情報保護學會論文誌
第13券 第4號, 2003. 8

상호인증서를 이용한 국제상호인증 모델 설계

김 재 중*, 이 동 훈**

Design of International Cross Certification Model using Cross Certificate

Jae-Jung Kim*, Dong Hoon Lee**

요 약

기존 상호인증 모델이 이론적인 모델로써 보다 구체적인 실제 상호인증에 필요한 많은 부분들이 정의되지 않거나 구체적으로 표준을 어떻게 사용하여야 하는지에 대하여 명확히 설명하지 못하여 이를 해결하기 위해서 상호인증 인증서를 통한 국제상호인증 모델을 제안하고자 한다. 이를 위해서 인증기관 간 필요한 인증서 프로파일을 제안하고, 이를 보관할 디렉토리 서버에 필요한 스키마를 설계하고, 인증기관이 다른 기관에서 제공하는 저장매체에 손쉽게 접근하도록 하기 위해 PKCS#11을 통한 표준 방식을 제안하여 확장성과 편리성을 제공하고자 한다. 또한 서로 다른 응용 애플리케이션에서 상호인증서 사용 시 CRL을 통한 인증서 검증을 위한 인증서 경로 획득에 대한 방법을 제안하고자 한다.

ABSTRACT

In this paper we propose an international cross certification model using cross certificate. We propose a new model by analyzing and solving current problems of the National PKI. We recommend a certificate profile, design a directory schema, and propose a method to access PSE(personal security environment) using PKCS#11, which gives the expansibility and convenience. Finally, we propose a certificate path verification method using RFC 3280 and show how to get the certificate chain by using the trust anchor. This model is recommended to the detailed level of specification for the interoperability of each country's PKI.

keyword : *PKI, cross certification*

Ⅰ. 서 론

기존의 대면을 기본으로 하는 거래구조가 인터넷을 이용하는 전자거래의 형태로 변환되어 감에 따라서 거래 당사자들 간의 신뢰성과 안전성에 대한 보호가 중요한 부분을 차지하게 되었다. 이를 위해 세계 각 국은 전자서명법과 같은 관련법을 통해 공개키 기반구조(Public Key Infrastructure 이하 PKI)를 구축하여 시행하고 있다.

세계 각 국은 ISO, IETF 등의 표준을 준용하여 PKI를 구축하고 있지만, 각 국가별로 구축된 PKI간에는 해석 및 구현에 있어 약간의 차이점들이 존재한다. 따라서, 국가 간 혹은 기업 간의 전자거래의 상호 연동성을 보장하기 위해서는 표준에서 제시된 방법을 확장하여 구체적으로 구현 가능하도록 할 필요가 있다. 본 논문는 현 National PKI(이하 NPKI)의 구조를 분석하고 이를 토대로 확장하여 국제상호인증이 가능하도록 각 구성 요소들이 갖추어야 할 가

* 한국정보인증 정보인증센터 선임연구원(jjkim@signgate.com)
** 고려대학교 정보보호대학원 부교수(donghlee@korea.ac.kr)

장 적합한 표준을 논의하고자 한다.

1.1 CA-CA간 상호인증 모델

국가마다 구축된 PKI를 서로 연동하여 사용자들로 하여금 서로 다른 국가의 인증서 사용자들 간에 전자서명 기능을 사용하고자 하는 요구사항을 충족시키기 위하여 서로 다른 도메인을 연동하는 여러 가지 상호인증 모델이 제안되어 있다. 현재까지 제안된 대표적인 상호인증 방법을 아래와 같이 분류할 수 있는데 각각의 개념을 간략하게 살펴보면 다음과 같다.

- 상호인정(CR: Cross Recognition): CA간의 협약에 의해서 서로 다른 도메인에 있는 송신자와 신뢰당사자의 CA 간에 관련성이 없는 경우 신뢰 당사자의 판단 하에 송신자의 CA를 신뢰하는 방법이다.
- 인증서 신뢰 목록(CTL: Certificate Trust Lists): 상호 인증하는 CA간 서로 신뢰하는 인증기관의 루트 인증서의 해쉬값을 신뢰 목록으로 작성하여 디렉토리에 게시해서 인증서 검증 시 사용하는 방법으로, 신뢰목록의 유효기간은 상호 협의하여 사용한다. 국내 Government PKI와 National PKI간에 사용[1]되고 있다.
- 상호인증(CC: Cross Certification): 한 인증기관(CA: Certification Authority)이 다른 CA에게 각각의 정책 매핑에 따라 인증서를 발급하여 상호인증을 수행하는 방법으로 단방향, 양방향의 인증서 발급이 모두 가능하며 기술적으로 구현이 용이하다.

