情 報 保 護 學 會 誌
第 12 券 第 1 號, 2002. 2

FORTEZZA 카드의 사용자관리를 위한 보안정책

이 훈 노*, 이 수 미*, 이 정 현*, 김 영 수**, 장 태 주**, 이 동 훈***, 임 종 인***

요 약

본 고에서는 미국 NSA가 주도하여 수행하고있는 다중등급 정보시스템 보안사업(MISSI ; Multi-level Informa tion System Security Initiative)에 사용되고 있는 보안모듈인 FORTEZZA 카드의 보안정책에 대하여 기술한다. MISSI와 같은 통합된 전산망에서 다중 등급 정보를 처리하기 위한 보안 모듈의 접근통제와 보안정책에 대해 조사하였다.

Ⅰ. 서 론

전 세계가 인터넷으로 연결되어 기존의 서류(書類)를 중심으로 이루어지던 사업이 전자상거래의 형태로 바뀌어감에 따라 정보시스템의 보안(保安)에 대한 요구가 증가되고 있다. 그러나 기존의 물리적인 보안과 신뢰에 바탕을 둔 보안은 전자적인 데이터에 대해서 더 이상 충분한 보호를 해주지 못하고 있는 실정이다. 이러한 환경 하에서 오늘날과 같이 각 국가기관 전용(專用)의 전산망이 독립적으로 구축되어 운영되고 있는데 해당 국가에서는 전산망의 효율적인 운영을 위하여 분리된 개개의 전산망을 통합해 하나의 전산망으로 구축·운영하려는 시도가 미국을 중심으로 하여 이루어지고 있다. 이 경우 통합된 전산망을 통해 서로 다른 보안등급(保安等級; security level)의 정보가 저장되고 처리될 뿐만 아니라 송·수신될 수 있으므로 이를 효과적으로 제어하고 선택적으로 분배할 수 있는 기술이 반드시 동반되어야 한다. 이는 국방분야 뿐만 아니라 지적사회 (知的社會; intelligence commun ity)의 필수 요구사항이다.

서로 다른 다중의 보안등급을 가진 정보를 처리할 수 있도록 하는 것이 다중등급 보안(MLS; Multi Level Security)이며 이러한 필요성을 배경으로 미 국가보안국은 국방 정보화 기반구조(國防 情報化基盤構造; Defense Information Infrastructure)를 구성하는 여러 요소들 간의 안전한 상호운용성(相互運用性; Secure inter-operability)을 제공할 수 있도록 하는 다중등급 정보시스템 보안사업(MISSI ; Multi-level Information System Security Init iative)을 주도적으로 추진하고 있다. 또한 MISSI는 현재뿐만 아니라 미래의 사용자의 요구까지 수용할 수 있도록 사용자의 특정한 환경에 기인하는 보안상 위협에 적절히 대응할 수 있는 시스템 차원의 보안대책을 제공한다.

다중등급 보안시스템 보안사업에 필수적으로 요구되는 접근통제(接近制御; Access Control) 기술은 컴퓨팅자원과 통신자원, 정보자원 등에 대하여 허가받지 않은 사용자의 접근을 막는 것이다. 허가받지 않은 사용자의 접근이란 허가받지 않은 사용자가 불법적으로 자원을 사용하거나 노출 또는 수정, 파괴와 같은 불법적인 행동을 포함한다. 즉, 접근통제는 각 자원에 대한 기밀성(機密性; confidentiality), 무결성(無缺性; integrity), 가용성(可用性; availability) 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 관여하여 이러한 서비스들에 대한 권한을 부여하는 수단이 된다. 이러한 접근통제 기술을 제공하기 위해 개발된 제품들 중 FORTEZZA 암호화 PC 카드는 기밀성 및 무결성, 인증(認證; authentication), 부인봉쇄(否認封鎖; non-repudiation)의 보안서비스를 제공할 수 있으며 이를 이용한 응용프로그램은 1급 비밀정보서부터 대외비수준 (對外秘; SBU; Sensiti ve But Unclassified)의 정보에 이르기까지 여러 등급의 비밀정보에 대한 보안

* 고려대학교 정보보호연구센터(CIST) ({hunnoh,smlee,moomoo46}@cist.korea.ac.kr)
** 한국전자통신연구원 국가보안기술연구소 (ysk@etri.re.kr)
*** 고려대학교 정보보호연구센터(CIST) ({jilim,donghlee}@tiger.korea.ac.kr)

서비스를 제공해 전자적 정보를 취급하는데 있어 신뢰할만한 안전성을 제공한다.

본 고에서는 국내 다중등급 정보시스템의 기술개발을 위한 추진 방향을 정립하기 위하여 다중등급 사용자 관리를 위해 이용될 수 있는 접근통제 기술을 조사하여 소개하며, FORTEZZA 카드에 대한 CA의 인증서 및 키관리를 위한 CA와 SORA의 역할을 설명하고 그에 따르는 보안 요구조건을 제시한다.

II. 접근통제 시스템

접근통제(接近制御)의 목적은 컴퓨팅 자원, 통신자원 및 정보자원 등에 대하여 허가되지 않은 접근을 방어하는 것이다. 접근통제는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한부여를 위한 수단이 된다. 대부분 컴퓨터 시스템의 사용자는 시스템을 사용하기 위하여 식별과 인증과 같은 검사과정을 통하여 시스템 사용을 시작한다. 식별과 인증은 각 시스템 자원을 보호하기 위한 외부의 1차적인 보호계층이다. 즉 접근통제 결정은 요청자의 신분이 완전히 인증되기 전까지는 수행될 수 없다. 여기서 언급하고 있는 인증은 인증의 정도에 따라 자원 접근대상 및 접근모드를 제한하는 정책시행이 가능하므로, 인증의 정도는 접근통제의 개별적인 정책에 의존적인 부분일 수 있다. 따라서 고유의 접근통제 정책을 위배하지 않는 조화된 보안정책 추진전략이 필요하다.

