제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

# 공개키 기반구조 기반 Proxy 키 관리 모델에 관한 연구

이진우*, 주미리**, 양형규***, 원동호*
*성균관대학교 컴퓨터공학과
**국가보안기술연구소
***강남대학교 컴퓨터미디어공학부
e-mail : jwlee@dosan.skku.ac.kr

# A Study on Efficient Key Management Model based on PKI using Proxy Server

Jinwoo Lee*, Miri Joo**, Hyungkyu Yang***, Dongho Won*
*Dept of Computer Engineering, Sungkyunkwan University
**National Security Research Institute
***School of Computer Media Engineering, Kangnam University

요 약

최근 인터넷과 네트워크 환경의 발달로 인한 전자상거래의 활성화는, 전송되는 정보의 기밀성과 무결성을 제공하기 위해 암호 기술을 요구한다. 이러한 암호 기술의 안전성은 암호학적 키에 의존하며, 사용자의 수가 증가함에 따라 안전하고 효율적인 키 관리 모델의 필요성이 대두되고 있다. 본 논문에서는 일반적인 공개키 기반구조(PKI : Public Key Infrastructure)기반 키 관리 시스템에서 키 관리 서버에 집중되어 있는 서비스들을 Proxy 서버에 분산함으로써 키 관리 서버의 과부하 및 통신량을 줄일 수 있는 효율적인 키 관리 모델을 제안한다.

## 1. 서론

네트워크 환경의 발달은 개인의 프라이버시, 기업경영 비밀 등의 정보보호를 위해 암호 기술들이 요구되고 있다. 이러한 암호 기술은 암호 알고리즘의 비밀성에 의존하는 것이 아니라 키의 기밀성에 의존하므로 키의 관리가 중요하다. 키 관리란, 인가된 개체들간의 공통된 키 정보를 유지·지속하기 위해, 암호 기술을 기반으로 하는 보안 시스템에서의 키 생성, 키 분배, 키 저장, 키 복구, 키 폐기와 관련된 일련의 과정을 의미한다. 일반적인 키 관리 모델은 키 관리 센터(KMC : Key Management Center)의 키 관리 서버가 키 생성, 키 분배, 키 저장, 키 복구, 키 폐기 기능들을 모두 제공한다. 하지만 이러한 중앙 집중식 모델은 네트워크 과부하 현상이 발생하며, 대규모 그룹에서의 효율적인 키 관리를 제공할 수 없다. 따라서, 본 논문에서는 전자상거래에서 사용되는 PKI 기반에서의 효율적인 키 관리 모델을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 키 관리 표준 규격 및 일반적인 키 관리 모델을 알아보고 3 장에서는 Proxy 서버를 이용한 키 관리 모델을 제안한다. 4 장에서는 결론 및 향후 연구 계획에 대해 설명한다.

## 2. 관련연구

본 장에서는 키 관리 시스템이 제공하는 기능에 대한 표준규격을 분석하고, 일반적인 키 관리 모델을 기술한다.

### 2.1 키 관리 기능

키 생명주기(key lifecycle)와 관계하여 키 관리 기능은 크게 키 생성, 키 분배, 키 저장, 키 복구, 키 폐기로 구분된다.

■ 키 생성 기능

키 생성 기능은 암호 알고리즘에서 안전하게 키를 생성하는 기능이며, 이는 랜덤 과정, 의사-랜덤 과정을 통해 위조할 수 없고 예측할 수 없도록 키를 생성하는 것을 의미한다. FIPS 186 은 서명에 사용되는 비밀키 생성에 필요한 안전한 파라미터에 대한 요구사항을 정의하고 있으며, DSA(Digital Signature Algorithm)에서의 공개키/개인키 쌍을 생성하는 과정에 대해 기술하고 있다. ISO 11568 에서는 공개키/개인키 쌍을 생성하기 위한 요구사항, 그리고 ISO 1594 에서는 타원곡선 상에서의 키 쌍 생성에 관한 정의를 하고 있다[1][2].

