GIS 유통 정보에 관한 보안 방안 연구

홍현기*, 김지홍**, 이상무***

초록

GIS 시스템 구축사업이 진행됨에 따라 편리성을 위한 연구와 함께, 최근에는 전산망 및 인터넷의 보안문제가 대두됨에 따라, GIS 시스템에서도 보안에 대한 관심을 갖게 되었다. 크게 GIS 시스템에서의 보안과 관련된 문제는 지금까지 전문가들을 위한 정보유통에서 최근 일반인들에 대한 정보유통으로 발생되는 유통정보에 대한 보안문제와 GIS 유통노드, 지리공간 데이터 서버에 대한 보안문제로 구별할 수 있다. 유통상의 정보에 대한 보안문제는 전송되는 유통정보에 대한 도청을 방지하기 위한 암호화 기술이 요구되며, 또한 전송도중 불법사용자에 의한 변조 혹은 삭제 등의 위협으로부터 유통정보에 대한 무결성을 입증하기 위한 인증기술이 요구된다. 이와 같이 암호 및 인증기술과 함께, 인터넷과 전산망의 급속한 보급에 따른 GIS 유통노드, 지리공간 데이터 서버에 대한 불법적인 접속 및 무단 변조에 대한 전산망 접속제어 기술도 요구된다. 결과적으로 GIS 시스템이 정상적으로 운용되기 위해서는 이러한 제반 문제 해결을 위한 방안이 제시되어야 하며, 이는 각종 범죄를 방지하고 건전한 정보화 사회를 구축하기 위한 선결과제이다. 따라서 본 고에서는 이러한 제반문제 해결을 위한 방안을 제시한다.

키워드

GIS, 인증, 공개키, 보안

1. 서론

공개키 기반구조 구축사업은 1999년도에 시작되어 현재 금융과 증권분야에서 인증기관 구축작업이 활발히 진행되고 있다. 인터넷상의 지형공간정보의 신뢰성 있는 유통을 위해서는 GIS 분야의 지형공간 데이타 서버 및 메타데이터 서버, 유통구조를 총괄하는 GIS용 인증기관을 구축하여야 한다. GIS용 인증기관(GIS PCA)은 GIS를 총괄하는 Clearinghouse 기능을 가진 게이트웨이 시스템일 수도 있다. GIS PCA는 공개키 기반구조 상의 상위 인증기관으로부터 인증서를 발급받을 뿐 만 아니라, 메타데이터 서버 및 지형공간데이터 서버에 대한 인증서를 발급함으로서, 유통구조내의 서버간의 신뢰성을 구축할 수 있으며, 공개키 기반구조내의 사용자들을위한 GIS 인증서와 관련된 인증정

* 세명대학교 전자공학과 석사과정
** 세명대학교 전자공학과 교수
*** 정보통신부 정보화지원과 행정사무관

책과 보안정책을 실시함으로서, 사이버공간 내에서의 비대면, 비접촉상황에서 GIS 데이터 교환을 신뢰성 있게 수행할 수 있는 방법을 제공한다. 일반적으로 공개키 기반구조 상에서 인증서를 이용함으로서 사용자 인증, 메시지 인증기능 및 인증서의 용도에 따라 적절한 암호알고리즘을 사용할 수 있으며, 기타 접속권한 제한 및 시스템 사용에 대한 과금 기능도 응용할 수 있다.

제 2절에서는 암호 및 인증, 서명용으로 사용될 수 있는 비대칭형 암호알고리즘으로서, 공개키 암호알고리즘에 대하여 살펴보고, 제 3절에서는 공개키 기반 구조의 구성 및 구성 요소들에 대해서 알아본다. 제 4절에서는 GIS 유통정보 보안을 위하여 이러한 공개키 기반 구조상에서의 GIS 인증기관 구축을 제안한다.

2. 공개키 암호시스템

공개키 암호시스템[1]은 비대칭키 암호시스템(Asymmetric Cryptosystem) 이라고도 불리우며, 수학적 함수를 기반으로 하여 한 개의 키 쌍이 존재한다. 하나의 키는 누구든지 사용할 수 있도록 공개하고, 다른 하나의 키는 자신만이 비밀스럽게 보관하는 방식을 말한다. 이때 공개하는 키는 공개키(public key)라고 하며 비밀스럽게 보관하는 키를 개인키(private key)라고 한다. 공개키 암호시스템은 암호화 키와 복호화 키가 서로 다르며, 두 개의 키는 수학적 이론에 의한 쌍으로 구성되며, 이들 중 한 개의 키를 알더라도, 그에 대칭되는 키를 알기 어려운 특성을 가진다. 이러한 방식은 관용 암호시스템에서의 키 관리 및 분배 문제를 해결할 수 있다. 공개키 암호시스템의 구성은 그림 2-1과 같다.