1. 접근통제 정책

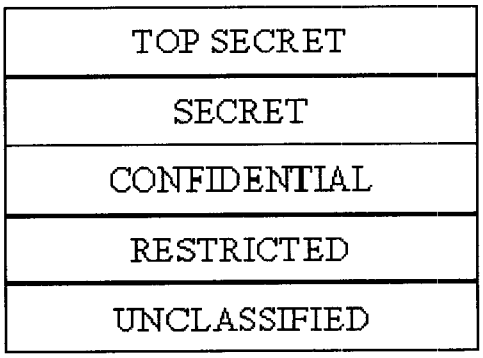
시스템자원에 접근하는 사용자의 접근모드 및 모든 접근제한 조건 등을 정의한다. 즉 시스템의 보안정책은 접근통제 시스템의 설계 및 관리를 다루기 위한 상위지침들이다. 일반적으로, 대상 시스템자원들을 보호하기 위해서 조직이 희망하는 기본적인 원칙들의 표현이다. 접근통제를 결정하는 문제는 어떤 주체가 어떤 객체에 대하여 어떤 목적을 갖고, 어떤 조건 하에서 접근할 수 있는지를 다루는 문제이다. 따라서 이러한 결정은 접근통제 정책에 반영이 되고, 접근요청은 접근정책을 시행하는 접근통제 동작절차를 통하여 시행된다.

1.1. 미 국방성 기밀 분류방법으로 유래된 접근통제 정책

1) 위임 접근통제 : 위임 접근통제 정책(MAC: Mandatory Access Control Policy)은 자동적으로 시행되는 어떤 규칙에 기반하고 있다. 그러한 규칙을 실제로 시행하기 위하여 사용자와 객체에 대해서 광범위한 그룹 형성이 요구된다.
2) 임의의 접근통제 : 임의의 접근통제 정책(DAC: Discretionary Access Control Policy)은 특별한 사용자별로 정보에 대한 접근을 제공하고 추가적 접근통제를 그 사용자에게 일임한다.

1.2. OSI 보안 구조에서 구분하는 접근통제 정책

1) 신분기반 정책 : 신분기반 정책(Identity-Based Policy)은 개인기반(IBP: Individual-Based Policy)과 그룹기반(GBP: Group-Based Policy) 정책을 포함한다
2) 규칙기반 정책 : 규칙기반 정책(Rule-Based Policy)은 다중등급 정책(MLP: Multi-Level Policy)과 부서기반(CBP: Compartment-Based Policy) 정책을 포함한다.
3) 직무기반 정책 : 직무기반 정책(Role-Based Policy)은 신분기반과 규칙기반 정책의 양쪽 특성을 가진다.



〔그림 1〕 분류등급

여기서 실제적인 목적에 있어서 신분기반과 규칙기반 정책은 각각 DAC 및 MAC 정책과 동일하고, 또한 이러한 정책들은 서로 연합될 수 있으며, 임계값의존 제어(VDC: Value-Dependent Control).

다중사용자 제어(MUC; Multi-User Control) 및 배경기반 제어(CBC; Context-Based Control) 등의 추가적 수단을 사용하여 제한 될 수 있다.

2. 다중등급 정책

위에 소개한 여러 정책들 중에 여기서 말하고자 하는 것은 다중 등급 정책이다. 다중등급 정책(MLP; Multi-Level Policy)은 정부의 기밀을 분류하는 환경에서 사용될 수 있다. 이 정책은 자동화된 강제적 시행정책을 따르는 방식으로서 일반적으로 허가되지 않은 노출로부터 정보를 보호하기 위하여 사용된다. MLP는 그림 1에서 보는 바와 같이 각 객체별로, 지정된 분류등급(classification)을 할당하여 운영한다. 각 사용자는 접근허가(clearance)를 부여받고 객체에 대한 접근을 제한 받는다.

이러한 형태의 정책을 사용한 예로는 미 국방부에서 추진하고 있는 다중등급 정보시스템 보안사업(MISSI: Multi-level Information System Security Initiative)이다.

Ⅲ. 다중등급 정보시스템

미 국방부는 국방 정보화 기반구조를 구성하는 여러 요소들 간의 안전한 상호운용성(secure interoperability)을 제공할 수 있도록 다중등급 정보시스템 보안사업(MISSI; Multi-level Information System Security Initiative)을 추진하고 있다. 또한 다중등급 정보시스템 보안사업은 현재 또는 미래의 사용자의 요구를 충족시킬 수 있도록 사용자의 특정한 환경에 기인하는 보안상의 위협에 적절히 대응할 수 있는 시스템 차원의 보안대책을 제공한다. 다중등급 보안시스템은 보안사업에 요구되는 제품들 중 FORTEZZA 암호화 PC 카드는 기밀성(機密性; confidentiality) 및 무결성(無缺性; integrity), 인증(認證; authentication), 부인봉쇄(否認封鎖; non-repudiation)의 보안서비스를 제공하며, 이를 이용한 응용 프로그램은 대외비 정보(SBU)/1급 비밀(TOP Secret)에 대한 보안 서비스를 제공함으로써 전자적 정보를 취급하는데 있어서 안전성을 제공한다. 미 국방부가 주도하여 구축되고 있는 다중등급 정보시스템 보안사업의 초기 형태는 국방 메시지 시스템(DMS; Defense Message System)과 통합 전술 전략 디지털 전산망(ITSDN; Integrated Tactical and Strategic Digital Network), 그리고 최고사령부(CINC; Command IN Chief)의 다중등급 정보처리를 위한 것이었다. 그러나, 현재 국방 정보화 기반구조를 구축하면서 국방 정보화 기반구조를 포함한 다양한 업무들간의 상호운용상의 안전성을 제공하기 위한 것으로 발전되었다.