위의 방법 중 CR과 CTL은 상호 협의나 소프트웨어적인 방법을 통하여 상호인증을 수행하므로 다소 불완전하여 이를 해결하기 위해서는 상호 인증서 기반으로 양방향 인증서를 교환하는 상호인증 체계가 필수적이다. 따라서 CC를 통한 안전하고 신뢰성 있는 국제상호인증 모델을 제안하고자 한다.

1.2 기존 상호인증 모델 비교

[표 1]에서 [표 3]은 기존상호인증 모델들의 장단점을 비교한 것이다.

1) KCAC.CTL 인증기관간 상호연동을 위한 기술규격 v1.01.

[표 1] CR 모델의 장단점

	내용
장점	• CC 협약과 같은 절차가 요구되지 않음
단점	• 신뢰 당사자가 신뢰유무를 확인 • 높은 보증이 요구되는 경우에는 부적합함 • 취소CA에 대한 정보 제공 방법이 불명확함 • CR을 설정하기 위한 평가항목이 없음 • 신로 당사자의 신뢰정보 제공방법이 정의되지 않음

[표 2] CTL 모델의 장단점

	내 용
장점	• 각각의 PKI 도메인 구조에 영향이 없음 • CA가 손상되더라도 상호연동에만 문제될 뿐 전체 PKI에 영향이 없음 • 하나의 신뢰 경로만 생김 • MS에서 제안한 것으로 사용자에게 익숙함 • 다른 신뢰목록 분배에도 사용 가능
단점	• CTL의 유효성 검증을 해야 함 • 복수개의 신뢰 포인트를 관리하기 위한 작업 필요 • 다른 도메인으로부터 신뢰경로에 대한 정보를 얻어야 함 • 사용자가 CTL을 분배하는 방법이 정의되어 있지 않음

[표 3] CC 모델의 장단점

	내 용
장점	• 양 CA의 인증서를 통해 상호연동 가능 • 인증기관의 손상 시 하부 사용자에게만 영향을 줌 • 로컬 사용자들 간에 인증경로가 짧음 • 하나의 신뢰지점 폐지가 용이함
단점	• 신뢰지점이 다를 경우 검증 시 신뢰 경로가 길어짐 • 원하지 않는 신뢰관계 확장이 생길 수 있음 • 양방향 상호인증일 경우 많은 수의 인증서가 생김 • 경로 생성이 복잡할 수 있음 • 검증 시 다른 도메인에 있는 폐지정보를 접근하여야 함

기존 모델들은 단순히 이론적인 모델로써 보다 구체적인 실제 상호인증에 필요한 많은 부분들이 정의되지 않거나 구체적으로 표준을 어떻게 사용하여야 하는지에 대하여 명확히 설명하지 못하고 있다. 따라서 실제 상호인증에 적용하기에는 상당히 어려움이 있다.

위의 모델 중 국제간 상호인증을 위한 모델은 상호인증서(CC)를 이용한 방법이 안전성과 신뢰성을 기준을 볼 때 가장 우수함으로 이를 통해 상호인증

모델을 제안하고자 한다.

II. 현 PKI 구조 분석

2.1 프로파일

2.1.1 문제점

대부분의 인증기관이 CRL 분배점(DP: Distribution Point)방법을 사용하여 CRL을 발행하고 있다. 인증서 폐지목록의 발급자 분배점(IDP)의 사용이 CRL 생성 시 선택사항[2]이라서 발급자 분배점(IDP)을 생성하지 않는 경우 Man-in-the-middle-attack의 공격이 가능하다.

첫째, 해당 서비스 기관이 인증서 검증 시 저장된 CRL 유효기간 동안 CRL을 파일로 저장하여 사용하고 다음 발급시간(nextUpdate)을 확인하여 만료되었을 때 다시 검색하여 저장하는 방법을 사용할 경우, 해당하는 DP 파일을 다른 DP의 파일로 복사하면 유효한 CRL이 되기 때문에 그 구간에 해당하는 인증서 검증 시는 모두 성공하는 결과를 낳는다.

둘째, 인증서 DP에 해당하는 CRL 목록을 디렉토리 서버에서 검색하는 경우에 공격자가 해당 CRL 목록을 다른 CRL 목록으로 바꾸는 경우에도 동일한 결과가 나온다.

