정보보증을 위한 국방PKI 구축 방안에 관한 연구

김종문, 남길현

국방대학교, 전산정보학과

A Study on the Development of Korea Defense PKI for Information Assurance

Jong-Mun Kim, Kil-Hyun Nam

Department of Computer & Information Science, National Defense University

요 약

현재 국방부는 국방 정보 통신망에서 소통되는 정보에 대한 기밀성 및 무결성을 보장하고, 접근통제, 사용자 식별 및 인증, 부인봉쇄 등의 보안서비스를 제공하기 위한 국방 인증체계 구축 사업을 추진하고 있다. 본 논문은 미 국방부의 미 국방 PKI를 연구하고, 현재 우리 군에서 추진하고 있는 국방 인증체계 구축 노력에 대한 문제점을 분석하여 앞으로 우리 군이 국방 인증체계 구축을 위해 추진해 나가야 할 방향을 제시하였다.

I. 서 론

IT기술의 발전과 함께 국방영역에서도 과학화, 정보화를 달성하기 위해 국방전산망을 중심으로 사무자동화, 국방자원관리체계, 전자메일, 국방 EDI, 웹 서비스 등 다양한 형태로 운영 중에 있으며, C4I체계를 비롯한 수많은 정보체계들의 구축이 활발히 추진되고 있다.

그러나 정보화가 급진전됨에 따라 파생되는 정보화 역기능 즉, 정보의 변조, 도청, 오남용 및 개인 프라이버시 침해 등의 부작용이 심각한 문제점으로 지적되고 있다. 정보시스템 의존도가 점점 더 높아짐에 따라 정보화의 역기능으로 인해 입을 수 있는 피해는 기하급수적으로 커지게 되는데, 이러한 피해를 차단하거나 최소화할 수 있는 정보보호 체계의 구축이 시급히 요구되고 있다.

이러한 정보보호 체계로서의 공개키 기반구조(Public Key Infrastructure)가 금융기관을 중심으로 한 인터넷 뱅킹, 전자상거래, 전자복권, 전자정부 구현 등 정보보호가 중요시되고 있는 분야에서 폭넓게 활용되고 있다. 또한 미 국방부에서도 전 세계적으로 주둔하고 있는 미군 정보체계의 정보보호를 위해 미 국방 PKI 체계를 구축·운용·진화시키고 있으며, 우리 국방부에서도 국방 인증체계 구축사업을 추진하고 있다.

본 논문은 미 국방부의 미 국방 PKI를 연구하고, 현재 우리 군에서 추진하고 있는 국방 인증체계 구축 노력에 대한 문제점을 분석하여 앞으로 우리 군이 국방 인증체계 구축을 위해 추진해 나가야 할 방향을 제시함으로써 타 공공기관이나 정부기관도 PKI 구축에 참조할 수 있도록 하고자 한다.

II. 공개키 기반구조(PKI)

공개키 기반구조(PKI)란 공개키 암호기술을 이용한 인증방법을 구현하기 위한 기술적·제도적 기반을 의미한다. 즉, 비밀키의 기밀성과 공개키의 가용성을 전제조건으로 가상 공간상의 전자문서, 전자거래 등 관련 전자 업무에서의 당사자 신분확인 기능, 전자서명을 비롯한 전자업무 내용의 정보보호 및 무결성 기능, 전자 행위에 대한 부인봉쇄 등의 기능을 수행할 수 있도록 하는 기반구조이다.

1. PKI 구성요소

PKI는 인증서의 발급, 사용 및 취소와 관련된 서비스를 통하여 기밀성, 무결성, 접근제어, 인증, 부인 봉쇄의 보안서비스를 제공하며, 인증기관, 등록기관, 디렉토리 서비스, 사용자 등의 요소로 구성된다.

