通信情報保護學會論文誌
第 10 券 第 4 號, 2000. 12

# 전자정부 구현을 위한 효율적인 GPKI 구축 방안

장 홍 종*, 박 인 재*, 이 정 현**

# Implementation of Efficient GPKI for E-Government

Hong-Jong Chang*, In-Jae Park*, Jung-Hyun Lee**

요 약

전자정부 구현에 있어 온라인 상에서 유통되는 각종 행정정보들에 대한 정보보호는 필수적인 선결 조건이다. 미국 등 각국에서는 전자정부의 정보보호 기반 구축을 위하여 가상행정 환경에서 당사자의 신원 확인, 기밀성, 무결성, 부인봉쇄 등을 보장하는 정부차원의 PKI(Public Key Infrastructure)를 구축·운영 중에 있다. 본 논문에서는 미국 등 선진국의 사례 연구 분석을 통하여 우리나라 실정에 적합한 효율적인 GPKI(Government PKI) 구축방안을 제시하였다.

ABSTRACT

It is an essential prior condition that information security of all sorts of administration-information on line for E-Government. Every country including United States has been constructing and managing Government PKI(Public Key Infrastructure) of information security of one's own authentication, confidentiality, integrity, non-repudiation in administration environment on line for information security base construction of E-Government. In this paper, we present an efficient GPKI(Government PKI) implementation suitable for Korea actual circumstance through study and analysis of superior case such as United State.

**keyword** : *E-government, GPKI, Bridge CA, GPKI 인증서 프로파일, GPKI CRL 프로파일*

## Ⅰ. 서 론

지식 정보화 사회에서 정부의 행정환경은 종이문서위주, 대면위주의 사무처리방식에서 비대면 온라인 전자문서기반으로 전환되어 하나의 정보기술 공유기반 위에서 정부의 각종 정보와 행정서비스를 신속하게 제공하게 될 것이다.

그러나 네트워을 통한 정부 주요 문서 및 개인 정보의 유통이 급격히 증가하게 됨에 따라 온라인 상에 노출되는 정보들에 대한 불법적인 도청, 위·변조 및 신분위장 등 각종 역기능에 의한 위협이 예상되고 있다.

이에 미국을 비롯한 선진 각국에서는 전자정부의 안전성·신뢰성 확보를 위해 행정 분야에 공개키 암호기술을 적용하여 가상 행정환경에서 당사자의 신원확인, 전자문서의 정보보호 및 무결성 보장, 전자행위에 대한 부인봉쇄 등을 제공하는 PKI(공개키기반구조 :Public Key Infrastructure)[1]를 구축하고자 노력하고 있다.

우리나라에서도 정부차원 GPKI 구축계획을 수립·시행 중에 있으나, 행정기관 공통의 기술표준이 정립되지 않은 상태이다. 따라서 각 기관별·사업별로

* 행정자치부
** 인하대학교

인증 기반구조를 구축할 경우, 부처간 상호연동성을 확보할 수 없어 효율적인 GPKI의 조성이 어렵게 될 것이므로 관련 기술표준과 효율적인 구축방안에 대한 연구가 시급한 실정이다.

이에 본 논문에서는 미국 등 선진사례들에 대한 연구·분석을 통해 대하여 우리나라 실정에 맞는 효율적인 GPKI (Government PKI) 구축방안을 제시하고자 한다.

## II. GPKI 구성방안

### 2.1 구성요소 및 외국 사례

본 논문에서 제안하는 GPKI는 〔표 1〕과 같이 5개의 구성요소로 이루어져 있으며, 가교 CA는 국가기관의 보안정책에 의해 국가기관의 암호체계와 민간의 암호체계의 상이함을 보완하여 인터넷을 통한 전자민원서비스 등을 국민에게 제공하는 역할을 수행한다.

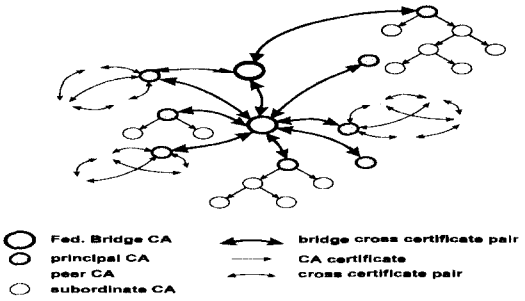
PKI 구성방안에는 최상위 CA를 중심으로 계층적으로 배치되어 운영되는 계층형 구조와 독립적으로 CA를 구축하여 상호 연계하는 네트워구조로 대별된다.

미국의 FPKI는 각 부처별로 구축·운영중인 CA들을 Bottom-up의 형태를 구성한 후 FBCA(연방가교 CA)와의 상호연동을 통하여 연방전체의 PKI를 구축하는 단계에 있으며, 민간의 PKI와 연계를 위한 BCA는 별도로 구축하여 운영될 예정이다.

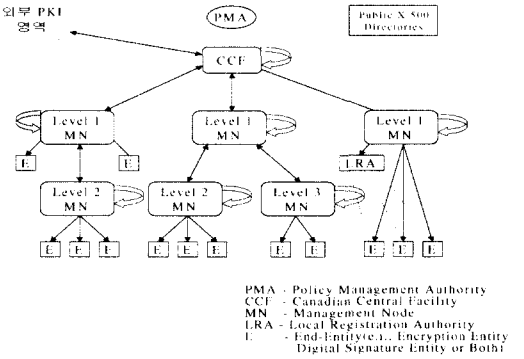
전체 구성은 〔그림 1〕과 같이 복잡하여 연방차원에서 보면, 계층적 구조와 네트워구조가 혼합된 형태를 보이고 있어 전체적으로 볼 때 효율적인 연계가 어려울 것으로 보여진다.

〔표 1〕 인증 구조상의 기관별 기능

| 구 분 | 설 명 | 기 능 |
|---|---|---|
| 정책 관리 기관 (PMA) | · GPKI에서 사용할 인증서 정책을만듬<br>· 인증기관이 사용할 인증 업무 준칙 (CPS : Certification Practice Statement)을 인가[7] | · 인증기관을 신임하는 것에 대한 평가기준을 만들고 그 평가 기준에 따라 GPKI내에 있는 모든 인증기관들을 주기적으로 평가<br>· 이름 관리기관 (NA : Naming Authority) : 모든 사용자들이 유일한 이름을 갖도록 조절, 이름의 인가 및 사용자들의 이름을 인증기관들이 정하는 방법을 설정<br>· 문서보관소 : 서명 확인에 필요한 정보를 영구히 저장한다. 각 인증기관은 발급한 인증서 및 인증서 폐기목록에 대한 문서보관소의 역할 |
| 최상위 인증 기관 | · 최상위인증기관은 GPKI 정책을 구현<br>· 다른 국가 정부나 민간 지역 사회와 같은 외부기관과 상호 인증하는 공통 지점을 제공 | · GPKI의 레벨 1 인증기관들을 인증<br>· 정책관리기관에 의해 요청된 외부 PKI를 인증<br>· 인증서와 인증서 폐기목록을 디렉토리에 게시<br>· 자신이 생성한 모든 인증서와 인증서 폐기목록을 문서보관<br>· 감사 기록문서 보관 |
| 가교 CA | · GPKI신뢰도메인 외부의 공인인증기관 등과의 상호연동을 제공하는 기관<br>· G2G에 대한 인증서와 인증서 폐기목록을 발급하는 서비스는 제공할 수 없음 | · 민·관간 연계를 위한 사용자의 인증서 등록, 변경, 폐기 신청<br>· 민·관간 연계를 위한 사용자의 신분을 확인<br>· 민·관간 연계용 인증서 폐기 요청을 수령하고 인가<br>· 민·관간 연계를 인가받은 사용자들에게 개인토큰을물리적으로 분배, 회수 |
| 하위 인증 기관 (CA) | · GPKI의 정책에 따라 설치·운영<br>· 사용자, 원격등록소,하부인증기관을 관리할 책임<br>· 인증기관은 인증서를 발급하고 폐기된 인증서들의 목록을 발급 | · 사용자 공개키에 대한 인증서를 생성, 확인<br>· 인증서 갱신, 폐기<br>· LDAP을 이용한 디렉토리 서버 접근<br>· 인증서 폐기목록 생성<br>· 사용자 이름의 유일함을 점검<br>· 공개키의 유일함을 확인<br>· 주 단위로 백업 실행<br>· 거래를 로그<br>· 영구한 문서보관소 유지<br>· 인증서 소유자에 대한 정보 관리 |
| 등록 기관 (RA) | · 사용자와 인증기관이 지리적으로 멀리 떨어져 있는 경우 사용자와 인증기관 사이의 간격을 이어주는 역할<br>· 인증서와 인증서 폐기 목록을 발급하는 서비스는 제공할 수 없음 | · 사용자의 인증서 등록, 변경, 폐기 신청<br>· 사용자의 신분을 확인<br>· 인증서 폐기 요청을 수령하고 인가<br>· 인가된 사용자들에게 개인토큰을 물리적으로 분배, 회수 |