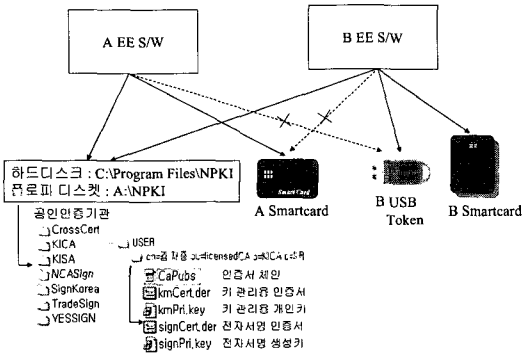
2.1.2 해결방안

위의 문제를 해결하기 위해서는 CRL 발행 시 확장필드에 IDP를 필수적으로 적용하고 인증서 검증 시 해당 인증서의 CRL DP와 디렉토리 서버 또는 Cache로부터 읽은 CRL의 IDP가 같은지를 반드시 비교하여야 한다.

2.2 인증서 저장 매체 환경(PSE)

2.2.1 문제점

각 인증기관의 PSE환경은 [그림 1]처럼 하드디스크나 플로피디스켓인 경우 NPKI\인증기관\USER\사용자명(DN)을 만들고 그 안에 전자서명 인증서(signCert.der), 전자서명 생성키(signPri.key), 키관리용 인증서(kmCert.der), 키관리용 개인키(kmPri.key)를 DER (Distinguished Encoding Rules)형식으로 저장[3]한다.



[그림 1] 현 NPKI에서의 PSE 연동 현황

또한 스마트카드는 Microsoft의 PC/SC를 이용하여 공통의 MAP(DF(F300) ,DF(F400))을 통하여 접근[4]하도록 되어 있지만 USB 토큰에 대한 표준은 아직 정해지지 않은 상태이다. 이러한 구조는 새로운 인증기관 추가 시나 새로운 저장매체 추가 시 모든 사용자 S/W에 대해 수정하여야한다.

2.2.2 해결방안

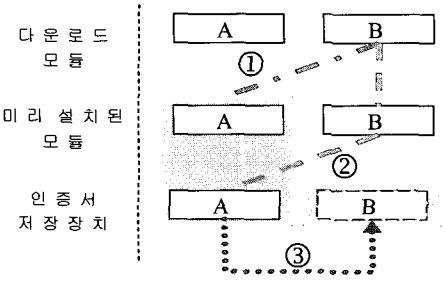
PSE를 연동하는 방법은 [그림 2]처럼 각 Layer별로 3가지 방법이 존재한다.

첫째는 CDSA(Common Data Security Architecture), Microsoft의 CryptoAPI 등의 공통 모듈 이용 방법이고, 둘째는 PKCS #11을 이용한 공통 토큰 이용 방법이고, 셋째는 PKCS#12을 이용한 키 전송 방법이다.

각각의 방법의 특징을 살펴보면 아래와 같다.

① 공통 모듈 이용(CDSA or CryptoAPI)

- 어플리케이션 요구사항에 매우 적합하며 각 도메인의 모든 요구사항 수용
- 매우 구현이 어려우며 제약조건에 대한 의견 조율이 불가능 (언어, 플랫폼 등)



[그림 2] PSE 연동 방법

2) TTAS.KO-12.0013 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준.

3) KCAC.UI 공인인증기관 상호연동 기술규격 v1.0.

4) KCAC.SC PKI 관련 스마트카드 기술규격 v1.0.

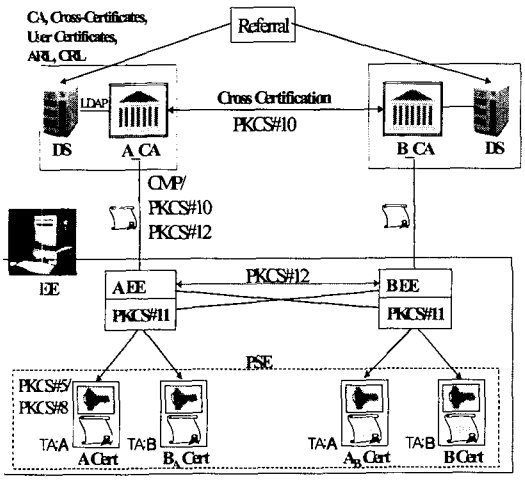
• 신규 적용시 적합한 방식
② 공통 토큰 이용 (PKCS#11)
• 제약 조건이 상대적으로 적음 (저장매체 종류, 서비스 방식, 호환성 등)
• 사용자 편의성 제공, 비교적 쉬운 구현
③ 키 전송 (PKCS#12)
• 다른 도메인의 어플리케이션 사용
• 사용자의 편의성 저해 (각 어플리케이션을 모두 사용하여야 함)
• 다른 도메인의 기능을 지원하기 위해 지속적인 구현이 필요 (확장 불가능)

위의 방법 중 현 국가간에 PKI가 구성되어 있는 상황에서 PSE 연동을 위해서 공통 토큰 이용 방식인 PKCS#11을 이용하는 것이 사용자의 편의성을 제공하고 구현상에도 편리성이 존재하므로 이 방식을 제안 모델에서 사용하고자 한다.