- 인증기관 : 인증기관은 인증정책을 수립하고, 인증서 및 인증서 효력정지 및 폐기목록을 관리하며, 다른 CA와 상호 인증을 지원한다.
- 등록기관 : 사용자와 CA의 중간위치에서 사용자의 인증서 요구를 받고 이를 확인한 후, CA에게 인증서 발급을 요청하고, 발급된 인증서를 사용자에게 전달하는 역할을 한다
- 디렉토리 서비스 : 디렉토리 서비스는

PKI 관련 정보인 인증서와 사용자 관련정보, 상호 인증서 쌍, 인증서 효력정지 및 폐기목록 등을 저장 및 검색하는 장소로서 응용분야에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다.

• 사용자(User, Client, Application) : PKI 내에서 사용자의 의미는 사람뿐만 아니라 사람이 이용하는 장비 및 응용프로그램 등 시스템 모두를 의미한다. 이 사용자는 인증서 생성 및 취소를 요구하며, 인증경로 검증, 인증서 활용(전자서명), 디렉토리 서버로부터 인증서 및 인증서 효력정지, 폐기목록을 획득하여 활용한다.

2. PKI 프로세스

PKI는 사용자에게 안전한 서비스를 제공하기 위하여 서로 정확하게 동작되어야 하는 여러 프로세스들로 구성되어 있다. 이러한 프로세스들은 등록, 인증서 요청, 키 생성, 인증서 및 토큰 생성, 배달, 키 복구, 키 갱신, 파기, 정책작성, 행정지원, PKI 관련 부가 프로세스(백업, 타임스탬프, 공증인 서비스 등), 책임추적, 위험요소 제거 등이 있다.

III. 한·미 국방 PKI 분석

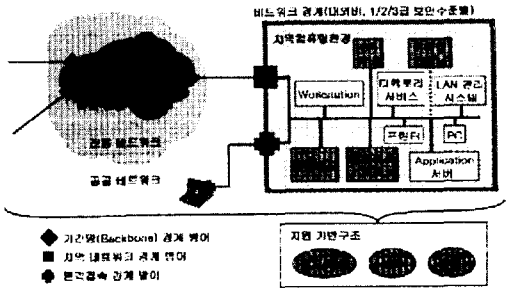
1. 미 국방 PKI

1) 정보보증 및 종심방어

미 국방 정보 보증 프로그램(DIAP) 2000 년도 보고서는 *"정보 우세(IS : Information Superiority)는 현대 전투에 대한 우리의 비젼의 기저에 위치하며, 정보보증(IA : Information Assurance)은 이러한 우세를 달성하고 유지하는데 필수적이다. 정보보증은 Joint Vision 2020의 핵심부분이며, 정보, 지휘 통제 및 전장 인식 기능을 합동 및 연합작전으로 통합하는 능력이다"* 라고 정보우세를 위한 정보보증을 강조하고 있다

미 국방성의 정보보증 전략은 독립된 하나의 요소만으로 적절한 보증이 불가능하다고 인식하고, 다양한 강도 및 보증수준을 가진 방어 계층들을 배치하는 종심방어 개념을 적용하고 있다. 이러한 종심방어 계층은 예방 및 차단이 실패한 경우 연쇄적인 침해를 차단할 수 있게 하며, 그 계층들은 **컴퓨팅 환경의 방어**, **네트워크 및 기반구조의 방어**, **공격 탐지· 경고·대응**, **키관리 기반구조 서비스**로 분류된다.

미 국방부는 정보보증을 위한 기술적 전략으로 종심방어 개념을 적용하고 있으며, PKI는 종심방어 전략을 지원하는 핵심적인 기반구조로서 작용한다.



<그림 1> 종심방어 개념

2) 인증서 보증 수준

미 국방부는 X.509 인증서 정책 문서에서 인증서 보증수준을 **Class 2**, **Class 3**, **Class 3H**, **Class 4**, **Class 5**로 구분하여 정의하였으며, 이러한 공개키 인증서의 보증 수준은 가입자를 자신의 공개키 및 권한과 묶어주는 신뢰의 정도이며, 인적·물리적·절차적·기술적 보안 통제들이 인증서 보증 수준에 영향을 미친다.

