□ 研 究 論 文 □

韓國國防經營分析學會誌
第36卷 第1號, 2010. 4. 30.

# PKI 인증기반 전장관리체계 웹 연동에 관한 연구

## (A Study on Sharing Web Application between Battlefield Management System based on PKI Authentication)

김 영 성(Young Sung, Kim)*, 이 윤 호(Yun Ho, Lee)**,이 수 진(Soo Jin, Lee)***

초 록

전장관리체계 상호간의 자원 공유를 위한 웹 연동은 정보우위 달성을 위해 매우 중요한 요소이다. 하지만 전장관리체계의 인증체계는 각 군의 체계 구축 계획에 의거 개별적으로 추진됨에 따라 인증서를 상호 획득하고 검증을 수행할 수 있는 기능이 고려되지 않았다. 이러한 문제로 체계 상호간 웹 연동을 통한 정보 공유가 제한될 뿐만 아니라 타 체계 사용을 위하여 별도의 네트워크 및 단말기를 구성해야하는 비효율적 임무 수행을 초래하게 되었다. 본 논문에서는 이를 개선하기 위한 타 체계 사용자 인증서 획득 및 검증 알고리즘을 제안한다. 제안하는 알고리즘을 전장관리체계에 실제 적용하여 KJCCS 연동망을 통해 KJCCS · 육 · 해 · 공군 전술 C4I 체계 상호간 인증서 획득을 통한 타 체계 웹 접속이 가능함을 실험을 통해 확인한다.

ABSTRACT

Interworking Web Application to share the resource between Battlefield Management Systems(BMS) is critical issues for accomplishment of information superior. However, authentication system of BMS differ from each other because of having the independent plan for system build. This problem causes inefficiency such as the information insufficiency owing to not share web application and the need of additional laptops. To solve the problem, in this paper, we propose the improved certificate acquisition and verification algorithm for the user of different BMS. By testing the proposed algorithm appling to the real field, we verify the performance of proposed method.

**Keywords : Battle Management System, PKI, MPKI, Authentication, Certificate, Web Application**

**논문접수일 : 2010년 3월 18일 논문게재확정일 : 2010년 4월 13일**

* 육군 제 7군단 정보체계지원실

** 국방대학교 전산정보학과 박사과정

*** 국방대학교 전산정보학과 교수

## 1. 서 론

현재의 네트워크 환경은 인터넷 기술을 근간으로 하는 인트라넷의 증가와 함께 같은 목적을 가지는 기관, 기업 그리고 학교 등이 서로 하나의 네트워크를 구성하여 사용하고 있다. 하지만 이러한 네트워크 환경에서 무엇보다도 상대방 자원의 공유에 있어서 일차 수단이 되는 것이 송·수신자가 정당한지 확인한 후에 서비스를 제공해주는 인증이라 할 수 있겠다. 이러한 인증 방법에는 여러 가지 가 존재하지만 현재의 네트워크 분산 환경에 적합한 정보환경을 제공하는 것이 공개키기반구조(Public Key Infrastructure : PKI)이다.

PKI는 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 공개키 인증서(Public Key Certificate)를 제공한다. 인증서는 모두가 신뢰할 수 있는 제 3자(인증기관)의 서명문으로 사용자의 공개키에 대한 신뢰성을 확인시켜주는 역할을 수행하며, 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 구성되어 있다. 이러한 PKI는 전자서명, 암호화, 식별 및 인증 등과 같은 다양한 정보보호 서비스를 효율적으로 구현하는데 공통적으로 활용될 수 있는 기반을 제공하고 있다.

우리 군도 '05년 국방인증체계(Military Public Key Infrastructure : MPKI)를 구축하여 국방 인력 및 체계를 대상으로 공개키 인증서 및 관련 정보를 발급, 제공, 관리함으로써, 임무 및 목적에 따라 구축되는 국방정보체계에 필수적으로 요구되는 무결성, 기밀성, 인증, 부인방지, 가용성 등의 정보보호 기능 구현을 통합적으로 지원하고 있다.

그러나 이러한 PKI를 적용한 국방인증체계라 하더라도 이를 일반적인 국방정보체계와는 차별화된 특성을 가지는 전장관리체계에 직접적으로 적용하기에는 많은 어려움이 따른다. 전장관리체계는 미래 전장 개념의 군사력 건설 방향에 부합되도록 지휘통제체계(C4I), 감시정찰체계(Information Surveillance Reconnoiter : ISR) 및 정밀타격 체계 같은 전력요소에 정보기술 능력을 부가하여, 통합성 및 지능화를 발휘할 수 있도록 운용하는 통합 및 상호운용성 중심 네트워크 체계 구축을 목표로 구축되어 왔지만, 전장관리 각 체계별로 사업을 추진하여 전력화하였고, 전력화 초기에는 각 체계 간 통합인증을 고려하지 않았기 때문에 동일한 인증시스템이 수평적으로 운용되고 체계별로 접속환경이 상이하여 체계 간 상호인증이 제한 되었다. 또한 각 체계의 인증서버 고정으로 인한 인증서 획득 알고리즘 한계의 문제점이 있다. 뿐만 아니라 합동 지휘통제 체계(Korea Joint Command& Control System : KJCCS)를 포함한 해·공군 전술 C4I는 웹 방식으로 개발되었으나 육군 전술 C4I의 경우 웹보다는 CS체계(클라이언트-서버) 중심으로 구축 및 운용되고 있음으로 시스템 자체적으로 타체계와의 연동에 대한 제한사항을 가지고 있다.

이러한 문제를 해결하고, KJCCS 및 육·해·공군 전술 C4I 체계 간의 원활한 체계 연동과 비밀문서 유통을 보장하기 위해서는 전장관리체계에 적합한 인증체계에 대한 연구가 반드시 필요하며, 각 전장관리체계 간에 웹 연동을 위한 체계접속에 대한 표준화 및 상호 운용성 보장 방안에 대한 연구가 진행되어야만 한다.

본 논문의 구성은 다음과 같다. 2장에서는 전장관리체계, PKI 및 국방인증체계에 대해 기존의 연구들을 고찰·분석하고, 3장에서는 전장관리체계에서의 인증체계 구성과 운영개념을 분석하고, 문제점을 도출한다. 4장에서는 도출된 문제점을 바탕으로 전장관리체계간 상호인증을 통해 웹 연동을 위한 인증서 획득 알고리즘을 제시한다. 5장에서는 제안된 인증서 획득 알고리즘의 적용 가능성을 검증하기 위해 실제 구성환경에서 실시한 운영시험 결과 및 분석내용을 기술하고, 마지막으로 6장에서 결론을 맺고자 한다.

## 2. 관련연구

### 2.1 전장관리체계

전장관리체계는 미래 전장 개념의 군사력 건설 방향에 부합되도록 지휘통제체계(C4I), 감시정찰체계 및 정밀타격체계(Precision Guided Munitions : PGM) 같은 전력요소에 정보기술 능력을 부가하여, 통합성 및 지능화를 발휘할 수 있도록 운용하는 네트워크 중심의 체계 구축을 목표로 하고 있다.

우리 군은 컴퓨터 기술과 전자장비의 급속한 발달로 각종 전장감시체계(ISR)와 정밀타격체계를 지휘통제체계(C4)와 직접 연결하여 실시간으로 전장상황을 종합하고, 타격 우선순위를 정하는 등의 전술지휘를 수행하기 위한 전장관리체계를 구축 및 운영하고 있으며, 이는 현대의 전쟁수행 개념에 있어 필수적이라고 할 수 있다.

앞으로의 전쟁은 전장을 가시화하기 위한 다양한 형태의 정보를 제대 간, 기능 간, 지역 간, 시간적으로 통합하여 보다 정확하고 빠르게 전파하고 공유하기 위한 새로운 형태의 속도전으로서 데이터와의 전쟁이 될 것이다. 또한 다량의 수집된 정보를 신속히 융합하여야 하며, 신뢰할 수 있는 정보를 생산, 공유하여 신속히 의사를 결정해야 통합전투력 발휘로 전투시너지 효과를 얻을 수 있다. 이러한 목적을 달성하기 위해 국방에 구축한 전장관리체계는 <표 1>과 같이 전력화하여 운영 중에 있다. 전장관리체계의 범주 및 기능은 <표 2>와 같다.