〔그림 1〕 미국 FPKI 모델




〔그림 2〕 GoC PKI 모델

이에 비해 캐나다의 경우(〔그림 2〕)에는 구축 초기단계부터 정부차원의 단일기반구축을 목표로 정부분야의 표준화 등을 선행·추진되고 있어 단순하고 획일적인 구성을 가짐을 알 수 있다.

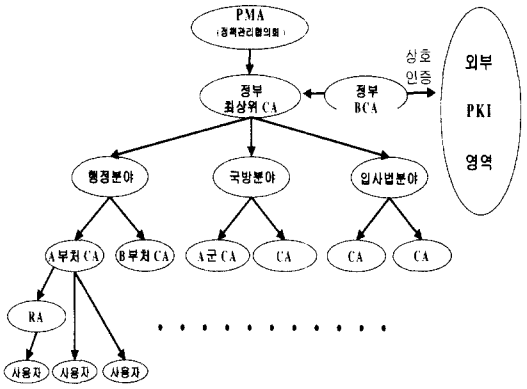
## 2.2 GPKI 구성 방안

본 논문에서는 미국, 캐나다 정부의 예와 국내 현황을 고려하여 우선 정부차원의 공통기술표준의 제정을 선행한 후, 〔그림 3〕과 같이 정부내부는 계층형 모델로 구성하고 민·관간 연계를 위한 BCA를 별도로 구축·운영하는 모델을 제안하였다.

### 2.2.1 GPKI 모델

정부의 최상위 CA를 두고 그 하부에 행정분야, 국방분야, 입·사법분야 등 3개 분야로 분류하여 계층형 구조로 구성하고 각 분야별로 계층형 구조를 구성하며, 외부영역과의 연계를 BCA를 구성한다.

정부분야를 3개 분야로 제안하는 이유는 행정, 국방 등 각 분야에서 적용되는 암호기반을 차별화 하여 어느 한 분야의 암호체계에 노출되더라도 피해를 최소화하며, 전자서명기반과 밀접한 키 관리기반을 분




〔그림 3〕 제안된 GPKI 모델

야별로 효율적인 구축·운영함으로써 보다 강한 정부차원의 정보보호체계가 마련될 것이다.

또한 정부 내에서 정보의 유통은 대개 각 분야내의 기관간에 이루어지므로 효율적인 경로검색 및 계층형 구조를 가지는 디렉토리(저장소) 이름 등 관리·운영상의 효율성을 얻을 수 있을 것이다.

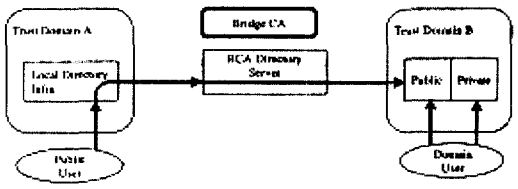
### 2.2.2 가교 CA 구성 방안

〔그림 3〕에서의 민·관간 상호연계를 위한 가교 CA는 외부 인증 체계의 최상위 또는 대표인증기관과 상호 인증 함으로써 다양한 형태의 모델에서의 효율적인 인증서 검색이 되도록 하였고 인증서비스 영역의 확장을 쉽게 하므로 써 민·관이 연계되는 전국단위의 광역 공개키 기반구조를 구성할 수 있다.[2,11]

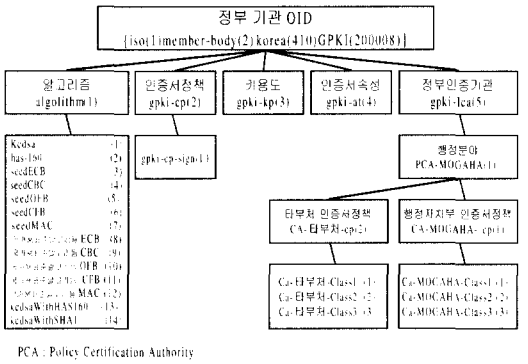
상대의 신뢰영역의 디렉토리 접근 방법으로는 직접 접근 구조 방식과 경계 디렉토리 서버 접근 구조가 있다. 인증서 검색 절차가 효율적이고 기존의 신뢰영역에 추가적인 부담이 없는 〔그림 4〕와 같은 직접 접근 구조 방식을 본 논문에서는 제안한다.

### 2.2.3 OID 구성방안

OID(Object IDentifier) 등록 추진체계는 국제 표준단체 및 기구에 의한 여러 가지 등록 방법으로 구성 할 수 있다.




〔그림 4〕 신뢰영역 디렉토리 직접 접근 구조




[그림 5] 정부전자서명 인증관리 OID 체계도

첫 번째로 X.680[10]을 인용하여 ITU-T의 TSB (Telecommunication Standardization Bureau)에 의 Identified Organization이하의 Arc 값을 할당하는 방법, 두 번째로는 ISO의 각국의 Member Body를 통하여 OID를 할당받는 방법, 세 번째로는 BSI(ISO 6523 등록기관)의 ICD(International Code Designator)를 이용하는 방법, 네 번째로는 ISO/ITU-T로부터 할당받는 방법들이 있으나 본 논문에서는 국내의 관련기관(산업자원부)에 직접 등록 및 할당([그림 5])이 가능한 두 번째 방법을 제안한다.

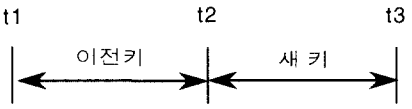
## Ⅲ. GPKI 구축 방안

### 3.1 키 및 인증서 관리

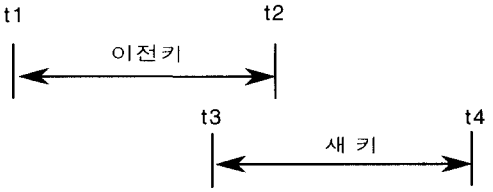
#### 3.1.1 키 관리

본 논문에서는 RSA 알고리즘[3]을 이용한 키 전송 방법을 지원한다. 데이터 암호화에는 대칭키(symmetric key)를 사용하게 되고, 암호화를 수행하는 쪽에서 암호학적으로 안전한 난수 발생 방식을 이용하여 생성한다. 대칭키는 수신자의 RSA 공개키로 암호화되어 보내진다. 서명용 키쌍은 사용자에 의해 생성한다. 그러나, 특정 업무 또는 인증 정책의 경우에는 중앙 집중 방식, 즉 인증기관에서 직접 생성할 수도 있다. 사용자가 생성하여 공개키에 대한 인증서를 발급받는 경우에는 공개키의 무결성과 이와 쌍이 되는 비밀키를 사용자가 가지고 있음을 증명하는 과정이 꼭 포함되어야 한다.