■ 키 분배 기능

키 분배 기능은 인가된 개체들 사이에 키 또는 키 자료(key material)가 안전하게 공유되는 것을 의미한다. 이와 관련된 키 분배 표준을 살펴보면, [표 2-1]과 같다[3][4][5][6][7].

[표 2-1] 키 분배 표준

| 관련 표준 | 내용 |
|---|---|
| IEEE P1363 | • 이산대수와 타원곡선 기반의 D-H(Diffie-Hellman)형 키 분배 프로토콜<br>• 패스워드 기반의 키 분배 프로토콜 |
| PKCS #3 | • 이산대수 D-H형 키 분배 프로토콜 |
| ANSI X9.42 | • 이산대수 D-H형 키 분배 프로토콜<br>• MQV 키 동의 기법 |
| ANSI X9.44 | • RSA형 키 동의와 키 전송 프로토콜 |
| ANSI X9.63 | • 타원 곡선 기반 D-H 키 분배 프로토콜<br>• 11개의 키 동의 프로토콜 1-pass, 3-pass 2개의 키 전송 프로토콜 |

■ 키 저장 기능

키 저장 기능은 키를 사용하거나, 복구를 위한 백업을 위해 키를 안전하게 저장하는 것을 의미한다. KS X6318 에서는 안전한 암호장치에 키를 저장하는 경우와 물리적으로 안전한 환경에서 키를 저장하는 방식에 대해 정의하고 있으며, 키 저장 시 키 암호화 키(KEK : Key Encryption Key)로 키를 암호화 하여 저장하는 기법에 대해 기술하고 있다. ISO 11568 에서는 공개키 암호 방식의 공개키로 대칭키를 암호화, 공개키 암호 방식을 이용한 공개키의 암호화, 그리고 대칭키 암호 방식을 이용한 공개키의 암호화 기법을 정의하고 있다[2][8].

■ 키 복구 기능

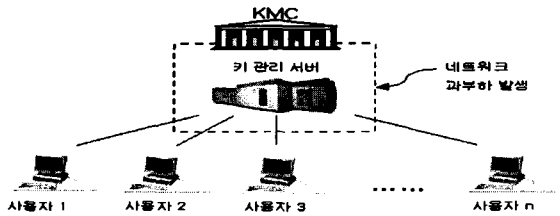
키 복구 기능은 합법적인 상황에서 암호문을 복호화하거나, 사용자가 자신의 비밀키를 분실했을 경우 등의 유사시에 허가된 사용자만이 복호화를 할 수 있는 기능을 제공하기 위해 이루어진다. FIPS 185 에서는 암호키 복구를 위한 LEAF(Law Enforcement Access Field)를 정의하고 있으며, 키에 문제가 발생하였을 경우 LEAF 를 사용하여 데이터 복구 기관을 통해 키를 복구한다[9].

■ 키 폐기 기능

키 폐기 기능은 더 이상 사용될 필요가 없는 키의 안전한 폐기를 위해 이루어진다. 키를 폐기한다는 것은 모든 기록을 제거함으로써 폐기 후에 남아있는 어떠한 정보를 가지고도 폐기된 키를 다시 복구 시킬 수 없도록 하는 것을 의미한다. ISO 11568 에서는 공개키와 개인키 폐기에 대해 기술하고 있다[2].

### 2.2 일반적인 키 관리 모델

키 관리 시스템은 하나의 키 관리 서버가 키 생성 기능, 키 분배 기능, 키 저장 기능, 키 복구 기능, 키 폐기 기능 모두 수행함으로써 다수의 사용자가 접속할 경우, 네트워크 과부하로 인한 통신장애, 통신속도 저하, 데이터 처리 능력 감소 등 여러 가지 문제가 발생할 수 있다. 또한, KMC 가 다수의 키 관리 서버를 가지고 있을 경우에도 키 관리 서버의 중앙 집중적인 처리 능력은 해결되지 않는다. [그림 2-1]은 일반적인 키 관리 모델의 개념도이다.




[그림 2-1] 일반적인 키 관리 모델

## 3. 제안하는 Proxy 서버를 이용한 키 관리 모델

본 장에서는 Proxy 서버의 특징과 제안하는 키 관리 모델의 구성요소 및 동작과정에 대해 기술한다.