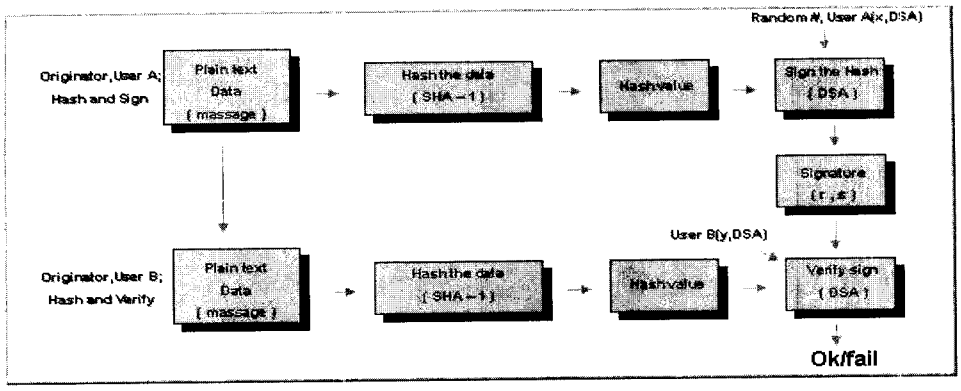
1. FORTEZZA 분석

FORTEZZA 암호화 카드는 개인 사용자를 위한 개인용 보안 장비(token)이다. 카드의 크기는 두꺼운 신용카드의 크기로 국제 PC카드 표준에 따라 제작된다. FORTEZZA 암호화 카드는 여러 업체에서 생산하고 있으나 기능적으로 동일한 제품이다. 다중등급 정보시스템 보안사업의 보안관리 기반구조(SMI)는 FORTEZZA 암호화 카드의 초기화를 지원한다. 초기화된 카드는 사용자 신분에 대한 효과적인 인증 및 접근권한을 제공한다.

1.1. FORTEZZA 카드가 수행하는 암호화 기능

1) 해쉬(Hash) : 데이터에 SHA-1(FIPS 180-1) 해쉬 알고리즘을 사용하여 160bit (20byte)의 해쉬값을 생성해 데이터의 무결성을 제공한다.
2) 디지털서명(Digital Signature) : 수신자가 송신자를 식별하거나 송신자의 행위에 대해 부인봉쇄를 하기 위해 디지털서명 표준(Digital Signature Standard, FIPS-186)의 디지털 서명 알고리즘(DSA; Digital Signature Alg orithm)을 사용한다.
3) 기밀성(Confidentiality) : 데이터를 불법적인 사용자로부터 보호하기 위해 송신자와 수신자가 키 교환 알고리즘을 통해 공유한 키로 SKIP JACK 알고리즘(FIPS-185)을 이용해 데이터를 암호화/복호화하며, 이때 키는 카드에 의해 무작위로 생성된다.
4) 키 교환(Key Exchange) : 암호화 알고리즘에 필요한 키를 안전하게 수신자에게 전송하기 위해 키교환 알고리즘 (KEA)이 사용된다.

모든 메시지는 해쉬함수를 사용해 출력된 해쉬값에 디지털서명을 함으로써 데이터의 무결성과 해쉬값에 대한 서명자의 인증과 무결성이 제공된다. 그림 2와 같이 사용자 B가 메시지에 대한 무결성과



〔그림 2〕 해쉬와 전자서명

사용자 인증 보안서비스를 요구할 경우, 사용자 A는 메시지에 대한 해쉬값에 사용자 A의 FORTEZZA 카드에 저장되어 있는 비밀키 및 카드에 의해 생성된 난수를 사용해 디지털서명을 하게되면, 20바이트 크기의 매개변수 'r'과 's'가 메시지에 대한 디지털서명의 값으로 얻어진다. 이렇게 얻어진 디지털서명과 메시지가 사용자 B에게 전송된다. 사용자 B는 독립적으로 수신된 메시지를 해쉬해 얻은 해쉬값과 사용자 A의 공개키 및 디지털서명 (r,s)을 사용하여 메시지에 대한 무결성과 인증을 확인한다.

그림 3는 TEK(Token Encryption Key)를 생성함으로써 수신측에서 복호화하기위해 필요한 메시지 암호화 키(MEK; Message Encryption Key)를 어떠한 방법으로 안전하게 수신자에게 송신하는가를 보여준다. 먼저 키교환 알고리즘은 송신자 A의 개인키 x_A와 수신자 B의 공개키 y_B와 두개의 난수 R_a와 R_b를 입력으로 받아 TEK를 생성한다. 이렇게 생성된 TEK는 메시지 암호화 키(MEK)를 암호화해 수신자B에게 송신한다. 암호화된 MEK를 수신한 수신자 B는 자신의 비밀키 x_B와 송신자 A의 공개키 y_A와 두개의 난수 R_a와 R_b를 사용해 TEK를 구하고, TEK를 이용해 암호화된 MEK를 복호화한다.