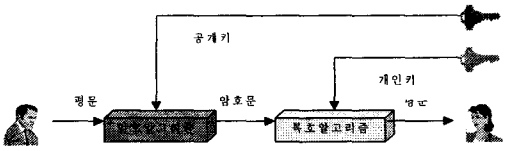

그림 2-1 공개키 암호시스템
암호화/복호화 과정

- 각 사용자들은 각각 개인키와 공개키를 생성한다.
- 각 사용자의 공개키는 공개 디렉토리 혹은 공개 파일에 등록한다. 반면 개인키는 비밀리에 간직한다.
- 송신자가 메시지를 보내고자 할 경우, 수신자의 공개키를 사용해 메시지를 암호화한다.
- 수신자는 자신의 개인키를 이용하여 메시지를 복호한다. 수신자만이 수신자의 개인키를 가지고 있기 때문에 다른 어느 수신자도 메시지를 복호할 수 없다.

공개키 암호시스템의 또 다른 기능은 인증과 서명기능이다. 그림 2-2과 같이 개인키와 공개키를 사용함으로서, 인증 기능을 제공할 수 있다. 송신자는 수신자에게 전송할 메시지를 준비하고 송신자의 개인키를 사용하여 메시지를 암호화하여 전송한다. 수신자는 송신자의 공개키를 사용하여 메시지를 복호할

수 있다. 메시지가 송신자의 개인키를 사용하여 암호화하기 때문에 송신자만이 메시지를 생성할 수 있으므로 송신자의 '디지털서명' 이라 할 수 있다. 디지털 서명문은 송신자의 개인키로 생성되기 때문에, 전송 중에 메시지 변경이 불가능하기 때문에 데이터 무결성을 보장할 수 있다.

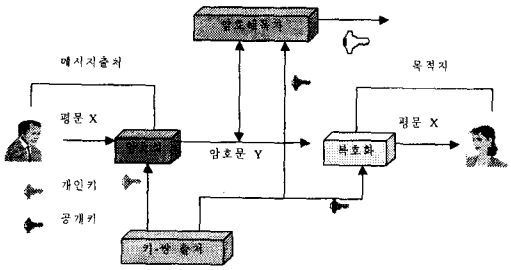

그림 2-2 공개키 암호시스템 : 인증

표 2-1 관용 암호 시스템과 공개키 암호 시스템의 비교

구분	관용 암호 시스템	공개키 암호 시스템
장점	암호화/복호화 속도 빠름 키의 길이가 짧음	키 분배 및 관리 용이 키 변화의 빈도 적음 여러 분야에서 응용 가능
단점	키 분배 및 관리의 어려움 키 변화의 빈도 많음 응용분야 제한적	암호화/복호화 속도 느림 키의 길이가 길다

이러한 공개키 암호 시스템은 비밀키 암호 시스템에 비해 데이터 암호화속도가 매우 느리기 때문에 일반적으로 데이터 암호화에는 사용하지 않으며, 키 분배나 디지털 서명 등에 사용되고 있다. 공개키 암호 시스템의 대표적인 것으로는 인수분해의 어려움을 이용한 RSA 방식과 Knapsack 문제를 이용한 Merkle-Hellmam Knapsack 암호화 방식과 Graham- Shamir 암호화방식, McEliece 암호화 방식과 타원곡선 암호화 방식 등이 있다 표 2-1은 관용 암호시스템과 공개키 암호시스템의 장/단점을 비교하였다.

3. 공개키 기반 구조

공개키 기반 구조(PKI, Public Key Infrastructure)[3]는 전자우편 보안을 위한 PEM(Privacy Enhanced Mail) 시스템의 인증기반 시스템에서 기초되었다. PEM 시스템 구조의 최상위 계층에는 IPRA(Internet Policy Registration Authority)라고 하는 전체 인터넷을 관리하는 서버 기능을 가진 시스템을 두고, 제 2계층으로 PCA(Policy Certification Authority)들을 둔다. PCA는 각 국가 단위로 연결된 여러 개의 CA(Certification Authority)들을 관리하며, 이들 CA는 상호 인증기능을 가진다. 또한 최하위 계층의 CA는 주로 그룹 및 회사, 단체에 해당되며, 그룹 내의 각 사용자들에게 공개키가 포함된 인증서(Certificate)를 발급/관리하는 기능과 비정상적인 상황에서 발생되는 CRL (Certificate Revocation List)을 관리하는 기능을 가진다. 이러한 인증서는 전산망에 접속할 자격이 부여된 사용자임을 나타내며, 또한 이러한 인증서에 기록된 사용자의 공개키는 전송된 메시지에 대한 디지털 서명문을 해석하는데 사용되므로 사용자간의 전송 메시지에 대한 인증기능도 포함된다.

일반적인 PKI 기능은 첫째 사용자의 신원과 그들의 공개키를 비밀리에 결합시키는 공개키 인증서 생성기능, 둘째 직접 혹은 간접적으로 타 사용자의 인증서를 제공하는 기능, 마지막으로 직접 혹은 간접적으로 인증

서 폐지를 통지하는 기능으로 요약해 볼 수 있다.