### 3.1 Proxy 서버

Proxy 서버란 '어떠한 작업을 대신해 주는 서버'라는 의미로 클라이언트와 서버 사이에 데이터를 중계하는 역할을 하며 사용자와 서버사이에 존재한다. 다음 [표 3-1]은 Proxy 서버의 대표적인 기능을 나타낸 것이다.

[표 3-1] Proxy 서버의 특징

| 기능 | 특징 |
|---|---|
| 캐쉬(Cache)기능 | • 네트워크의 트래픽을 줄이고, 데이터 전송 시간을 향상 |
| 방화벽(Firewall)기능 | • 네트워크 외부로부터 허가 받지 않은 접속을 제한 |

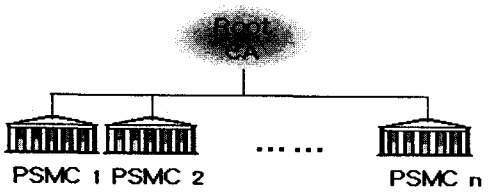
### 3.2 구성 요소

1) Proxy 서버 관리 센터(PSMC : Proxy Server Management Center) : PSMC 는 제 3 의 신뢰기관(TTP: Trusted Third Party)으로, 하나의 Proxy 관리 서버와 다수의 Proxy 서버를 가지고 있으며 이 센터의 주요 서비스는 다음과 같다.
   - 인증(Certification)
     : 인증서와 CRL(Certificate Revocation List)을 발행
   - 등록(Registration)
     : 사용자의 이름을 구분, 등록, 관리를 수행
   - 검증(Validation)
     : 인증서의 유효 기간 확인
     OCSP 서버(Online Certificate Status Protocol)
   - 디렉토리(directory)
     : 사용자의 공개키를 등록하며, 인증서와 CRL 을 저장하는 곳으로 사용자 접근이 가능
   - 키 관리(Key management)
     : 사용자의 키 생성, 분배, 저장, 복구, 폐기 등 전반적인 키 관리를 수행

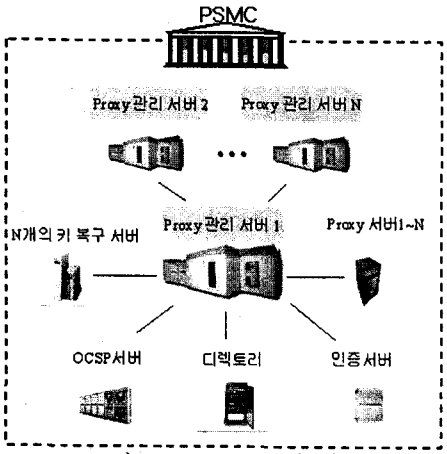
2) Proxy 관리 서버 : 다수의 Proxy 서버를 관리하며, 키 복구 정책 관리 기능, 정책에 따른 키 복구 기능과 키 저장, 키 폐기, 키 감사 기능을 담당한다.

3) Proxy 서버 : 키 생성, 키 분배 기능을 담당하다.

[그림 3-1]과[그림 3-2]는 PSMC 계층과 PSMC 구성 서버를 도식화한 것이다.




[그림 3-1] PSMC 계층




[그림 3-2] PSMC 구성 서버

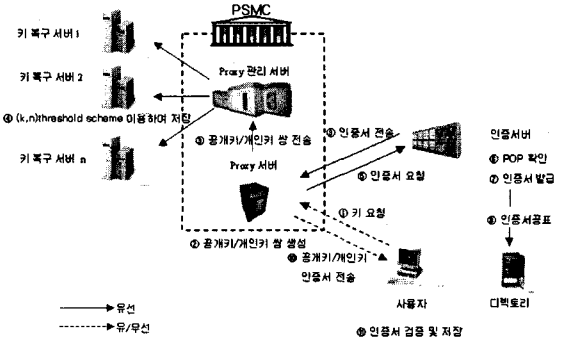
### 3.3 동작과정

■ 키 생성

Proxy 서버가 담당하며, 사용자가 암호통신을 하기 위해 키 쌍을 요청하면, 유무선 환경에 가능하도록 Proxy 서버는 ISO 15946 표준에 준거하여 키 쌍을 생성한다.