2. FORTEZZA 시스템

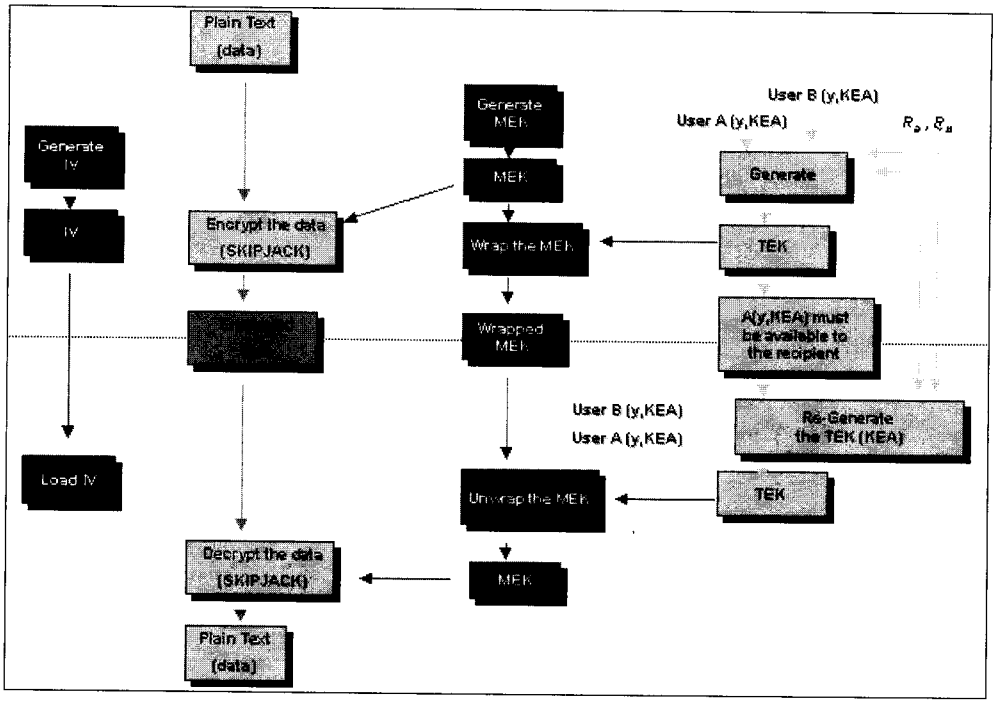
2.1. 키관리

암호화 키를 생성하고 분배, 확인, 만기 및 폐지 등과 같이 키를 관리하기 위해서는 인증서와 인증서 폐기목록(CRL; Certificate Revocation List), 노출된 키 목록(CKL; Compromised Key List)이 필요의 데이터에 변화가 있을 시, 즉 사용자가 이사를 하여 주소가 변화가 있다던가 카드가 파손되는 경우, 그리고 더 이상 인증서가 필요하지 않아 폐지된 인증서의 정보를 저장하고 있는 CRL이 있다. CKL은 카드의 PIN을 분실하거나 시스템의 보안이 깨지는 경우를 대비해 CRL에 함께 저장된다.

2.2. 인증서 인증체계

FORTEZZA 키관리는 그림 4과 같이 X.509에서 권고한 다중등급 체계(multilevel hierarchy)에 기반한다.

1) CA(Certificate Authority) : 하부 사용자의 키와 인증서를 생성 및 인증, 폐지할 수 있는 권한을 가진다.
2) PCA(Policy Creation Authority) : 계층의 최상위에 위치하며 CA를 생성 및 인증, 폐지하는 책임을 지닌다.
3) PAA(Policy Approval Authority) : 계층에서 PCA의 상위에 있지만 PCA의 생성에는 제한이 있으며, 또한 CRL이나 CKL에 대한 권한이 없고 어떠한 인증서도 폐지할 수 없다.
4) 사용자(User) : 최하위 계층에 위치하며 CA에 의해 카드가 발급된다.
5) ORA(Organizational Registration Authority) : CA와 User의 중간 단계로 CA를 도와 키와 카드를 발급한다.



〔그림 3〕 암호화/복호화 및 키 교환 과정

2.3. FORTEZZA 카드 발급절차

FORTEZZA 카드의 발급절차는 크게 등록(Registration), 키 생성(Key Generation), 키와 카드 분배(Distribution)의 3단계로 구성된다.

1) 등 록

(1) 사용자는 CA에게 FORTEZZA 카드를 발급하도록 요청한다.
(2) SRA는 ORA에 사용자 이름(ID)을 부여한다.
(3) SRA는 X.500 디렉토리에 등록한다.
(4) SRA는 CA에게 키를 생성하도록 요구한다.

2) 키 생성

(1) CA는 키와 인증서를 생성한다.
(2) CA는 X.500 디렉토리 시스템에 인증서를 저장한다.

3) 분 배

(1) CA는 개인식별번호(PIN: Personal Identification Number)를 사용자에게 직접 전달한다.
(2) CA는 FORTEZZA 카드를 ORA에 전달한다.
(3) ORA는 사용자에게 FORTEZZA 카드를 배달한다.