Ⅲ. 제안된 상호인증 모델

상호인증을 위한 기본 시나리오는 다음과 같다. 첫째, 인증기관 간 CA, 상호인증서, 사용자의 인증서 프로파일을 결정하고, 둘째, 결정된 프로파일에 의해 인증서를 발행하여 디렉토리 서버에 게시하고, 셋째, 사용자가 End Entity(EE) S/W를 통하여 다른 도메인의 저장매체(PSE)에 접근하여, 넷째, 다른 도메인의 응용 애플리케이션에서 전자서명을 사용한다.

이번 장에서는 위의 시나리오를 만족시킬 수 있는 상호인증을 위한 인증서 프로파일을 제안하고 디렉토리 서버에 대한 스키마를 설계하고 서로 다른 도메인간의 PSE를 효율적으로 접근하기 위한 방안으로 PKCS#11과 PKCS#12의 사용을 제안한다. 또한 해당 애플리케이션이 상호인증서 검증 시 사용되는 인증서 경로 획득 방법과 인증서 검증 방법을 제안한다. 이와 같이 기존의 표준을 바탕으로 구체적으로 상호인증이 가능한 모델을 제시하고자 한다.



〔그림 3〕 상호인증 전체 구성도

3.1 인증서 프로파일

3.1.1 인증서 기본필드

기본적인 인증서 프로파일은 IETF의 PKIX RFC 3280을 준용한다.

3.1.2 인증서 확장필드

기존의 확장필드를 바탕으로 인증기관, 상호인증서, 사용자에 대해 아래의 표와 같이 제안하고자 한

〔표 4〕 인증서 확장필드 설명

Field	Descriptions
기관 키 식별자	자신을 서명한 인증기관의 공개키에 대한 해쉬값을 가짐
주체 키 식별자	자기 자신의 공개키의 해쉬값
키 사용 (Key Usage)	해당 인증서의 용도를 나타내며, CA는 Certificate Signing, Off-line CRL Signing, CRL Signing을 사용하고, 사용자는 전자서명용 시 Digital Signature, Non-Repudiation을 사용하고 암호화 시 keyEncipherment를 사용함
인증서 정책 (Certificate Policy)	인증기관의 경우 해당 인증기관을 구별하는 고유한 값으로 부여되고 사용자의 경우 인증서의 사용등급을 나타내는 고유한 값으로 설정
기본제한 (Basic Constraints)	사용자가 인증기관의 역할을 수행하는 것을 방지하며 이를 위하여 인증기관의 여부 및 인증경로의 길이를 제한함
주체대체이름 (Subject Alternative Name)	추가적인 정보를 저장하는 곳으로 전자우편이나 본인확인에 필요한 식별번호가 포함되어 있음
CRL 분배점 (CRL Distribution Points)	인증서 발급 시 해당 일련번호의 특정간격에 따라서 CRL DN을 만들어 디렉토리 서버의 정보와 함께 인증서에 반영한 것으로 CRL을 이용하여 인증서 검증 시 사용
기관정보액세스 (Authority Information Access)	온라인 인증서 상태 프로토콜을 사용 시 해당하는 OCSP(Online Certificate Status Protocol) 서버의 접근방법 및 위치정보를 포함

〔표 5〕 제안된 인증서 확장필드

Field	Self		Cross		EE	
AuthorityKeyIdentifier	M	NC	M	NC	M	NC
SubjectKeyIdentifier	M	NC	M	NC	M	NC
Key Usage	M	C	M	C	M	C
CertificatePolicies	O	C	M	C	M	NC
PolicyMappings	-	C	M	NC	-	
SubjectAltName	O	NC	-		O	NC
IssuerAltName	O	NC	-		-	
BasicConstraints	M	C	M	C	-	
NameConstraints	-		O	C	-	
PolicyConstraints	-		O	C	-	
CRLDistributionPoints	O		O			
DistributionPoint	M	NC	M	NC	M	NC
fullName	M		M			
AuthorityInfoAccess	O	NC	O	NC	O	NC

다. 표에서 M(Mandatory)은 필수항목이고 O(Optional)는 선택사항을 의미한다. 확장필드의 생성 시 C(Critical)과 NC(Non-critical)를 구분해야 한다. 만약 C인 경우는 반드시 인증서 검증 시 확인해야 한다.

3.2 인증서 폐지목록 프로파일(CRL)

3.2.1 인증서 폐지목록 기본필드

기본필드는 버전(Version), 서명알고리즘(Signature), 발급자(Issuer),발급일자(This Update), 다음 발급일자(Next Update), 폐지 목록(Revoked Certificates)을 포함한다.