GPKI에서는 암호화용 키쌍 중에서 비밀키를 안전한 방법을 통하여 인증기관에게 전달하는 방법을 사용한다. 사용자의 경우 키 갱신은 이전키의 유효기간이 만료되는 시점으로부터 새로운 유효기간이 시작되게 처리된다.




인증기관의 경우에는 새 키의 유효기간이 이전키의 유효기간이 만료되는 시점으로부터 시작되게 하면 사용자 공개키 인증서 발급에 문제가 된다. 사용자 공개키 인증서의 유효기간은 사용자 공개키를 서명하는 인증기관 비밀키의 유효기간 내에서만 설정될 수 있기 때문이다. 사용자 공개키 인증서 발급에 문제가 없게 하기 위해서는 최소한 사용자 공개키 인증서 유효기간 정도의 기간동안 인증기관 이전키와 새 키의 유효기간이 겹쳐야 한다.




최상위 인증기관 키 갱신은 기본적으로 인증기관 키 갱신과 동일하게 처리된다. 키 갱신 처리 시 최상위 인증기관이 새 공개키를 이전의 비밀키로 보호하고, 이전의 공개키를 새 비밀키로 보호하는 방법을 사용하며 최상위 인증기관이 키를 갱신 시 이전 키에 대한 인증서와 새 키에 대한 인증서 이외에 두 개의 추가적인 최상위 인증기관 인증서를 저장소에 게시해야 하며 최상위 인증기관이 키를 갱신할 때 이전의 공개키를 안전한 방법으로 획득한 사용자들이 영향을 받게 된다. 이 사용자들은 이전의 공개키를 이용하여 보호된 새 공개키를 찾아 내야한다. 사용자는 인증서가 만료되는 경우에 루트의 새 공개키를 제공받게 된다.

이전 그리고 새 공개키를 보호하기 위해 인증서의 key-Identifier 확장을 사용하는 인증서가 사용된다. 최상위 인증기관 운영자는 다음과 같이 처리하여야 한다.

- 새 키쌍 생성
- 새 키로 서명된 이전 공개키를 포함하는 인증서 생성

- 이전키로 서명된 새 공개키를 포함하는 인증서 생성
- 새 키로 서명된 새 공개키를 포함하는 인증서 생성
- 저장소에 인증서 게시
- 새 최상위 인증기관 공개키를 알림

인증서를 확인하는 것은 다음과 같이 4가지 경우가 발생한다.

서명 확인자

| 서명자 | 구분 | 새 공개키 | 이전 공개키 |
|---|---|---|---|
| | 새공개키 | 1. 저장소에 조회없이 직접 인증서 확인 가능 | 3. 확인자는 저장소에 접근하여 새 공개키를 찾아내야함. |
| | 이전 공개키 | 2. 확인자는 저장소에 접근하여 이전의 공개키를 찾아내야함 | 4. 저장소 조회없이직접 인증서 확인 가능 |

2번의 경우 확인자는 다음을 실행해야 하며,
- 저장소에서 적당한 인증서를 조회
  (새 키로 서명된 이전 공개키를 포함하는 인증서)
- 자신이 갖고 있는 새 공개키로 이것의 정당성을 확인
- 정당하면 서명자의 인증서를 이전 공개키로 확인

3번의 경우 확인자는 다음을 실행해야 한다.
- 저장소에서 적당한 인증서를 조회
  (이전 키로 서명된 새 공개키를 포함하는 인증서)
- 자신이 갖고 있는 이전 공개키로 이것의 정당성을 확인
- 정당하면 서명자의 인증서를 새 공개키로 확인

최상위 인증기관 및 인증기관 키 갱신시 인증서 폐기목록의 서명확인도 인증서의 서명확인 같이 복잡해진다. 인증서 폐기목록의 발급자 키 식별자 확장영역을 활용할 경우, 인증서 폐기목록을 서명한 최상위 인증기관 키에 대한 구분이 가능하다.

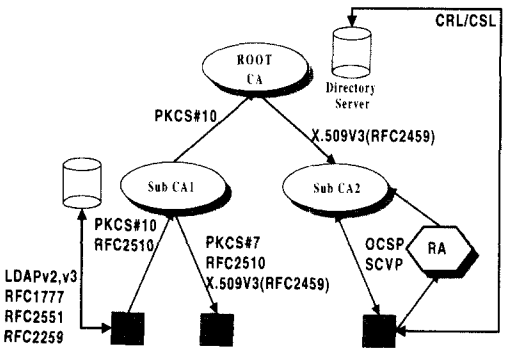
### 3.1.2 인증서 상태

본 논문에서는 인증서 폐기목록를 확인하고 싶은 사용자가 직접 저장소로부터 인증서 폐기목록을 요청하여 확인하는 PULL 분배모델을 따른다. 인증서 폐기목록을 얻기 위한 통신비용의 최소화를 위해 몇 가지 다음 방법이 사용될 수 있다.

- 한 개의 인증서를 확인하면서 필요한 정보를 최소화하기 위해 delta CRL 또는 인증서 폐기목록 분배점(CRL distribution point)이 사용될 수 있다.
- 인증서 폐기목록을 작게 하기 위해 인증서 유효기간을 조정할 수 있다. 폐기된 인증서가 만료되면 인증서 폐기목록으로 부터 제거된다.
- 세분화되지 않은 이름의 사용은 이름변경에 의한 폐기를 최소화할 수 있다.

### 3.1.3 인증서 관리

새 인증기관을 설립할 때는 특정 조치들이 필요하다. 초기 인증서 폐지목록이 생성되어야 하며 인증기관의 공개키가 알려져야 한다. 인증기관은 상위 인증기관으로부터 [그림 6]과 같이 제안된 구성도에 의해 인증기관 인증서를 발급 받아야 하며 최상위 인증기관은 자신이 자신의 인증서를 생성한다. 사용자는 자신의 이름, 인증기관 이름, 자신의 키쌍, 최상위 인증기관의 공개키, 최상위 인증기관으로부터 자신의 인증기관까지의 인증경로를 설치해야 한다. 최상위 인증기관의 공개키는 out-of-band 방법으로 안전하게 받아야 하고 사용자가 인증서를 발급받기 위해서는 인증기관에게 자신을 알리는 등록 작업을 하여야 한다. 인증기관은 사용자에게 공개키 인증서를 발급하고, 그것을 사용자에게 배달하고 디렉토리 서버에 게시하는 작업을 한다. 모든 키쌍은 주기적으로 갱신될 필요가 있다. 갱신 시 새 키쌍이 생성되고 인증서가 발급되며 두 인증기관이 상호 인증하기 위한 정보를 교환한다. 상호인증 갱신은 키쌍 갱신의 경우와 비슷하다. 인증서 및 폐지목록은 LDAP[9]을 지원하는 디렉토리 서버에 게시하며 인증서 폐지의 경우는 인가된 사용자가 인증기관에게 인증서 폐지 요청을 하여야 한다.




[그림 6] 인증서 관리 메커니즘 구성도

## 3.2 데이터 구조

### 3.2.1 인증서

X.509 인증서의 주요 목적은 사용자의 공개키와 이름을 연관시키는 것이다. 본 논문에서는 [그림 7]과 같은 X.509 V3 인증서를 사용한다. 인증서는 인증기관의 비밀키로 서명된다. 표준화된 확장필드들은 다음을 포함한다.