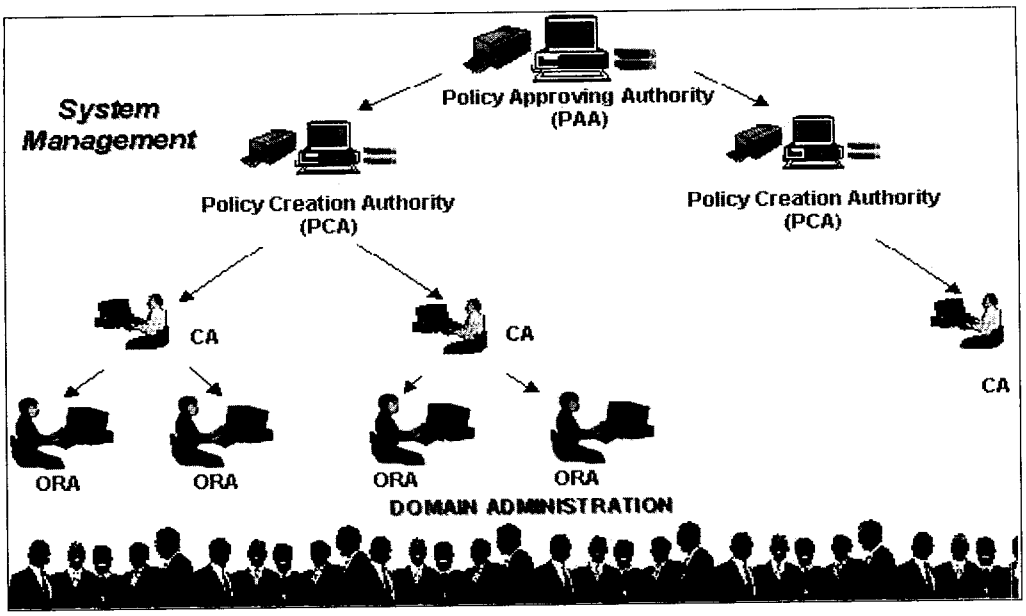
Ⅳ. FORTEZZA 카드의 키와 인증서 관리정책

FORTEZZA 카드를 다중등급 정보시스템에 적용하기 위한 키와 인증서의 관리정책에 대해 기술하였다.

1. 실사용자 개인 인증서 생성(Create End user Individual Certificate)

1) 목 적

CA/SORA는 허가받은 실사용자가 MISSI X.509 인증서가 있는 FORTEZZA 카드를 요구할 때나 무인 네트워크의 구성 요소(unmanned network component)가 FORTEZZA 카드를 요구할 때 개인의 인증서; 조직 초기인증서(Organization Firstborn certificate)와 조직 동류 인증서(Sibling certificate)를 독립적인 방법으로 생성한다.



〔그림 4〕 인증서의 인증 체계

2) 설 명

사용자가 FORTEZZA 카드를 요구하기 전에 CA는 사용자 등록을 시작한다. 예를 들어, 기본 명령권자가 등록해야할 개인의 명단과 권한을 CA에게 제공하면 CA는 이를 바탕으로 인증서를 생성한다. CA는 실사용자의 하드웨어 토큰(token)에 프로그래밍하고 실사용자의 X.509 인증서에 디지털 서명을 할 책임을 가진다.

3) 보안 요구사항

- CA/SORA는 실사용자의 신원을 확인하고 인증서에 필요한 실사용자의 권한 및 등급 확인한 뒤에 그에 준하는 인증서를 발급해야 한다.
- CA/SORA는 X.509 Version 1정의에 따라 X.509 인증서를 생성해야 한다.
- 실사용자 등록 처리과정에서 CA/SORA가 각 개인에게 주어진 권한과 그에 맞는 인증서를 발급할 수 있도록 사용자들은 충분한 개인식별정보(identification)를 CA/SORA에게 제공해야 한다.
- SORA는 X.509 인증서에 서명할 수 없다. 따라서 SORA는 CA에게 인증서에 서명을 해달라고 요청을 하고 서명된 인증서를 CA로부터 되돌려받아 서명된 인증서를 실사용자의 FOT EZZA 카드에 저장해야 한다.

2. 실사용자에게 카드와 PIN 분배(Distribute End User Card and PIN)

1) 목 적

CA/SORA가 FORTEZZA 카드와 PIN을 실사용자에게 직접 전달하거나 지정된 우편을 통해 안전하게 분배한다.

2) 설 명

CA/SORA가 새로운 사용자의 카드를 초기화하거나 사용자가 FORTEZZA 카드에 대한 인증서를 요구할 때 또는 사용자가 CA/SORA에게 PIN의 변경을 요구할 때마다 FORTEZZA 카드와 PIN을 분배한다.

3) 보안 요구사항

- CA/SORA가 카드에 프로그래밍을 하고, 사용자에게 안전하게 분배해야 한다. 이 과정은 다음을 보증한다:
  - 카드와 PIN은 해당 사용자에게 전달된다.
  - 카드와 PIN은 직접 건네지 않으면 각각 따로 전달된다.
  - 카드는 변경되지 않는다.
  - PIN은 노출되지 않는다.
- CA/SORA가 FORTEZZA 카드와 PIN을

분배할 때에는 다음을 따라야 한다:

- 사용자들은 FORTEZZA 카드와 함께 배달되는 수령증에 서명하고 되돌려 줌으로써 카드와 PIN의 수령을 인증해야 한다.
- 카드와 PIN을 분배할 때에는 가능한 한 직접 전달해야한다. CA/SORA는 카드와 PIN을 건내주기전에 사용자의 신원을 확인해야만 한다.
- 카드를 직접 전달하는 것이 불가능할 때에는 즉 등기우편과 같이 카드가 전달될 동안 지속적으로 책임을 질 수 있는 방법으로 전달해야 한다. PIN은 카드의 주소와 다른 곳으로 배달되어야 한다. 이것이 불가능하다면 PIN은 카드가 도착한 후 3일이 지난 후에 배달되도록 해야한다.
- 사용자들은 카드와 PIN 모두를 다 받은 후에 수령증에 서명을 해야한다.
- CA/SORA가 카드를 전달한 뒤 60일이 지나도록 수령증을 되돌려받지 못했다면 카드의 모든 인증서가 손상되었다고 생각해야 한다.
- 프로그래밍된 카드와 PIN을 받지 못한 사용자는 CA/SORA에 그 사실을 통보해야만 한다.
- CA가 카드를 ORA에 보낸 후부터 2주안에 카드에 대한 수령증을 받지 못했다면 CA는 카드에 대한 처리를 결정하기 위해 ORA에 연락해야 한다.

• 비밀취급 인증서(Secret certificate)가 저장된 FFC 카드와 PIN의 분배는 SBU 카드의 분배방법과 유사한 방법으로 행해져야 한다.

3. 사용자 PIN 변경(Change User PIN)

1) 목 적

CA/SORA는 CA/SORA의 환경설정 파일에 설정되어 있는 PIN의 길이와 항목에 따라 새로운 PIN을 생성한다.