〈표 1〉 전장관리체계 전력화 시기

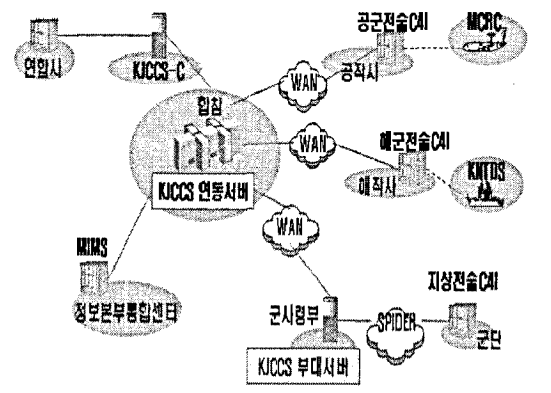
| 체계명 | KJCCS | 육군 전술C4I | 해군 전술C4I | 공군 전술C4I |
|---|---|---|---|---|
| 전력화시기 | '08.1 | '07.12 | '07.8 | '07.6 |

〈표 2〉 전략/전술 C4I 체계별 범주 및 기능

| 구 분 | 주 요 기 능 |
|---|---|
| 합동지휘 통제체계 (KJCCS) | 작전사급 이상제대 합동작전용 지휘통제체계 |
| 육군전술 C4I체계 (ATCIS) | 군단급 이하 전술제대 전투수행 절차 자동화 |
| 해군전술 C4I체계 (KNCCS) | 작전사급 이하 전술제대 전투 수행절차 자동화 |
| 공군전술 C4I체계 (AFCCS) | 작전사급 이하 전술제대 전투 수행절차 자동화 |

#### 2.1.1 합동지휘통제체계(KJCCS)

KJCCS는 <그림 1>에서 보는 바와 같이 합참을 중심으로 각 군 작전사급 10개 부대와 수방사, 특전사, 항작사, 유도탄 사령부에 설치하여 전·평시 합동작전 수행을 위한 지휘통제 수단으로 운용된다. KJCCS는 타 체계 연동 및 체계 내 사용자 입력을 통하여 체계에 입력되는 모든 데이터를 통합 관리하기 위한 통합 데이터 서버와 타 체계와의 연동을 전담 수행하는 연동서버를 구축하여 KJCCS 연동망을 이용해 군사정보통합처리체계(Military Intelligence Management System : MIMS), 각 군 전술C4I 체계와 연동하여 필요한




〈그림 1〉 전장관리체계 구성

정보를 제공받을 수 있으며, 보안상의 목적으로 접근통제를 위해 정적 라우팅 정책(Static Routing Table Policy)을 통해 최소한의 검증된 IP에 대해서만 통신을 허용하고 있다. [1][6]

### 2.1.2 육군 전술지휘정보체계

전장에서 피·아 상황을 가시화하고, 실시간 탐지 전력과 타격 전력을 연동하며, 지휘결심에 필요한 정보를 적시에 제공할 목적으로 육군 전술지휘정보체계(Army Tactical Command Information System : ATCIS)를 구축하여 운용 중에 있으며, 현재 2차 성능 개선을 위해 준비 중에 있다. ATCIS 체계구성도는 <그림 2>와 같고 주요기능은 정보, 작전, 화력, 전투근무지원 및 공통분야로 나누어지고, 부대단위별 별도의 네트워크로 연결된다.[4] 전술제대의 작전임무를 위하여 전술통신체계 네트워크를 중심으로 전장기능(정보, 작전화력, 전투근무지원)과 통합하여 작전임무수행이 가능한 지휘·통제 수단으로 운용하고 있으며, 해상전, 공중전에 필요한 정보는 KJCCS를 통해 연동 및 획득한다.

전술통신체계는 전장 환경에 적합한 격자형(Grid)의 유·무선 네트워크로 연결되어 있으며, 보안성 강화를 위해서 암호장비를 이용하여 터널링을 구성해 운영되고 있다. 다른 전장관리체계와는 달리 웹방식이 아닌 클라이언트-서버 방식으로 개발되었다.

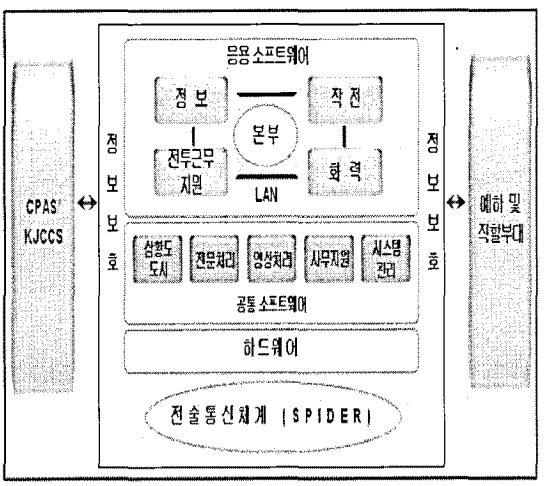
### 2.1.3 해군 지휘통제체계

해군 지휘통제체계(Korean Naval Command& Control System : KNCCS)는 해작사를 중심으로 전술부대 지휘관의 전·평시 임무수행을 위한 계획, 지시, 조정 및 통제하는 수단으로 운용하고 있다.

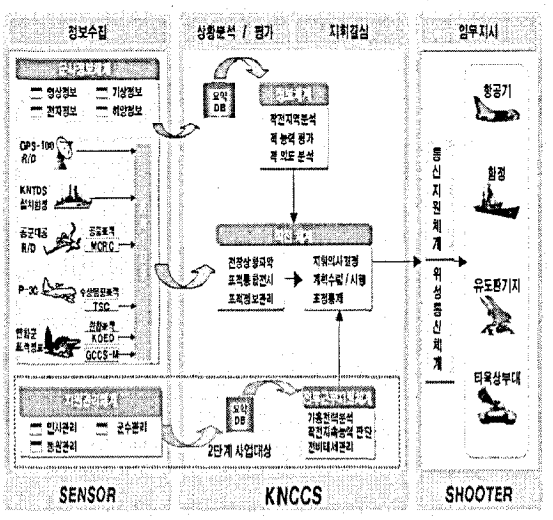
전술제대의 작전임무 자동 지원을 위하여, 해군 전술자료처리체계(Korean Naval Tactical Data System : KNTDS)의 정보를 근간으로 하여 <그림 3>과 같이 전장 기능(정보수집, 임무지시)과 통합하여 작전임무 수행이 가능한 지휘·통제수단으로 운용한다. [1]

### 2.1.4 공군 지휘통제체계

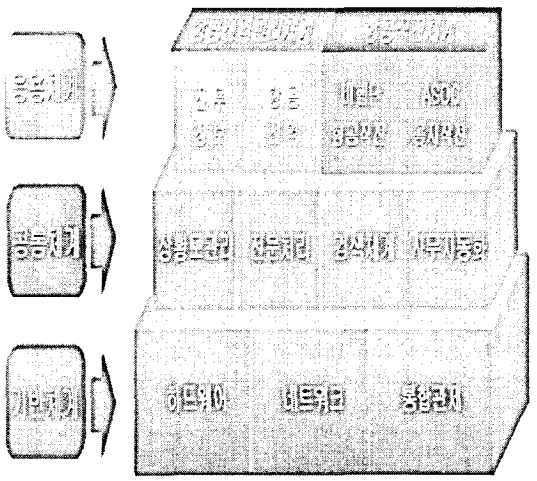
공군지휘통제체계(Air Force Command& Control System : AFCCS)는 공작사를 중심으로 전술




〈그림 2〉 육군 전술 C4I(ATCIS) 구성도




〈그림 3〉 해군 전술 C4I(KNCCS) 체계도



〈그림 4〉 공군 전술 C4I(AFCCS) 체계도

부대 지휘관의 전·평시 임무수행을 위한 계획, 지시, 조정 및 통제하는 수단으로 운용하며, 공작사, 비행단, 방공포병부대, 전술항공통제부대에 구축되었다.

전술제대 작전임무 지원을 위해 전 항공권역에 대한 감시/식별 및 방공작전을 지휘·통제하는 중앙방공통제소(MCRC)를 근간으로 전장기능(정보, 작전, 전투근무지원)과 통합하여 작전임무 수행이 가능한 지휘·통제수단으로 운용하며 체계구성은 <그림 4>와 같다.[1]

## 2.2 공개키기반구조(PKI)

### 2.2.1 개요

인증관리 기반기술에는 ID-PASSWORD, PKI, 생체인식 등 다양한 기술이 있다. 이 중 PKI는 공개키 암호기술이 안전하게 사용되는 기반 인프라로서 활용이 가능하고, 인터넷 뱅킹과 같은 다양한 정보보호 응용체계 서비스 영역에 적용 가능한 암호 기술을 제공한다.

PKI는 공개키 암호시스템에서 사용하는 공개키를 안전하고 신뢰성 있게 인증하는 수단을 제공한다. 공개키 암호시스템에서의 사용자는 일반적으로 공개키와 개인키의 쌍을 간직하고 있으며 중요한 메시지를 수신자에게 전송할 때 메시지는 수신자의 공개키로 암호화하며 이를 받은 수신자는 자신의 개인키로 메시지를 복호화 한다. 이때 상대방의 공개키가 신뢰성이 있는지 여부를 확인하기 위해 인증기관이 자신의 개인키를 사용하여 전자서명을 생성한 후 인증서에 첨부하는 것이다.