3) 현재의 미 국방 PKI

① FORTEZZA 기반 Class 4 PKI

미군은 1990년대 전반에 국방 전문 체계(DMS)의 보안을 위해 GOTS 기술을 사용하는 FORTEZZA 기반 PKI 체계를 구축하였다. 여기에서는 인증서를 저장하기 위한 토큰으로 FORTEZZA 하드웨어 토큰(PCMCIA장치)을 사용하고 있다. 최초 X.509 v1 인증서를 지원하였으며 현재는 X.509 v3를 지원하면서 현재까지 계속 사용되고 있다.

② Class 3 PKI

미군은 기밀은 아니지만 민감한(SBU) 정보에 대한 보호를 위해 민간부문에서 만들어진 기술들을 전자적인 업무처리에 투입하는 것이 미 국방부의 작전 및 임무수행에 엄청난 이익을 줄 것이라고 인식하였다. 미 국방부는 상용기술에 의존하는 Medium Assurance PKI 및 일련의 어플리케이션 초기 프로그램들을 구축해 봄으로써 급속하게 진화하는 민간PKI 기술들을 평가하기로 결정하였고, 이러한 초기사업들의 성공을 기초로 하여, Class 3 PKI Release 2.0이 2000년 7월에 운용승인을 받았다. 현재는 Class 3 PKI Release 3.0이 운영되고 있다. 여기에서는 CAC라 불리는 스마트카드를 인증서를 담기위한 기본 토큰으로 사용하고 있다.

4) 미 국방 목표 PKI(Class 4 PKI)

미 국방 목표 PKI는 비 비화망(NIPRNet : Non-classified IP Router Network) 및 비화망(SIPRNet : Secret IP Router Network) 모두를 지원하려고 하고 있다. 지속적으로, 현재 미 국

방 Class 3 PKI 및 FORTEZZA 기반 Class 4 PKI에 의해 지원되는 어플리케이션들은 목표 PKI로 전환할 것이다. 미 국방 목표 PKI는 다음과 같은 특징을 갖는다 : **강화된 보안, 광범위한 운영적 지원, 상호 운용성, 확장성, 표준 기반, 투명성, 진화적 변경, 모듈화 된 디자인, 단일 (Class 4) 보증 수준**

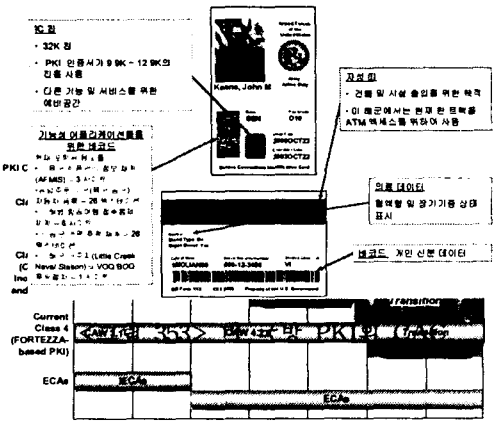
5) 미 국방 목표 PKI 추진 일정

최근 C3I 국방 차관보 정책에서 발표된 것처럼 미 국방 PKI는 현재의 Class 3 PKI 서비스 기능들을 기반으로 그 기능 위에 Class 4 요구사항들을 지원할 수 있도록 구현될 것이다. 미 국방 PKI가 진화를 계속하는 동안, 현존 PKI 기능들은 효과적인 전환을 용이하게 하기 위해 <그림 2>와 같이 일정기간동안 병행 운용될 것이다.

6) 미 국방 PKI 토큰

토큰은 가입자들의 개인 키 및 인증서를 저장하고, 디지털 서명과 같은 암호학적 기능들을 수행하기 위하여 사용되어진다. 미 국방부는 다양한 방식의 인증토큰에 대한 검토를 수행하였으며, 신원 및 부가 정보의 기록 등 활용성의 장점 때문에 스마트 카드 기술을 기반으로 한 국방 공통 접근카드(CAC : Common Access Card)를 기본 가입자 토큰으로 결정하였다(<그림 3> 참조).