2) 설 명

사용자가 인증서를 갱신하거나 PIN이 노출되었다고 여겨질 때마다 또는 초기화된 날부터 3년이 경과한 후에 PIN을 변경해야한다. 이 것은 카드에 저장된 모든 인증서가 같은 CA/SORA에 의해서 만들어지고 유효기간이 같은 시간에 만기되는 경우이다. 카드의 PIN은 반드시 카드를 초기화한 CA/SORA에 의해서 변경되어야 한다.

3) 보안 요구사항

• 사용자 FORTEZZA 카드는 인증서가 갱신되거나 키가 바뀔 때마다 또는 PIN이 손상을 입었다고 의심될 때마다 PIN을 바꾸어야만 한다.

• 카드를 초기화한 CA/SORA만이 그 카드의 PIN을 바꿀 수 있다.

4. 인증서 재발급(Renew Certificate)

1) 목 적

CA/SORA는 CAW 데이터베이스 내에 있는 실사용자의 인증서 유효기간을 연장하기 위해 인증서를 재발급한다.

2) 설 명

CA/SORA가 일반적으로 만기가 다된 유효한 인증서에 새로운 유효기간을 설정하기 위해서 인증서를 재발급한다. FFC와 SBU 인증서들은 생성 후 최대 3년까지 유효하며, 새로 갱신된 인증서는 일련번호와 유효기간을 제외하면 이전 인증서의 내용과 동일하다. SORA는 인증서에 서명을 할 수 없기 때문에 재발급된 모든 인증서를 CA에게 보내고 CA는 서명한 인증서를 SORA에게 되돌려 준다. 기존 인증서는 만기 때까지 유효하지만, CAW 데이터베이스에 '재발급(RENEW)'이라는 표시가 되어 나중에 더 이상 기간을 연장하거나 키를 재발급 받을 수 없게된다.

3) 보안 요구사항

• 카드와 키의 재발급 기간은 최대 3년이다. FORTEZZA 카드를 3년동안 사용한 실사용자는 인증서와 키의 재발급을 위해 CAW에 직접 반납해야 한다.

• 최초의 인증서를 생성한 CA/SORA만이 재발급할 수 있으며, 폐지되거나 갱신된 인증서는 재발급할 수 없다.

• CA/SORA는 CAW 데이터베이스에 저장되

어 있는 인증서만 재발급할 수 있다.
- 실사용자의 카드로 인증서를 전송받기 위해서는 인증서 재전송 함수가 사용되어야 한다.
- 지정된 시간 내에 해당 CA/SORA에 카드를 제시하지 못한 사용자들의 인증서는 CRL에 저장되고, 앞으로의 인증서 사용이 금지된다.
- 만약 같은 인증서가 복사된 다른 카드들이 존재하면 카드를 CA/SORA에 반납한 뒤 새로운 인증서를 카드에 다시 발급받아야 한다.

5. 실사용자의 인증서 키 재발급(Rekey End User Certificate)

1) 목 적

CA/SORA가 사용자 인증서의 키를 재발급한다.

2) 설 명

X.509 인증 요청 양식에 의해 유효한 인증서나 키로 검증되기 위해서는 만기일 30일 이전에 키를 갱신해야 한다. 따라서 키 재발급은 유효기간 내의 언제라도 신청할 수 있지만 반드시 만기일 30일 이전에 신청해야한다. 인증서의 키가 재발급 되면, 새로운 KEA 키 또는 DSS 키를 발급받게 되는 것 외에 인증서의 내용은 기존 인증서의 내용과 동일하다. 기존 인증서는 만기 때까지 유효하지만, 데이터베이스에 '키 재발급(REKEYED)'이라고 표시되어 이 후에 인증서의 기간을 연장하거나 다시 키를 재발급 받을 수 없다.

3) 보안 요구사항

- 카드와 키의 재발급 기간은 최대 3년이다. FORTEZZA 카드를 3년동안 사용한 실사용자는 인증서와 키의 재발급을 위해 CAW에 직접 반납해야 한다.
- 지정된 시간 내에 해당 CA/SORA에 카드를 제시하지 못한 사용자들의 인증서는 CRL에 저장되고, 앞으로의 인증서 사용이 금지된다.
- 최초의 인증서를 생성한 CA/SORA만이 재발급할 수 있으며, 폐지되거나 갱신된 인증서는 재발급할 수 없다.
- CA/SORA는 유효한 인증서의 키만 재발급할 수 있다.
- 실사용자의 카드로 인증서를 전송받기 위해서는 인증서 재전송 함수가 사용되어야 한다.
- 최초 인증서의 사용자 KEA 키의 값 X가 CA의 데이터베이스에 저장되어 있을 때, CA는 새로운 인증서에 사용자 KEA 키의 값 X를 저장할 것인지에 대한 선택권을 갖게된다. 그러나 최초 인증서의 사용자 KEA 키의 값 X가 CA의 데이터베이스에 저장되어 있지 않다면, 이러한 선택권은 주어지지 않는다.
- SORA는 X.509 인증서에 서명할 수 없다. 따라서 SORA는 CA에게 인증서에 서명을 해달라고 요청을 하고 서명된 인증서를 CA로부터 되돌려받아 서명된 인증서를 실사용자의 FOT EZZA 카드에 저장해야 한다.

6. 인증서 폐기(Revoke Certificate)

1) 목 적

CA/SORA는 폐기할 인증서를 CRL에 등록한 후에 CA/SORA 데이터베이스에 있는 인증서를 폐기한다.

2) 설 명

CA/SORA는 인증서 만기일 전에 사용자가 더 이상 인증서를 필요로 하지 않을 때나 인증서와 연관된 키가 손상되었다고 예상될 때, 또는 PCA가 인증서 폐기를 요구할 때 해당 인증서를 폐기한다. 사용자가 카드를 분실해 CA/SORA에게 새로운 DSS 키를 요청할 때 CA/SORA는 분실된 사용자 카드의 인증서를 폐기한다. 고장이 잦거나 오동작을 일으키는 카드로 인해 30일 안에 인증서를 재발급할 때에도 CA/SORA는 해당 인증서를 폐기한다.

