情報保護學會論文誌
第12券 第3號, 2002. 6

# 국내 PKI 시스템 평가 기준 제안

심 주 걸*, 박 택 진**, 이 철 원***, 원 동 호****

# The Proposal of Security Evaluation Criteria for PKI Systems in Korea

Joo-geol Sim*, Taek-jin Park**, Cheol-won Lee***, Dong-ho Won****

요 약

정보보호 기술의 운용에 있어서 기반기술로 작용하는 PKI 시스템의 신뢰성 확보를 위해서는 PKI 시스템에 대한 평가가 반드시 필요하나, 국제적으로 아직까지 체계적인 평가 및 인증체계가 갖춰지지 않은 것이 사실이다. 국내의 경우에도 침입차단시스템과 침입탐지시스템에 대한 평가 및 인증은 이루어지고 있으나, PKI 시스템 평가에 대한 연구는 미비한 실정이다. 이에 따라 본 논문에서는 국내 PKI 시스템에 적용할 수 있는 PKI 시스템 평가기준을 제안하고자 한다. 평가기준은 최근 정보보호 시스템 평가에 있어서 국제적인 조류에 맞춰 국제 공통 평가기준(CC)와 호환 가능성을 고려하고, 현재 진행되고 있는 국내 평가제도를 고려하여 작성하였다.

ABSTRACT

To ensure PKI systems' reliability, the security for PKI systems evaluation is required. But, unfortunately, the systematic security evaluation and certification of PKI systems is insufficient. In Korea, Firewall and intrusion detection system's security evaluation and certification has been enforced, but research of PKI systems' evaluation is insufficient. This paper provides a PKI system evaluation criteria. This paper specifies a 7 level of the functional and assurance security requirements for a PKI system. And this PKI system evaluation criteria provides a compatibility with CC(Common Criteria) and KISES(Korea Inforamtion Security Evaluation Systems).

**Keyword** : *PKI systems, evaluation, certification*

## Ⅰ. 서 론

정보통신기술의 발달로 전자적으로 처리되는 정보량이 증가함에 따라 사회 각 분야에서 구축·운영되는 공공 및 민간분야 정보통신시스템의 안전성 확보의 필요성이 증대하고 있다. 최근 발생한 Yahoo를 비롯한 CNN, 아마존닷컴 등 유명사이트들의 해킹 사건에서 알 수 있듯이 안전성이 입증되지 않은 취약한 정보보호시스템을 사용한 정보시스템 구축은 오히려 그 취약성을 증가시키는 위험성을 내포하고 있음을 의미하고 있어 정보시스템의 안전성 및 신뢰성 검증이 새삼 중요해 지고 있다. 이와 같은 정보보호 시스템의 신뢰성 확보를 위한 제도적 장치로서 미국, 캐나다, 영국, 독일 프랑스 등 선진국에서는 20여전부터 독자적인 정보보호시스템 평가·인증제도를 마련하여 정보보호시스템에 대한 평가를 해 오고 있다.[1]

또한 국내에서도 이미 1995년부터 정보보호시스템 평가와 관련된 법규의 정비 및 평가기준 제정이

* 성균관대학교 전기전자및컴퓨터공학부(juwangsan@hanmail.net)
** 영동전문대학 전자과
** 국가보안기술연구소 정보보증연구부
**** 성균관대학교 전기전자및컴퓨터공학부(dhwon@dosan.skku.ac.kr)

이루어져, 현재는 침입차단시스템과 침입탐지시스템에 대한 평가가 실시되고 있다.

한편, 여러 가지 다양한 정보보호시스템 가운데에서도 최근 가장 주목받고 있는 분야는 공개키 암호기술을 이용한 각종 정보보호 어플리케이션 부분이라고 할 수 있다. 특히 전자상거래 및 무선인터넷 기술의 발전과 함께 암호기술에 기반한 정보보호 서비스의 중요성은 더욱 강조되고 있으며, 이에 따라 공개키 암호기술 운용의 기반 기술로 작용하는 PKI 시스템의 역할 또한 커지고 있다.

특히 PKI 시스템의 구축은 국가적인 차원에서 진행되고 있는 것이 특징인데, 국내의 공인인증체계 및 정부 PKI, 미국의 연방 PKI(FPKI : Federal Public Key Infrastructure), 호주의 GPKI(Government Public Key Infrastructure) 등이 그 대표적인 예이다. 그러나 PKI 시스템은 다른 정보보호 기술에 비해서 비교적 최근에 급격히 발전한 분야로 체계적인 평가 및 인증체계가 갖추어져 있지 않다. 최근들어, 미국 IATF(Information Assurance Task Force)를 중심으로 PKI 시스템에 대한 평가기준이 마련되고, 기준에 대한 NIAP(National Information Assurance Partnership)의 승인이 완료된 바 있으며,[2] Entrust PKI 5.1이 영국으로부터 CC체계에 의하여 평가를 받은 바 있다.[3]

이에 따라 본 논문에서는 국제적인 PKI 평가추세에 보조를 맞추어 국내 관련 기술의 안전성 입증의 계기를 마련하고자 국내 PKI 시스템 평가에 적용될 수 있는 PKI 시스템 평가기준을 제안하고자 한다. 이 때, 최근 정보보호시스템 평가에 있어서 국제적인 조류에 맞추어서 CC와 최대한 호환이 가능하도록 하면서, 동시에 현재 진행되고 있는 국내 평가제도를 고려하여 평가기준을 작성하였다.

본 논문의 2, 3, 4장에서는 PKI 시스템 평가와 관련한 최근 연구활동에 대해서 살펴본다. 2장에서는 미 국방부의 CA 적합성 테스트에 대해서 살펴보고, 3장에서는 미국과 캐나다의 공인회계사 단체인 AICPA/CICA(American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants)의 CA 평가기준에 대해서 살펴본다. 그리고 4장에서는 미국 NIST(National Institute of Standards and Technology)의 CA 시스템 보호프로파일인 CIMCPP(Certificate Issuing and Management Component Protection Profile)에 대해서 살펴본다. 그리고 5장에서 본 논문에서 제안하는 PKI 시스템 평가기준에 대해서 설명하고, 마지막으로 6장에서 결론을 맺는다.

## II. DOD의 IECA X.509 인증서 적합성 테스트

### 2.1 테스트 개요

자체적인 PKI 구축에 대한 연구를 지속적으로 수행해오고 있는 미 국방부(DOD : Department of Defense)의 PKI의 특징 가운데 하나는 DOD PKI 내에서 민간 인증기관의 활동을 허용하고 있는 점이다. 즉, 외부 인증기관(IECA : Interim External Certification Authority)으로 하여금 DOD PKI 내에서 사용되는 인증서 발급 업무를 수행할 수 있도록 하고 있다.[4,5]

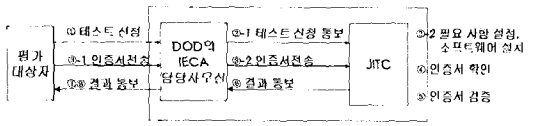
이와 같은 외부 인증기관의 수용을 위해 가장 먼저 해결해야 할 것은 상호운용성의 문제이다. 즉, 외부의 인증기관과 DOD PKI의 연동이 올바르게 이루어져야 한다. 이와 관련된 작업은 DOD 내의 JITC (Joint Interoperability Test Command)에서 주관하고 있는데, JITC에서는 IECA가 표준을 준수하는지 여부를 결정하기 위해서 IECA가 생성하는 SSL 클라이언트 인증서, 전자우편 인증서, 서버 인증서 등에 대한 테스트를 수행한다.[6] 이 테스트의 목적은 IECA가 다음과 같은 능력을 갖추었는지 평가하는 것이다.

- X.509 V3 인증서 생성 능력
- DOD PKI 중급 X.509 인증서 표준 프로파일 지원 능력
- SSL 사용자 인증서 지원 능력
- 사용자 전자우편 인증서 지원 능력
- SSL 서버 인증서 지원 능력

테스트는 JITC PKI 연구소에서 이루어지는데, 테스트에 소요되는 시간은 5일이 넘지 않으며, DOD의 가장 최신 인증서 표준 프로파일에 기준해서 이루어진다. JITC는 평가대상자들이 제출한 샘플 인증서를 분석하여 이들이 필요한 테스트 기준을 준수하는지 평가한다. 이에 대해서 보다 자세하게 살펴보면 다음과 같다.