인증기관에 가입한 모든 사용자는 상대방의 인증서를 인증기관에게 요구할 수 있으며, 인증기관의 공개키를 이용하여 상대방의 인증서를 확인함으로써 정당한 사용자임을 확인할 수 있으며, 인증서에는 인증서 사용자에 대한 공개키와 신분에 대한 정보들을 포함하고 있다. [2][7][8][9][10]

### 2.2.2 구성요소

PKI는 공개키 암호기술의 활용과 관련한 이와 같은 문제점을 해결하기 위해 고안된 방법으로, 기본적으로 모두가 신뢰할 수 있는 제 3자가 제공 및 보증하는 정보를 통해 사용자의 공개키에 대한 신뢰성을 확인하는 구조이다. PKI의 구성요소는 <표 3>에서 보는 바와 같이 인증기관, 등록기관, 디렉토리, 응용 4가지이다.

〈표 3〉 PKI 주요 구성 요소

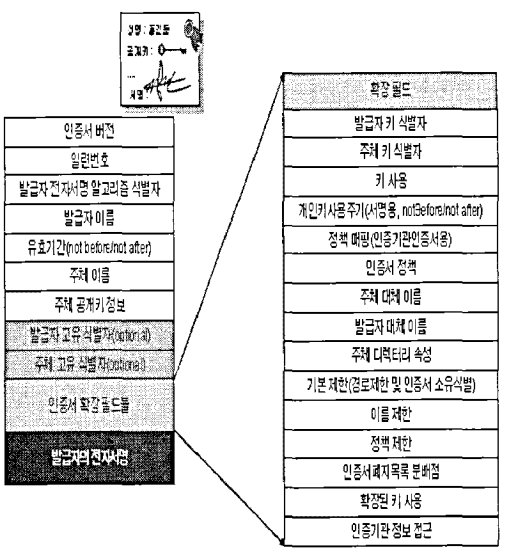
| 구성요소 | 역 할 |
|---|---|
| 인증기관(CA) (Certification Authority) | · 인증정책을 수립<br>· 인증서 및 인증서 취소 목록 관리(생성, 공개, 취소 등)<br>· 다른 CA와 상호 인증 |
| 등록기관(RA) (Registration Authority) | · 사용자 신분 확인<br>· PKI를 이용하는 응용과 CA간 인터페이스 제공 |
| 디렉토리 (Directory) | · PKI 관련 정보 공개 |
| PKI를 이용하는 응용 (사람/시스템) | · 인증서 생성, 취소 등을 요구/인증경로 검증<br>· 인증서 활용(전자서명)<br>· 디렉토리로부터 인증서 및 인증서 취소 목록 획득 |

### 2.2.3 인증서

인증서는 한 쌍의 공개키/비밀키와 특정 사람/기관을 연결시켜 주는 매개체로 해당 키가 특정인의 것이라는 것을 보증한다. 전자서명에 사용된 비밀키와 상응하는 공개키를 제공하여 그 공개키가 서명인의 것이라는 것을 확신할 수 있는 증거로 사용된다. 인증서의 표준 규격인 X.509의 구조는 <그림 5>와 같다.

## 2.3 국방인증체계(MPKI)

국방인증체계(Military Public Key Infrastructure : MPKI)는 국방정보체계에서 필수적으로 요구되는 기밀성, 무결성, 인증, 가용성 및 부인방지 등의 정보보호 기능 요소를 통합적으로 지원하기 위해 공개키 기반의 인증서를 발급, 배포하며, 이러한 신뢰 정보의 유효성을 항상 확인할 수 있도록 지원하는 체계로, 전·평시 국방정보체계의 안전한 운용을 지원하는데 목적이 있다.[5] 국방인증체계는 <그림 6>에서 보는 바와 같이 인증정책관리기관, 최상위인증기관, 인증기관, 키관리 기관, 등록기관, 지역등록기관, 가입자로 구성되어 있고 각 기관에 대한 세부적인 임무는 <표 4>에 제시되어 있다. [3]




〈그림 5〉 X.509 인증서 구조

MPKI의 적용효과로는 대면을 통한 인증서발급으로 신원 확인 강화, 정보체계별 PASSWORD 관리의 간소화, 통신상의 ID/비밀번호 유출방지 등의 기존의 ID/PASSWORD방식의 단점이 보완, 데이터 암호화를 통한 무결성 확보, 정보체계의 신원을 국방인증기관이 인증함으로써 부인방지할 수 있고, 전자관인을 통해 타 부대와의 전자문서

〈표 4〉 국방인증체계 관련기관 임무

| 구 분 | 임무 및 기능 |
|---|---|
| 인증정책 관리기관 | · 국방인증정책의 수립, 구현, 갱신 및 실행 계획 수립<br>· 군 및 기관 간 국방인증정책 조정<br>· 인증업무 수행기관의 지정<br>· 인증업무 수행기관의 준거성 감사결과 검토 |
| 최상위 인증기관 | · 인증기관 및 키관리 기관 인증서 발급<br>· 인증기관 목록 관리 |
| 인증기관 | · 등록기관/가입자인증서 발급/재발급/갱신/폐지<br>· 인증업무세부지침 수립<br>· 서명용 키 쌍 생성 및 배부<br>· 소관 등록기관/지역등록기관을 지정, 운영<br>· 인증서폐지목록의 생성/게시<br>· 인증서 기반 응용 프로그램 구현 지원 (보안 API 제공)<br>· 가입자 정보 및 기록 관리 등 |
| 등록기관 | · 가입자 정보 등록 및 변경<br>· 가입자 신원 확인<br>· 인증서 발급/재발급/갱신/폐지 관련 등록관리대장 유지<br>· 인증서 가입/폐지 신청 승인 및 인증 기관 이첩<br>· 가입자 키 및 인증서 저장매체의 제공 및 회수 등 |
| 가입자 | · 정확한 신원정보 제공<br>· 국방인증정책에 따른 개인키/인증서 보호, 관리 및 사용<br>· 개인키 훼손 또는 분실 시, 해당 사실을 신고/통보 |

유통이 가능하게 되었다.

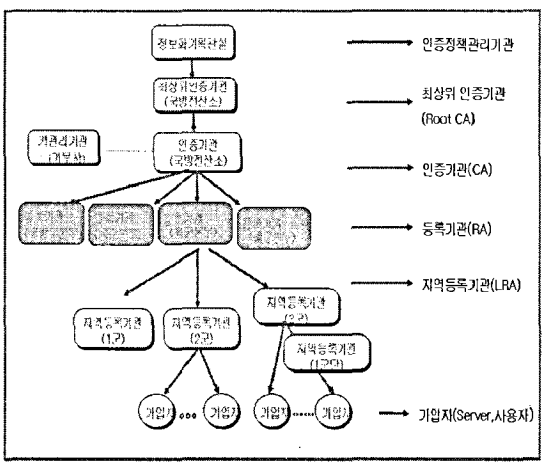
## 3. 현실태 및 문제점 분석

### 3.1 전장관리체계 인증시스템

#### 3.1.1 전장관리 인증체계 구성

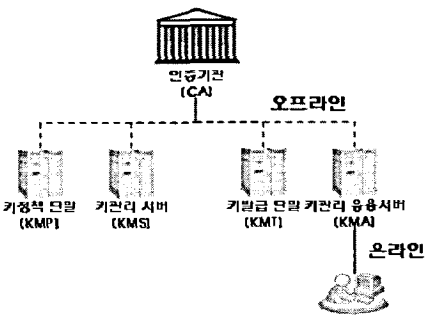
전장관리체계의 인증체계 구성은 <그림 7>에서 보는 바와 같이 하위 장비에 대한 인증서를 발급, 관리하는 인증기관(CA)를 비롯하여 정책단말(KMP), 키관리 서버(KMS), 키발급 단말(KMT) 및 키관리 응용서버(KMA)로 구성되며, 현재 전장관리체계에서 운영 중인 인증체계는 '02년 구축된 개념으로 인증기관서버, 키관리 서버, 키정책 단말 및 키발급 단말은 보안성 강화를 목적으로 오프라인으로 운영되고 있다. 내부적으로 동작하는 소프트웨어의 논리적 흐름은 비공개를 원칙으로 한다.

단, 키관리 응용서버는 전장관리체계의 주요 서버와 네트워크로 연결되어 전장관리체계의 응용체계에 PKI 인증 및 암호화 기능을 지원하고 있다. 키관리 응용서버가 실제 사용자의 인증서 검증 역할을 수행함으로 본 논문에서는 키관리 응용서버를 편의상 인증서버로 칭한다.




〈그림 6〉 국방인증체계 구성

이러한 인증체계 주요기능을 구성요소별로 살펴보면, <표 5>에서 보는 바와 같다. 여기서 중요한 것은 KMA의 역할이다. KMA에는 KMA를 구분하는 KDN(Key Domain Name)값 및 해당 KMA 서버의 IP정보가 설정되어 있으며, 사용자의 인증서 정보 및 전체 KMA에 대한 KDN 값 및 IP 정보를 가지고 있다.




