러한 형식으로 인코딩된 인증서를 디코딩하여 DER 인증서로 변환한 후에 ASN.1 형식으로 변환할 수 있다.

V. 결 론

전자서명법 및 공인인증기관 지정제도의 시행과 함께 국내에서도 활발한 인증서비스 제공이 기대되며, 이를 기반으로 한 다양한 응용 서비스가 개발될 것으로 예상된다. 인증서를 발급 및 관리하는 PKI 정보보호 제품은 인증 서비스 및 그 응용 서비스 제공에 있어서 매우 중요한 위치를 차지하고 있기 때문에 안전하고 신뢰성있는 기능을 제공해야 한다. 이를 위해서는 X.509 등 관련된 기술 표준을 정확하게 구현하는 것이 필수적이다.

PKI 정보보호 제품이 관련된 기술 표준을 적합한 방식으로 구현하였는지를 확인하기 위해서는 표준의 구현 여부를 검증할 수 있는 전문적인 도구가 필요하다. 미국 등 일부 국가에서는 자국의 표준 알고리즘 등에 대해서 이와 같은 검증을 수행할 수 있는 도구의 개발이 이미 이루어지고 있다.

본 논문에서는 PKI 정보보호 제품이 사용한 인증기술이 표준에 따라 적합하게 구현되었는지 확인할 수 있는 시험도구를 구현하였다. 시험도구는 인증기술의 표준 적합성 검증을 위해서 인증서, 인증서폐지목록 및 인증서신청양식이 표준을 따르는 정확한 포맷으로 생성되었는지 테스트하고, 이 들 각각이 관련 표준인 X.509 버전3 인증서, X.509 버전2 인증서폐지목록, PKCS#10에 따라 정확한 포맷으로 생성되었는지 테스트하고, 유효성 검사를 수행한다. 이 때 테스트에 사용되는 개수 및 파일 이름 등은 검증 수행자가 지정할 수 있도록 하였다. 또한 인증서에 대한 검증에서는 검증 수행자가 반드시 구현되어야 하는 확장필드를 지정하여 이에 대한 검증을 수행하고 확장필드의 critical 여부를 확인할 수 있도록 하였다. 또한 추가적으로 인증서의 인코딩 방식을 변환하는 기능과 인증서의 내용을 텍스트 및 ASN.1 형식으로 볼 수 있는 기능을 제공한다.

본 논문에서 구현한 시험도구를 통해 인증 서비스 사용자에게 표준에 적합하게 구현된 PKI 정보보호 제품을 통해 서비스를 제공받을 기회를 부여함으로써 전자상거래를 보다 활성화시키고, 정보화를 촉진하여 국민생활의 편익을 증진하는데 기여할 것으로 기대된다.

참 고 문 헌

[1] DOD, "Guidelines for External Certification Authority Interoperability with the Department of Defense Public Key Infrastructure Version 0.7", 1999. 4. 29

[2] DOD, "Interim External Certification Authority(IECA) X.509 Certificate Compliance Test Plan", 1999. 5. 10

[3] IETF PKIX RFC2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999. 1

[4] RSA Laboratories, "PKCS#10: Certification Request Syntax Standard", 2000. 3

[5] Bruce Schneier, "Applied Cryptography 2nd Edition", John Wilet & Sons, Inc., 1996

[6] William Stallings, "Network and Internetwork Security", Prentice Hall, 1999

[7] http://www.openssl.org

[8] http://www.cs.auckland.ac.nz/~pgut001

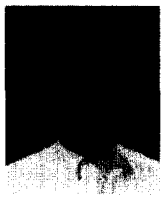
〈著者紹介〉

이 종 후 (Jung-Who Lee)
1997년 2월 : 충남대학교 컴퓨터과학과 졸업
1999년 2월 : 충남대학교 컴퓨터과학과 석사
1999년 3월 : 충남대학교 컴퓨터과학과 박사과정
관심분야 : 공개키기반구조, 무선인터넷 보안, 보안프로토콜 분석

김 충 길 (Choong-Gil Kim)
1998년 2월 : 충남대학교 물리학과 졸업
2000년 2월 : 충남대학교 컴퓨터과학과 석사
관심분야 : 공개키기반구조, 무선인터넷 보안

이 석 래 (Seok-lae Lee)

1992년 2월 : 한양대학교 전자통신공학과 졸업
1994년 2월 : 한양대학교 전자통신공학과 석사
1994년 2월~1999년 6월: LG 전자
1999년 7월~현재: 한국정보보호센터 연구원
관심분야 : 데이터 보안, 통신공학



이 재 일(Jae-il Lee)

1986년 2월 : 서울대학교 계산통계학과 졸업
1988년 2월 : 서울대학교 계산통계학과 석사
1991년 1월~1996년 6월 : 한국 IBM
1996년 7월~현재 : 한국정보보호센터 선임연구원/팀장
관심분야 : 유·무선 PKI, 전자상거래 보안

김 학 범 (Hakbeom Kim)

본 호의 "국내 정보보호제품의 표준적합성 시험과 인증체계" 저자소개 참조

류 재 철 (Jae-Cheol Ryou)

1985년 2월 : 한양대학교 산업공학과 졸업
1988년 5월 : Iowa State Univ. 전산학 석사
1990년 12월 : Northwestern Univ. 전산학 박사
1991년 2월~현재: 충남대학교 정보통신공학부 부교수
관심분야 : 인터넷 보안, 전자지불시스템