- 키와 보안정책 정보
- 인증서 발급자와 피발급자 속성
- 인증경로 제한
- 인증서 폐지목록 식별

#### 3.2.1.1 기본 필드

(1) 버전(Version)

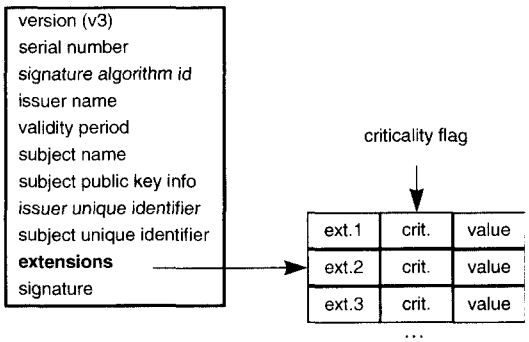
이 필드는 인코딩된 인증서의 버전을 기술한다. 확장을 사용할 경우에는 버전 3(값은 2임)를 이용한다. 확장은 없으나 UniqueIdentifier가 존재할 때는 버전 2(값은 1임)를 사용한다. 기본 필드만 존재할 때는 버전 1을 사용한다. 구현은 모든 버전의 인증서를 수용할 수 있어야 하지만, 버전 2 인증서의 생성은 본 논문에서는 고려하지 않는다.

(2) 일련 번호(Serial number)

일련 번호는 인증기관에 의해 각 인증서에 부여되는 유일한 정수이다. 즉, 발급자 이름과 일련 번호가 인증서의 유일성을 식별할 수 있어야 한다.

(3) 서명 알고리즘 식별자(Signature algorithm id)

이 필드는 해당 인증서를 서명하기 위해 인증기관에 의해 사용된 알고리즘에 대한 알고리즘 식별자를 포함하며 인증서에 있는 서명 알고리즘과 동일한 알고리즘 식별자를 포함한다.




[그림 7] X.509 V3 인증서 구조

(4) 발급자 이름(Issuer Name)

이 필드는 인증서를 서명한 인증기관의 유일한 이름을 나타낸다. 본 논문에서는 X.500 DN을 사용한다. 이름의 속성 유형은 일반적으로 directoryString이다.

directoryString은 PrintableString, TelexString, BMPString, UTF8String, UnivercalString중 하나로 정의된다.

본 논문을 준용하는 인증기관은 이 옵션들을 다음과 같이 선택하여 사용하여야 한다:

(a) 문자 세트가 만족되면 문자열은 PrintableString로 표기한다.
(b) (a)로는 모자라고 bmpString 문자 세트로 만족되면 문자열은 BMPString으로 표기한다.
(c) (a), (b)로도 되지 않으면 문자열은 UTF8String으로 표기한다. 이중에서 (a)와 (b)의 조건을 만족하더라도 UTF8String을 사용할 수 있으며, 2004년부터는 오직 UTF8String만을 사용한다.

LDAP 디렉토리 서버는 RFC 2559[9] 형태의 DN을 사용한다. 디렉토리에서 DN으로 한글이 사용되는 경우 UTF8String을 지원해야 한다.

(5) 유효 기간(Validity)

이 필드는 인증서가 정당해지는 날짜(notBefore)와 정당함이 만료되는 날짜(notAfter)를 표시한다. 이 필드에 사용되는 UTCTime은 GMT(Zulu)로 표시되어야 하며 초 단위까지 YYMMDDHHMMSSZ 표시된다. YY가 50과 동일하거나 크면 19YY로 해석하고 YY가 50보다 작으면 20YY로 해석한다. UTCTime은 향후 연도를 4자리로 표시하는 GeneralizedTime으로 대치될 예정이다. 인터넷 표준에서와 마찬가지로 기 발급 인증서와의 호환을 고려하여 본 논문에서도 2049년까지는 UTCTime을 사용하고, 2050년 이후에는 GeneralizedTime만 사용할 것을 권고한다.

(6) 피발급자 이름(Subject Name)

이 필드는 인증서 피발급자의 유일한 이름을 나타

낸다. 본 논문에서는 X.500 DN을 사용하고 LDAP 디렉토리 서버는 RFC 2559 형태의 DN을 사용한다.

(7) 피발급자 공개키 정보(Subject Public Key Info)

이 필드는 공개키와 키가 사용되는 알고리즘을 식별한다. 즉, 공개키와 알고리즘 식별자 필드로 이루어져 있고 알고리즘 식별자는 알고리즘과 파라미터 필드로 이루어져 있다.

(8) 고유 식별자(Unique Identifiers)

고유 식별자는 피발급자 또는 발급자 이름의 재사용 가능성을 다루기 위해 존재한다. 본 논문에서도 이름의 재사용을 허용하지 않으며 본 논문을 준용하는 인증기관은 이 필드를 포함하는 인증서를 생성하지 않아야 한다.

(9) 발급자 서명(Signature)

인증기관 개인키로 서명한 공개키 인증서의 서명값이 이 필드에 들어간다. 서명되는 데이타에는 알고리즘 식별자와 실제 서명인 비트 스트링을 사용한다. 알고리즘 식별자의 파라미터 필드는 사용하지 않는다.

### 3.2.1.2 확장 필드

GPKI 인증서 확장영역 프로파일은 [표 2]와 같이 제안하며 항목별 기능 설명은 다음과 같다.

(1) 발급자 키 식별자(Atuthority Key Identifier)

이 확장은 서명을 확인하는데 필요한 인증기관의 특정 공개키를 식별하는 수단을 제공한다. 이 확장은 인증기관이 여러개의 서명키를 갖고 있을 때 사용된다.

본 논문에서는 키 식별자가 사용되고, 키 식별자의 값으로 공개키를 DER 인코딩한 결과의 160비트 SHA-1 해쉬를 반드시 사용하여야 한다. 이 확장은 non-critical로 설정된다.

(2) 피발급자 키 식별자(Subject Key Indentifier)

이 확장은 응용에 사용된 특정 공개키를 식별하는 수단을 제공한다. 본 논문에서는 키 식별자가 사용되고, 키 식별자의 값으로 공개키를 DER 인코딩한 결과의 160비트 SHA-1 해쉬를 반드시 사용하여야 한다. 이 확장은 noncritical로 설정된다.

[표 2] GPKI 인증서 확장영역 프로파일

| 항 목 | | 인증서 | | | | | |
|---|---|---|---|---|---|---|---|
| | | 최상위 인증기관 | | 인증기관 | | 사용자 | |
| | | 사용여부 | C | 사용여부 | C | 사용여부 | C |
| Key Information | Authority Key Identifier | | | Y | F | Y | F |
| | Subject Key Identifier | Y | F | Y | F | Y | F |
| | Key Usage | | | Y | T | Y | T |
| | Extended Key Usage | | | | | | |
| | Private Key Usage Period | | | | | | |
| Policy Information | Certificate Policies | | | Y | O | O | O |
| | Policy Mappings | | | O | F | | |
| Subject and Issuer Attributes | Subject Alternative Name | | | O | F | O | F |
| | Issuer Alternative Name | | | O | F | O | F |
| | Subject Directory Attributes | | | | | | |
| Certification Path Constraints | Basic Constraints | Y | F | Y | T | | |
| | Name Constraints | | | O | T | | |
| | Policy Constraints | | | O | T | | |
| CRL Identification | CRL Distribution Points | | | Y | O | Y | O |

- 사용여부
  Y - YES, 빈칸 - 사용하지 않음,
  O - 인증정책에 따라서 사용여부를 결정
- C (Criticality)
  T - TRUE, F - FALSE, O - 인증정책에 따라 critical의 여부를 결정

(3) 키 용도(Key Usage)

이 확장은 인증서에 포함된 키의 용도를 정의한다. 이 확장은 critical로 설정되며 키 용도에 있는 비트들은 [표 3]과 같이 사용된다. encipherOnly 비트는 keyAgreement 비트와 함께 설정되었을 경우에 피발급자 공개키가 키 합의를 수행하는 동안 데이터 암호용으로만 사용되고 decipher Only 비트는 keyAgreement 비트와 함께 설정되었을 경우에 피발급자 공개키가 키 합의를 수행하는 동안 데이터 복호용으로만 사용될 것이다. 본 논문은 키 용도 확장들의 조합에 제한을 두지 않는다.