3.1 공개키 기반 구조의 구성

(1) 순수 계층 구조 : 순수 계층 구조는 그림 3-1와 같이 구성된다. 최상위 계층의 루트 CA는 전반적인 PKI 정책을 수립하고, 제 2 계층의 CA는 루트 CA에 의해 설정된 정책 하에서 자신의 정책을 수립하며 제 3계층의 CA를 인증한다. 그리고, 제 3계층의 CA는 사용자를 인증하는 구조로 이루어진다. 이 구조는 최상위 인증기관들 간의 상호인증은 허용하지만, 하부 CA 간의 상호인증은 원칙적으로 배제한다. 그러나 이 방식은 루트 CA간의 상호인증을 통한 국제간 상호 동작을 원활하게 하는 장점이 있다.

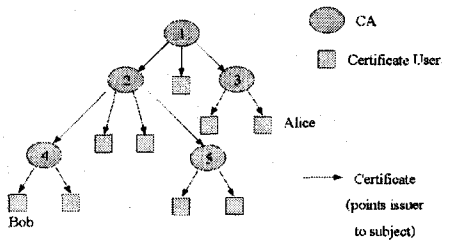

그림 3-1 순수 계층 구조

(2) 네트워크 구조 : 네트워크 기반 구조는 그림 3-2와 같이 모든 CA가 평면적으로 구성되어 있다. 이는 모든 CA간의 상호인증을 허용한다. 그러나 모든 CA간의 상호인증이 허용되면, 상호인증의 수가 대폭 증가하는 단점을 가지게 된다.

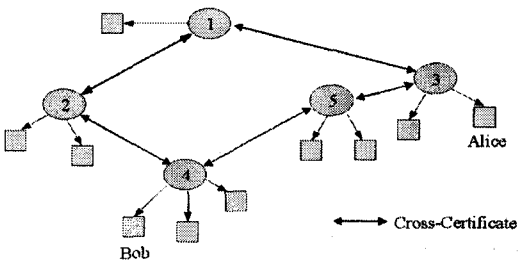

그림 3-2 네트워크 기반 구조

3.2 PKI의 구성 요소

(1) PAA(Policy Approving Authority) : 전체 PKI 시스템 내에서 수행되는 정책을 설정하는 당국이다. PAA는 모든 사용자와 사용자의 연합, CA들이 지켜야 할 전반적인 사용 지침이나 정책을 생성한다. 또한 사용자와 공동목표를 가진 집단, 조직의 정책에 대해 이를 승인하고 감독하는 책임을 가진다. 미국 FPKI의 PAA, 호주 PKAF의 PARRA, 캐나다 GOC PKI의 PMA, 유럽 ICE-TEL PKI의 ICE-TEL CA 등이 여기에 속한다.

(2) PCA(Policy Certification Authority) : PCA는 PAA에서 승인된 전반적인 정책을 확장하거나, 세부 화된 정책을 생성한다. 따라서 PCA는 정책 인증기관이라고 하기 보다는 정책 생성 당국(Policy Creation Authority)이라고 하는 것이 더 적합하다. PCA의 기능 중 중요한 부분은 정책 공표 기능이지만, 일반적으로 PCA는 정책 승인 당국으로 사용되고 있다. 각 PCA는 조직 혹은 공동사회를 대표하며, 미국 FPKI의 PCA, 호주 PKAF의 ICA, 캐나다 GOC PKI의

CCF, 유럽 ICE-TEL PKI의 각 참여 국가들이 이에 해당된다.

(3) CA(Certification Authority) : PKI에는 나름대로의 정책을 가지고 있거나 혹은 정책을 가지고 있지 않은 수많은 CA들이 존재한다. CA는 PAA 및 PCA 정책에 따라서 사용자에게 공개키 인증서를 발급한다. 또한 CA는 PCA의 정책 규제 조건을 만족하는 키 생성 계수를 사용하여 키 쌍을 생성하거나, 사용자가 생성한 키 쌍에 대하여 PCA의 규제 조건을 만족하는지의 여부를 확인한다. 대부분의 CA는 사용자들과 연결될 수 있지만, 하위에 또 다른 CA를 둠으로써 일종의 PCA 역할을 겸할 수도 있다. PKAF의 OCA와 각 PKI 별 CA들이 이에 해당한다.

(4) RA(Registration Authority) : RA는 각 사용자와 CA가 서로 원거리에 위치해 있는 경우에, 사용자와 CA 위치에서 사용자의 인증서 요구를 받아 이를 확인한 후, CA에게 인증서 발급 요청을 한다. 이후 RA는 CA가 발급한 인증서를 사용자에게 전달하는 역할을 한다. GOC PKI에서는 LRA (Local Registration Authority)라 칭하고 있다.