### 2.2 테스트 절차

평가대상자들은 평가에 앞서서 JITC에서 배포하




〔그림 1〕 IECA X.509 인증서 적합성 테스트 절차

는 질문에 응답함으로서 인증기관을 운용하는데 필요한 지식과 경험을 보유하고 있음을 증명해야 한다. 실제 테스트는 DOD PKI 중급 X.509 V3 인증서 표준 프로파일의 준수 여부를 확인하는 것으로 이루어진다. 테스트를 위해서 평가대상자는 다음과 같은 사항을 만족시켜야 하며, 구체적인 평가절차는 〔그림 1〕과 같다.

- 인증서는 전자적 매체 또는 마그네틱 미디어를 통해서 ASCII Base64 인코딩 되어 전달되어야 한다.
- 평가되는 인증서는 최소한 SSL 인증서 10개와 전자우편용 인증서 10개로 이루어져야 한다.

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 전달한다. 담당 사무실에서는 이를 다시 제출 시간과 함께 JITC에 전달한다.
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.

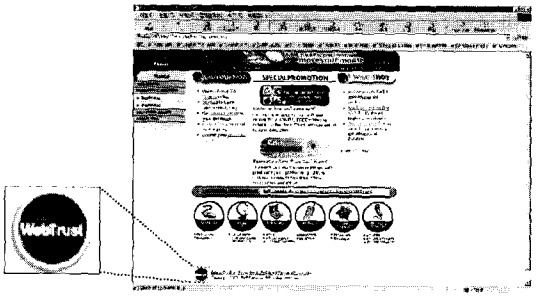
테스트가 수행되는 동안 JITC는 테스트 항목별 로그 데이터를 시간 순으로 기록한다. 이 때, 테스트 수행자와 테스트에 소요된 시간이 함께 기록된다. 만약 테스트가 연기되는 경우에는 그 사유가 기록되어야 한다. 테스트에 사용된 인증서 등의 정보는 JITC에 의해서 12개월 동안 보관되며, 12개월이 지난 후에 모든 정보는 파괴된다.

## Ⅲ. AICPA/CICA의 CA 인증 프로그램

### 3.1 AICPA/CICA의 인증 프로그램

AICPA와 CICA는 각각 미국과 캐나다의 공인 회계사 단체이다. AICPA/CICA는 전자상거래의 활성화에 대비하여 여러 가지 관련된 서비스를 제공하고 있는데, 그 가운데 하나가 WebTrust라는 신용인증 서비스이다.

WebTrust 서비스는 1999년 6월부터 제공되기 시작했는데, 이 때는 WebTrust 서비스를 신청한 웹 사이트가 AICPA/CICA에서 제시하는 웹 사이트 평가원칙 및 평가기준을 만족하는지 여부를 시험한 후, 암호 메커니즘에 의해서 보호되는 마크(〔그림 2〕 참조)를 웹 사이트에 발급하는 형태였다. 평가를 통과한 웹 사이트는 이 마크를 자신의 사이트에 게시할 수 있으며, 평가를 통과한 웹 사이트의 목록은 AICPA/CICA의 사이트에서 볼 수 있다.




〔그림 2〕 WebTrust 인증마크

AICPA/CICA의 평가는 사이트의 성격에 따라 다르게 적용되는데, 우선 B2C 사이트에 대한 평가원칙은 다음과 같다.

- 고객의 개인정보 보호(18)
- 거래의 무결성 보장(7)
- 거래정보 보호

ISP 전자상거래 사이트에 대해서는 역시 다음과 같은 3가지의 평가원칙을 적용하고 있다.

- 가용성 확보(10)
- 고객의 개인정보 보호 및 기밀정보 보호(10)
- 서비스 무결성 확보(6)

CA에 대한 평가원칙 및 평가기준에 대해서는 뒤에서 좀 더 자세하게 살펴본다.

이와 같은 평가원칙 및 평가기준에 의해서 AICPA/CICA로부터 인증 받은 웹 사이트에게는 앞에서 살펴본 인증마크가 부여되며, 미국의 인증 서비스 업체인 Verisign사로부터 SSL 서버용 인증서가 발급된다. 만약 이미 Verisign의 SSL 서버용 인증서를 사용하고 있는 곳이라면, 기존 인증서를 새로운 인증서로 대체한다. 즉, AICPA/CICA로부터 인증 받은 업체는 SSL을 이용한 보안 서비스를 제공함으로써 사용자의 개인정보 및 거래정보와 같은 기밀성 유지가 필요한 정보를 보호해야 한다.

이 때, 인증마크는 단순한 이미지로써 AICPA/CICA로부터 인증을 받지 않은 웹 사이트에서도 인증마크를 자신의 웹 페이지에 게재함으로써 마치 인증을 받은 웹 사이트로 가장하는 것이 가능하다. 이와 같은 문제의 해결을 위해서 인증마크를 클릭하면 Verisign의 웹 페이지로 연결되어 Verisign에서 관리하고 있는 인증마크 발급 업체 목록에 현재 접속하고 있는 웹 페이지가 포함되어 있는지 확인하도록 하고 있다.

### 3.2 CA 평가원칙 및 평가기준

AICPA/CICA의 CA 평가원칙은 크게 다음과 같은 3가지로 구성된다.[7]

- CA 업무 공개 : CA는 인증서 관리 업무를 포함한 CA의 주요 업무가 이루어지는 절차를 공개해야 하며, 공개된 내용에 따라 실제 업무가 진행되어야 한다. 공개된 정보는 CA로부터 인증서를 발급 받은 가입자뿐만 아니라, CA가 발급한 인증서를 이용하는 모든 사용자가 쉽게 볼 수 있도록 해야한다. 이와 같은 CA의 업무 공개는 일반적으로 인증서 정책(CP : Certificate Policy), 혹은 인증업무준칙(CPS : Certification Practice Statement)의 형태를 지닌다.
- 서비스 무결성: CA는 다음과 같은 CA의 서비스 제공과 관련된 사항을 보장할 수 있도록 효율적인 관리 시스템을 유지해야 한다.
  - 가입자가 제출한 가입자 정보에 대한 적절한 인증절차 확보
  - CA가 관리하는 키 및 인증서에 대한 무결성 확보
- CA 운영 환경 관리: CA는 다음과 같은 CA 운영 환경 유지와 관련된 사항을 보장할 수 있도록 효율적인 관리 시스템을 유지해야 한다.
  - CA 가입자와 사용자의 정보는 CP나 CPS에 의해서 허가되지 않은 기관 또는 사람의 접근으로부터 보호되어야 한다.
  - 지속적인 키 및 인증서 관리
  - CA 시스템의 무결성 유지를 위한 인가 받은 관리자에 의한 CA 시스템의 개발, 유지, 운영

이와 같은 CA 평가원칙을 적용하는데 있어서 평가 대상에게 규격화된 가이드라인을 제시하기 위해서 AICPA/CICA의 CA 인증 프로그램에서는 CA 평가원칙을 구체화한 CA 평가기준을 제시하고 있다. 이 평가기준은 CA가 자체적으로 서비스 및 시스템을 점검하는데 사용될 수 있으며, AICPA/CICA의 인가 받은 평가자가 CA를 평가하는데도 사용된다.

평가기준은 평가원칙에 따라 크게 CA 업무 공개, 서비스 무결성, CA 운영 환경 관리 등 3부분으로 구분되며, 각각의 원칙에 대해서 자세한 평가기준이 제시된다. 평가기준에서는 인증서 관리, 키 관리, CA 운영 환경 관리 등 구체적인 내용에 대해서 다루고 있다.

또한 AICPA/CICA의 평가자가 평가원칙 및 평가기준에 의해서 CA에 대한 평가를 수행하기 위해서는 CA 모델에 대한 이해가 선행되어야 한다. 이는, 경우에 따라서 CA가 키 위탁, 인증서 효력 중지 등 일부 서비스는 제공하지 않을 수 있는데, 이러한 경우에는 해당되는 서비스의 평가를 수행하지 않아야 하기 때문이다.

## Ⅳ. NIST의 CIMC PP

NIST에서는 PKI 여러 가지 요소 가운데, CA 및 RA(Registration Authority) 시스템에 대한 보호 프로파일(PP : Protection Profile)을 작성하는 연구를 진행하고 있다.[8] 이는 CC의 PP 형식

을 따르고 있으며, CC에서 제공되는 PP를 사용하며, CA 및 RA 시스템의 특성에 따라 요구사항이 추가되기도 하였다.