CAC는 Class 3 및 목표 Class 4 인증서를 위



<그림 2> PKI 진화를 위한 일정 요약

한 기본적인 토큰 플랫폼이며, 이 인증서들은 모든 현역 장병, 일부 예비역 및 군무원, 인가된 계약자들이 사용한다.

7) PKI 프로그램 관리 사무국 운영

NSA는 1999년 8월 9일 발행된 C3I 국방 차관보의 정책문서에 따라 미 국방 PKI 프로그램 관리 사무국(미 국방 PKI PMO)를 설립하였으며, NSA가 프로그램 관리자(PM)를, DISA가 프로그램 부 관리자(DPM)를 맡고 있으며, 자원관리, 기술, 공보, 프로그램 집행을 담당하는 참모를 두고 있다.

PKI PMO는 NSA, DISA, 각 군 및 기관들의 PKI 대표자들, 합참, DIAP, 그리고 PKI PMO가 요구하는 부서들과의 조정을 수행한다. PKI PMO는 정보기관, 연방 PKI 및 NATO등과 같은 국방부 외부 PKI와의 조정활동도 수행한다.

PKI PMO는 이러한 조정활동을 위하여 업무 워킹그룹(Business Working Group), 인증서 정책 관리 워킹그룹(CPMWG), 기술 워킹그룹(Technical Working Group)을 이용한다.

2. 한국군 국방 PKI 추진체계 문제점 분석

1) 국방 PKI 추진 실태

국방 정보 통신망은 대외 망과 단절된 독립된 망으로 운영되고 있으나 자료유출 및 위·변조 등의 위협요소가 상존하고 있으며, 유통된 전자문서 및 자료에 대한 기밀성, 무결성 및 부인봉쇄 등의 보안 서비스를 제공하지 못하고 있다. 국방부에서는 이러한 문제점을 극복하고 정보의 안전성 및 신뢰성을 확보하기 위한 방안으로 공개키 기술을 사용하는 기반구조를 구축하려는 노력이 진행되고 있다. 본 절에서는 우리 군의 PKI 체계 구축을 위한 노력과 미 국방부의 추진실태를 비교하면서 우리 군의 PKI체계 구축을 위한 노력의 문제점들을 파악하고자 한다.

2) 국방 PKI 추진체계 문제점 분석

① 이원화 된 PKI 체계 구축 노력

우리 군의 국방 인증체계 구축은 국방 정보화 전략회의에서 의결된 '국방 정보화 추진 10대 프로젝트'에 포함되어 추진되고 있다. 이 사업은 현재 세부 개념연구가 진행되고 있다.

그러나 이러한 국방 인증체계 구축에 대한 논의가 있기 훨씬 이전에 육군 전술 C4I체계 구축 사업과 함께 C4I의 보안체계에 대한 연구가 추진되어 왔으며, 그 결과 PCMCIA 카드를 기본 토큰으로 사용하는 PKI를 시제품을 완성해 놓은 상태이다.

국방 인증체계 구축 사업은 미군의 Class 3 PKI를 모델로 하고 있으며, 육군 전술 C4I용 PCMCIA 카드 기반 PKI는 미군의 FORTEZZA 기반 Class 4 PKI를 모델로 하여 추진되고 있다. 이상과 같이 국방부를 위한 PKI는 서로 비슷한 기술 및 기반구조를 사용하는 체계를 서로 다른 목적을 가지고 이원화되어 추진되고 있는 실정이다.