〈그림 7〉 전장관리 인증체계 구성

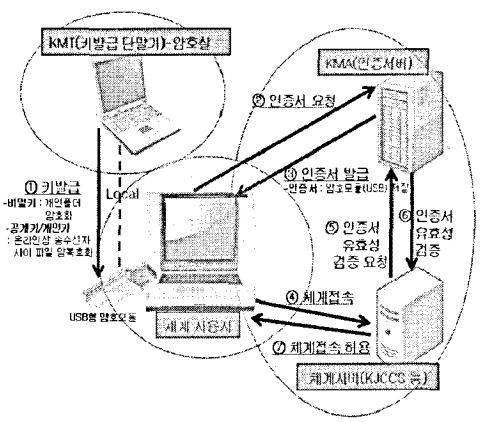
〈표 5〉 인증체계 주요기능

| 구성요소 | 주 요 기 능 |
|---|---|
| 인증기관 (CA) | · 정책단말, 키관리 서버, 키관리 응용서버의 인증서 발급 및 관리<br>· 하위 장비용 개인키 및 인증서 백업 |
| 정책단말 (KMP) | · 사용자용 인증서 정책 설정, 키발급 단말 주입 프로그램 전달, 키발급 단말에서 발급하는 사용자 키 생성 및 분배, 각종 이력관리 |
| 키관리 서버 (KMS) | · 키발급 단말에서 등록, 발급한 사용자 키 주입 이력관리 및 분석 |
| 키관리 응용서버 (KMA) | · 사용자 인증서 관리 및 게시<br>· 상대방 인증서 획득 및 인증서 검증 |
| 키발급 단말 (KMT) | · 사용자 정보 등록, 암호장비 프로그램 주입, 암호키 및 인증서를 포함한 PC 암호모듈 관리 |

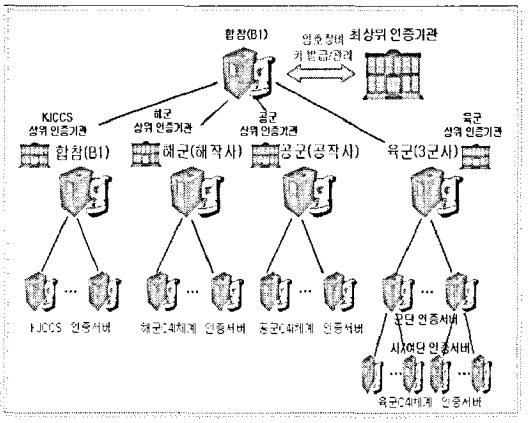
CA : Certification Authority
KMS : Key Management System
KMT : Key Management Terminal
KMP : Key Management Policy
KMA : Key Management Application

전장관리 체계의 사용자 인증 절차를 보다 상세히 살펴보면 <그림 8>과 같다. 먼저 사용자의 키발급은 해당부대 암호실에서 키발급 단말기인 KMT를 통해 로컬에서 비밀키, 공개키, 개인키를 USB형 암호모듈로 직접 주입을 받는다. 두 번째로 USB형 암호모듈을 사용자 PC에 장착후에 기본정보 즉, 부대, KMA서버 IP, 포트번호 등을 입력한 후에 해당 KMA서버에 인증서 요청을 하게 된다. 세 번째로 KMA서버는 요청된 인증서를 자신의 디렉토리에 복사하고 사용자에게 인증서를 발급하게 되는데 이때, 인증서는 PC가 아닌 암호모듈에 저장되게 된다. 네 번째로 인증서 발급후 사용자는 체계서버에 접속요청을 하게 된다. 다섯 번째로 체계서버는 사용자 접속 시 암호모듈로부터 인증서를 식별할 수 있는 인증서식별자 정보를 추출하여 KMA서버에 인증서 유효성 검증을 요청하게 된다. 여기서 인증서 식별자 추출 알고리즘은 국가보안연구소에서 제공하는 블랙박스화 된 암호화 함수인 CAPI(Cryptographic Application Program Interface)를 사용한다. 여섯 번째로 KMA서버는 인증서식별자를 통해 해당 사용자의 인증서 유효성 유무를 판단하여 서버에 통보한다. 마지막으로 사용자의 인증서가 유효하면 체계 접속을 허용한다.

### 3.1.2 체계별 인증시스템 구조




〈그림 8〉 사용자 인증 세부 절차



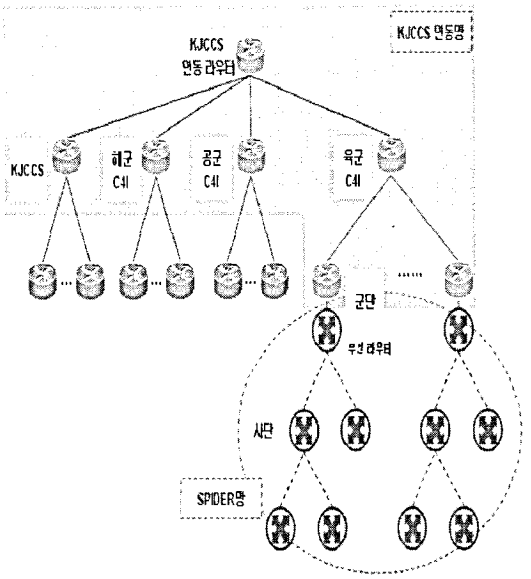

〈그림 9〉 전장관리체계 인증시스템 구조

전장관리 인증체계 네트워크 형상은 합참 및 각 군의 C4I 체계별 범주 및 기능에 따라 작전적 요구사항에 의해 특징적으로 구성하고 있다.

KJCCS와 육 · 해 · 공군 전술 C4I 체계는 각 체계별 상위 인증기관을 두어 키 정책 및 운영 관리를 수행한다. 인증서버의 네트워크 형상은 부대 구조에 따라 <그림 9>와 같이 KJCCS와 해 · 공군 전술 C4I 체계별 인증기관을 중심으로 전술 C4I 체계 운영부대의 키관리 응용서버는 동일한 레벨의 수평적인 구조를 갖고 있고, 육군 인증서버의 네트워크 형상은 전술적 작전 요구사항을 고려하여 육군의 3군사령부에 육군 상위 인증기관을 두고 군단별 키관리 응용서버를 중심으로 하위 운영부대(사·여단급)의 키관리 응용서버가 계층구조를 하고 있다. 그리고 각 체계의 최상위 인증기관으로 암호장비 키발급/관리를 국방부(국군지휘통신사령부)에서 임무를 수행하고 있다.

### 3.1.3 전장관리체계 네트워크 구조

전장관리체계의 네트워크 특징은 유선망과 무선망(전술통신체계)을 모두 사용한다는 특징이 있다. 전장관리체계의 네트워크 구성은 <그림 10>




〈그림 10〉 전장관리체계 네트워크 구조

과 같다.

위와 같이 KJCCS 연동 라우터를 중심으로 KJCCS를 비롯한 각 군의 C4I체계들이 E1급 회선으로 네트워크를 구성해서 각 체계별로 필요한 데이터를 연동하거나 평문 및 비밀전문을 교환하고 있다.

육군의 경우, 전술통신체계를 이용하는 사단급 이하 부대는 암호장비를 이용한 터널링을 구성하여 네트워크의 보안 취약점을 보완하여 운영하고 있다. 터널링이란 인터넷을 사적이며 안전한 네트웍의 일부로서 사용하는 것으로서, 여기에 사용되는 프로토콜 을 PPTP[1] 라고 부르는데, 이것은 인터넷상의 "터널"을 통해 가상사설망을 구축할 수 있도록 하기 위해 제안되었다. 전술통신체계는 IP 기반의 안정적인 연결이 보장되는 KJCCS 연동망과는 달리 전술통신체계는 작전적, 지리적 상황 및 통신장비의 특성을 고려하여 네트워크 경로상에 있는 중간노드의 중계가 단절되더라도 우회하여 목적지까지 도달할 수 있도록 격자형(Grid) 구조로 이루어져 있다.

### 3.1.4 보안 요구사항

#### 가. 전장관리체계 간 사용자 인증

전장관리체계는 각 C4I 체계별로 혹은 육군의 경우 전술적 부대 단위로 사용자 인증이 가능하다. 그러나, 동일 체계나 전술 부대 단위의 사용자 인증은 근래에 들어 합동성이 강조되고 상호운용성이 강조되는 상황에 부합하지 않으며, 전체 전장관리체계 차원에서의 상호 인증을 요구하고 있다.