3.3 인증서

인증서는 CA가 단말개체를 인증하는 증서로써, 객체 사용자가 합법적인 사용자임을 입증하기 위하여, CA는 자신의 개인키를 사용하여 디지털 서명문을 생성하여 첨부한다. 네트워크에 가입된 모든 사용자는 상대방의 인증서를 CA에게 요구할 수 있으며, 또한 CA의 공개키를 이용하여 상대방의 인증서를 확인함으로써 합법적인 사용자임을 확인할 수 있다. CA에서 발급한 인증서는 크게 인증서, 서명 알고리즘, 서명문의 3부분으로 나뉘어 진다. 인증서 영역은 일종의 비트 계열로 이루어지며, 인증서와 관련된 발급자, 사용자 객체, 유효기간, 사용자 객체의 공개키 정보 등이 포함된다. 서명 알고리즘 영역은 해당 CA가 인증서를 발급하면서 사용한 디지털 서명 알고리즘에 대한 정보를 포함하며, 서명문 영역은 인증서 전체를 일종의 해쉬 알고리즘에 해당되는 압축 알고리즘을 이용하여 압축하고, 이를 자신의 개인키로 암호화한 비트 계열 형식의 ASN.1 DER 형태로 구성된다.

3.4 인증서 취소 목록(CRL, Certificate Revocation List)

인증서 소유자가 인증서를 발행 받은 조직을 탈퇴하거나, 인증서의 공개키에 부합되는 개인키가 손상되었거나 유출이 의심스러운 경우 등에는 인증서의 유효기간이 만료되지 않았다 할지라도 취소될 필요가 있다. 인증서를 취소하기 위해 X.509에 정의된 메커니즘이 CRL이다

3.5 PKI 운영 프로토콜

인증서를 사용하는 클라이언트 시스템에서 인증서의 상태를 조회하거나 인증서 및 CRL을 획득하기 위해 사용하는 프로토콜을 말한다[3].

(1) OCSP(Online Certificate Status Protocol) : 최종개체가 특정의 인증서에 대한

유효성과 취소 정보를 신속하고 효율적으로 온라인 상에서 알 수 있게 한다. 이는 인증서 상태에 관한 정보를 조회하는 프로토콜이다. OCSP는 인증서의 상태를 조회하는 클라이언트, 클라이언트의 요구에 따라 상태 정보를 전달하는 OCSP 서버, 그리고 일부 인증서 들의 상태정보를 저장하는 CA로 구성된다.

(2) LDAP(Lightweight Directory Access Protocol) : LDAP는 Repository Read, Repository Search, Repository Modify로 동작한다. Repository Read는 최종개체와 CA가 엔트리의 이름을 알고 있을 경우 저장소로 부터 특정 엔트리와 관련된 PKI 정보를 검색하는데 이용되며, Repository Search는 엔트리의 이름이 알려지지 않은 경우 해당 엔트리를 필터링할 수 있는 정보를 저장소로 보내어 해당 엔트리에 대한 PKI 정보를 검색하려 할 때 사용된다. Repository Modify는 저장소에 보관되어 있는 PKI 정보를 첨가하고, 삭제/변경하기 위한 수단을 제공한다.

(3) FTP(File Transfer Protocol) : 실제적으로 인터넷 상의 대부분의 서버들은 LDAP 디렉토리 서비스를 이용하지 않고 있으므로, URI 형태의 주소를 이용하여 인증서 및 CRL 저장소에서 필요한 정보를 검색할 수 있다.

3.6 PKI 관리 프로토콜

(1) 등록 : 사용자가 자신을 직접 CA에게 알리거나, RA를 경유하여 등록하는 과정

(2) 초기화 : 키와 관련된 키 자재(Key Material)의 설치

(3) 인증 : CA에 의한 사용자 공개키 인증서의 발행으로, 발행된 인증서는 사용자의 클라이언트 시스템으로 보내지고 공개 디렉토리에 보관된다.

(4) 키 쌍 복구 : 사용자 클라이언트 시스템의 키 자재를 CA 또는 키 백업 시스템을 이용하여 복구하는 과정으로 선택적으로 이용된다.

(5) 키 쌍 갱신 : 정기적인 키 쌍 갱신을 원칙으로 하며, 키 쌍이 갱신되었을 경우에는 새로운 인증서가 발급된다.

(6) 인증서 폐지 요구 : 인증서의 취소 사유가 발생했을 경우에는 인증서 폐지 요구를 통해 인증서를 폐지한다.

(7) 상호 인증 : CA간에 이루어지는 인증으로, 단방향 상호인증과 양방향 상호인증이 있으며 상호 인증서를 발행한다.

4. 공개키 기반 구조에서의 GIS 유통정보 보안방안

정보통신 기술의 발달로 사회의 모든 분야에서 인터넷의 활용이 급속히 확산되어 전자결제, 전자상거래, 인터넷 뱅킹 등의 편리한 서비스가 제공되고 있다. 그러나 인터넷을 이용한 모든 거래는 거래 당사자간 비접촉, 비대면을 특징으로 하기 때문에, 온라인상의 편리함을 추구할 수 있는 반면에 거래당사자간의 상호신뢰에 있어서 취약성을 가진다. 이러한 단점을 해결하기 위하여 전세계적으로 공개키 기반구조(PKI : Public Key Infrastructure)라는 인증기반 구조를 도입함으로서 거래당사자들 간의 신뢰성과 안전성

을 추구하고 있다. 공개키 기반구조는 계층구조 형식의 인증기반구조를 채택함으로서, 하위 계층의 인증기관 혹은 사용자에게 공개키 인증서 라는 일종의 면허증을 발급함으로서, 인터넷 사용자에게 제3의 공인신뢰기관으로서의 자격을 부여하는 구조이다. 따라서 공개키 기반구조하에서의 모든 사용자는 공인인증기관으로부터 사용용도에 부합되는 공개키 인증서를 발급받고, 이를 이용하여 자신이 정당한 사용자임을 입증할 수 있다. 국내에서는 1999년 2월 5일 전자서명법을 제정하고, 인터넷을 이용한 전자상거래를 활성화시키기 위하여 공개키 기반구조를 도입하고 있다.