② 상호운용성 및 기술변화를 고려하지 않은 체계 개발

미 국방 PKI가 현재는 이원화 된 체계를 갖추고 있지만, 주목해야 할 부분은 <그림 2>에서와 같이 2006년까지 미 국방 PKI는 이 두 체계를 통

합하여 국방 전체에 단일화된 인증체계가 구축하도록 계획되어 있다. 미 국방 목표 PKI 체계는 Class 3 PKI를 기반으로 그 기능 및 인증수준을 강화시킨 Class 4 PKI이다. 이렇게 미 국방 PKI 통합이 추진되고 있는 배경은 가장먼저 상호운용성 보장 및 IT기술 변화에 적응을 위한 상업 기술 및 표준 적용 측면이고, 그 외에도 개발·발전(진화)·유지보수를 위한 비용절감, 운용 인력의 감축, 사용자의 불편(사용교육/사용환경등과 관련) 감소 등의 많은 실질적인 이유들이 존재하고 있다. 결과적으로, 현재의 미 국방 Class 3 PKI는 미 국방 목표 PKI로 진화하는 것이며, 현재의 미 국방 FORTEZZA 기반 Class 4 PKI는 점차 사라지는 체계라 할 수 있을 것이다.

이상과 같은 미 국방 PKI 체계의 현재 및 미래의 진화 및 상용 IT 기술의 발전을 고려할 때, 우리 군의 이원화된 PKI 체계 구축 노력은 비용 및 상호운용성 보장 측면에서 걸림돌이 될 것으로 예상되며, 반드시 통합되고 단일화된 체계구축이 되어야 할 것이다.

③ 정책 및 제도적 지원 부족

미 국방 PKI가 C3I 국방 차관보의 주도하에 NSA 및 DISA와 같은 전문연구기관에게 PKI 프로그램 책임을 부여하고, 전 국방부 차원의 워킹그룹(업무, 인증서정책관리, 기술)이 운영되면서 체계구축 및 진화를 관리해 나가고 있는 반면, 우리 군의 국방 인증체계 추진조직은 극소수 실무자 수준에서 이루어지고 있다.

IV. 국방 인증체계 추진방안

1. 국방 목표 인증체계 요구 특징

국방 목표 인증체계는 다음과 같은 특징을 갖도록 구현되어야 한다.

- 국방 내 단일 인증체계
- 단일 보증수준 인증서 제공
- 상업 기술 및 표준에 기반
- 보안 서비스 제공 : 사용자 식별 및 인증, 데이터 기밀성, 데이터 무결성, 접근통제, 부인봉쇄
- 광범위한 지원(업무/체계/어플리케이션)
- 상호 운용성 보장(NPKI, GPKI, 타 체계)
- 확장 가능성 / 모듈화
- 진화적, 지속적 발전
- 진화시 사용자에 대한 투명성 제공

2. 정책 및 조직 정비

1) 국방 인증체계 구축 및 진화를 관리하기 위한 조직 설치

우리 군의 규모, 국방 인증체계의 규모, 군 인력구조, 그리고 국방 인증체계 외에도 더 중요한 임무들이 존재함을 고려할 때, 미군의 PKI PMO과 대등한 수준의 기구를 갖는 것은 사실상 불가능하며, 그럴 필요성도 없을 것이다.

본 논문에서는 국방 인증체계구축 시에는 국방 인증체계 사업단(가칭)을 신설하여 체계구축을 추진하고, 일단 초기구축이 완료되면 이 조직을 '국방 인증센터(가칭)'로 재조직할 것을 제안한다. 국방 인증센터는 인증센터 운영을 위한 편성 외에 기존의 국방 인증체계 사업단을 축소하여 국방 인증체계 진화업무를 담당할 조직(가칭 '**국방 인증체계 관리과**')이 편성되어야 한다. 인증센터의 장은 국방 인증체계 프로그램 관리자로서의 임무를 겸하며, '국방 인증체계 관리과'에서는 국방 인증체계의 유지 및 진화와 관련된 정책설정, 문서화 등의 PMO 기능을 수행해야 한다. 그러나 이 조직이 기술적 부분까지 담당하기에는 인력운용 및 기술수준 측면에서 부적합할 것이다. 따라서 상용 기술 및 표준 연구를 포함한 각종 기술적인 부분은 적절한 외부 기관과 협력하여 임무를 수행할 수 있도록 한다.