3.2.2 인증서 폐지목록 확장필드

CRL확장필드 설명 및 제안된 프로파일이다.

〔표 6〕 인증서 폐지목록 확장필드 설명

Field	Descriptions
발급자 공개키 식별자(Authority Key Identifier)	CRL을 서명한 인증기관의 공개키의 대한 해쉬값이나 인증기관명과 일련번호를 통하여 인증기관을 식별
발급자대체명칭	인증기관의 추가적 명칭
인증서 폐지목록 번호(CRL Number)	CRL을 식별하는 일련번호로 순차적으로 증가하는 양의 정수를 사용
발급자 배포지점(Issuing Distribution Point)	특정한 CRL을 획득할 수 있는 위치정보. 해당 인증서의 CRL DP의 값으로 인증기관이나 사용자에 대한 CRL 정보를 포함

〔표 7〕 제안된 인증서 폐지목록 프로파일

Field	CRL		ARL	
IsureAltName	-		-	
AuthorityKeyIdentifier	M	NC	M	NC
CRLNumber	M	NC	M	NC
DeltaCRLIndicator	-		-	
IssuingDistributionPoint	M	C	M	C

* ARL: Authority Revocation List

3.3 디렉토리 스키마

사용자(End Entity), 인증기관(CA), CRL 분배점(DP)에 대한 디렉토리 스키마를 아래와 같이 제안하고자 한다. 아래 [표 8]은 제안된 디렉토리 스키마에 대한 객체(Object Class)와 속성(Attribute)을 보여준다. 만약 디렉토리 서버가 바이너리를 구분하는 경우 해당 속성 이름에 ';binary'를 붙여서 저장하도록 한다. 따라서 디렉토리에서 인증서를 검색하는 경우에는 두 가지 경우를 모두 검색하여 보아야 한다.

〔표 8〕 제안된 디렉토리 스키마

	Objectclass	Attribute
CA	person oranizationalPerson inetOrgPerson CertificateAuthority	commonName surName cACertificate crossCertificatePair certificateRevocationList authorityRevocationList
End Entity	person oranizationalPerson inetOrgPerson	commonName surName userCertificate
CRL DP	cRLDistributionPoint	ou certificateRevocationList
referral	country referral	country ref

3.3.1 사용자 인증서

사용자의 인증서는 userCertificate라는 속성에 DER 형식으로 게시되며 전자서명용과 암호화용이 있을 경우는 다중 값(Multi Value)으로 전자서명용을 먼저 저장한다.

3.3.2 상호인증 인증서(Cross Certificate)

상호인증 인증서는 디렉토리 서버의 cross-CertificatePair라는 속성에 DER 형태로 자신이 상대방에게 발행한 인증서(forward)와 상대방이 나에게 발행한

인증서(reverse)가 함께 게시된다.

상호인증서 속성인 crossCertificatePair의 ASN.1 구조는 아래와 같다.

```
SEQUENCE {
  Context Specific[0]   /* forward */
  Context Specific[1]   /* reverse */
}
```

3.3.3 CRL과 ARL

인증서 폐지목록은 certificateRevocation List 라는 속성에 DER형태로 게시된다. 인증기관이 하나의 CRL을 배포하는 경우에는 CA의 엔트리에 게시되고 CRL 분배점(DP)을 사용하여 여러 개의 CRL을 배포하는 경우에는 별도의 ObjectClass를 정의하여 certificate RevocationList에 게시된다.

ARL은 CA의 속성에 포함된 authority Revocation-List에 DER형태로 게시된다.

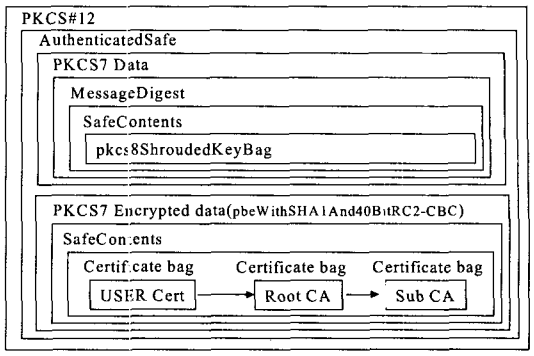
3.3.4 Referral

상호인증한 도메인의 디렉토리 정보를 얻기 위해서 Referral을 이용하여 해당 디렉토리 서버에 대한 정보를 할당한다. 이는 상호인증서 검증시 신뢰지점(TA: Trust Anchor)의 디렉토리 정보를 얻는데 사용된다.