4.1 공개키 기반구조에서의 인증기관

(1) PAA

공개키 기반구조에서의 최상위 계층의 인증기관을 PAA(Policy Approval Authority)라 하며, 국내에서는 "전자서명 인증관리센터"라 명명하고 정보통신부 산하의 정보보호센터가 담당하고 있다. 전자서명 인증관리센터의 기능에 대해서는 전자서명법 제25조의 "전자서명 인증관리업무"에 규정하고 있다. PAA는 인증기반구조의 최상위계층으로서, 전자상거래 뿐 아니라, ITS, GIS. EC-CALS 등 인터넷을 기반으로 하는 모든 정보유통에 대한 인증정책을 설정하는 기관이다. PAA의 정책설정을 위한 PAA 정책위원회는 국내 공개키 기반시스템을 운용하기 위한 전반적인 정책설정을 담당하는 기관으로서, 정보통신부의 정보보호센터, 국가 안보차원의 국가 정보원, 국방기밀을 다루는 국방부, 전자상거래의 실수요자와 관련된 통상산업부와 금융기관을 대표하는 은행감독원 그리고 GIS 정보유통을 담당하는 기관 및 교통정보를 담당하는 기관 등으로 구성된 협의회를 두고, 공개키 기반구조를 운용 하여야 하며, GIS 유통정보를 보호하기 위한 방안도 국내 공개키 기반구조를 바탕으로 설정되는 것이 바람직하다. PAA와 관련된 기능은 다음과 같다.

- 인증서와 관련된 기능
  - PAA 인증서(PAA 자신이 서명한 인증서) 발급
  - 하부 PCA에 대한 신원확인 및 인증
  - 하부 PCA에 대한 인증서 서명 및 인증서 발급
  - 하부 PCA의 인증서 관리
- 인증서 취소목록 (CRL : Certificate Revocation List) 관련된 기능
  - PCA의 인증서 취소요구를 확인하기 위한 절차 및 정보 상술
  - PCA의 인증서 취소요구 수신 및 확인
  - CRL 생성 및 공표
- 기타 기반시스템 운용 관련
  - 키 생성기능
  - 자신의 ID와 PCA에 관한 국부정보 공표
  - 인증서 및 CRL, 감사파일에 대한 레코드 보관
  - 국제 혹은 다국적 기반시스템의 근원 CA와의 상호인증

① 공개키 기반구조에서의 정보보호 정책

컴퓨터 및 네트워크의 대량 보급과 인터넷

의 급속한 확산으로 인하여, 전세계가 하나의 사이버 공간으로 연결되고 있다. 또한 사이버 공간상에서의 전자 거래가 급증함에 따라 기밀을 요하는 문서의 전달을 원활하게 하기 위하여 미국, 유럽, 호주 등 선진 각국에서는 자국내의 정보보호를 위한 암호정책을 규정하고 있으며, 범 세계적인 기구인 OECD, APEC 등에서는 각국의 암호정책에 대한 규제를 완화하고, 범 세계적인 전자거래의 활성화를 위하여 암호정책을 수립하고 있다.

가) 암호 알고리즘 : 미국 NIST (National Institute of Standards and Technology)에서는 미국연방 표준 데이터 암호화알고리즘으로 AES(Advanced Encryption Standard) 알고리즘을 제정하고 있으며, 현재까지는 대체적으로 DES, IDEA, RC4, RC5등의 알고리즘을 사용한다. 미국은 40비트 이상의 키를 사용하는 블록암호 알고리즘에 대하여 수출을 규제하고 있다. 국내에서는 정보보호센터에서 128비트 키를 사용하는 SEED 알고리즘을 개발하였고 향후 국내 표준 알고리즘으로 채택될 예정이다.

나) 인증 알고리즘 : 국제 표준알고리즘은 현재 없으며 대체적으로 RSA, DSA 등의 알고리즘을 사용한다. 현재 미국은 512 비트 이상의 키를 사용하는 인증알고리즘에 대하여 수출을 규제하고 있다. 국내에는 정보보호센터에서 KCDSA 알고리즘을 개발중이다.

다) 보안정책

- 하급 보안등급 : 전자메일 수준의 정보보호에 사용되며, 암호화키는 512 비트 정도를 사용하고 있다.
- 중급 보안등급 : 일반문서 수준으로서 정보보호에 사용되며, 암호화키는 768 비트 정도를 사용하고 있다
- 상급 보안등급 : 전자상거래, 비밀문서 수준의 정보보호에 사용되며, 암호화키는 1028 비트 이상을 사용하고 있다.