2) 국방 인증체계 관련 평가 및 승인기관 지정

국방 인증체계의 토큰, 인증기관 및 등록기관용 어플리케이션 및 장비, 그리고 국방 인증체계를 활용하는 어플리케이션 및 장비들은 암호모듈들을 탑재하여 보안기능을 제공하게 된다. 보안의 강도는 알고리즘의 강도에 의해 결정되지만, 아무리 강한 알고리즘이라 할지라도 구현방법에 따라 예기치 못한 취약점이 발생할 수 있기 때문에 알고리즘을 포함한 암호모듈, 제품, 그리고 어플리케이션 및 키관리 체계 등은 반드시 능력을 갖춘 기관에 의해 평가되고 승인을 받아야 한다.

국방 인증체계에서 사용할 각종 암호모듈을 탑재한 제품 및 어플리케이션들에 대한 시험 및 승인은 보안업무 시행규칙에 준해서 신뢰성 있는 기관에 의해 이루어져야 한다.

3. 국방 인증체계의 단계화 구축

국방 인증체계는 구축 초기에 모든 보안기능을 제공하도록 계획하는 것은 적절하지 않으며, IT 기술 및 표준의 발전을 고려할 때 지속적으로 진화되어야 하는 체계이다. 또한 국방 인증체계는 보안서비스를 제공하는 기반체계이며, 실질적인 보안의 구현은 이 체계를 활용하는 어플리케이션들에서 구현되어야 하는데 국방 내에서 사용 및 구축되고 있는 모든 체계들을 한꺼번에 공개키 기반기술을 갖추도록 변경하는 것은 불가능한 일이다. 따라서 국방 인증체계는 진화적 접근법을 사용하여 지속적으로 추진되어야 한다.

이러한 진화적 접근법은 크게 '**국방 인증체계 성능의 진화**'와 '**국방 응용체계/어플리케이션의 진화**'로 구분되어 추진되어야 한다. 국방 인증체계 성능의 진화는 국방 인증체계 관리과에서 진화단계를 설정하고 단계별로 추진되어야 하며, 국방 응용체계/어플리케이션의 진화는 정보화 기획

실 차원에서 전략/전술 C4I, 사무자동화, E-mail, 웹서버 등 각종 체계/이플리케이션들이 국방 인증체계를 활용하도록 강력하게 추진되어야 한다.

V. 결 론

본 논문에서는 현재 국방부에서 추진되고 있는 국방 인증체계 구축 사업을 미 국방 PKI와의 비교 분석을 통해 문제점들을 도출하고, 앞으로 구축될 국방 PKI의 발전방안에 대하여 제안하였다. 현재 이원화 추진되고 있는 국방 인증체계와 육군 전술 C4I용 PCMCIA 카드 기반의 PKI는 반드시 통합되어야 하며, 상업 기술 및 표준을 사용하는 단일화된 인증체계로 구축되어야 한다. 또한 이렇게 상업기반의 체계 구성요소들은 반드시 시험 및 승인 기관을 지정하여 검증을 거쳐야 하며, 이렇게 구축된 인증체계는 IT 기술 발전 및 위협의 증가를 고려하여 지속적으로 진화할 수 있도록 체계진화를 관리할 수 있는 조직이 설치 및 운용되어야 한다.

참고문헌

[1] 남길현외 7인, "국방전자정보인증체계 구축 방안 연구", 국방부, 2001년 9월

[2] DoD, "X.509 Certificate Policy for the United States Department of Defense", version 6.0, May. 2002.

[3] DoD, "Public Key Infrastructure Roadmap for the Department of Defense", version 5.0, Nov. 2000.

[4] DoD, "Public Key Infrastructure Implementation Plan for the Department of Defense", version 3.1, Dec. 2000.

[5] DoD, "Department of Defense Target Public Key Infrastructure Operational Requirements Document", version 51, Aug. 2001.

[6] DoD, "Operational Security Doctrine for the FORTEZZA User PCMCIA Card", Nov. 2001.