■ 키 동작과정

Proxy 관리 서버가 다수의 Proxy 서버를 두어 사용자의 접속을 원활하게 하며, 키 관리 서버가 키 생성 기능과 키 분배 기능을 Proxy 서버에게 위임함으로써 키 관리 서버의 과부하 및 통신량을 줄일 수 있다. PSMC 의 동작과정은 [그림 3-3]와 같다.



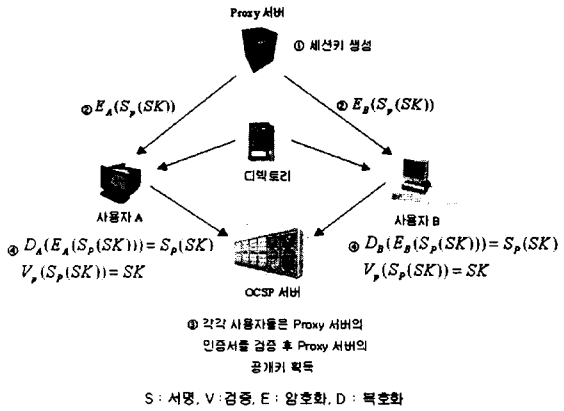

[그림 3-3] PSMC 동작과정

1) Proxy 서버는 사용자가 키를 요청하면 사용자의신원 확인 후 사용자의 공개키/개인키 쌍을 생성하여 Proxy 관리 서버에게 전송한다.
2) Proxy 관리 서버는 (k,n)-threshold scheme 을 이용하여 개인키를 n 개의 복구서버에 저장한다.
3) Proxy 서버는 인증서버에게 사용자의 공개키에 대한 인증서를 발급을 요청하고, 이를 요청받은 인증서버는 인증서 발급을 요청한 공개키에 대응하는 정당한 개인키를 Proxy 서버가 소유하고 있는지 여부를 (POP : Proof Of Possession) 확인한다.
4) POP 확인을 마친 인증서버는 공개키 인증서를 발급하여 Proxy 서버에게 전송함과 동시에 디렉토리 서버에 인증서를 등록한다.
5) Proxy 서버는 공개키/개인키 쌍과 인증기관으로부터 전송 받은 인증서를 사용자에게 전송한다.
6) 사용자는 Proxy 서버로부터 전송 받은 공개키/개인키 쌍과 인증서의 정당성을 확인하여 저장한다.
7) 사용자는 Proxy 서버로부터 받은 공개키/개인키 쌍을 이용하여 다른 사용자와 암호 통신 및 전자서명 등을 수행할 수 있다.
8) 만약, 사용자의 개인키가 손상된 경우 사용자는 Proxy 서버에게 재발급을 신청할 수 있으며, 분실된 경우에는 키 관리 서버에게 키 복구를

요청할 수 있다. 이때 Proxy 관리 서버는 합법적인 복구절차를 통하여 키 복구를 수행할 수 있다.

■ 키 분배과정

위와 같은 과정으로 키 쌍과 인증서를 받은 사용자 간 키 분배를 수행하는 과정은 [그림 3-4]과 같다.




[그림 3-4] PSMC 동작과정

1) Proxy 서버는 세션키 생성 후 자신의 개인키로 서명한 후 각 사용자의 공개키로 암호화하여 전송한다.
2) 각 사용자는 디렉토리에서 Proxy 서버의 인증서를 다운 받은 후 OCSP 서버를 통해 검증한다.
3) 각 사용자는 개인키로 복호화 후 Proxy 서버의 공개키로 서명 검증 후 세션키를 얻게 된다.