② 인증실무준칙(CPS: Certification Practice Statements)

PAA에서는 인증실무를 안전하고 신뢰성 있게 수행하기 위하여 인증관리센터 및 공인인증기관의 구체적인 실무에 관한 사항을 명시하는 인증실무 준칙을 마련하고 있다. 인증실무준칙은 인증기관이 인증서를 발급하기 위해 사용되는 실무절차에 관한 세부규정으로 정의할 수 있다

- 인증기관 측면 : 인증실무를 수행하는데 있어 준수하여야 할 실무절차, 비밀키 관리절차, 기타 관리규정 등 인증업무에 필요한 세부사항을 정한 것으로서 인증기관의 신뢰의 척도가 되는 인증서 정책, 가입자에 대한 인증절차, 전자서명 생성키 관리절차 등이 포함되어 있다
- 인증서 사용자 측면 : 인증서 사용자들이 인증실무를 이해하고 인증기관을 신뢰할 수 있게 해 준다.

(2) PCA

국내 공개키 기반시스템을 운용하기 위한 PCA 구성방법은 계층구조 방식을 이용한 구조로서 현재 증권분야와 금융분야의 공인인증기관이 설립되고 있다. PCA는 PAA 정

책을 근간으로 운용하며 조직 나름대로의 정책을 설정하기 위한 위원회를 구성할 수 있다. PCA와 관련된 기능은 다음과 같다.

● 인증서와 관련된 기능
- PAA가 서명한 자신의 인증서 공표
- 하부 CA에 대한 신원확인 및 인증
- 하부 CA에 대한 인증서 서명 및 인증서 발급
- 하부 CA의 인증서 관리

● 인증서 취소목록 (CRL : Certificate Revocation List) 관련된 기능
- CA의 인증서 취소요구를 확인하기 위한 절차 및 정보 상술
- CA의 인증서 취소요구 수신 및 확인
- CRL 생성 및 공표

● 기타 기반시스템 운용 관련
- 키 생성기능
- 자신의 ID와 하부 CA에 대한 국부정보 공표
- 인증서 및 CRL, 감사파일에 대한 레코드 보관
- PAA에서 기본적으로 설정된 정책을 자신이 필요로 하는 정책으로 확장하여 설정할 수 있다.

① 국내 GIS 공인인증기관 설립 제안

현재 국내에서 추진중인 공인인증기관은 금융과 증권분야가 준비중에 있다. 본 절에서는 GIS 유통정보를 보호하기 위하여 새로운 인증기관 설립을 제안한다. 제안된 구조는 그림 4-1에 나타냈다. GIS 인증기관은 공개키 기반구조에 기반한 인증관리체계의 구축, 운영 및 GIS 관련 인증기관에 대한 인증서발급 및 관리 등의 인증업무를 수행함으로서, 인증관리체계의 안전, 신뢰성 확보와 전자서명 인증제도 및 전자문서 이용 활성화 기반조성에 이바지 할 수 있다.

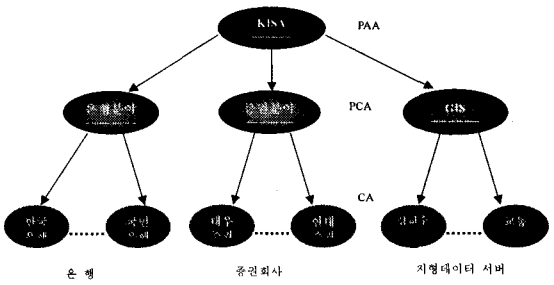

그림 4-1 GIS 분야를 포함한 국내 공개키 기반구조 형태

최근 인터넷을 이용한 전자상거래 시장의 양적, 질적 발전속도를 고려할 때, 인터넷상에서의 전자상거래를 원활하게 할 수 있는 인증기반 구조의 구축이 시급한 현안 과제로 대두되고 있다.

GIS 유통기구(Clearinghouse)를 주축으로 한 유통노드간의 검색망 뿐 아니라, 인터넷을 이용한 사용자들에게 신뢰성과 안전성을 부여하기 위해서는 GIS 유통기구들에 대한 인증기능이 부여되어야 한다. 은행을 감독하는 금융결재원, 증권분야의 한국증권전산㈜와 마찬가지로, GIS 정보유통을 총괄하는 기구가 설립되어, 미국 FGDC의 Clearinghouse와 같은 기능을 가진 PCA가 구성되어야 한다(이하 GIS PCA라 한다.). GIS PCA는 기능적으로 GIS 분야 뿐 아니라, ITS 분야도 포함할 수 있다. GIS PCA는 전국에 배치되어 있는 지형공간 데이터 서버들에 대하여 직접 혹은 간접적인 방법으로 인증 함으로서, 지리공간 정보 유통기구로서의 신뢰성을 줄 수 있다. 마찬가지로 인터넷을 이용하여,

지형공간데이터를 검색, 및 제공받고자 하는 경우에도, 사용자는 공개키 기반구조 상의 인증기관을 통하여 공개키 인증서를 획득하고, 인증서를 이용하여 상호 인증을 시행함으로써, 지형공간 데이터서버 및 사용자 모두에게 신뢰감을 줄 수 있다. GIS PCA는 이와같이 메타데이터 서버, 지형공간데이터 서버들을 총괄하여, 인터넷상의 신뢰성있는 GIS 데이터 유통을 위한 인증서 발급 및 폐지등을 규정하는 인증서 정책과 보안등급에 따른 공개키 발급정책을 수립하고 이를 운용하여야 한다.