#### 나. 전장관리체계 간 기밀성

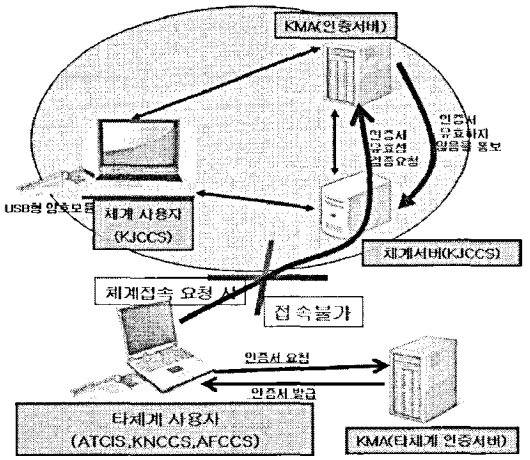
전장관리체계에서 주고받는 민감한 정보에 대한 기밀성을 보장하는 것은 유·무선 환경에서 공격자가 정보를 도청하는 것을 예방하기 위해서는 필수적이다. 기밀성을 제공하기 위해서는 표준화된 암호화 기법이나 통신하는 쌍방 간에 공개키를 이용하여 암·복호화 함으로써 정보에 대한 기밀성을 보장할 수 있어야 한다.

## 3.2 문제점 분석

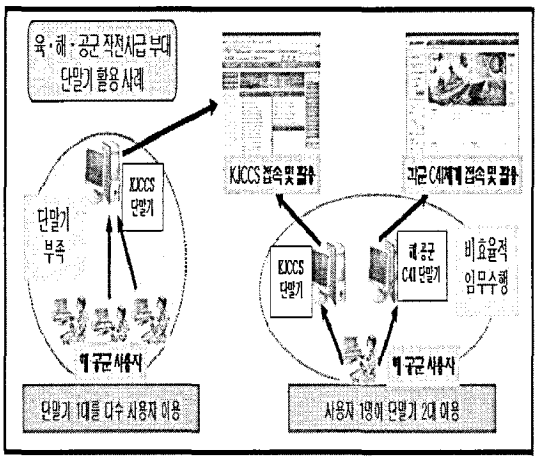
### 3.2.1 전장관리 체계 간 상호인증 불가

육군 ATCIS체계를 제외한 모든 전장관리체계가 웹 방식으로 개발되고 또한 동일한 네트워크 환경하에서 구성되어 있기 때문에 구조상으로는 충분히 상호간 웹 연동이 가능 하지만 전장관리체계의 인증체계는 각 군의 전술 C4I 체계 구축 계획에 의거 개별적으로 추진됨에 따라 전장관리체계의 인증체계를 통합하여 수행할 수 있는 즉, 전장관리체계 간 인증서를 상호 획득하고 검증을 수행할 수 있는 상호인증이 고려되지 않았다. 때문에, <그림 11>과 같이 전략C4I체계인 KJCCS를

1) PPTP(Point-to-Point Tunneling Protocol)는 기업(조직)들이 인터넷상의 사설 "터널"을 통해 자신들의 기업용 사설 네트웍을 확장할 수 있도록 해주는 프로토콜이다. 이러한 종류의 접속을 가상사설망, 즉 VPN이라고 부른다.




〈그림 11〉 타체계 사용자 인증 제한




〈그림 12〉 비효율적 임무수행

타체계 사용자 즉, 육·해·공군 전술 C4I 사용자들이 접속을 통해 정보공유를 하려고 해도 타체계 사용자 인증이 되지 않기 때문에 체계사용이 제한된다. 물론 KJCCS 사용자 입장에서도 웹환경인 KNCCS, AFCCS 접속을 시도해도 체계인증 및 접속이 되지 않는다.

단순히 타체계 사용자 접속에 대한 문제뿐 아니라 상호인증이 되지 않기 때문에 <그림 12>와 같이 육·해·공군의 사용자들이 합참의 KJCCS 체계를 사용하기 위해서는 별도의 KJCCS용 단말기와 암호모듈을 사용하다 보니 1대의 단말기를 다수의 사용자가 이용하게 되고, 또한 사용자 1명이 KJCCS단말기와 해당체계 단말기를 사용함으로써 단말기 부족 및 비효율적인 임무수행을 초래하게 된다.

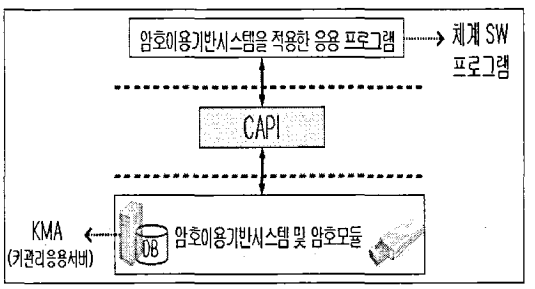
### 3.2.2 인증서 획득 알고리즘의 문제점

위에서 설명한 전장관리체계 간 상호인증에 대한 문제점은 바로 각 체계서버의 인증서 획득 알고리즘에서 문제의 원인을 찾을 수 가 있다.

이러한 전장관리체계의 인증서를 획득하고 검증하는 알고리즘은 국가정보원에서 제공하는 CAPI라는 블랙박스화 된 암호화 함수를 사용한다. CAPI를 제작하여 공공기관에 배포하고 있는 국가보안연구소는 보안상의 이유로 그 알고리즘 및 내부 동작을 비공개로 하고 있다. 그래서 본 논문에서는 간략히 CAPI에 대해서 소개 하고자 한다.

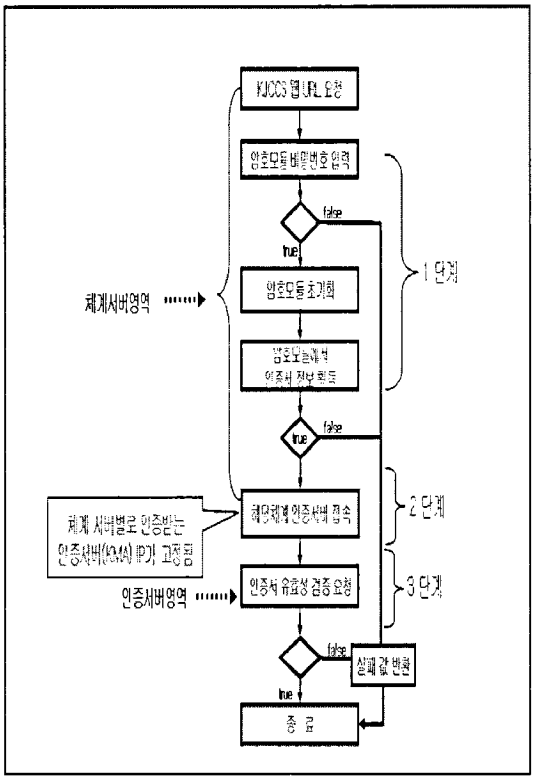
CAPI는 <그림 13>과 같이 응용프로그램에 암호화 서비스 적용을 위해 암호 이용 기반시스템 및 암호모듈과 연동, 보안기능을 제공하는 함수로서 제공되는 서비스로는 CAPI 및 암호모듈 초기화, 사용자 인증서 획득, 유효성 검증 등의 암호모듈 접근제어 및 인증기능을 제공하고 저장용, 전송용, 대용량 데이터 암복호화, 서명, 검증, Hash[2] 등의 데이터 기밀성과 무결성 서비스를 제공한다.

이러한 CAPI를 활용한 전장관리체계 사용자




〈그림 13〉 CAPI 제공서비스

2) Hash는 하나의 문자열을 보다 빨리 찾을 수 있도록 주소에 직접 접근할 수 있는 짧은 길이의 값이나 키




〈그림 14〉 인증서 검증 및 알고리즘

인증서 검증 및 획득 알고리즘은 <그림 14>와 같다. 1단계로 사용자는 체계서버의 웹 URL로 최초 접속하게 되면 개인이 지정한 암호모듈의 비밀번호를 입력한다. 이때 비밀번호를 3회 이상 실패 시 실패값을 반환한 후 종료된다. 다음으로 CAPI 함수를 통해 암호모듈 초기화와 인증서 식별자 정보를 획득한다. 그러나 암호모듈 인증서를 인증서버(KMA)에 등록되지 않았을 경우 인증서를 식별할 수 있는 KDN값을 획득 할 수 없음으로 체계접속에 실패하게 된다. 2단계로 체계서버에서 지정한 IP 정보를 기반으로 특정 서비스 포트를 이용해 인증서버와의 1:1 네트워크 접속을 시도한다. 마지막으로 3단계에서 인증서 유효성 검증을 요청하면 인증서버(KMA)는 접속된 암호모듈의 즉, 사용자의 인증서 유효성 유무를 체계서버에 통보하는데, 인증서 유효성에 실패하면 역시, 실패값을 반환한 후 종료 된다. 여기서 문제는 바로 2단계에 해당되는데 체계접속 시 사용자 인증을 위한 인증서버(KMA)가 해당체계의 인증서버(KMA)로 고정되어있기 때문에 타체계에서 접속한 사용자의 획득된 인증서는 체계별로 등록되어 있어 당연히 타체계 인증서버(KMA)에는 등록되지 않았을 것이고, 사용자 인증 및 체계접속이 제한된다.