### 4.1 CIMC 개요

PKI는 여러 가지 다양한 요소로 구성된다. 이 가운데 CIMS(Certificate Issuing and Management System)은 인증서 및 인증서 상태정보의 발행, 폐지, 관리를 책임지는 구성요소를 뜻한다. 따라서 일반적으로 CIMS는 CA와 RA를 반드시 포함하며 그밖에 CA 및 RA의 하위 구성요소를 포함한다.

CIMC(Certificate Issuing and Management Component)는 CIMS 기능을 수행하는데 필요한 하드웨어, 소프트웨어 및 펌웨어를 의미한다. 이 때, 기온과 같은 환경적인 요소나, 정책 및 인적 관리와 같은 관리적인 요소는 CIMC에서 제외된다.

CIMC 보호 프로파일은 CIMC에 대한 보안기능 요구사항 및 보증 요구사항을 정의한다. 따라서 CIMC 보호 프로파일의 목적은 CIMC에 대한 보안 요구사항과 특정 CIMC 하위 구성요소에 대한 보안 요구사항을 규정하는 것이라고 할 수 있다. 이는 CIMC의 구성요소가 어떤 기능을 수행하느냐에 따라 관계된 CIMC의 모든 기술적인 부분을 다룬다. 이 때, CIMC PP는 CA에서 수행되는 기능과 RA에 의해서 수행되는 기능을 구별하지 않는다.[8]

CIMC를 구성하는 모든 하위 구성요소를 하나의 요소로써 식별하는 것은 CIMC PP의 보안 요구사항을 준수하는 하위 구성요소가 안전한 방법으로 동작됨을 보장하는데 도움을 준다. 또한 이를 통해서 하위 구성요소 간의 상호호환성을 확보할 수 있다.

### 4.2 CIMC 키

CIMC에서 사용되는 비밀키 및 암호키의 안전한 관리는 필수적이다. 비밀키 및 암호키의 안전한 관리를 위해 CIMC PP에서는 CIMC 내에서 사용되는 키를 키의 사용 주체에 따라 다음과 같이 구분한다.

① CIMS 개인키(personnel key) : CIMC 내에서 개개인에 의해서 사용되는 비밀키 및 암호키이다. 이 키는 사용자 인증을 위해 사용될 수 있으며, CIMC의 출력되는 정보 또는 CIMC 내에서 사용되는 정보에 전자서명을 첨부하는데 사용되거나, 정보의 암호화에 사용된다.

② 구성요소 키(component key) : 인증서 및 인증서 상태정보에 대해서 전자서명을 수행하는데 사용되는 키이다. 구성요소의 공개키쌍은 키 교환, 감사정보 및 백업정보에 대한 전자서명, 전송 및 저장되는 정보의 무결성 보장을 위해서 사용된다. 또한 구성요소의 암호키는 CIMC 정보를 암호화하는데 사용된다.

③ 인증서 소유주 비밀키(certificate subject private key) : 이 키는 CIMC에서 발행한 인증서 내에 포함되는 공개키에 대응되는 비밀키이다. 이 키는 키 복구의 목적으로 CIMC에 의해서 관리될 수 있으며, 경우에 따라 키 생성 자체가 CIMC에 의해서 이루어질 수 있다.

또한 CIMC 내에서 사용되는 키는 키의 사용 용도에 따라 다음과 같이 분류할 수 있다.

① 인증서 및 인증서 상태정보 전자서명 키(certificate and status signing keys) : 인증서와 인증서폐지목록을 비롯한 인증서 상태정보에 대해서 전자서명을 수행하는데 사용되는 비밀키이다.

② 무결성 또는 승인 인증 키(integrity or approval authentication keys) : CIMC 간, 또는 CIMC의 하위 구성요소 간의 통신 내용의 보호를 위해서 사용되는 비밀키 또는 암호키이다. 인증서 발행 및 취소를 수행하거나 승인하는 정보를 보호하는데 사용된다.

③ 범용 인증 키(general authentication keys) : 사용자, 메시지 또는 세션을 인증하는데 사용되는 비밀키 또는 암호키이다. 인증서 발행 및 취소를 승인하는데 이용되는 정보에는 사용될 수 없으나, 인증서 발행 및 취소를 요청하는 정보를 보호하는 데는 사용될 수 있다.

④ 장기 비밀키 보호 키(long term private key protection keys) : 여러 개의 세션 또는 메시지에서 사용되는 비밀키의 보호를 위해서 사용되는 비밀키 또는 암호키이다.

⑤ 장기 기밀성 키(long term confidentiality keys) : PIN 혹은 패스워드와 같은 보안 관련 정보의 기밀성 유지를 위해서 사용되는 암호키이다. 비밀키는 이 범주에 속할 수 없다.

⑥ 단기 비밀키 보호키(short term private key protection keys) : 하나의 세션 또는 메시지에서 사용되는 비밀키의 보호를 위해서 사용되는

비밀키 또는 암호키이다.

⑦ 단기 기밀성 키(short term confidentiality keys) : 키와 관련된 정보를 포함하지 않는 하나의 세션 또는 메시지를 보호하는데 사용되는 암호키이다.

### 4.3 CIMC 보안 레벨

CIMC는 폐쇄적인 환경에서부터 인터넷과 같은 개방된 환경에 이르기까지 다양한 환경을 기반으로 해서 동작한다. 또한 CIMC에서 발행한 인증서를 통해 보호되는 정보들의 중요성도 매우 다양하다. 따라서 CIMC의 보안 레벨 역시 다양해질 수 밖에 없다. 즉, 사용자는 자신이 보호하려는 정보의 중요성 및 운영환경과 관련된 공격 위협의 정보 등을 종합적으로 평가하여 자신에게 맞는 보안수준을 갖는 CIMC를 운영해야 한다. 이와 관련하여 CIMC PP에서는 CIMC의 보안 레벨을 다음과 같은 4단계로 구분한다.

#### 4.3.1 보안레벨 1

보안레벨 1은 가장 낮은 수준의 보안을 제공한다. 보안레벨 1을 만족하도록 설계된 CIMC는 공격 위협이 매우 적은 것으로 판단되는 환경에 적합하다. 보안레벨 1의 CIMC는 불법적인 접근에 의한 불법적인 공개로부터 정보를 보호하지 못한다. 보안레벨 1의 CIMC에서 사용되는 모든 암호 알고리즘은 FIPS (Federal Information Processing Standards Publications)의 승인을 받은 것이거나, FIPS로부터 추천을 받은 것이어야 하며, FIPS 140[9]의 보안레벨 1에 의해서 검증 받은 암호모듈이 사용되어야 한다. 또한 보안레벨 1의 CIMC는 최소한 다음과 같은 2가지의 직무가 요구된다. 이 2가지 직무는 각각 독립적으로 관리되어야 한다.

- 계정 관리, 키 생성, 감사 설정
- 인증서 발행 및 취소

또한 보안레벨 1의 CIMC는 국제공통평가기준(CC) EAL(Evaluation Assurance Level) 1[10]에 의해서 평가된다. 현재 보안레벨 1을 만족시키는 제품은 상용화되어 있는 상태이다.

#### 4.3.2 보안레벨 2

보안레벨 2의 CIMC는 공격 위협이 심각하지 않은 환경에 적합하며, 네트워크를 통한 대부분의 공격에 대해 방어능력이 갖추어져야 한다. 이 레벨의 CIMC는 PKI 사용자가 불법적인 행동을 하지 않는다는 가정을 필요로 하며, 보안레벨 1과 마찬가지로 다음과 같은 2가지의 직무가 요구된다. 이 2가지 직무는 각각 독립적으로 관리되어야 한다.

- 계정 관리, 키 생성, 감사 설정
- 인증서 발행 및 취소

또한 보안레벨 1의 CIMC에 비해서 강화된 부분은 감사기록 및 시스템 백업에 있어서 보다 높은 보안이 요구되며, 감사 대상이 되는 사건의 수가 많아진다는 점이다. 그리고 키를 보호하는 목적으로 사용되는 암호모듈은 FIPS 140 레벨 2에 의해서 검증되어야 한다.

또한 보안레벨 2의 CIMC는 CSPP(Guide for COTS Security Protection Profile)에 규정된 보증 요구사항에 의해서 평가된다. CSPP 보증 레벨은 기술적인 상위 수준 설계(descriptive high-level design)를 제외하고는 EAL3과 동일하며, EAL4의 문제 추적 형상관리 범위(Problem Tracking Configuration Management Coverage), 비정형 TOE 보안정책 모델(Informal TOE Security Policy Model), 결함 보고 절차(Flaw Reporting Procedure), 분석 요소의 검증(Validation of analysis Component)이 추가되었다.