(4) 개인키 사용 기간(Private Key Usage Period)

본 논문은 이 확장을 가급적 사용하지 않을 것을 권고한다. 본 논문을 준용하는 인증기관은 개인키 사용 기간 확장이 critical로 설정된 인증서를 생성하지 않아야 한다. 이 확장은 non-critical로 설정된다.

(5) 인증서 정책(Certificate Policies)

이 확장은 정책 식별자와 선택적으로 수식자(qualifier)로 구성되는 정보들의 목록을 갖고 있다.

〔표 3〕 키 비트별 용도

| 비 트 | 용 도 |
|---|---|
| digitalSignature | 전자서명 확인 (부인봉쇄, 인증서 서명, 인증서 폐지목록 서명등) |
| nonRepudiation | 부인봉쇄 서비스를 위한 전자서명 확인 |
| keyEncipherment | 키 암호화 (예, 키 전송) |
| dataEncipherment | 데이타 암호화 |
| keyAgreement | 공개키 합의 키 |
| keyCertSign | CA 의인증서전자서명확인 (인증기관 인증서에만 해당) |
| cRLSign | CA 의 CRL 전자서명 확인 (인증기관 인증서에만 해당) |

본 논문에서는 정책 식별자만을 사용한다. 이 확장은 정책에 따라 ciritical 설정이 결정된다.

(6) 정책 매핑(Policy Mappings)

이 확장은 인증기관 인증서에만 사용되며 1개 이상의 정책 식별자 쌍을 대응시킨다. 각 쌍은 발급자 도메인 정책과 피발급자 도메인 정책을 포함한다. 이 확장은 non-critical로 설정된다.

(7) 피발급자 대체 이름(Subject Alternative Name)

피발급자 대체 이름 확장은 인증서 피발급자의 부가적인 식별정보를 제공하기 위한 것이다. 정의된 옵션들은 rfc822 이름(전자우편 주소), DNS(Domain Name System) 이름, IP 주소, URI를 포함한다. 본 논문에서는 이 확장 필드의 사용을 권고한다. 이 확장은 non-critical로 설정된다.

(8) 발급자 대체 이름(Issuer Alternative Name)

이 확장은 인터넷 방식의 식별정보를 인증서 발급자와 연관시키는 데 사용된다. 인증서에 포함된 발급자 식별정보만 대체 이름 형태(전자우편 주소 등)인 경우 발급자 DN은 NULL이고 발급자 대체 이름 확장은 반드시 존재하여야 한다. 이 확장은 non-critical로 설정된다.

(9) 피발급자 디렉토리 속성(Subject Directory Attributes)

피발급자 디렉토리 속성 확장은 인증서 이외의 LDAP 같은 외부 메카니즘을 통해 관리하는 것이 바람직하므로 본 논문을 준용하는 인증기관에서는 사용하지 않아야 한다. 이 확장은 non-critical로 설정된다.

(10) 기본 제한(Basic Constraints)

기본 제한 확장은 인증서 소유자가 인증기관인지 아닌지를 표시하고, 또한 인증 경로 길이 제한을 표시하며 인증 경로 길이 값이 0이면 사용자에게만 인증서를 발급하고, 값이 없으면 인증 경로 길이에 제한이 없다. 이 확장은 인증기관 인증서에만 해당된다. 이 확장은 critical로 설정된다.

(11) 이름 제한(Name Constraints)

인증기관 인증서에서만 사용되는 이름 제한 확장은 인증 경로상의 후속 인증서들에 있는 모든 피발급자 이름들이 주어지는 이름 공간을 나타낸다. 본 논문에서 최대 또는 최소 필드들은 이름 형태로 사용되지 않으며 최소 값은 항상 0 이고 최대값은 항상 존재하지 않는다. 이 확장은 critical로 설정된다.

(12) 정책 제한(Policy Constraints)

정책 제한 확장은 인증기관에게 발급된 인증서들에 사용되고 정책 제한 확장은 2가지 방법으로 인증 경로를 제한한 다. 정책 매핑 금지 필드(inhibit-PolicyMapping)가 존재할 경우, 이것은 정책 매핑이 금지되기 전에 경로상에 존재할 수 있는 인증서의 개수를 의미하고 정책 식별자 요구 필드(require-ExplicitPolicy)가 존재하면 후속 인증서들은 수용가능한 정책 식별자를 포함해야 한다. 이 필드 값은 명시적인 정책이 적용되기 전에 허용되는 경로상에 존재할 수 있는 인증서들의 개수을 의미한다. 2가지 중에서 최소한 1개가 존재해야 한다. NULL 정책 제한과 관련한 클라이언트들의 동작에 관해서는 본 논문에서는 언급하지 않는다. 이 확장은 critical로 설정된다.

(13) 인증서 폐지목록 분배점(CRL Distribution Points)

이 확장은 인증서 폐지목록 정보를 획득하는 방법을 기술한다. 분배점에 폐지사유 필드를 생략하면 인증서 폐지목록은 모든 사유에 대한 폐지를 포함한다. 분배점에 폐지목록 발급자 필드를 생략하면 인증서 폐지목록은 인증서를 발급한 인증기관에 의해 발급된다. 본 논문에서는 인증기관 및 클라이언트들이 이 확장을 지원하기를 권고한다. 이 확장은 정책에 따라 critical 설정이 결정된다.

(14) 확장 키 용도 필드(Extended key usage field)

이 필드는 키 용도 확장 필드에 표시된 기본 용도

들에 추가 또는 대신해서 1개 이상의 공개키 용도를 표시한다. 키 용도들은 필요로 하는 기관에 의해 정의될 수 있다. 키 용도들을 명시하기 위해 사용된 객체 식별자들은 ITU-T X.660|ISO/IEC 9834-1에 따라 설정되어야 한다. 이 확장은 non-critical로 설정된다.

### 3.2.2 인증서 폐지목록

인증서 소유자가 단체를 떠나거나 개인키의 신뢰가 손상이 되었을때 인증서를 폐지할 필요가 있다.

본 논문에서는 [그림 8]과 같은 X.509 V2 인증서 폐지목록이 인증서 폐지에 사용된다

#### 3.2.2.1 기본 필드

(1) 버전(Version)

인증서 폐지목록 버전을 의미한다. 버전 2 인증서 폐지목록을 나타내기 위해 1이 사용된다.

(2) 서명 알고리즘 식별자(Signature algorithm id)

이 필드는 인증서 폐지목록을 서명하기 위해 사용된 알고리즘 식별자를 포함한다.

(3) 발급자 이름(Issuer Name)

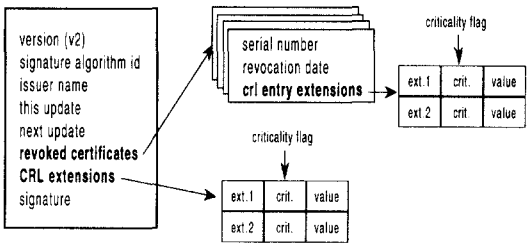
발급자 필드는 인증서 폐지목록을 서명하는 인증기관의 유일한 식별을 제공한다. 발급자 이름은 X.500 이름을 사용한다.

(4) 갱신일(This Update)

갱신일 필드는 현 인증서 폐지목록의 발급일을 표시한다. UTCTime이 사용되고 인증서의 유효기간 필드를 참조한다.