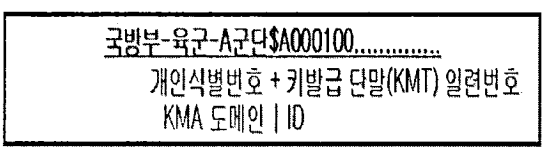
## 4. 전장관리 체계 인증방법 개선 방안

### 4.1 인증서 식별자 정보 분석

앞에서 기술한 바와 같이 기 구축된 전장관리 체계들 간의 상호인증의 문제로 인해 합참, 육·해·공군 C4I체계들 간의 웹자료 활용이 제한됨에 따라 타체계 접속 시 타체계 사용자의 인증서를 안정적으로 획득하고 검증 할 수 있는 알고리즘을 제안하고자 한다.

현재, 육군을 제외한 모든 전장관리체계들이 웹 방식으로 운용되고 있고 체계서버 접속 시 인증에 대한 알고리즘은 유사하다. 따라서 제안하는 알고리즘은 모든 체계에 대한 알고리즘의 수정보다는 전장관리 중심체계인 KJCCS 프로그램을 대상으로 한다. 또한 KJCCS 전체 프로그램 대한 영향성을 최소화하는 알고리즘 수정을 통해 현재 육·해·공군 C4I체계 사용자가 KJCSS 접속 시 타체계 인증서 검증 및 획득이 가능하도록 설계한다.

기존의 체계접속 시 사용자 인증서 획득과 검증을 위한 알고리즘은 내부적으로 고정된 목적지 IP 즉, KJCCS의 사용자인 경우 KJCCS의 인증서버(KMA) IP, 육·해·공군 체계의 경우 마찬가지 자신들의 인증서버 IP를 직접적으로 요청하였으




〈그림 15〉 인증서 식별자 정보

나, 제안하는 알고리즘은 <그림 15>와 같이 인증서 내부의 키 값을 불러오는 인증서 식별자(KMA_도메인_ID)를 통해 부대 구분, 즉, 체계별 인증서 구분이 가능하다는 데서 착안해 고정된 인증서버가 아닌 분석된 인증서 식별정보를 통해 사용자가 어느 체계에 속해있는지만 확인되면 타체계 사용자의 인증서 정보를 해당 인증서버로 연결 가능하다는 것이다.

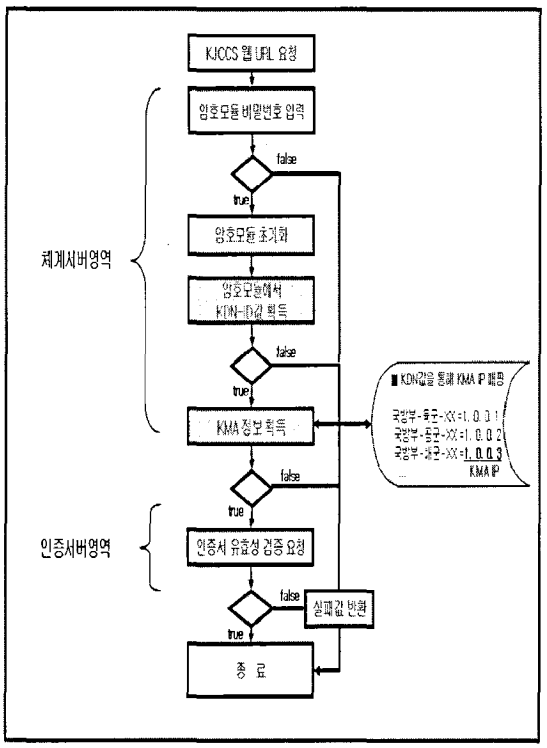
인증서 식별정보를 보다 세부적으로 살펴 보면 예를 들어 육군의 A군단 사령부에 대한 인증서 식별자(KMA_도메인_ID)를 계층적으로 나타내면, <표 6>처럼 표현할 수 있다. 마찬가지로 해군체계를 사용하는 해작사, 공군체계를 사용하는 공작사에 대한 KMA 도메인 역시 계층적 구조로 이를 정의한다. 이렇게 정의된 인증서 식별자 정보를 통해 타체계 사용자가 전장관리체계에 접속할 때, 해당체계(타체계 사용자가 속해있는 체계)의 인증서버(KMA)로 인증 요청을 할 수 있다면 상호 체계간의 인증이 가능하다. 이러한 KMA 도메인 ID는 KDN-ID(KMA Domain Name ID)로 표현한다.

〈표 6〉 인증서 식별자 적용 예

| No. | 부 대 명 | KMA 도메인 | KMA 형태 |
|---|---|---|---|
| 1 | 육군부대 | 국방부-육군-A군단 | Root Main |
| 2 | 해군부대 | 국방부-해군-해작사 | Main |
| 3 | 공군부대 | 국방부-공군-공작사 | Main |

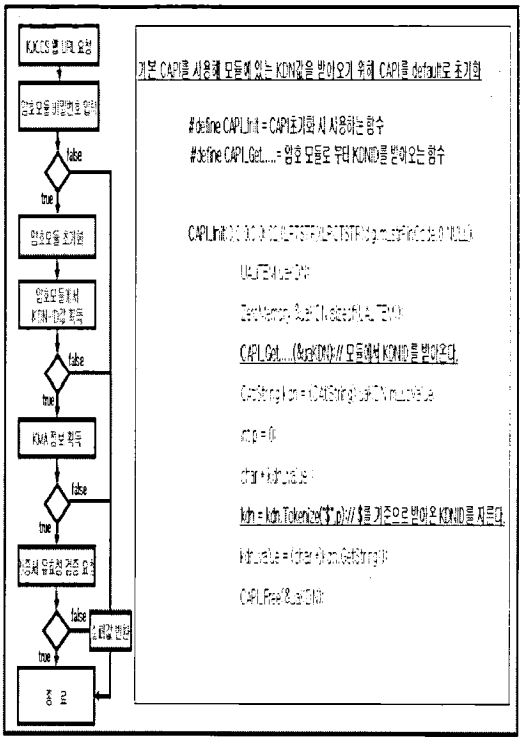
## 4.2 타체계 사용자 인증서 획득 및 검증 알고리즘 제안

위에서 정의한 인증서 식별자를 이용하여, 타체계 사용자에 대한 인증서 획득 및 검증 알고리즘은 <그림 16>과 같다. 알고리즘 수행절차를 살펴보면 첫 번째로 육·해·공군 C4I 사용자가 KJCCS 웹 URL을 요청을 하면 암호모듈 자체의 유효성 검증을 위해 사용자가 지정한 암호모듈의 비밀번




〈그림 16〉 사용자 인증서 획득·검증 알고리즘

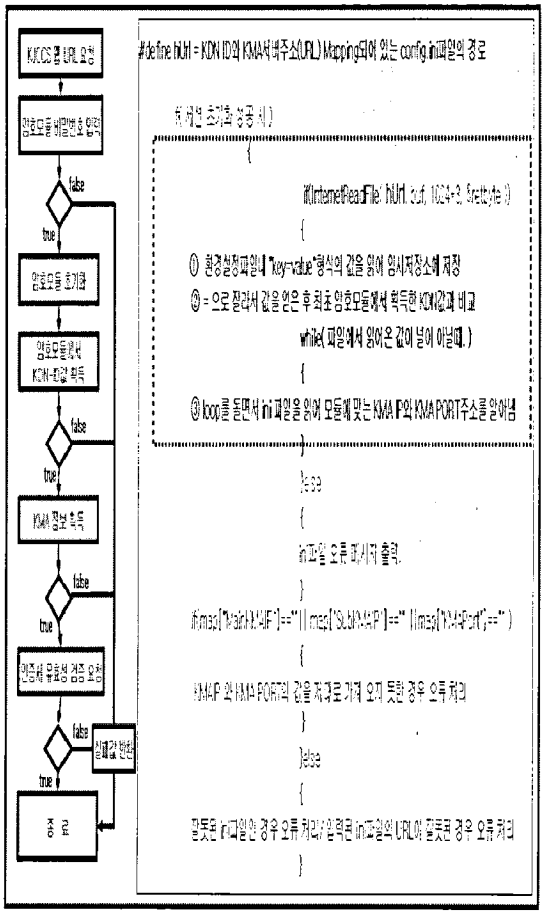
호를 입력하게 된다. 이때 비밀번호가 3회 이상 실패하면 실패값을 반환하고 종료된다. 두 번째로 인증서 식별 정보 추출을 위해 암호모듈 초기화를 수행하는데 이것은 앞에서 설명했던 CAPI 함수를 이용하여 암호모듈을 초기화하는 단계이다. 세 번째로 역시, CAPI 함수를 이용하여 암호모듈에서 KDN-ID 즉, 인증서 식별 정보(예: 국방부-XX$A00000....)를 획득한다. 그러나 최초에 암호모듈 인증서를 KMA에 등록하지 않을 경우 KDN-ID값 자체가 생성되어 있지 않기 때문에 KDN-ID를 확인할 수 없어서 실패 값을 반환한 후 종료한다. 네 번째는 제안하는 알고리즘의 핵심이 되는 부분으로서 획득한 KDN-ID값 중 $ 문자열 앞의 KDN 값 추출 및 사전에 작성된 Config 파일에서 해당 KDN 값을 갖는 KMA IP 정보를 획득한다. Config 파일에는 <그림 16>의 우측과 같이 KDN값을 통해 부대별(체계별) KMA IP를 매핑하는 정보가 들어 있다. 그러나



〈그림 17〉 암호모듈에서 KDN-ID값 획득하는 코드

Config 파일에서 획득한 KDN 정보가 없는 경우 실패 값을 반환한 후 종료한다. 다섯 번째로 획득한 KMA IP 정보를 통해 해당 KMA 서버로 접속하여 인증서 유효성 검증을 요청한 후 유효할 경우 체계 접속이 가능해 진다. 이때 인증서가 만료되었거나 유효한 인증서가 아닌 경우 실패 값을 반환한 후 종료된다.