#### 4.3.3 보안레벨 3

보안레벨 3의 CIMC는 어느 정도의 데이터 누출 및 무결성 저해에 대한 위협이 있는 환경에 적합하며, 추가적인 무결성 관리가 필요하다. 또한 물리적인 접근에 대한 방어대책과 CIMC의 기능이 안전하게 제공됨을 보장할 수 있는 추가적인 보증 요구사항이 포함된다. 보안레벨 3의 CIMC의 직무는 다음과 같이 3가지로 구분할 수 있다.

- 계정 관리, 키 생성, 감사 설정
- 인증서 발행 및 취소
- 감사기록 관리

보안레벨 3 CIMC는 비밀키 및 암호키 내보내기(export)와 가져오기(import)에 대해 이중화된 관리를 필요로 하며, 인증서 및 인증서 상태 정보에

대한 전자서명을 수행하는 비밀키를 관리하는 암호 모듈은 FIPS 140 레벨 3의 검증을 통과해야 한다. 또한 전자서명에 의해서 보호되어야 하는 메시지의 종류가 보안레벨 2에 비해 많다.

보안레벨 3 CIMC는 방법론적인 시험과 검사에 있어서는 EAL3, 방법론적 설계, 시험 및 검증에서는 EAL4의 보증 요구사항이 적용된다. 주로 적용되는 것은 EAL3인데, EAL3은 "회색박스" 검사에 의한 분석 및 개발자의 시험 결과 확인, 개발자의 취약성 분석 확인 등을 제공한다.

#### 4.3.4 보안레벨 4

보안레벨 4 CIMC는 데이터 누출 및 무결성 저해에 대한 위협이 매우 큰 환경에 적합하며, 보안수준이 가장 높은 경우로써 불법적인 사용자에 의한 불법적인 접근에 대한 방어대책이 필요하다. 보안레벨 4의 CIMC의 직무는 다음과 같은 4가지로 구분할 수 있다.

- 계정 관리, 키 생성
- 감사기록 관리
- 인증서 발행 및 취소
- 백업

보안레벨 4에서는 보안기능이 적합하게 기능을 수행함을 보장해야 하며, 제3자의 타임스탬핑에 의한 감사기록의 무결성 유지가 요구된다. 또한 인증서 및 인증서 상태 정보에 대한 전자서명을 수행하는 비밀키를 관리하는 암호모듈은 FIPS 140 레벨 4의 검증을 통과해야 한다. 현재 CIMC 보안레벨 4를 만족하는 CA나 RA 시스템은 존재하지 않는다.

보안레벨 4의 CIMC는 CC EAL4(방법론적인 설계, 시험 및 검증)와 EAL5(준정형 설계 및 시험)의 보증 요구사항이 적용된다. 주로 적용되는 것은 EAL4이며, EAL5는 개발자가 엄격한 개발 규칙에 기반한 공학적인 방법에 의한 최대한의 보증을 요구하며, 특화된 보안기술이 적용되어야 한다.

## V. PKI 시스템 평가기준 제안

### 5.1 개요

본 장에서는 국내 환경에 적합한 PKI 시스템 평가기준을 제안하고자 한다. 이 때, 고려한 사항으로는 다음과 같은 것들이 있다.

- 국제적인 평가기준과의 호환성 유지 : 정보보호 시스템에 대한 평가에 있어서 최근의 국제적인 추세는 CC를 적용하는 것이다. 이미 많은 국가에서 CC에 기반해서 정보보호시스템을 평가하고 있으며, CC를 적용하는 국가는 향후에도 계속해서 증가할 전망이다. 이에 따라 국내의 정보보호 시스템 평가기준 역시 CC의 수용이 필요하다. 이는 국내 정보보호 제품의 해외시장 진출에도 도움을 줄 것으로 기대된다. 그러나 국내에서 사용되는 정보보호시스템에 대해서는 국내 환경을 고려한 CC의 적용이 고려되어야 할 것이다. 따라서 최대한 CC와의 호환을 유지하면서 국내 환경을 효율적으로 적용할 수 있는 평가기준의 개발이 필요하다.
- 적용기술의 국제 표준 지원 : CC와의 호환뿐만 아니라 평가기준 내에서 적용되는 기술 역시 국제 표준을 지원해야 한다. 즉, 인증서 및 인증서 폐지목록 프로파일, 인증서 상태 확인 메커니즘, 인증서 관리 프로토콜, 전자서명 알고리즘, 해쉬 알고리즘 등의 기술을 PKI 시스템 평가기준에 적용시 이들 기술이 관련된 국제표준을 준수하도록 해야 한다.
- 국내에서 개발된 암호 알고리즘의 적용 및 보안 강도 강화 : 국내에서는 이미 독자적인 암호 알고리즘이 개발되어 정부/금융을 비롯한 여러 분야에서 사용되고 있다. 국내 CA 평가기준에서는 이와 같은 국내 암호 알고리즘을 수용함으로서 국내의 독자적인 보안체계를 구축하여 안전성을 향상시킬 수 있다. 또한 경우에 따라서는 국제적인 평가기준보다 높은 강도의 보안을 요구하여야 할 것이다.
- 국내 타 정보보호시스템 평가기준과의 일관성 유지 : 국내에서는 이미 침입차단시스템, 침입탐지 시스템 등 일부 정보보호 제품에 대한 평가 및 인증이 실시되고 있으며, 평가 대상이 되는 정보보호 제품은 계속해서 늘어날 전망이다. PKI 시스템 평가기준은 체계나 절차의 측면에서 기존 정보보호시스템 평가기준과 최대한 일관성을 유지함으로써 평가의 효율을 향상시켜야 한다.

본 장에서는 이와 같은 사항들을 고려하여 국내 환경에 적합한 PKI 시스템 평가기준을 제안하고자 한다. 평가기준은 CC와의 호환을 고려하여 NIST의 CIMCPP에 기반해서 작성되었다. 이에 따라 PKI

시스템 내에서 사용되는 키의 구분이나 직무의 분류 등은 CIMCPP를 그대로 따랐으나, 추가적인 보안 레벨을 설정하여 보다 강화된 보안을 제공하도록 하였다. 여기에 대하여, 현재 국내에서 진행되고 있는 평가체계와의 일관성을 고려하여 총 7레벨로 구성하였다. 이 과정에서 보안 기능 요구사항 및 보증 요구사항은 CIMCPP보다 더 엄격한 보안이 적용되었다.

### 5.2 PKI 시스템 보안 레벨

3장에서 살펴본 바와 같이, 현재 NIST의 CIMCPP는 보안레벨을 4단계로 구분하고 있다. 본 논문에서 제안하는 평가기준에서는 CIMCPP의 보안레벨을 그대로 수용하면서 3개의 레벨을 추가하였다.

즉, 1레벨부터 4레벨은 CIMCPP의 보안 레벨과 동일하며, 5, 6, 7레벨은 추가된 레벨이다. 국외에서 사용될 제품이나 국내 민간분야에서 사용될 제품은 평가기준 1-4레벨을 따르며, 국내 공공분야에서 사용될 제품은 보다 강화된 레벨인 5-7레벨을 따라 평가된다. 1-7레벨 모두 국내에서 사용된다는 점을 고려하여 반드시 국내에서 개발된 암호 알고리즘을 사용하도록 하였다. 따라서 CIMCPP에 의해서 평가받은 제품이라 하더라도, 국내에서 사용되기 위해서는 KCDSA, SEED, HAS-160 등의 국내에서 개발된 암호 알고리즘이 보안레벨 2 이상에서는 반드시 지원되어야 한다. 또한, 추가적인 보안 레벨을 정의하는데 있어서 필요한 암호 알고리즘 및 암호모듈을 승인하는 기관과 인증서 및 인증서폐지목록 프로파일, OCSP 프로파일을 정의하는 기관은 각각 '승인기관'과 '담당기관'으로 서술한다. 이 때, 업무의 특성상, 이 두 기관은 국가기관에서 담당하는 것이 적절하다. 5, 6, 7레벨의 보다 자세한 사항은 다음과 같다.