(5) 다음 갱신일(Next Update)

다음 갱신일 필드는 다음 인증서 폐지목록 발급일을 표시한다.




[그림 8] X.509 V2 인증서 폐지목록 구조

(6) 폐지 인증서(Revoked Certificates)

폐지 인증서 필드는 폐지된 인증서 목록을 표시하고 각 폐지된 인증서는 다음을 포함한다.

- userCertificate 필드는 폐지된 인증서의 일련번호를 갖는다. 이것과 인증기관 이름을 사용하여 만료되지 않은 폐 지된 인증서를 식별한다.
- revocationDate 필드는 인증서 폐지일을 UTC Time 형태로 표시하고 인증서의 유효기간 필드를 참조한다.

(7) 발급자 서명(Signature)

서명 필드는 인증서 폐지목록에 대한 전자서명 값을 포함한다.

#### 3.2.2.2 인증서 폐지목록 확장 필드

본 논문에서의 인증서 폐지목록 확장 프로파일의 구성은 [표 4]와 같으며 기능별로 살펴보면 다음과 같다

(1) 발급자 키 식별자(Authority Key Identifier)

이 확장은 인증서 폐지목록을 서명 확인하는데 필요한 인증기관의 특정 공개키를 식별하는 수단을 제공한다. 이 확장은 인증기관이 여러 개의 서명키를 갖고 있을 때 사용된다. 인증서의 발급자 키 식별자 확장을 참조한다. 이 확장은 non-critical로 설정된다.

(2) 발급자 대체 이름(Issuer Alternative Name)

발급자 대체 이름 확장을 통해서 인증서 폐지목록

[표 4] GPKI 인증서 폐지 목록 확장영역 프로파일

| 항 목 | | 인증서 폐지 목록 | |
|---|---|---|---|
| | | 사용여부 | C |
| CRL Entry Extensions | Reason Code | Y | F |
| | Hold Instruction Code | | |
| | Invalidity Date | | |
| | Certificate Issuer | O | T |
| CRL Extensions | Authority Key Identifier | O | F |
| | Issuer Alternative Name | O | F |
| | CRL Number | Y | F |
| | Issuing Distribution Point | O | O |
| | Delta CRL Indicator | O | F |

- 사용여부
  Y - YES, 빈칸 - 사용하지 않음,
  O - 인증정책에 따라서 사용여부를 결정
- C (Criticality)
  T - TRUE, F - FALSE, O - 인증정책에 따라 critical의 여부를 결정

발급자에 대한 추가 식별정보가 더해진다. 인증서의 발급자 대체 이름 확장을 참조한다. 이 확장은non-critical로 설정된다.

(3) 인증서 폐지목록 번호(CRL Number)
인증서 폐지목록 번호는 인증기관이 발급한 일련번호를 나타낸다. 이 확장은 non-critical로 설정된다.

(4) delta CRL 지시자(delta CRL Indicator)
delta-CRL은 가장 최근 폐지된 인증서 폐지목록이다. 이 확장은 non-critical로 설정된다.

(5) 분배점 발급(Issuing Distribution Point)
분배점 발급 확장은 인증서 폐지목록이 사용자 인증서 폐지용인지, 인증기관 인증서 폐지용인지, 아니면 사유 코드에 의한 폐지용인지를 식별하게 해 준다. 이 확장은 정책에 따라 critical로 설정된다.

#### 3.2.2.3 인증서 폐지목록 엔트리 확장 필드

(1) 사유 코드(Reason Code)
이 확장은 해당 인증서의 폐지 사유를 구분하는데 사용된다. 본 논문을 준용하는 인증기관은 인증서 폐지목록 엔트리에 사유코드 확장을 반드시 포함할 것을 권고한다. 사유 코드 중 unspecified 코드는 사용하지 않는다. 이 확장은 non-critical로 설정된다.

(2) 정지 명령어 코드(Hold Instruction Code)
정지 명령어 코드는 정지 상태에 있는 인증서 처리에 관련한 등록된 명령어 식별자를 확장이다. 본 논문에서는 이 확장을 사용하지 않는다. 이 확장은 non-critical로 설정된다.

(3) 무효 일자(Invaildity Date)
무효 일자는 개인키가 손상되었거나 아니면 인증서가 무효화된 것으로 알려진 일자를 제공하는 확장이다. 이 확장은 non-critical로 설정된다.

(4) 인증서 발급자(Certificate Issuer)
이 확장은 간접 인증서 폐지목록, 즉 분배점 발급 확장에 설정된 indirectCRL 지시자를 가지는 인증서 폐지목록에 있는 엔트리와 관련된 인증서 발급자를 식별한다. 이 확장은 critical로 설정된다.

### 3.2.3 인증 경로 검증

인증서 검증이란 인증서에 포함된 피발급자의 정보와 피발급자의 공개키 간의 연결관계에 대한 검증이다. 이를 위해서는 검증하고자 하는 인증서(End Entity 인증서 또는 최말단 인증서)와 최상위 인증기관 인증서를 연결하는 인증서들의 집합, 즉 인증 경로(Certification Path)를 찾아내야 하며 이에 대한 검증을 수행해야 한다. 본 논문에서의 인증서 경로 검증 절차들은 RFC 2459[8]를 근간으로 한다.

### 3.2.4 PKI 메시지 구성 요소

본 논문에서 사용하는 모든 메시지는 다음과 같은 구조로 되어 있다.

| PKI Header | PKI Body | PKI Protection | extraCerts (Sequence of Certificate) |
|---|---|---|---|

(1) PKI Header
모든 PKI 메시지들은 주소 지정과 트랜잭션 식별을 위한 헤더 정보를 요구한다. 이 정보를 포함하기 위해 PKI Header 자료 구조가 사용된다.

(2) PKIBody
PKIBody는 초기등록, 키 갱신·폐지 등 PKI의 효율적 관리를 위해 다음의 자료구조를 DER로 인코딩한 것이다.

```
PKIBody ::= CHOICE {
      -- message-specific body elements
  ir        [0]  CertReqMessages,
            --Initialization Request
  ip        [1]CertRepMessage,
            --Initialization Response
  cr        [2]  CertReqMessages,
            --Certification Request
  cp        [3]  CertRepMessage,
            --Certification Response
```

```
p10cr       [4]  CertificationRequest,
            --imported from [PKCS10]
popdecc     [5]  POPODecKeyChallContent,
            --pop Challenge
popdecr     [6]  POPODecKeyRespContent,
            --pop Response
kur         [7]  CertReqMessages,
            --Key Update Request
kup         [8]  CertRepMessage,
            --Key Update Response
rr          [11] RevReqContent,
            --Revocation Request
rp          [12] RevRepContent,
            --Revocation Response
ccr         [13] CertReqMessages,
            --Cross-Cert. Request
ccp         [14] CertRepMessage,
            --Cross-Cert. Response
ckuann      [15] CAKeyUpdAnnContent,
            --CA Key Update Ann.
cann        [16] CertAnnContent,
            --Certificate Ann.
rann        [17] RevAnnContent,
            --Revocation Ann.
crlann      [18] CRLAnnContent,
            --CRL Announcement
conf        [19] PKIConfirmContent,
            --Confirmation
nested      [20] NestedMessageContent,
            --Nested Message
genm        [21] GenMsgContent,
            --General Message
genp        [22] GenRepContent,
            --General Response
error       [23] ErrorMsgContent
            --Error Message
 }
```

(3) PKI Protection

모든 PKI 메시지의 무결성을 보장한다. PKI-Protection을 계산하기 위한 입력은 다음 자료구조를 DER 인코딩한 것이다.

```
ProtectedPart ::= SEQUENCE {
    header  PKIHeader,
    body    PKIBody
}
```

### 3.2.5 송수신 메시지

본 논문에서 다루는 송수신 메시지 프로파일은 RFC 2510[5]과 RFC2511[6]의 표준을 준용하며 송수신 메시지 프로파일은 다음의 세 가지 파트로 구성되어 있다.