3) 보안 요구사항

- 인증서가 만기되기 전에 DN을 바꾸려면 해당 인증서를 폐기해야한다.
- 키가 손상되었다고 예상될 때마다, 해당되는 키를 폐기하고 인증서를 CRL에 등록한다.
- 실사용자의 카드에 결함이 있다면, CA는 이전의 메시지들을 복호화할 수 있도록 새로운 카드에 이 전의 인증서를 다시 저장해야 한다. 이것은 실사용자에게 예전의 인증서의 정보를 새로운 인증서로 다시 암호화할 수 있도록 한다. CA는 이 작업 후에 예전의 인증서를 30일

안에 폐기해야 한다.

- 인증서가 폐기되었을 때 CA/SORA는 인증서의 일련번호를 CRL과 디렉토리에 등록해야 된다.
- CA/SORA가 인증서를 폐기하는 것은 데이터베이스의 인증서를 폐기하는 것이다. 디렉토리에 저장되어있는 CRL을 제외하고 사용자의 카드에 있는 인증서에는 영향을 끼치지 않는다. 따라서 CA/SORA는 사용자의 카드에 있는 개인 인증서도 삭제를 해야한다.

7. 카드내용 초기화(Zeroize Card)

1) 목 적

CA/SORA가 FORTEZZA 카드의 모든 데이터의 내용을 지우기 위해서 카드의 내용을 초기값인 0으로 한다.

2) 설 명

CA/SORA는 사용자의 요구가 있을 때나 오동작을 하는 카드를 제조업체에 반납하기 전에 또는 이전에 사용하던 카드를 재사용하기 전이나 사용자가 더 이상 카드를 사용할 필요가 없을 때 카드의 내용을 초기화한다.

3) 보안 요구사항

- SBU 인증서는 이전에 사용되던 SBU FORTEZZA 카드에 저장될 수 있지만 카드의 내용은 반드시 지워진 상태여야 한다.
- 이전에 사용된 SBU 카드는 새로 분류되는 비밀을 다루는데 사용되는 카드로 사용될 수 없다. 새로이 분류되는 비밀을 다루는데 사용될 카드는 새로 만들어진 카드를 사용해야 한다. 그러나 이전에 사용되었던 카드를 재사용할 때에는 카드의 내용이 반드시 지워진 상태여야 한다. 새로운 1급 비밀(Top Secret)용 카드는 반드시 새로 만들어진 카드를 사용하거나 이전에 1급 비밀용으로 사용되던 카드를 재사용할 때에는 반드시 카드의 내용을 지운 것을 사용해야 한다.
- 카드의 내용을 지우기 전에 CA/SORA는 반드시 카드에 저장되어있는 모든 인증서들을 취소하고 CRL에 등록해야 한다.
- CA/SORA가 어떤 이유에서든지 카드의 내용을 지울 수 없거나 카드의 보증기간이 지났을 때, 카드는 반드시 등록된 우편을 통해 특정기관(해당기관의 카드담당기관 등)으로 보내져야 한다.
- 사용자는 사용할 수 없거나 고장난 카드를 직접 또는 지정된 방법을 통해 카드를 발급한 CA에 반드시 반납해야 한다.
- 보증기간이 남아있으면서 오동작을 일으키는 카드나 고장난 카드는 모든 내용을 지운 후에 제조업체에 반납하지 않고, 승인된 방법에 따라 파기해야 한다.

8. DB에서 카드목록 지우기(Delete Card from Database)

1) 목 적

CA/SORA는 내용이 지워진 카드를 재사용하기 위해 CA/SORA의 DB에 저장되어 있는 카드의 일련번호를 비롯한 카드 정보를 삭제한다.

2) 설 명

이 전에 프로그래밍된 카드가 더 이상 필요하지 않아 카드의 모든 내용이 지워졌을 때, 예를 들어 SBU 카드를 사용하던 사용자가 기관을 떠나거나 카드의 인증서가 더 이상 필요치 않을 때, CA/SORA는 카드의 내용을 지우고, DB의 목록에서 카드의 정보를 삭제해 미래의 SBU 카드사용자가 재사용할 수 있도록 한다. 프로그래밍된 카드가 고장나서 카드의 모든 내용을 지울 수 없을 때, 카드가 보증기간이 남은 SBU 카드일 경우 제조업체에 카드를 반납하기 전에 DB의 목록에서 카드에 대한 정보를 삭제해야 한다. 카드가 FFC 카드인 경우 카드를 파기하기 전에 DB 목록에서 카드 정보를 삭제해야 한다. 참고로 FFC 카드는 보증기간이 남았더라도 제조업체에 반납해서는 안된다.

3) 보안 요구사항

- SBU용으로 사용되었던 카드는 다음에도 SBU용 카드로만 사용되어야 한다. SBU용으로 사용되었던 카드에 1급 비밀(Top Secret)이나 2급 비밀(Secret)의 인증서를 저장하는 것은 보안정책에 위배되는 사항이다. 추가적으

로 이전에 되었던 카드가 2급 비밀의 인증서를 가지고 있던 FFC용 카드이면 다음에도 재사용될 때에도 2급 비밀용 인증서를 사용할 수 있도록 초기화되어야 한다. 이전에 사용되었던 카드가 1급 기밀의 인증서를 가지고 있던 FFC 카드이면 다음에도 1급 기밀용 인증서를 사용할 수 있도록 초기화되어야 한다.