#### 5.2.1 보안레벨 5

- 개요 : PKI 시스템 보안레벨 5는 데이터 누출 및 무결성 저해에 대한 위협이 매우 큰 환경에 적합하며, 보안레벨 4에 비해 직무 요구사항을 강화함으로써, 외부로부터의 공격뿐만 아니라 내부에서의 시스템 오용 및 남용에 대한 보안 강도를 향상시켰다.
- 암호 알고리즘 및 모듈 : 승인기관으로부터 보안레벨 4에 해당하는 인증을 받은 암호 알고리즘 및 암호 모듈이 적용된다. 또한 국내 담당기관에서 정의한 인증서 및 인증서폐지목록 프로파일 및 인증서 상태정보 프로파일을 지원해야 한다. 이 때, 어떤 알고리즘이 사용되는지 여부는 공개되어야 한다.
- 직무 요구사항 : 기존의 계정 관리 및 키 생성/ 감사기록 관리/ 인증서 발행 및 취소/ 백업 직무 요구사항 가운에서 백업으로부터 키의 백업 직무를 분리하였다. 이를 위해서 CIMCPP에서 정의된 4가지 직무인 Administrator, Operator, Officer, Auditor 외에 Key Backup Admin 직무를 추가하였고, 이 들 각각이 5가지 직무 요구사항을 독립적으로 수행하도록 하였다. 또한 Administrator은 반드시 복수로 존재하여야 한다.
- 보증 요구사항 : 방법론적인 설계, 시험 및 검증에 대해서는 EAL4 적용, 준정형화된 설계 및 시험에 대해서는 EAL5를 적용하되, 주로 적용되는 것은 EAL4이며, EAL5는 개발자가 엄격한 개발 규칙에 기반한 공학적인 방법에 의한 최대한의 보증을 요구하며, 특화된 보안기술이 적용되어야 한다.

#### 5.2.2 보안레벨 6

- 개요 : 보안레벨 6은 보안레벨 5에 비해서 강력한 보안기능을 제공하며, PKI 시스템을 이용하는 환경에서 취급되는 정보의 중요도가 높은 경우에 적합하다. 즉, 정부기관 등에서 주요 정보를 다루는 경우에 적합하다.
- 암호 알고리즘 및 모듈 : 승인기관으로부터 보안레벨 4에 해당하는 인증을 받은 암호 알고리즘 및 암호 모듈이 적용된다. 또한 국내 담당기관에서 정의한 인증서 및 인증서폐지목록 프로파일 및 인증서 상태정보 프로파일을 지원해야 한다. 또한 사용되는 알고리즘은 비공개로 유지되어야 한다. 이를 위해서 보안레벨 5까지에서 사용되는 알고리즘 외에 다른 알고리즘이 사용될 수 있다.
- 직무 요구사항 : 보안레벨 5에서의 5가지 직무 외에 register 직무가 추가되어 인증서 신청 요청의 처리와 인증서 신청 요청에 대한 승인 직무를 분리하였다. 또한 보안레벨5와 마찬가지로 Administrator는 반드시 복수로 존재해야 한다.
- 보증 요구사항: EAL5의 보증 요구사항이 적용된다.

#### 5.2.3 보안레벨 7

- 개요 : 보안 수준이 가장 높은 경우에 해당하며, 데이터 누출 및 무결성 저해에 대한 위협이 매우 크고 취급되는 정보가 고도의 국가 기밀과 같이 중요도가 매우 높은 환경에 적합하다.
- 암호 알고리즘 및 모듈 : 승인기관으로부터 보안레벨 4 이상의 인증을 받은 암호 알고리즘 및 암호 모듈이 적용된다. 또한 국내 담당기관에서 정의한 인증서 및 인증서폐지목록 프로파일 및 인증서 상태정보 프로파일을 지원해야 한다. 또한 사용되는 알고리즘에 대한 비밀 유지가 이루어져야 한다. 이를 위해서 보안레벨 6까지에서 사용되는 알고리즘 외에 다른 알고리즘이 사용될 수 있다.
- 직무 요구사항 : 보안레벨 6과 동일하다.
- 보증 요구사항 : EAL7의 보증 요구사항을 고려할 수 있으나, 국내의 수준을 고려하여 EAL6의 보증 요구사항을 적용한다.
- 강화된 접근통제 적용 : 데이터 출력, 키 생성, 비밀키 로드, 암호키 저장, 비밀키 및 암호키 제거, 인증서 및 인증서 상태정보 접근, 사용자 정보 접근 등에서 보안레벨 1-6에 비해서 강화된 접근통제가 적용된다.

### 5.3 보안 기능 요구사항

CIMC PP는 TOE(Target of Evaluation)에 부과되는 일련의 보안 요구사항을 정의한다. TOE는 범용 운영체제가 설치된 정보시스템으로, CIMC TOE는 네트워크로부터 독립적으로 동작하는 시스템일 수도 있으며, 네트워크 환경에서 동작하는 여러 가지 구성요소의 집합일 수도 있다. CIMC TOE는 하나 이상의 프로세서, 여러 명의 사용자에 의해서 공유되는 주변기기, 저장장치 및 정보 등을 허용한다. 각각의 사용자에게는 유일한 신분(identity)이 할당된다. CIMC PP에 기술된 모든 보안 요구사항 및 대응하는 보호 프로파일의 목록은 〔표 1〕과 같다.

본 논문에서 제안하는 CA 평가기준의 보안 기능 요구사항은 CIMC PP를 기반으로 작성하였으나, 몇 가지 사항이 추가되었다. 추가된 요구사항은 모두 CA 보안레벨 5, 6, 7에만 해당한다. 추가된 사항에 대한 설명은 다음과 같다.

- FCS_COP_CIMC.1(확장된 암호 운영) : 보안레벨 5 이상의 PKI 시스템은 반드시 다음과 같은 국내 표준 암호 알고리즘을 지원해야 한다.
  - 전자서명 알고리즘: KCDSA
  - 해쉬 알고리즘: HAS-160
  - 비밀키 암호 알고리즘 : SEED
- FCS_COP_CIMC.2(고도화된 암호 운영) : 보안레벨 6 이상의 PKI 시스템은 시스템 내에서 사용되는 암호 알고리즘을 비밀로 유지해야 한다.
- FDP_ACF_CIMC.1(확장된 접근통제에 기반한 암호 속성) : 보안레벨 7의 PKI 시스템의 경우, 〔표 2〕와 같이 접근통제가 적용되어야 한다.
- FMT_MOF_CIMC.7(확장된 보안기능 동작 관리) : 보안레벨 5의 CA는 다음과 같은 요구사항을 만족해야 한다.
  - 키의 생성을 담당하는 직무와 키의 관리를 담당하는 직무는 분리되어야 한다.
  - 키의 백업 및 복원은 키의 생성 및 관리와 분리되어 수행되어야 한다.
  - 인증서 신청 요청을 처리하는 부분과 인증서를 생성 및 발급하는 부분은 분리되어야 한다.
  - 사용자 정보 관리는 인증서 및 키 관리와 분리되어 수행되어야 한다.
- FMT_MOF_CIMC.8(고도화된 보안기능 동작 관리) : 보안레벨 5의 CA는 다음과 같은 요구사항을 만족해야 한다.
  - 키의 생성을 담당하는 직무와 키의 관리를 담당하는 직무는 분리되어야 한다.
  - 키의 백업 및 복원은 키의 생성 및 관리와 분리되어 수행되어야 한다.
  - 인증서 신청 요청을 처리하는 부분과 인증서를 생성 및 발급하는 부분, 인증서 신청 요청을 승인하는 부분은 모두 독립적으로 수행되어야 한다.
  - 사용자 정보 관리는 인증서 및 키 관리와 분리되어 수행되어야 한다.
- FMT_MOT_CIMC.9(고도화된 인증서 프로파일 관리) : 국내 담당기관에서 정의한 인증서 프로파일을 준용해야 한다.
- FMT_MOT_CIMC.10(고도화된 인증서폐지목록 프로파일 관리) : 국내 담당기관에서 정의한 인증서폐지목록 프로파일을 준용해야 한다.
- FMT_MOT_CIMC.11(인증서 상태 정보 관리) : 국내 담당기관에서 인정하는 인증서 상태 정보 관리 메커니즘을 준용해야 한다.