- 초기 등록 및 인증(Initial Registration/Certification)
- 키 갱신(Key update)
- 인증서 폐지(Revocation)

#### 3.2.5.1 초기등록 및 인증(Initial Registration/Certification)

(1) ir message

ir message 형식은 [표 5]과 같으며 PKIBody의 CertReqMessages에는 1개 이상의 CertReqMsg가 들어갈 수 있다.

[표 5] GPKI ir Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 사용자/원격등록소의 고유이름(DN) |
| recipient | 인증기관의 고유 이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 사용자 - MAC 알고리즘/ 원격등록소 - 전자서명 알고리즘 |
| senderNonce | 난수 |

◆ PKIBody

ir (CertReqMessages)

| | | | | |
|---|---|---|---|---|
| CertReqMsg | certReq | certReqId | | 0 |
| | | certTemplate | version | v3(2) |
| | | | subject | 사용자의 고유 이름(DN) |
| | | | publicKey | 새 인증서의 전자 서명용 공개키 |
| | | | extentions | 확장영역 |
| | pop | signature | algorithmIdentifier | 서명 알고리즘 |
| | | | signature | certReq의 DER 인코딩한 값에 대한 서명값 |

| | | | | |
|---|---|---|---|---|
| CertReqMsg | certReq | certReqId | | 1 |
| | | certTemplate | version | v3(2) |
| | | | subject | 사용자의 고유 이름(DN) |
| | | | publicKey | 새 인증서의 암호화용 공개키 |
| | | | extentions | 확장영역 |
| | pop | keyEncipherment | thisMessage | 암호화용 공개키를 인증기관의 공개키를 이용해 암호화한 값 |

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 사용자 | header와 body의 DER 인코딩한 값의 MAC 값 |
| | 원격등록소 | header와 body의 DER 인코딩한 값의 서명값 |

▒ 이 부분은 선택 영역을 나타낸 것이다.

즉, 전자 서명용 인증서 요청을 기본적으로 할 수 있고 정책에 따라 암호화용 인증서 요청을 함께 할 수 있다.

(2) ip message

본 논문에서의 ip message 형식은 [표 6]과 같으며 또한 최상위 인증기관의 공개키 인증서가 out-of-band 방식으로 사용자에게 전해졌다는 가정 하에 송수신 메시지를 전송한다. 따라서 PKIProtection에서 인증기관이 MAC[4]값으로 메시지를 보호하는 방식을 사용하지 않고 인증기관의 전자 서명을 통해 메시지를 보호한다.

[표 6] GPKI ip Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 인증기관의 고유 이름(DN) |
| recipient | 사용자/원격등록소의 고유이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 인증 기관의 전자 서명 알고리즘 |
| senderNonce | 난수 |
| recipNonce | ir message의 senderNonce 값 |

◆ PKIBody

ip (CertRepMessage)

| | | | | | |
|---|---|---|---|---|---|
| response | CertReponse | certReqId | | | 0 |
| | | status | status | | "granted"(0) or "rejection"(2) |
| | | certifiedKeyPair | certOrEncCert | certificate | 인증서:status가 "granted"일 때만 |
| | CertReponse | certReqId | | | 1 |
| | | status | status | | "granted"(0) or "rejection"(2) |
| | | certifiedKeyPair | certOrEncCert | certificate | 인증서:status가 "granted"일 때만 |

◆ PKIProtection

| | | |
|---|---|---|
| protection | 인증기관 | header와 body의 DER 인코딩한 값의 서명 값 |

[표 7] GPKI confMessage 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 사용자/원격등록소의 고유이름(DN) |
| recipient | 인증기관의 고유 이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 사용자 - MAC 알고리즘/ 원격등록소 - 전자서명 알고리즘 |
| senderNonce | ip message의 recipNonce 값 |
| recipNonce | ip message의 senderNonce 값 |

◆ PKIBody

PKIConfirmContent: ASN.1 NULL

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 사용자 | header와 body의 DER 인코딩한 값의 MAC 값 |
| | 원격등록소 | header와 body의 DER 인코딩한 값의 서명값 |

(3) conf message

본 논문에서의 conf message 형식은 [표 7]과 같이 제안한다.

### 3.2.5.2 키 갱신(Key update)

(1) kur message

PKIBody의 CertReqMessages에는 1개 이상의 CertReqMsg가 들어갈 수 있다. 즉, 전자 서명용 인증서요청을 기본적으로 할 수 있고 정책에 따라 암호화용 인증서 요청을 함께 할 수 있다. PKIProtection의 protection은 사용자가 이미 기존의 전자 서명용 인증서를 발급받은 상태이기 때문에 MAC 방식이 아닌 전자 서명을 통해 메시지를 보호한다. kur message 형식은 [표 8]과 같다.

(2) kup message

kup message 형식은 [표 9]와 같이 제안한다.

[표 8] kur Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 사용자/원격등록소의 고유이름(DN) |
| recipient | 인증기관의 고유 이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 사용자/원격등록소 - 전자서명 알고리즘 |
| senderNonce | 난수 |

◆ PKIBody

kur (CertReqMessages)

| | | | | |
|---|---|---|---|---|
| CertReqMsg | certReq | certReqId | | 0 |
| | | certTemplate | version | v3(2) |
| | | | subject | 사용자의 고유 이름(DN) |
| | | | publicKey | 새 인증서의 전자 서명용 공개키 |
| | | | extentions | 확장영역 |
| | pop | signature | algorithmIdentifier | 서명 알고리즘 |
| | | | signature | certReq의 DER 인코딩한 값에 대한 서명값 |

| | | | | |
|---|---|---|---|---|
| CertReqMsg | certReq | certReqId | | 1 |
| | | certTemplate | version | V3(2) |
| | | | subject | 사용자의 고유 이름(DN) |
| | | | publicKey | 새 인증서의 암호화용 공개키 |
| | | | extentions | 확장영역 |
| | pop | keyEncipherment | thisMessage | 암호화용 공개키를 인증기관의 공개키를 이용해 암호화한 값 |

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 사용자/ 원격등록소 | header와 body의 DER 인코딩한 값에 대한 서명값 |

〔표 9〕 kup Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 인증기관의 고유 이름(DN) |
| recipient | 사용자/원격등록소의 고유이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 인증 기관의 전자 서명 알고리즘 |
| senderNonce | 난수 |
| recipNonce | kur message의 senderNonce 값 |

◆ PKIBody

| ip | (CertRepMessage) | | | | |
|---|---|---|---|---|---|
| response | CertReponse | certReqId | | | 0 |
| | | status | status | | "granted"(0) or "rejection"(2) |
| | | certifiedKeyPair | certOrEncCert | certificate | 인증서:status가 "granted"일 때만 |
| | CertReponse | certReqId | | | 1 |
| | | status | status | | "granted"(0) or "rejection"(2) |
| | | certifiedKeyPair | certOrEncCert | certificate | 인증서:status가 "granted"일 때만 |

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 인증기관 | header와 body의 DER 인코딩한 값의 서명 값 |

### 3.2.5.3 인증서 폐지 (Revocation)

(1) rr message

본 논문에서의 rr message 형식은 〔표 10〕과 같고 원격등록소에서 인증서 폐지 요청을 대행하는 방식을 사용한다.

사용자가 원격등록소에 인증서 폐지요청을 신청하는 방식은 본 논문에서는 다루지 않는다.