<그림 17>과 <그림 18>은 본 논문에서 제안하는 KJCCS 체계 접속 시 타체계 사용자에 대한 인증서 획득 및 검증 알고리즘의 실제 구현 코드의 일부분을 발췌한 부분이다. 인증서 초기화, 획득, 검증, 파일 암호화 등을 할 때 사용되는 CAPI함수 자체가 대외비로 관리되고 있기 때문에 여기서 표현된 CAPI의 모듈명은 실제 사용되고 있는 모듈이 아닌 임의로 명명한 모듈명이며 보안상에 문제가 되는 일부 코드부분은 주석처리 한다. 또한 제안한 알고리즘의 실제 프로그램 구현에 있어 이 체계를 유지보수하고 있는 국군지휘통신사령부



〈그림 18〉 KDN-ID값을 이용 KMA IP 매핑하는 코드

체계개발팀과 협력하여 구현하였음을 밝혀 두는 바이다.

<그림 17>은 암호모듈에서 인증서 식별정보를 획득하기 위한 CAPI함수 초기화와 CAPI함수를 이용하여 KDN-ID를 획득하고 획득한 KDN-ID에서 부대(체계)를 확인할 수 있는 정보만 추출하는 코드이다.

<그림 18>는 KDN-ID와 KMA서버IP를 매핑해서 사용자 인증서 정보를 갖고 있는 인증서버(KMA)로 연결하는 부분의 코드로서 먼저 KDN-ID와 KMA서버 IP가 매핑 되어 있는 Config 파일을 불러와서 임시저장소에 저장하고 두 번째로 Config 파일의 구성이 '국방부-육군-XX=1.0.0.1, Port=8070' 라고 가정 했을 때 처음

의 '=' 이후의 값을 제거한 후 최초 암호모듈에서 획득한 KDN-ID값과 비교하여 존재여부 확인한다. 세 번째로 값(KDN ID)이 존재하면 loop를 돌면서 Config 파일을 읽어서 값과 매핑되는 KMA IP와 KMA포트의 주소를 알아내기 위한 것으로서 이러한 과정을 통해 인증서버(KMA)에 인증서 유효성 검증을 요청한다.

## 5. 운영 시험 결과 분석

본 장에서는 제안된 전장관리체계 간 상호인증을 통합 웹 연동에 대한 적용결과 확인을 위해 KJCCS를 대상으로 타체계에서 접속 시 운영 시험 결과를 기술한다. 이를 위해, 관계 부서의 협조를 통해 제안된 알고리즘이 적용된 변경 프로그램을 합참에서 운용하는 KJCCS서버에 적용하여 운영시험을 진행하였다.

### 5.1 일반사항

체계 간 상호인증을 통한 웹 연동을 테스트하기 위해 인증서버(KMA)를 운영하는 42개 부대 중 <표 7>과 같이 21개 부대를 대상으로 연동 테스트 후 결과를 분석하였다.

합참 정보보호과의 협조를 받아 합참의 전장관리 체계인 KJCCS 부대서버에 제안된 알고리즘이 적용된 프로그램을 설치하고, 시험에 참가하는 타체계의 시험 단말기가 KJCCS 센터서버에 접속 가능토록 KJCCS 네트워크 정책을 설정하였다. 그리고 KJCCS 센터서버에서는 시험참가 부대의 시험용 아이디를 사전에 생성하였고 각 부대별로 1일 2회(오전/오후), 총10회에 걸쳐 실시했다.

시험은 크게 기술 및 기능시험으로 분류하여 진행하였다. 기술시험은 <표 8>와 같이 본 논문에서 제안하는 타체계 사용자 인증서 검증 및 획득 알고리즘을 적용하여 실제 인증 및 접속여부를 확인하는 것이고 기능시험은 접속된 이후에 웹 기능들의 정상 사용여부를 확인하는 것이다. 웹기능 시험 중에 시험 제외 기능으로 Live COP[3]은 각 전장관리체계별로 COP 소프트웨어가 상이하기 때문에 제외 하였다. 또한 전자결재, Web Meeting[4], 전장 아키텍처 등은 합참 고유의 업무로 인해 시험에서 제외하였다.

〈표 7〉 시험대상(21개 부대)

| 구분 | KJCCS | ATCIS (육군) | KNCCS (해군) | AFCCS (공군) |
|---|---|---|---|---|
| 참가 부대 | 합 참 | 1군단 외 10개 부대 | 해본 외 6개 부대 | 공본 외 4개 부대 |
| 비고 | 프로그램 적용 체계서버 | 타체계 사용자 | 타체계 사용자 | 타체계 사용자 |

〈표 8〉 시험항목

| 구분 | 기술시험 | 기능 시험 | | |
|---|---|---|---|---|
| 항목 | 인증/접속 | 웹기능 | 비밀자료 조 회 | 단말기 해상도 |
| 세부 내용 | ① 타체계 사용자 정상 인증 여부<br>② 오류 메시지 정상 표시 여부 | ①로그인<br>②상황일지<br>③상황관리<br>④정기보고<br>⑤주요상황<br>⑥Web Cop<br>⑦공지사항<br>⑧작전명령<br>⑨자료실<br>⑩현황자료 | 비밀자료 게시판 열람 가능 여부 | 1280 × 1024 이상 지원 가능 여부 |

3) Live COP : COP은 Common Operation Picture, 즉, 공통작전상황도의 약자로서 Live COP은 하나의 일시적으로 캡처된 상황도 화면이 아닌, 지속적으로 업데이트되고 있는 상황도를 뜻함.

4) Web Meeting : 네트워크 상에서 두명 이상의 사용자가 웹캠을 통하여 음성 및 화상으로 실시간으로 대화 및 회의 등을 할 수 있는 기능

## 5.2 체계 구성 및 시험방법

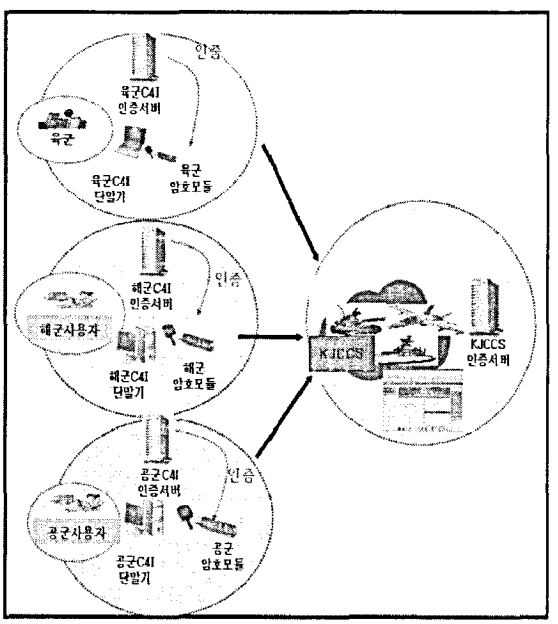
타체계 사용자의 인증서 획득 및 검증을 통한 웹 연동을 위한 운영 시험 환경 구성은 <그림 19>에서 보는 바와 같이, KJCCS체계서버와 인증서버(KMA), 육·해·공군 인증서버(KMA)와 사용자 단말을 준비하였다.

시험방법은 육·해·공군의 사용자가 자신이 사용하는 암호모듈 즉, 각 전술 C4I의 암호모듈을 통해 KJCCS에 URL에 접속 요청을 해서 인증서 획득 및 검증의 가능여부와 부여받은 시험용 ID로 접속한 이후에 웹기능을 포함한 다양한 기능의 활용 가능 여부를 테스트 하였다.

## 5.3 운영시험 결과 분석

타체계 사용자 접속 시 인증서 획득 및 검증을 통한 웹 연동 가능성을 확인한 운영 시험 결과를 요약해 보면 <표 9>에서와 같이 일부 미흡사항이 발생했지만, 대부분 정상적으로 작동되었다.