〔표 1〕 CA 보안기능 요구사항(계속)

| 기능 요구사항 | | CIMC PP 항목 |
|---|---|---|
| FAU_GEN.1 | 감사정보 생성 | 보안감사 |
| FAU_GEN.2 | 사용자 신원 확인 | 보안감사 |
| FAU_SAR.1 | 감사 검증 | 보안감사 |
| FAU_SAR.3 | 선택적 감사 검증 | 보안감사 |
| FAU_SEL.1 | 선택적 감사 | 보안감사 |
| FAU_STG.1 | 감사 추적 저장장치 보호 | 보안감사 |
| FAU_STG.4 | 감사정보 손실 방어 | 보안감사 |
| FCO_NRO_CIMC.3 | 원본 증명 | 원격 정보 입력 및 내보내기 |
| FCO_NRO_CIMC.4 | 고도화된 원본 증명 | 원격 정보 입력 및 내보내기 |
| FCO_CKM.1 | 암호키 생성 | 키 관리 |
| FCO_CKM.4 | 암호키 파괴 | 키 관리 |
| FCO_CKM_CIMC.5 | CIMC 비밀키 및 암호키 초기화 | 키 관리 |
| FCS_COP.1 | 암호 운영 | 암호모듈 |
| FCS_COP_CIMC.1 | 확장된 암호 운영 | 암호모듈 |
| FCS_COP_CIMC.2 | 고도화된 암호 운영 | 암호모듈 |
| FDP_ACC.1 | 접근통제에 기반한 암호 속성 | 접근통제 |
| FDP_ACF_CIMC.1 | 확장된 접근통제에 기반한 암호 속성 | 접근통제 |
| FDP_ACF.1 | 접근통제에 기반한 암호 속성 | 접근통제 |
| FDP_ACF_CIMC.2 | 사용자 비밀키 기밀성 유지 | 키 관리 |
| FDP_ACF_CIMC.4 | 사용자 암호키 기밀성 유지 | 키 관리 |
| FDP_CIMC_BKP.1 | CIMC 백업 및 복구 | 백업 및 복구 |
| FDP_CIMC_BKP.2 | 확장된 CIMC 백업 및 복구 | 백업 및 복구 |
| FDP_CIMC_BKP.3 | 고도화된 CIMC 백업 및 복구 | 백업 및 복구 |
| FDP_CIMC_CERT.1 | 인증서 생성 | 인증서 등록 |
| FDP_CIMC_CRL.1 | 인증서 취소 | 인증서 취소 |
| FDP_CIMC_CSE.1 | 인증서 상태 공개 | 원격 정보 입력 및 내보내기 |
| FDP_CIMC_OCSP.1 | 기본 응답 검증 | 인증서 취소 |
| FDP_CIMC_POP.1 | 키 관리 키를 위한 소유 증명 | 인증서 등록 |
| FDP_ETC_CIMC.4 | 사용자 비밀키 및 암호키 내보내기 | 키 관리 |
| FDP_ETC_CIMC.5 | 확장된 사용자 비밀키 및 암호키 내보내기 | 키 관리 |
| FDP_ITT.4 | 기본적인 내부 전송 보호 | 원격 정보 입력 및 내보내기 |
| FDP_SDI_CIMC.4 | 저장된 공개키의 무결성 모니터링 | 키 관리 |
| FDP_UCT.1 | 기본 정보 교환 기밀성 | 원격 정보 입력 및 내보내기 |
| FIA_AFL.1 | 인증 실패 처리 | 신원 확인 및 인증 |
| FIA_ATD.1 | 사용자 속성 정의 | 신원 확인 및 인증 |
| FIA_UAU.1 | 인증 시각 | 신원 확인 및 인증 |
| FIA_UID.1 | 신원 확인 시각 | 신원 확인 및 인증 |
| FIA_USB.1 | 사용자와 인증서 소유주 바인딩 | 신원 확인 및 인증 |
| FMT_MOF.1 | 보안기능 동작 관리 | 직무 |
| FMT_MOF_CIMC.7 | 확장된 보안기능 동작 관리 | 직무 |
| FMT_MOF_CIMC.8 | 고도화된 보안기능 동작 관리 | 직무 |

〔표 1〕 CA 보안기능 요구사항

| 기능 요구사항 | | CIMC PP 항목 |
|---|---|---|
| FMT_MOT_CIMC.2 | 인증서 프로파일 관리 | 인증서 프로파일 관리 |
| FMT_MOT_CIMC.3 | 확장된 인증서 프로파일 관리 | 인증서 프로파일 관리 |
| FMT_MOT_CIMC.9 | 고도화된 인증서 프로파일 관리 | 인증서 프로파일 관리 |
| FMT_MOT_CIMC.4 | 인증서폐지목록 프로파일 관리 | 인증서폐지목록 프로파일 관리 |
| FMT_MOT_CIMC.5 | 확장된 인증서폐지목록 프로파일 관리 | 인증서폐지목록 프로파일 관리 |
| FMT_MOT_CIMC.10 | 고도화된 인증서폐지목록 프로파일 관리 | 인증서폐지목록 프로파일 관리 |
| FMT_MOT_CIMC.6 | OCSP 프로파일 관리 | OCSP 프로파일 관리 |
| FMT_MOT_CIMC.11 | 인증서 상태 정보 관리 | 인증서 상태 정보 관리 |
| FMT_MSA.1 | 보안 속성 관리 | 직무 |
| FMT_MSA.2 | 안전한 보안 속성 | 직무 |
| FMT_MSA.1 | 정적 속성 초기화 | 직무 |
| FMT_MTD.1 | TSF 정보 관리 | 직무 |
| FMT_MTD_CIMC.4 | TSF 비밀키 기밀성 유지 | 키 관리 |
| FMT_MTD_CIMC.5 | TSF 암호키 기밀성 유지 | 키 관리 |
| FMT_MTD_CIMC.6 | TSF 비밀키 및 암호키 내보내기 | 키 관리 |
| FMT_MTD_CIMC.7 | 확장된 TSF 비밀키 및 암호키 내보내기 | 키 관리 |
| FMT_SMR.2 | 보안 직무에 대한 제한 | 직무 |
| FPT_AMT.1 | 가상 머신 테스팅 | 자체 테스트 |
| FPT_CIMC_TSP.1 | 감사기록 전자서명 사건 | 보안감사 |
| FPT_CIMC_TSP.2 | 감사기록 타임스탬프 사건 | 보안감사 |
| FPT_ITC.1 | TSF 간 기밀성 유지 | 원격 정보 입력 및 내보내기 |
| FPT_ITT.1 | 기본 내부 TSF 전송 보호 | 원격 정보 입력 및 내보내기 |
| FPT_STM.1 | 신뢰할 수 있는 타임스탬프 | 보안감사 |
| FPT_TST_CIMC.2 | 소프트웨어/펌웨어 무결성 검사 | 자체 테스트 |
| FPT_TST_CIMC.3 | 소프트웨어/펌웨어 로드 검사 | 자체 테스트 |
| FTP_TRP.1 | 신뢰할 수 있는 구간 | 신원 확인 및 인증 |

〔표 2〕 강화된 접근통제 방안

| | |
|---|---|
| 데이터 export 및 출력 | ■ 기밀정보의 export 또는 출력은 Administrator와 Officer의 요청에 의해서만 가능하다. |
| 키 생성 | ■ component 키 생성은 복수의 Administrator에 의해서 이루어지거나, Administrator와 Officer의 공동조작에 의해서 이루어져야 한다. |
| 비밀키 로드 | ■ 비밀키를 암호모듈로 로드하는 것은 복수의 Administrator에 이루어지거나, Administrator와 Officer의 공동조작에 의해서만 가능하다. |
| 암호키 저장 | ■ CIMC 암호키를 암호모듈로 로드할 수 있는 권한은 복수의 ADministrator로 제한된다. |
| 비밀키 및 암호키 파괴 | ■ CIMC 비밀키 및 암호키를 초기화 할 수 있는 권한은 복수의 Administrator, Officer, Operator, Auditor로 제한된다. |
| 인증서 및 인증서 상태 정보 접근 | ■ TOE 내에 저장된 인증서 및 인증서폐지목록, 인증서 상태 정보에 대한 접근은 Administrator로 제한된다. |
| 사용자 정보 접근 | ■ 인증서를 제외한 인증서 소유주 정보에 대한 접근은 Officer으로 제한된다. |

## 5.4 보증 요구사항

### 5.4.1 보안레벨 1 보증 요구사항

CIMC 보안레벨 1에 대한 보증요구사항은 CC EAL1에 대한 요구사항이며, 기능 검사와 TOE 보안기능 평가 강도가 추가된다. 이와 같은 요구사항은CIMC 기능이 CIMC PP를 준수하며, 식별된 위협에 대해 적절한 방어수단을 제공함을 증명하는데 사용된다.