### 3.3 제안하는 모델의 특징

제안하는 키 관리 모델에서 사용자는 암호 통신을 할 경우, Proxy 관리 서버에 요청할 필요 없이 Proxy 서버에 접속하여 사용할 키를 분배 받을 수 있으며, Proxy 서버의 데이터 캐쉬기능으로 키 재발급 시 Proxy 서버는 사용자 확인 절차 후 바로 사용자에게 전송해준다. 또한, Proxy 서버의 방화벽으로 인해 제 3 자가 Proxy 서버는 물론, 키 관리 서버 및 키 복구 서버로의 접속을 제한함으로써 키 관리 서버가 저장하고 있는 키를 안전하게 보호할 수 있다. 제안하는 모델은 여러 개의 Proxy 서버에게 Proxy 관리 서버가 키 생성 기능, 키 분배 기능을 위임함으로써 일반적인 키 관리 모델에서 키 관리 서버의 중앙 집중 처리 능력을 분산 시킬 수 있다. 처리 능력을 분산시킴으로써 키 관리 서비스의 확장성이 뛰어나며, 특정 그룹 키 관리 시 전용 Proxy 서버를 사용하여 효율적으로 키 관리를 할 수 있다. [표 3-2]은 특징을 간략하게 정리한 것이다.

[표 3-2] 제안하는 모델 특징

| 특징 | 내용 |
|---|---|
| 기존 PKI와의 상호연동 | • 기존 CA시스템 변경없이 사용 가능 |
| 키에 대한 접근성/안정성 보장 | • Proxy 서버의 방화벽 사용(접근통제)<br>• 키 복구 권한의 분산으로 키 안전성 보장 |
| Proxy 서버 사용 | • 데이터 캐쉬 기능으로 통신 속도 향상<br>• Proxy 관리 서버의 중앙 집중식 처리 능력 분산<br>• 확장성 용이<br>• 특정 그룹 키 관리 시 전용 Proxy 서버를 동으로써 효율적인 키 관리 제공 |
| 다양한 환경에 적용 | • Proxy 서버를 이용함으로써 이동 통신 환경 등 다양한 환경에 적용 가능 |

## 4. 결론 및 향후 연구과제

최근 정보통신 기술의 발달과 함께 전자상거래 활성화로 다양한 암호 응용서비스의 사용자가 증가하였다. 이에 개인 및 기업의 프라이버시를 보호하기 위해 암호 기술들이 적용되고 있으나, 이러한 암호 기술에 사용되는 키 관리 시스템의 개발은 미흡한 실정이다. 이에 본 논문에서는 Proxy 서버를 이용하여 중앙 집중식 키 관리 모델의 단점인 서버의 과부하 및 통신 장애를 해결하고, 이동 통신환경에서도 적용할 수 있는 모델을 제안하였다. 현재 키 관리 시스템은 독립적으로 개발되기 보다는 다른 암호학적 서비스의 부가적으로 제공되고 있다. 따라서 안전하고 효율적인 통합 키 관리 모델에 관한 연구가 필요하다.

## 참고문헌

[1] NIST, "FIPS-PUB 186 Federal Information Processing Standards Publications: Digital Signature Standard", 1994
[2] ISO, "ISO 11568 Banking-Key management", 1998
[3] IEEE, "IEEE P1363 Standard Specifications For Public Key Cryptography", 2001
[4] RSA research, "PKCS #3 Diffie-Hellman Key Agreement Standard", 1999
[5] ANSI, "ANSI X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of symmetric keys Using discrete Logarithm Cryptography", 1998
[6] ANSI, "ANSI X9.44 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Factoring-Based Cryptography", Draft
[7] ANSI, "ANSI X9.63 Public Key Cryptography for the financial Services Industry: Key Agreement and Key Transport Using Elliptic Key Cryptography", Draft
[8] 기술표준원, "KS X 6318 Banking-Key management(retail)", 1995
[9] S. H. Oh and D.H. Won, "Method for key distribution using proxy server", 2002
[10] PKI X.509, "Intranet X.509 Public Key Infra- structure Certificate and CRL Profile", 1999
[11] NIST,"FIPS-PUB 185 Escrowed Encryption Standard", 1994
[12] 기술표준원, "KS X 6317 Banking-Key management (wholesale)", 1996