3.4 인증서 전달 방법 - PKCS#12

PKCS#12은 암호화된 개인키, 사용자 인증서, 인증서 경로를 다른 시스템으로 전달하는 표준이다. 인증서를 PKCS#12 형태로 추출(Export)하여 다시 타 기관에 PKCS#12 형태로 입력(Import)하는 방법을 사용한다. 인증기관이 인증서를 PKCS#12 형태로 발급하여 전달하는 방법을 사용하거나 다른 플랫폼으로 이동시키기 위해서는 인증기관들 간에 아래와 같은 규약을 지키도록 제안한다.

개인키는 국제 표준인 Triple DES, ACE를 이용하여 PKCS#5 형식으로 만들어 PKCS#8 형식으로 저장되어야 하고, 인증서는 전자서명용 인증서와 키 관리용 인증서를 모두 포함 가능해야하며, 개인키의 LocalKeyID와 대응하는 인증서의 값은 동일하여야 한다. 인증서의 체인은 포함을 권고하며 순서는 사용자 인증서, 루트 인증서, 하위 CA인증서 순으로 한다. CRL 데이터는 포함하지 않는다. PKCS#12를 암호화하는 값은 개인키를 암호화하는 값과 동일하거나 다를 수 있다.



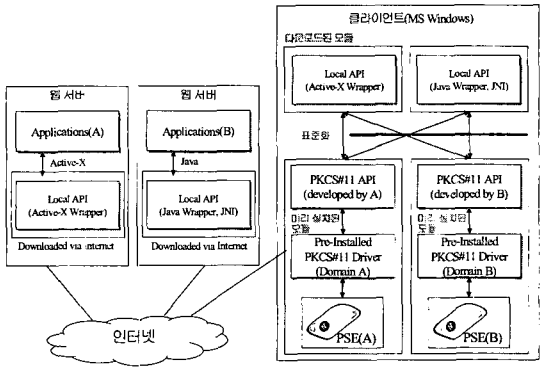
〔그림 4〕 PKCS#12 구조

3.5 인증서 저장매체(PSE) - PKCS#11

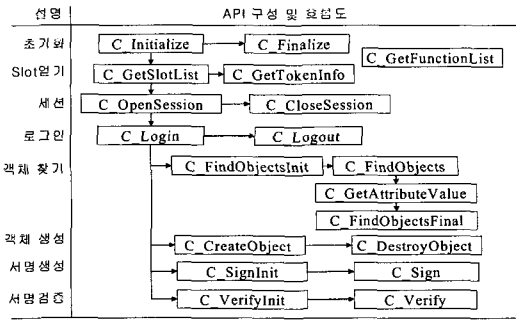
PKCS#11는 응용 애플리케이션들과 다양한 휴대용 보안 장치(예를 들어 스마트카드, PCMCIA 카드, 스마트 디스크, USB토큰 등)와의 인터페이스에 관한 표준으로, 디바이스와 응용 애플리케이션간의 프로그램 인터페이스를 제공하고 응용프로그램에 보안 디바이스에 대한 공통 모델을 제공한다. 또한 멀티 쓰레드 환경에서의 리소스 공유를 지원한다.

[그림 5]는 각 인증기관이 자신의 PSE에 대하여 PKCS#11 드라이버를 통하여 최소한의 함수를 제공하면 각 인증기관은 미리 배포된 모듈을 통하여 다른 기관의 PSE를 자유롭게 접근할 수 있도록 하는 구조를 제안하고 있다. 이 구조는 기존 인증기관의 PSE 구조의 단점을 보완하여 새로운 기관의 추가 시에는 추가된 기관의 PKCS#11에 대한 드라이브만 새로 추가하면 되고 새 매체의 추가 시에도 변경된 기관의 PKCS#11 모듈을 재배포하면 자연스럽게 사용이 가능하다.

상호인증을 위해서 PKCS#11에서 최소한 요구되



〔그림 5〕 PKCS#11을 이용한 상호인증 모델



〔그림 6〕 최소 지원해야1할 PKCS#11 API 목록

는 API는 초기화, 종료함수, 슬롯관련함수, 세션 관련 함수, 로그인, 로그아웃함수, 객체 찾기, 생성관련 함수, 전자서명, 검증 함수 등이 최소한으로 요구되는 함수이다. [그림 6]은 API들 간의 관계를 설명한 것이다.

3.6 상호인증서 검증 절차

응용 프로그램에 상호인증을 적용하려면 많은 부분에 대하여 고려하여야 한다. 이 중 CRL을 통한 인증서 검증 시 인증경로 획득방법과 신뢰지점에 따라 인증서를 검증하는 방법을 제시하고자 한다.

3.6.1 인증서 검증 경로 구성

인증서 경로 구성하는 방법은 신뢰지점에 따라서 아래와 같이 구성된다.