### 5.4.2 보안레벨 2 보증 요구사항

CIMC 보안레벨 2에 대한 보증 요구사항은 CSPP - Guidelines for COTS Security Protection Profiles에 기술된다.[11] CSPP 보증 레벨은 기술적 상위수준의 디자인을 제외하고는 EAL3와 동일하다. 또한 다음과 같은 사항에 대해서는 EAL4의 보증 요구사항이 적용된다.

- 문제 추적 형상관리 범위
- 비정형 TOE 보안정책 모델
- 결함 보고 절차
- 분석 요소의 검증

CSPP의 보증 요구사항은 또한 다음과 같은 사항에 대해서는 제3자의 독립적인 분석을 포함한다.

- 시스템 생성 및 설치 절차의 인가
- 시스템 보안 상태에 대한 검증
- 업체 기능 검사의 견본에 대한 검증
- 명확한 취약성 검색
- 독립적인 기능 검사

### 5.4.3 보안레벨 3 보증 요구사항

CIMC 보안레벨 3에 대한 보증 요구사항은 EAL3

〔표 3〕 보안레벨 6 보증 요구사항

| 보증 클래스 | 컴포넌트 ID | 컴포넌트 타이틀 | EAL 레벨 |
|---|---|---|---|
| 형상관리 | ACM_AUT.1 | 부분적인 형상관리 자동화 | EAL5 |
| | ACM_CAP.4 | 생성 지원 및 인수 절차 | EAL5 |
| | ACM_SCP.3 | 개발도구의 형상관리 범위 | EAL5 |
| 배포와 운영 | ADO_DEL.2 | 변경의 감지 | EAL5 |
| | ADO_IGS.1 | 설치, 생성, 시동 절차 | EAL5 |
| 개발 | ADV_FSP.3 | 준정형 기능명세 | EAL5 |
| | ADV_HLD.4 | 준정형 상위수준 설계 | EAL5 |
| | ADV_IMP.2 | TSF 구현 | EAL5 |
| | ADV_INT.1 | 모듈화 | EAL5 |
| | ADV_LLD.1 | 하위수준 설계 설명 | EAL5 |
| | ADV_RCR.2 | 준정형 일치성 시연 | EAL5 |
| | ADV_SPM.3 | 정형 TOE 보안정책 모델 | EAL5 |
| 설명 | AGD_ADM.1 | 관리자 설명서 | EAL5 |
| | AGD_USR.1 | 사용자 설명서 | EAL5 |
| 생명주기 지원 | ALC_DVS.1 | 보안대책의 식별 | EAL5 |
| | ALC_LCD.2 | 표준화된 생명주기 모델 | EAL5 |
| | ALD_TAT.2 | 구현 표준에 순응 | EAL5 |
| 시험 | ATE_COV.2 | 대상 범위 분석 | EAL5 |
| | ATE_DPT.2 | 하위수준 설계 시험 | EAL5 |
| | ATE_FUN.1 | 기능 시험 | EAL5 |
| | ATE_IND.2 | 표본에 대한 독립적인 시험 | EAL5 |
| 취약성 평가 | AVA_CCA.1 | 비밀채널 분석 | EAL5 |
| | AVA_MSU.2 | 분석의 검증 | EAL5 |
| | AVA_SOF.1 | TOE 보안기능 강도의 평가 | EAL5 |
| | AVA_VLA.3 | 중간의 내성 | EAL5 |

과 EAL4로부터 추출된다.

#### 5.4.4 보안레벨 4 보증 요구사항

CIMC 보안레벨 4에 대한 보증 요구사항은 EAL3 과 EAL4로부터 추출된다.

#### 5.4.5 보안레벨 5 보증 요구사항

보안레벨 5의 보증 요구사항은 보안레벨 4의 보증 요구사항과 동일하다.

#### 5.4.6 보안레벨 6 보증 요구사항

PKI 시스템 보안레벨 6에 대한 보증 요구사항은 EAL5로부터 추출되며, 이를 요약하면 〔표 3〕과 같다. PKI 시스템 보안레벨 6은 개발자가 엄격한 상업적 개발 관계에 기초하여 보안공학을 적용함으로써 얻을 수 있는 최대의 보증을 제공한다. 엄격한 상업적 개발관계란 전문적인 보안공학 기법을 완화시켜 응용하는 것을 말한다. 그러나 TOE는 EAL5 보증을 달성할 의도로 설계되고 개발되어야 한다. EAL5에서 엄격한 개발에 기인하는 추가 비용은 많지 않다.

그러므로 EAL5는 개발자나 사용자가 계획된 개발에 따라 높은 수준의 독립적인 보증을 요구하며, 전문적인 보안공학기술에 따르는 부당한 비용의 부담 없이 엄격한 개발 접근방법을 사용할 것을 요구하는 경우에 적용 가능하다.

#### 5.4.7 보안레벨 7 보증 요구사항

CA 시스템 보안레벨 7에 대한 보증 요구사항은 EAL6으로부터 추출되며, 이를 요약하면 〔표 4〕와 같다. EAL6은 개발자가 중대한 위험으로부터 높은 가치의 자산을 보호하기 위한 뛰어난 TOE를 생산

〔표 4〕 보안레벨 7 보증 요구사항

| 보증 클래스 | 컴포넌트 ID | 컴포넌트 타이틀 | EAL 레벨 |
|---|---|---|---|
| 형상관리 | ACM_AUT.2 | 완전한 형상관리 자동화 | EAL6 |
| | ACM_CAP.4 | 향상된 지원 | EAL6 |
| | ACM_SCP.3 | 개발도구의 형상관리 범위 | EAL6 |
| 배포와 운영 | ADO_DEL.2 | 변경의 감지 | EAL6 |
| | ADO_IGS.1 | 설치, 생성, 시동 절차 | EAL6 |
| 개발 | ADV_FSP.3 | 준정형 기능명세 | EAL6 |
| | ADV_HLD.4 | 준정형 상위수준 설명 | EAL6 |
| | ADV_IMP.3 | TSF의 구조화된 구현 | EAL6 |
| | ADV_INT.2 | 복잡성 제거 | EAL6 |
| | ADV_LLD.2 | 준정형 하위수준 설계 | EAL6 |
| | ADV_RCR.2 | 준정형 일치성 시연 | EAL6 |
| | ADV_SPM.3 | 정형 TOE 보안정책 모델 | EAL6 |
| 설명 | AGD_ADM.1 | 관리자 설명서 | EAL6 |
| | AGD_USR.1 | 사용자 설명서 | EAL6 |
| 생명주기 지원 | ALC_DVS.2 | 보안대책의 충분함 | EAL6 |
| | ALC_LCD.2 | 표준화된 생명주기 모델 | EAL6 |
| | ALD_TAT.3 | 모든 부분에서 구현 표준에 순응 | EAL6 |
| 시험 | ATE_COV.3 | 시험범위의 엄밀한 분석 | EAL6 |
| | ATE_DPT.2 | 하위수준 설계 시험 | EAL6 |
| | ATE_FUN.2 | 순서화된 기능시험 | EAL6 |
| | ATE_IND.2 | 표본에 대한 독립적인 시험 | EAL6 |
| 취약성 평가 | AVA_CCA.2 | 체계적인 비밀채널 분석 | EAL6 |
| | AVA_MSU.3 | 안전하지 않은 상태의 분석 및 시험 | EAL6 |
| | AVA_SOF.1 | TOE 보안기능 강도의 평가 | EAL6 |
| | AVA_VLA.4 | 고도의 내성 | EAL6 |

하기 위하여 엄격한 개발환경에서 보안공학 기법을 응용하여 얻을 수 있는 높은 보증을 제공한다.

그러므로 EAL6은 보호되는 자산의 가치가 추가적인 비용을 정당화할 수 있는 높은 위험 상황에서 사용하기 위한 안전한 보안 TOE를 개발할 경우에 적용 가능하다.

## Ⅳ. 결 론

정보보호시스템에 대한 신뢰성 향상이라는 측면에서 정보보호시스템 평가 및 인증의 중요성은 강조되고 있다. 또한 최근에는 국가간에 CC 기반의 상호인정협정이 체결되는 등 평가와 관련된 많은 연구가 이루어지고 있으며, 국내에서의 관심 또한 높아지고 있다.