(3) CA

CA(Certification Authority)는 PCA의 하부구조로서 PCA에 의해 설정된 정책을 수행하는 기관으로써 GIS 분야에서는 전국의 시도에 분포된 유통기구 및 지형공간 데이터 서버들이 이에 속한다. CA는 하부에 사용자 혹은 또 다른 CA를 둘 수 있다. CA의 기능은 다음과 같다.

● 인증서와 관련된 기능
- PCA가 서명한 자신의 인증서 공표
- 하부 CA 및 사용자에 대한 신원확인 및 인증
- 하부 CA 및 사용자에 대한 인증서 서명 및 인증서 발급
- 하부 CA 및 사용자의 인증서 관리

● 인증서 취소목록 (CRL : Certificate Revocation List) 관련된 기능
- 하부의 인증서 취소요구를 확인하기 위한 절차 및 정보 상술
- 하부의 인증서 취소요구 수신 및 확인
- CRL 생성 및 공표

● 기타 기반시스템 운용 관련
- 키 생성기능 및 사용자에 대한 키 생성 및 발급기능
- 자신의 ID와 하부 구성에 대한 국부정보 공표
- 인증서 및 CRL, 감사파일에 대한 레코드 보관
- PCA에서 설정된 정책을 따른다.

(4) RA

RA(Registration Authority)는 CA의 기능을 대행하며, 키생성 기능과 인증서 발급 기능을 가지고 있지 않으며, 필요에 따라 설치될 수 있다. RA 기능은 다음과 같다.

● 인증서와 관련된 기능
- PCA에 의해 명시된 정책에 의한 사용자의 신원확인과 인증기능
- 사용자 ID 정보를 OCA에게 전달
- CA로부터 발급된 사용자 인증서(상부계층의 인증서 포함) 전달

● 인증서 취소목록 (CRL : Certificate Revocation List) 관련된 기능
- 인증서 취소요구를 확인한 후 CA에게 전달

4.2 공개키 기반구조에서의 인증방법

공개키 인증서는 공개키 기반구조내의 인증기관(PCA, CA, RA)을 통하여 사용자들에게 발급하는 CA 인증서와 CA 혹은 RA를 통하여 사용자들에게 분배하는 사용자 인증서, CA 간의 상호 인증서 등으로 분류되며, 용도에 따라 금융거래용 인증서, 전자상거래

용 인증서, 일반 사용자용 인증서, GIS용 인증서 등으로 분류되며, 인증서 형식은 X.509 v3 형식을 따른다.

(1) 인증서 발급과정

사용자는 CA 혹은 RA로부터 자신을 입증할 수 있는 신분증을 제출하여 자기 자신임을 입증할 수 있어야 인증서를 발급 받을 수 있으며, CA나 RA는 상위 인증당국으로부터 지정된 절차에 의해 확인과정을 거친 후, 공개키 인증서를 발급 받을 수 있다. 이러한 과정은 그림 4-2와 같다. 일반적으로 단일 사용자에게 사업상, 직무상 또는 용도별 동일키 다중 인증서 혹은 다중키 다중 인증서를 발행하는 것을 허용하며, 필요에 따라 익명의 인증서를 발급 받을 수도 있다.

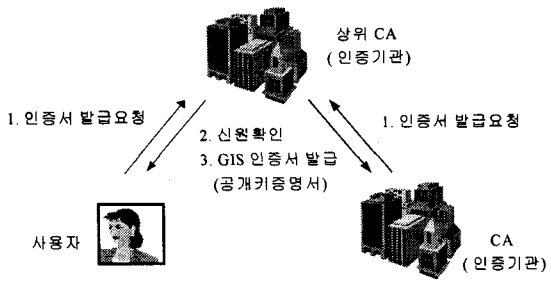

그림 4-2 인증서 발급과정

(2) 인증서를 이용한 지형공간서버 접속과정

인터넷상에서 게이트웨이 및 모든 메타데이터서버, 지형공간 데이터서버가 공개키 기반구조 상의 GIS PCA 인증기관으로부터 신뢰체인을 형성하면, 사용자는 인증기관으로부터 GIS 인증서를 발급받고, GIS 인증서를 이용하여 Clearinghouse에 접속한다.

Clearinghouse와 사용자간의 인증서 교환을 통하여 신뢰체인을 형성하고, 검색이 완료되면 원하고자 하는 지형공간데이터서버에 접속하고, 다시 인증서 교환을 통하여 지형공간데이터서버와 사용자간의 신뢰체인을 형성한다. 이러한 절차는 그림 4-3과 같다. 그러나 사용자는 웹브라우저상에서 메타데이터 검색과정과 지형공간데이터 접속과정을 동시에 수행할 수 있도록 연구가 수행되고 있으므로, 향후에는 두 번의 인증서 교환절차가 한 번의 인증서 교환을 통하여 Clearinghouse 및 지형공간데이터서버와 사용자간의 신뢰라인을 형성할 수 있을 것으로 예상된다.