1) A_User가 자신의 도메인의 A 응용 애플리케이션을 사용하는 경우는 신뢰지점이 A_RootCA가 되어 인증 경로가 A_RootCA 인증서, A_User 인증서 순으로 구성된다.
2) B_User가 자신의 도메인의 B 응용 애플리케이션을 사용하는 경우는 신뢰지점이 B_RootCA가 되어 인증 경로가 B_RootCA 인증서, B_User 인증서 순으로 구성된다.
3) B_User가 B_CA가 발급한 A 도메인용 상호인증서(A_B User)를 사용하여 서명하고 A응용 애플리케이션이 검증하는 경우 신뢰지점은 A_RootCA가 되어 A_RootCA 인증서, A-B 상호인증 CA인증서, A_B User 인증서 순으로 인증서 경로가 구성된다.
4) A_User가 A_CA가 발급한 B 도메인용 상호인증서(B_A User)를 사용하여 서명하고 B 응용 애플리케이션이 검증하는 경우 신뢰지점은 B_RootCA가 되어 B_RootCA 인증서, B-A 상호인증 CA인증서, B_A User 인증서 순으로 인증경로가 구성된다.

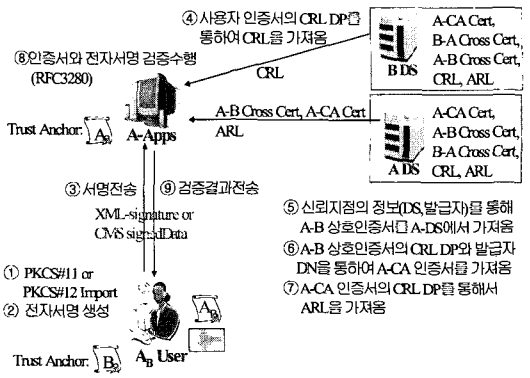
〔표 9〕 인증 경로 구성 및 검색 위치

			Trust Anchor	
			A	B
USER	A	Chain	A_CA	B_CA→B-ACA
		CRL	A_DS	A_DS
		ARL	A_DS	B_DS
	B	Chain	A-BCA→A_CA	B_CA
		CRL	B_DS	B_DS
		ARL	A_DS	B_DS

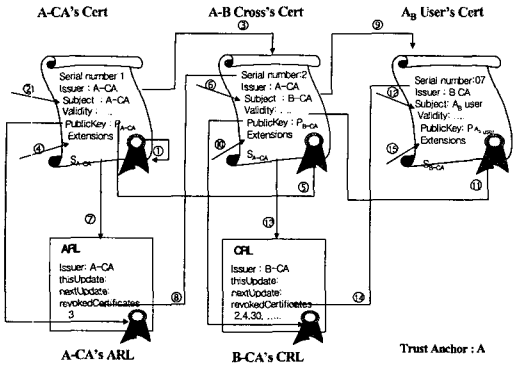
3.6.2 상호인증 경로 검증(Certification Path Validation)

인증서 검증을 수행하기 위해서는 인증경로를 먼저 구성하여야 한다. 신뢰지점이 B인 사용자가 신뢰지점이 A인 응용프로그램을 사용하는 경우의 인증경로 구성방법을 예로 들면 다음 그림과 같다.

① B_User가 PKCS#12를 통하여 A 도메인의 EE S/ W에 삽입한 상호인증서(A_B User)를 이용하거나 PKCS#11의 인터페이스를 이용하여 전자서명을 생성한다.
② 전자서명은 암호화되어 있는 개인키를 복호화하여 원문을 해쉬하고 해쉬한 결과를 공개키 알고리즘(RSA)을 이용하여 생성한다. 전자서명된 값을 인코딩하는 방법에는 CMS(RFC 2630: Cryptographic Message Syntax)의 signedData, XML Signature(RFC 3275) 등이 있다.
③ 전자서명한 결과를 A 응용 애플리케이션 서버(A_Apps)에 전달한다. 여기에는 원문, 서명한 사용자의 상호인증서, 전자서명값 등이 포함된다.



〔그림 7〕 상호인증 검증 시나리오



〔그림 8〕 CRL을 이용한 인증서 검증 방법 예제

④ A 응용 애플리케이션 서버는 사용자 B의 상호인증서의 인증서 폐지목록(CRL)의 분배점(DP)내의 URI정보를 이용하여 CRL을 디렉토리 서버에서 검색하여 온다.

⑤ A 응용 애플리케이션의 신뢰지점(TA)으로부터 디렉토리 정보와 발급자를 통하여 A-B상호인증 CA 인증서를 검색하여 온다.