현재 국내에서는 침입차단시스템과 침입탐지시스템에 대한 평가가 이루어지고 있다. 그러나 최근 들어 급격한 성장을 거듭하고 있는 PKI 시스템의 중요성을 고려할 때, PKI 시스템에 대한 평가가 시급히 이루어져야 한다. 특히 전자서명법에 따른 공인인증기관이 운영되고 있는 국내 현황을 고려하면, PKI 시스템 평가의 필요성은 더욱 커지고 있다. 또한 정부, 군 등 국가 안보에 결정적인 영향을 줄 수 있는 정보를 취급하는 환경에서는 PKI 시스템에 대한 평가가 필수적이라고 할 수 있다.

이에 본 논문에서는 국내 환경에 적합한 PKI 시스템 평가기준을 제안하였다. 제안된 평가기준은 국제적인 평가기준인 CC에 기반한 CA 평가기준인 NIST의 CIMCPP와 최대한 호환을 유지하면서, 현재 국내에서 시행되고 있는 평가체계를 반영하였다. [표 5]는 NIST의 CIMCPP와 본 논문에서 제안한 PKI 시스템 평가기준을 비교한 결과이다. 제안한 평가기준은 7단계의 보안레벨로 구성되는데, 1-4레벨은 CIMCPP와 동일하게 하여 국내에서 평가된 PKI 시스템이 외국에서도 인정받을 수 있도록 하였으며, 여기에 국내에서 개발된 암호 알고리즘을 반드시 사용하도록 하였다. 5-7레벨에서는 보안 요구사항을 강화하고, 승인기관으로부터 허가된 안전한 암호 알고리즘을 사용하도록 하여 국내 공공분야에서 안전하고 신뢰할 수 있는 보안 서비스를 제공할 수 있도

[표 5] CIMCPP와 제안된 PKI 시스템 평가기준의 비교

| | NIST CIMCPP | 제안 CA평가기준 |
|---|---|---|
| 보 안 레 벨 | 총 4 단계 | 총 7 단계 |
| 기능 요구사항 | 15개 영역 59개 항목 | - 15개 영역 65개 항목<br>- 접근통제, 직무의 분리 등에서 CIMCPP에 비해서 강화됨 |
| 보증 요구사항 | EAL1 - EAL7 적용 | - EAL1 - EAL7 적용<br>- 보안레벨 5, 6, 7에 대한 보증요구사항 추가 |
| 키 의 구 분 | - 사용 주체에 따라 4개로 구분<br>- 키의 용도에 따라 7개로 구분 | - 사용 주체에 따라 4개로 구분<br>- 키의 용도에 따라 7개로 구분 |
| 기 준 내 에 서 기 술 된 표 준 | - X.509 v3 인증서<br>- X.509 v2 CRL<br>- IETF OCSP | - X.509 v3 인증서<br>- X.509 v2 CRL<br>- IETF OCSP<br>- KCDSA, SEED, HAS-160 |
| 기반 평가기준 | CC | CC/CIMCPP |
| 장 점 | - 암호모듈 평가에 FIPS140-1 적용 가능<br>- 국내에서 평가받은 제품을 수정 없이 외국에서도 평가 받을 수 있음<br>- 디렉토리에 대한 평가기준까지 제시 | - 국내 독자적인 평가기준 적용으로 보다 보안성이 강화된 PKI 시스템을 국내 환경에 적용 가능<br>- 관련 국내 기술 표준의 활용폭 확대 |
| 단 점 | - 관련된 국내 기술 표준의 활용폭 축소 및 국내 기술 표준을 적용치 못함으로서 국내 환경에 부적합한 부분 발생.<br>- 고도화된 국가 기밀과 같은 중요 정보 취급에 부적합한 부분 발생 | - 현재 암호모듈 평가에 적용할 수 있는 국내 기준이 없어 외국의 평가기준을 준용하거나, 별도의 국내 평가 기준 제정이 필요<br>- 외국에서 CC에 의해 평가 받은 제품이 국내 진출시 별도의 평가를 다시 받아야 하는 번거로움 |

록 구성한 것이 가장 큰 특징이다.

평가 및 인증제도는 정보보호시스템의 안전성과 신뢰성을 보증하고 우수한 정보보호시스템 개발을 유도한다. 이제까지는 국가별로 각 국가 내에서 사용될 정보보호시스템에 대한 평가 및 인증을 수행하는 경우가 대부분이었으나, 최근의 흐름은 CC를 기반으로 하여 각 국에서 실시한 정보보호시스템에 대한 평가결과를 상호인정 하려 하고 있으며, 이러한 협정에 참여하는 국가도 계속해서 증가하고 있다. 이를 통해 한 국가에서 평가 및 인증을 받은 제품이 다른 국가에서 또 다시 평가를 받지 않게 됨으로서 평가의 효율을 높이고 정보보호 제품의 국제적인 시장 확대에 도움을 줄 것으로 기대되고 있다.

이와 같은 정보보호시스템에 대한 국제상호인정협정이 확산됨에 따라 국내에서도 적절한 대처가 요구되고 있다. 이에 따라 본 논문에서는 현재 가장 중요한 정보보호 제품의 하나로 인식되고 있는 PKI 제품에 대한 평가기준을 CC에 기반하여 작성하는 동시에, 국내의 독특한 환경을 적절히 적용하였다. 이를 통해 국제적인 조류에 효율적으로 대응하고, 국내 정보보호시스템의 품질을 향상시키는데 도움이 될 것으로 기대된다.

## 참 고 문 헌


[1] 이경구, "국제공통평가기준 기반의 상호인정협정 대응", 정보보호뉴스 1월호, 통권40호, 한국정보보호센터.

[2] http://niap.nist.gov/cc-scheme/PP-Registry.html

[3] http://www.cesg.gov/assurance/iacs/itsec/cpl

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

[5] 이종후, 김충길, 류재철, "암호기술 표준 적합성 검증", 2001년도 한국통신정보보호학회 영남지부 학술발표회논문집, 2001. 2.

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

[7] WebTrust Program for Certification Authorities, AICPA/CICA, 2000. 8.

[8] NIST, "Certificate Issuing and Management Components Protection Profile", 2000. 9.

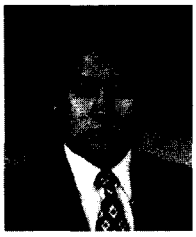
[9] NIST, "FIPS PUB 140-1 Security Requirements for Cryptographic Modules", 1994. 1

[10] Common Criteria Version 2.1, 1999. 8.

[11] NIST, CSPP - Guidelines for COTS Security Protection Profiles Version 1.0, 1999.12.

## 〈著者紹介〉

**심 주 걸 (Joo-geol Sim) 종신회원**
1979년 : 중앙대학교 전자공학과 졸업
1991년 : 건국대학교 전자공학과 석사
2000년 : 성균관대학교 전기전자 및 컴퓨터공학부 박사과정 수료
2000년~현재 국가보안기술연구소 전문위원
〈관심분야〉 정보보안정책, 보안평가인증, 암호이론



**박 택 진 (Taek-jin Park)**
1985년 서울산업대학교 전자공학과 졸업
1990년 한양대학교 전자공학과 석사
1998년 KAIST/성균관대학교 전기전자 및 컴퓨터공학과 박사과정 수료
1993년~현재 영동전문대학 전자과 조교수
〈관심분야 〉 정보보호 및 암호

**이 철 원 (Cheol-won Lee)**
1987년 : 충남대학교 수학과(이학사)
1989년 : 중앙대학교 전자계산학과(이학석사)
2001년 : 아주대학교 컴퓨터공학과 박사과정 수료
1989년~1996년 한국전자통신연구원 선임연구원
1996년~2000년 한국정보보호센터 선임연구원/통신모델링 과제책임자
2000년~현재 ETRI부설 국가보안기술연구소 팀장
관심분야 : 컴퓨터 및 네트워크 보안, 정보통신기반보호,
정보보호시스템 평가기준

**원 동 호 (Dong-ho Won) 종신회원**
성균관대학교 전자공학과 졸업(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 공경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국무총리실 국가정보화 추진위원회 자문위원
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1999년~2001년 : 성균관대학교 전기전자 및 컴퓨터공학부 학부장
1999년~2001년 : 성균관대학교 정보통신대학원 원장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터공학부 교수
1999년~현재 : 한국정보보호학회 수석 부회장
2000년~현재 : 정보통신부 지정 정보보호인증기술연구센터 센터장
〈관심분야〉 암호이론, 정보이론, 공개키 기반구조