이번 운영 시험 결과를 분야별로 분석해 보면




〈그림 19〉 시험 구성도

먼저 기술시험의 경우 최초 본 논문에서 의도했던 대로 타체계 사용자에 대한 인증서 획득 및 검증을 통해 웹 연동하는 부분은 시험 대상 부대 전체가 100% 충족되었음을 확인 했다. 두 번째로 기능 시험분야에서 육군부대의 단말기 해상도의 경우 단말기 노후로 인해서 사용자 편의성이 다소 미흡하나 작전운용은 가능한 것으로 판단되었으며, 접속이후 각 웹 기능에 대해서도 대상 기능 전체가 이상 없이 사용가능 함을 확인 하였다.

마지막으로 비밀문서 조회 기능으로 육군의 경우는 비밀문서 조회 기능을 할 수 있는 DRM((Digital

〈표 9〉 운영시험 결과

| 구 분 | | | 기술시험 | | 기능시험 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 인증 | 접속 | 해상도 | 웹기능 | 비밀문서조회 | |
| 육군(46대) | 1군사 | 2군단 | ○ | ○ | △ | ○ | - | 암호키 상이에 의해 조회불가 |
| | | 3군단 | ○ | ○ | △ | ○ | - | |
| | | 8군단 | ○ | ○ | △ | ○ | - | |
| | | 3기갑 | ○ | ○ | △ | ○ | - | |
| | | 11사단 | ○ | ○ | △ | ○ | - | |
| | 3군사 | 1군단 | ○ | ○ | △ | ○ | - | |
| | | 5군단 | ○ | ○ | △ | ○ | - | |
| | | 6군단 | ○ | ○ | △ | ○ | - | |
| | | 7군단 | ○ | ○ | △ | ○ | - | |
| | | 수도군단 | ○ | ○ | △ | ○ | - | |
| 해군(26대) | 해본 | | ○ | ○ | ○ | ○ | × | |
| | 해작사 | | ○ | ○ | ○ | ○ | × | |
| | 군수사 | | ○ | ○ | ○ | ○ | × | |
| | 1함대사 | | ○ | ○ | ○ | ○ | × | |
| | 2함대사 | | ○ | ○ | ○ | ○ | × | |
| | 3함대사 | | ○ | ○ | ○ | ○ | × | |
| | 해병대사 | | ○ | ○ | ○ | ○ | × | |
| 공군(22대) | 공본 | | ○ | ○ | ○ | ○ | × | |
| | 공작사 | | ○ | ○ | ○ | ○ | × | |
| | 남부사 | | ○ | ○ | ○ | ○ | × | |
| | 방포사 | | ○ | ○ | ○ | ○ | × | |

Rights Management) 프로그램이 설치되지 않아서 제외됐고 나머지 해·공군의 경우 <표 10>과 같이 합참에서 사용하고 있는 DRM 프로그램과 암호키 방식이 상이하여 비밀문서 조회가 불가능 하였다.

합참 KJCCS의 경우 주요 게시판(작전명령 및 지침, 일반 공지사항, 공통자료실)에 업로드된 자료는 DRM을 통해 암호화된 이후 사용자 조회 시에 사용자 단말에 전송 및 관리 되고 있다. 따라서 KJCCS DRM이 적용된 자료인 경우 입력은 제한사항이 없으나 조회 할 때는 사용자 단말기에 암호화된 자료를 복호화 할 수 있는 에이전트가 설치 되어 있어야 한다. 그러나 각 체계별 독자적으로 DRM 운용을 하고 있는 상태에서 에이전트 프로그램이 설치되어있다 할지라도 암호키 방식이 서로 상이하기 때문에 비밀자료 열람이 제한된다.

〈표 10〉 체계별 DRM 운용 현황

| 구 분 | KJCCS | 육군 C4I | 해군 C4I | 공군 C4I |
|---|---|---|---|---|
| DRM 운용 | ○ | - | ○ | ○ |
| 도입업체 | 마크애니 | - | 마크애니 | 마크애니 |
| 암호키 방식 | 상용 | - | 상용 | 상용 |

## 6. 결 론

본 논문에서는 타체계 사용자에 대한 인증서 획득 및 검증 즉, 상호인증을 통해 타체계 웹 연동에 대한 방안을 제안 하였다. KJCCS 및 육·해·공군 전술 C4I 체계별로 인증서버를 별도로 운영하다보니, 타 체계와의 인증서 획득 및 검증이 제한됨에 따라 타 체계 웹 연동이 제한되고 사용자가 2개 체계의 단말기를 활용하거나 타체계 단말기가 부족하여 여러명이 한 개의 단말기를 공유해야하는 비 효율적 임무수행을 초래해 왔다.

이를 개선하기 위해 타체계 사용자 인증서 획득 및 검증 알고리즘을 제안하였다. 그리고, 제안된 알고리즘을 프로그램으로 구현하여 실제 KJCCS서버에 적용해서 육·해·공군 전술 C4I 체계를 운용하는 21개 부대를 대상으로 실험을 실시한 결과, KJCCS 연동망을 통해 인증서 획득 및 검증이 원활하게 이루어져 타체계에서 웹 접속 시 인증을 통해 체계 간 웹 연동이 가능함을 확인할 수 있었다.

또한, 단순히 타체계 사용자의 인증서 획득 및 검증 뿐만 아니라 체계접속 이후 여러 가지 웹 기능 활용 여부를 확인 한 결과 타체계에서 활용 가능한 기능 전체가 원활하게 활용 됨 을 볼 수 있었다.

그러나 본 논문에서 제안하고 있는 체계 간 상호인증을 통한 웹 연동이 비록 전장관리체계의 인증 알고리즘이 유사하다고 할지라도 KJCCS체계에만 적용되었기 때문에 웹 방식으로 운용되고 있는 해·공군 전장관리체계에 대한 알고리즘에 대한 보다 면밀한 분석을 통해 해·공군 전장관리체계에도 적용하기 위해 웹 환경에서 운용되는 전장관리 체계 간 완전한 웹 연동의 모델 분석 및 연구도 필요 할 것이다.

그 이외에도 전장관리체계별로 상용 DRM 프로그램을 적용하여 운용함으로써 체계 간 비밀 문서 조회가 제한 되는 부분에 있어서는 암·복호화를 담당하는 암호키 방식을 전장관리 체계의 인증 및 비밀문서 유통에 활용되는 CAPI 암호모듈을 공통 적용함으로써 그 해결책을 찾을 수 있을 것으로 판단됨으로 차후에 보다 상세한 분석 연구가 필요한 부분이다.

결론적으로, 현재의 전장관리체계에 영향성을 최소화하는 수준에서의 상호 인증을 통해 웹 연동 증대를 위한 방안만을 제시하였으나 향후에는 전장관리 전체가 통합화하는 전장관리 인증체계의 공통 인프라를 발전시키고, 발생 가능한 다양한 문제점을 식별하고, 미비점을 보완함으로써 제안된 알고리즘의 효율성을 강화시키고자 한다.

## 참고문헌


〔1〕 합동참모본부, "장기 합동 지휘통제 통신 발전 방향", 2008.

〔2〕 남길현, "정보시스템 보안론", 국방대학교, 2008.

〔3〕 최인수, 조성림, 안병오, "NCW를 대비한 국방 인증체계 종합발전방안 연구", 국방연구원, 2008.

〔4〕 방위사업청, "육군전술지휘정보체계(ATCIS) 체계소개 및 운용가이드", 2006.

〔5〕 한국정보보호학회, "국방전자정보인증체계구축 방안 연구", 국방부, 2001.

〔6〕 권미영, "한국군 합동지휘통제체계 보안체계 설계 방안 연구", 국방과학연구소 2007.

〔7〕 Alexandra Boldyreva, Marc Fischlin, Adriana Palacio, Bogdan Warinschi, "A Closer Look at PKI : Security and Efficiency", Spinger Berlin, 2007.

〔8〕 Asia PKI Forum, "Asia PKI Forum 2005", 2005.

〔9〕 Antonio F. Gomez Skarmeta, Gregorio Martirez Perez, "New Security Services Based on PKI", 2003.

〔10〕 Steve Dohrmann and Carl Ellision, "Public Key Support for Collaborative Groups", Internet2 PKI Workshop, 2003

## 저자소개

**김 영 성**(E-mail: topys@hanmail.net)

2009 국방대학교 전산정보학과 석사
현재 7군단 정보체계지원실 운영계획장교
관심분야 인증, IDS

**이 윤 호**(E-mail: yunholee@gmail.com)

2005 서울대학교 컴퓨터공학과 석사
현재 국방대학교 전산정보학과 박사과정
관심분야 IDS , Ad hoc security, WSN

**이 수 진**(E-mail: cyberkma@kndu.ac.kr)

1996 연세대학교 컴퓨터과학과 석사
2006 한국과학기술원 전산학과 박사
현재 국방대학교 전산정보학과 교수
관심분야 IDS, 모바일 웹 보안