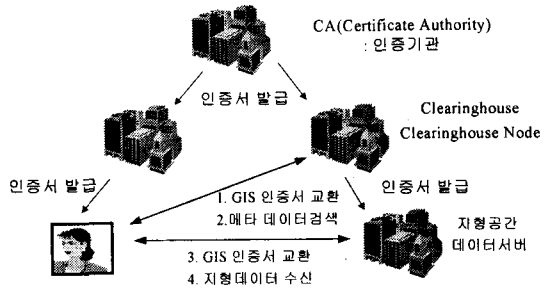

그림 4-3 GIS 지형공간 데이터서버 접속과정

(3) 인증서 확인과정

공개키 기반구조하에서의 인증서 확인절차는 그림 4-4와 같다. 송신자 A가 사용자 B에게 메시지를 보내고자 할 경우를 설명한 것으로, 송신자 A는 자신이 보내고자 하는 메시지를 해쉬 알고리즘으로 압축시킨 후, 이를 송신자 A 자신의 개인키 KsA로 암호화하여 서명문 s를 만들고, 서명문 s와 메시지 M, 자신의 공개키인증서 C를 사용자 B에게 보낸다. 수신자 B는 송신자 A의 인증서를 수신하고, 송신자 A에 대한 공개키인증서를 발행한 인증기관에 대한 공개키 KpCA

를 입수한다. KpCA를 이용하여 송신자 A의 인증서에서 송신자 A의 공개키 KpA를 획득하고, 이를 이용하여 송신자 A가 보낸 서명문을 복호하여 압축문 MD[M]을 생성한다. 또한 수신된 메시지 M으로부터 해쉬 알고리즘으로 압축한 결과와 비교하여 결과가 같으면 인증이 된 것으로 간주하고, 결과가 서로 다르면 거절한다.

(4) 인증서 갱신과정

초기에 인증서를 발급 받고 이를 갱신하여야 할 경우에는 현재 자신이 사용중인 개인키에 의해 디지털 서명된 인증서 갱신 요구 메시지를 필요로 한다. 그러나 사용중인 인증서가 폐지될 경우에는 초기인증서 요구 절차에 의해 발급 받는다.

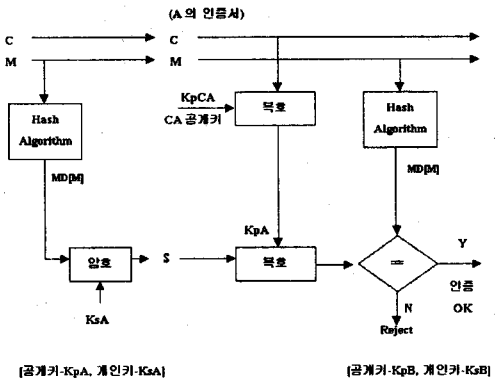

그림 4-4 인증서 확인절차

(5) 인증서 취소목록(CRL, Certificate Revocation List)

CA는 인증서의 유효기간이 만료되었거나, 인증서가 손상되었을 경우, 또는 사용자의 요구가 있을 경우에는 즉시 이를 폐지하고 CRL에 등록하여야 한다. 인증서 취소요구는 전적으로 해당 인증서 소유인이 하여야 하며, 한번 발행된 인증서는 변경될 수 없다. 만일 변경을 요구 할 때에는 해당 인증서는 폐지되고, 새로운 인증서가 발행되어야 한다.

5. 결 론

GIS 유통정보 보안에 대한 총체적인 방안으로 공개키 기반구축 사업과 연계되어야 한다. 공개키 기반구조 내에 GIS 유통정보를 위한 GIS PCA를 구축하고, 게이트웨이 시스템, 메타데이터 서버, 지형공간데이터 서버들을 인증하고, 인터넷상의 신뢰성있는 GIS 데이터 유통을 위한 인증서 발급 및 폐지 등을 규정하는 인증서 정책, 보안등급에 따른 공개키 발급정책 및 운용정책을 수립하고 이를 운용하여야 할 것으로 사료된다.

참 고 문 헌

[1] B.Schneier, *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, Wiley, 1994.

[2] FGDC, *"The FGDC Standard for Digital Geospatial Metadata"*, 1999,11.

[3] IETF, Security Area, *"X.509 (pkix) Document"*, http://www.ietf.org, 1999,7.

[4] US Library of Congress, *"The Z39.50 Standard, Related Agreements, Amendments, Etc"* , .http://lcweb.loc.gov/z39.50/agency/, 1999.

[5] 이만영, 김지홍, 송유진, 염흥렬, 이임영, 류재철, *전자상거래 보안기술*, 1999,8.

[6] 한국전산원, *"NGIS 정보유통을 위한 정보기록방식 표준화를 위한 연구"*, 1997,11.