〔표 10〕 rr Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 원격등록소의 고유이름(DN) |
| recipient | 인증기관의 고유 이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 원격등록소 - 전자서명 알고리즘 |
| senderNonce | 난수 |

◆ PKIBody

| rr | (RevReqContent) | | |
|---|---|---|---|
| RevDetails | certDetails | issur | 인증서 발행자의 고유 이름(DN) |
| | | subject | 인증서 주체의 고유 이름(DN) |
| | | serialNumber | 폐지 요청 인증서의 시리얼번호 |
| | revocationReason | | 폐지 요청 사유 |

| | | | |
|---|---|---|---|
| RevDetails | certDetails | issur | 인증서 발행자의 고유 이름(DN) |
| | | subject | 인증서 주체의 고유 이름(DN) |
| | | serialNumber | 폐지 요청 인증서의 시리얼번호 |
| | revocationReason | | 폐지 요청 사유 |

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 원격등록소 | header와 body의 DER 인코딩한 값에 대한 서명값 |

〔표 11〕 rp Message 형식

◆ PKIHeader

| | |
|---|---|
| pvno | 1 |
| sender | 인증기관의 고유 이름(DN) |
| recipient | 원격등록소의 고유이름(DN) |
| messageTime | 현재 시간 |
| protectionAlg | 원격등록소 - 전자서명 알고리즘 |
| recipNonce | rr message의 senderNonce 값 |

◆ PKIBody

| rp | (RevRepContent) | | |
|---|---|---|---|
| status | status | | "granted"(0) or "rejection"(2) |
| | status | | "granted"(0) or "rejection"(2) |
| revCerts | CertId | issuer | 인증서 발행자 |
| | | serialNumber | 인증서의 시리얼 번호 |
| | CertId | issuer | 인증서 발행자 |
| | | serialNumber | 인증서의 시리얼 번호 |
| crls | certificateList | | CRL(1개 이상일 수 있다.) |

◆ PKIProtecton

| | | |
|---|---|---|
| protection | 인증기관 | header와 body의 DER 인코딩한 값에 대한 서명값 |

PKIBody의 RevReqContent에는 1개 이상의 복수개의 RevDetails가 들어갈 수 있다. 즉, 여러 개의 인증서 폐지 요청을 함께 할 수 있다. 즉, 전자 서명용 인증서 폐지요청을 기본적으로 할 수 있고 정책에 따라 암호화용 인증서 폐지 요청을 함께 할 수 있다. 이 때 PKIBody의 revDetails의 순서에 따라 rp message의 내용이 구성된다.

(2) rp message

rp message 형식은 〔표 11〕과 같이 제안한다.

rp message에서 status, revCerts의 정보 순서는 rr message의 RevReqContent 순서에 따른다. revCerts는 폐지 요청을 받은 인증서이다. crls에는 CRL이 1개이상 여러 개가 들어갈 수 있다. 즉, 정책에 따라 필요한 경우 deltacrl도 함께 넣어 보낼 수 있다. 인증서 폐지 요청 및 응답에서는 conf message를 사용하지 않는다.

## Ⅳ. 결 론

정보화 사회에서의 전자정부는 하나로 연결된 각종 정보와 서비스를 행정기관 방문 없이 인터넷을 통해 국민에게 직접 제공하게 될 것이다.

그러나 가상환경에서는 현실세계(대면행정)수준의 신원확인 등 안전성 확보가 필수적이므로 정부차원의 전자서명 인증 기반구축이 선행되어야만 한다.

정부전자서명 인증기반은 기존 산업사회에서 종이문서의 효력을 부여하는 행정기관의 관인 또는 실세계의 주민등록증을 대체할 수 있는 핵심기반이며,

가상공간에서의 민원인의 신원확인, 민원관련 전자문서의 진위성 등을 보장하므로 국가차원의 사회간접자본이라 할 수 있다.

따라서 효율적인 GPKI의 구축은 정부와 국민이 자유롭고 안전하게 정보를 교환할 수 있는 사이버 행정처리기반의 완성을 의미하므로, 본 논문에서 제시한 기술표준에 부합되는 정부전자서명 인증체계(GPKI)의 구축과 더불어 민·관간 인증체계가 함께 어울어질 수 있도록 관계 부처가 협력하여 국가차원의 종합적인 관리방안을 수립하여야 할 것이다.

## 참 고 문 헌


[1] ITU-T RecommandationX.509(1997) ISO /IEC 9594-8, 1997, *Information Tehnology -Open Systems Interconnection The Directory : uthentiation Framework*, 1997.

[2] ITU-T X.500, *The Directory - Overview of Concepts, Models and Services*, ITU-T, 14 November, 1988.

[3] PKCS #1: RSA Encryption Standard, Version 1.4, RSA Data Security, Inc., 3 June, 1991.

[4] RFC2104, *HMAC: Keyed-Hashing for Message Authentication*, H. Krawczyk, M. Bellare, and R.Canetti, February 1997.

[5] RFC2510, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, C. Adams, and S. Farrell, March 1999.

[6] RFC2511, *Internet X.509 Certificate Request Message Format*, M. Myers, C. Adams, D. Solo, and D. Kemp, March 1999.

[7] RFC2527,Internet *X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, S. Chokhani, and W. Ford, March 1999.

[8] RFC2459,Internet *X.509 Public Key Infrastructure Certificate and CRL Profile*, R. Housley, W. Ford, W. Polk, and D. Solo, January 1999.

[9] RFC2559,Internet *X.509 Public Key Infrastructure Operational Protocols - LDAPv2*, S. Boeyen, T. Howes, and P. Richard, April 1999.

[10] ITU-T Recommandation X.680 (1997) *ISO/IEC 8824-1. 1998, Information Technology -Abstract Syntax Notation One (ASN. 1) : Specfication of Basic Notation, 1998.*

[11] 최영철, 정권성, 이재일, 홍기웅 "효율적인 인증 경로를 갖는 공개키 기반구조 모델" 제11회 정보 보호와 암호에 관한 학술대회, 한국전자통신연구원 1999. 9.

## 〈著者紹介〉

**장 홍 종(Hong-Jong Chang) 정회원**
1992년 2월 : 한양대학교 전자계산공학과 (공학석사)
2000년 2월 : 인하대학교 전자계산공학과 (박사과정수료)
1983년~1998년 : (재)건설기술교육원 전산실장
1999년 3월~2000년 2월 : 경인여자대학 겸임교수
2000년 3월~현재 : 성결대학교 겸임교수
2000년 5월~현재 : 행정자치부 전문위원
〈관심분야〉 정보보호시스템 평가, 음성인식, 암호학, HCI

**박 인 재 (In-Jae Park)**
1991년 2월 숭실대학교 대학원 전자공학과(공학석사)
1997년 2월 숭실대학교 대학원 전자공학과(공학박사)
1993년 11월~1996년 12월 대우통신(주) 종합연구소 연구원
1997년 2월~현재 행정자치부 정부전산정보관리소 전문위원
1997년 5월~현재 개방형컴퓨터연구회 TG/LAN 기술위원
2000년 9월~현재 숭실대학교 정보통신전자공학부 겸임교수
〈관심분야〉 전자서명인증기반, 정보전대응기반 등 정보보호분야

**이 정 현 (Jung-Hyun Lee)**
1977년 인하대학교 전자공학과 졸업
1980년 인하대학교 대학원 전자공학과(공학석사)
1988년 인하대학교 대학원 전자공학과(공학박사)
1979년~1981년 한국전자기술연구소 시스템 연구원
1984년~1989년 경기대학교 전자계산학과 교수
1989년~현재 인하대학교 전자전기컴퓨터공학부 교수
〈관심분야〉 자연어처리, HCI, 정보검색, 음성인식, 음성합성, 컴퓨터구조, 정보보안