⑥ A-B상호인증 CA인증서의 CRL DP와 발급자 DN을 가지고 A Root인증서를 가져온다.

⑦ A Root 인증서의 CRL DP를 이용하여 ARL을 가져온다.

⑧ 인증서 경로 및 ARL/CRL을 통하여 인증서 경로 검증을 수행한다. 인증서 경로 검증은 RFC 3280을 준용한다.

⑨ 검증한 결과를 사용자에게 전달한다.

3.7 제안 모델의 특징

제안된 상호인증 모델의 특징은 다음과 같다.

1) CR, CTL, CC 중 가장 신뢰성 있고 안전한 CC를 기반으로 상호인증 모델을 설계하였다.
2) NPKI가 지니는 문제점을 해결하여 국내 상호연동을 국제상호인증이 가능하도록 하는 구체적인 모델을 제시하였다.
   - 프로파일에 CRL의 IDP를 필수로 적용함으로써 발생 가능한 Man-in-the-middle-attack을 방지하였고 PSE 확장 및 변경시의 문제점을 PKCS#11을 이용하여 사용자 편의성 및 구현의 간편성을 제공하였다.
3) PKCS, IETF의 PKIX 등의 표준을 기반으로 하여 확장성 및 구체적인 구현방법을 제시하였다.
   - 상호인증을 위해서 RFC 3280을 기반으로 인증서 및 인증서 폐지목록의 프로파일을 제시하였다.
   - PKCS#12를 이용하여 인증서의 전달방법을 제시하고 인증서에 맞는 기본 구조를 제안하였다.
   - 기존의 디렉토리 스키마를 기반으로 상호인증이 가능하도록 스키마를 확장 설계하였다.

Ⅳ. 결 론

제안된 상호인증 모델은 기존의 인증기관간 상호연동체계가 갖고 있는 문제점을 해결하여 국제상호인증체계로 발전시키고자 하였다. 이를 위해 인증서 프로파일에서 CRL DP와 IDP에 대한 설정을 필수사항으로 제안했다. 또한 기존 인증서 저장매체의 한계점을 극복하기 위해서 PKCS#11을 이용한 표준 인터페이스 사용을 제안하여 응용 애플리케이션과의 API 연동을 가능하게 하였다. 그리고 기존의 인증서 검증 방법인 RFC 3280을 기반으로 이를 상호인증 사용자 인증서에 적용하여 신뢰기관에 따른 검증 시나리오를 제안하였다. 제안된 모델은 PKCS, IETF의 표준을 기반으로 하여 기존의 상호인증 모델에 대한 해석과 구현상에 존재하는 문제점을 보완할 수 있는 구체적인 상호인증 방법을 제시하고 있다.

참 고 문 헌

[1] RFC 3280, IETF, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, 2002.

[2] RFC2510, IETF, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, 1999.

[3] RFC 2251, IETF, *Lightweight Directory Access Protocol (v3)*, 1997.

[4] PKCS#1 v2.0, RSA, *RSA Cryptography Standard*, 1998.

[5] PKCS#5 v2.0, RSA, *Password- Based Cryptography Standard*, 1999.

[6] PKCS#8 v1.2, RSA, *Private Key Information Syntax Standard*, 1993.

[7] PKCS#10 v1.7, RSA, *Certificate Request Syntax Standard*, 2000.

[8] PKCS#11 v2.2, RSA, *Cryptographic Token Interface Standard*, 2003.

[9] PKCS#12 v1.0, RSA, *Personal Information Exchange Syntax Standard*, 2000.

[10] RFC 2560, IETF, *Online Certificate Status Protocol*, 2002.

[11] Steve Lioyd, David Fillingham, Steve Orlowski and John Weigelt, *CA-CA Interoperability*, PKI Forum White Paper, 2001.3

[12] TTAS.KO-12.0012, TTA, *전자서명 인증서 프로파일 표준*, 2000.

[13] TTAS.KO-12.0013 TTA, *전자서명 인증서 효력정지 및 폐지목록 프로파일 표준*, 2001.

[14] KCAC.UI, KISA, *공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격 v1.00*, 2002.

[15] KCAC.CTL, KISA *인증기관간 상호연동을 위한 기술규격 v1,01*, 2002.

〈著者紹介〉

김 재 중 (Jae-Jung Kim) 정회원

1997년 2월 : 충남대학교 컴퓨터과학과 학사
2003년 8월 : 고려대학교 정보보호대학원 석사
1996년 12월~1999년 7월 : LG-EDS 시스템 연구원
1999년 7월~현재 : 한국정보인증 선임연구원
<관심분야> 정보보호, PKI

이 동 훈 (Dong-Hoon Lee) 종신회원

1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 부교수