- DB 목록에서 카드 정보를 삭제할 때에는 보안 요구사항이 없다. 그러나 CA/SORA는 DB 목록에서 카드정보가 삭제되지 않는 한 카드를 재사용할 수 없다.

V. 결 론

보안 기술이 발달함에 따라 많은 분야에서 각각의 상황에 알맞은 등급의 보안기능을 사용하게 되었다. 이러한 서로 다른 등급의 보안기능들은 서로 다른 전산망을 통해 사용되어 왔지만 최근에는 전산망의 효율적인 관리를 위한 전산망 통합 시도가 세계 곳곳에서 생기고 있다.

서로 다른 등급의 보안기능들을 통합하게 되면 각 보안등급에 따른 차별적인 접근통제가 이루어져야 하는데 미국에서 개발한 MISSI에서는 다중등급 보안 문제를 해결할 수 있는 방안을 제시하고 있다. MISSI에서는 다중등급 보안 문제 해결을 위해 기밀성 및 무결성, 인증, 부인봉쇄 등의 보안서비스를 제공해주는 FORTEZZA 카드를 통해 접근통제 기능을 제공하고 있다.

본 연구에서는 다중등급 사용자 암호모듈에 이용되는 접근통제 시스템에 대한 기능적 구분을 통해 FORTEZZA 카드에 이용될 수 있는 전반적인 접근통제 기술을 제시하였다. 또한 FORTEZZA 카드가 가지는 보안성과 FORTEZZA 카드의 데이터 파일을 보호하기 위해 구현되는 접근통제 모델을 분석하여 보안장치로서의 FORTEZZA 카드를 이해할 수 있게 하였다. 외부 실체가 FORTEZZA 카드의 파일 및 데이터에 대한 접근을 시도할 경우 접근통제 메커니즘에서 정의한 접근규칙에 따라서 접근을 허가 또는 금지하게 할 수 있게 해주는 기능에 대해서 기술하였다.

본 연구가 우리나라 실정에 맞는 다중등급 보안을 위한 FORTEZZA 카드 설계 개발의 지침으로 활용되기를 기대한다.

참 고 문 헌

[1] 김종기, "미 국방부의 다수준 정보시스템 보안사업(MISSI)",정보처리 제4권, 제2호, 1997. 3.

[2] 이동훈외 4인, "보안 모듈 관리 시스템 개발에 관한 연구", 한국전자통신연구원

[3] 이철원외 3인, "국가기간전산망을 위한 MISSI 분석", 한국통신정보보호학회지, pp.35—54, Vol. 7, No.2, 1997.

[4] http://www.armadillo.huntsville.al.us/Fortezza_docs/ovrvw40a.pdf

[5] http://www.rnbo.com/PROD/rmadillo/p/ptoc.html," Fortezza Application Implementor Guide for the PCMCIA based FoRTEZZA Cryptologic Card", 199 5.

[6] http://www.armadillo.huntsville.al.us/Fortezza_docs/cipg152.pdf, "Fortezza Cryptologic Interface Programmers Guide", January 30, 1996.

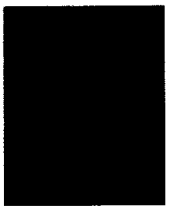
[7] http://www.kisa.or.kr/technology/sub3/AC_9901.html, "접근통제기술 개요".

[8] Edward G, Amoroso, "Fundamentals of computer security technology", 1993.

[9] CAW Release 3.1, 2 Feb, 1998.

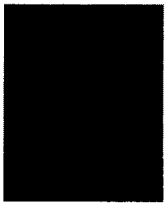
〈者 著 紹 介〉

이 훈 노(Hun noh Lee)
2000년 2월 : 고려대학교 전산학과 졸업
2000년 3월~현재 : 고려대학교 전산학과 석사과정
관심분야 : 암호 프로토콜



이 수 미(Su Mi Lee)
1995년 : 순천향대학교 화학과 졸업
2001년 : 고려대학교 정보보호대학원 석사과정 재학중
관심분야 : 암호프로토콜

이 정 현(Jung Hyun Lee)
2000년 : 고려대학교 전산학과 졸업
2001년 : 고려대학교 정보보호대학원 석사과정 재학중
관심분야 : 암호프로토콜



김 영 수(Young Soo Kim)
1986년 : 한남대학교 전자계산공학과 학사
1990년 : 한남대학교 수학과 석사
1996년~현재 : 한남대학교 컴퓨터공학과 박사과정
1986년~현재 : 한국전자통신연구원 국가보안기술연구소 선임연구원
관심분야 : 네트워크 정보보호, 컴퓨터 정보보호

장 태 주(Tae Joo Chang)
1982년 : 울산대학교 전기공학과 학사
1990년 : 한국과학기술원 전기및 전자공학과 석사
1998년 : 한국과학기술원 전기및 전자공학과 박사
1982년~2000년 : 국방과학연구소 선임연구원
2000년~현재 : 국가보안기술연구소 책임연구원
관심분야 : 정보보호, 컴퓨터통신, 통계학적신호처리

이 동 훈(Dong Hoon Lee)
정회원
1984년 : 고려대학교 경제학과 졸업
1987년 : Oklahoma Univ. 전산학과 석사
1992년 : Oklahoma Univ. 전산학과 박사
1993년~현재 : 고려대학교 전산학과 교수
2000년~현재 : 고려대학교 정보보호 대학원 교수
관심분야 : 암호이론, 암호 프로토콜, 정보이론

임 종 인 (Jong-In Lim)
정회원
1980년 : 고려대학교 수학과 졸업
1982년 : 고려대학교 수학과 석사
1986년 : 고려대학교 수학과 박사
1986년~현재 : 고려대학교 수학과 교수
2000년~현재 : 고려대학교 정보보호 대학원 원장
관심분야 : 암호이론, 암호 프로토콜, 정보이론