情報保護學會論文誌
第12券 第2號, 2002. 4

Enterprise PKI에서의 고속 인증 경로 탐색 알고리즘의 설계 및 구현

유 종 덕*, 이 주 남*, 이 구 연**

Design and Implementation of High-Speed Certification Path Discovery on Enterprise PKI

Jong-Duk Yu*, Ju-Nam Lee*, Goo-Yeon Lee**

요 약

전자상거래 등 보안을 요구하는 정보보호 시스템 분야에서는 공개키 기반구조(PKI: Public Key Infrastructure)가 폭넓게 사용되고 있다. PKI 도메인들이 더 많이 설립될수록 더 많은 상호 인증을 필요로 하게 된다. 더구나 각국은 더욱 복잡한 상호 인증을 필요로 하는 많은 인증기관을 가지고 있다. 그러므로 상호 인증을 위한 경로 탐색시 가능한 인증 경로를 빨리 찾기 위한 알고리즘이 필요하다. 이것은 PKI 시스템이 커짐에 따라 더욱 필수 불가결한 요건이 될 것이다. 그러므로 본 논문에서는 그러한 요구에 따라 고속 인증 경로 탐색 알고리즘을 설계하고 구현하였으며 또한 설계된 시스템의 동작 특성을 조사하였다.

ABSTRACT

In the field of secure information systems including electronic commercials, public key infrastructure(PKI) is widely used for secure services. The more PKI domains are established, the more needs are required for cross-domain certifications. Furthermore, each country has many certificate authorities(CA) which requires more complex cross certification. We may need a fast algorithm in order to find the possible certification paths. This will be more indispensible in the growing PKI systems. Thus, in this paper we design a high-speed certification path discovery algorithm and implement it. Also we investigate the feature of operation of the system.

keyword : *pki, 인증 경로, 인증서, 상호 인증*

Ⅰ. 서 론

고도의 정보화 사회가 도래하면서 인터넷을 비롯한 정보 통신 기술이 급속하게 발전되었다. 이로 인해 인터넷을 이용한 전자 상거래와 같은 상업적 서비스가 널리 사용되면서 정보 보호의 중요성이 점차 증대되고 있다. 전자상거래는 서비스 주체나 사용자 모두 인터넷을 기반으로 하는 가상공간에서 정보를 교환한다. 이때 발생하는 여러 형태의 위험을 극복하기 위해서는 end-to-end 개념의 복합적이고 세밀한 수준의 보안 기술이 적용되어야 한다. 또한 사이버 공간에서 교환되는 정보의 내용과 커뮤니케이

* 강원대학교 컴퓨터정보통신공학과 석사과정(juruju@kwnu.kangwon.ac.kr, leejn@kwnu.kangwon.ac.kr)
** 강원대학교 컴퓨터정보통신공학과 교수(leegyeon@cc.kangwon.ac.kr)

션 자체를 입증해 주고 중재해 줄 수 있는 공공성을 지닌 서비스가 필요하게 되었다.[1,3]

현재 전자상거래 등 보안을 요구하는 정보 보호 시스템은 대부분 공개키 기반 구조(PKI: Public Key Infrastructure)를 사용하고 있으며, PKI에서는 인증서를 수령하였을 경우에 수령한 인증서에 대한 검증 과정을 필요로 한다. 공개키 사용자는 원하는 인증기관의 검증된 공개키를 가지고 있지 않을 경우 그 공개키를 획득할 수 있는 추가적인 인증서 연결 구조를 필요로 한다. 인증서 연결구조는 특정 인증기관에서 발행한 인증서와 다른 인증기관에서 발행한 인증서들로 구성되며 이를 인증 경로라 한다.[2]

각 국가 및 기관에서 서로 다른 인증기관을 운영함에 따라 다른 도메인에 속한 인증기관끼리의 인증 과정이 필요하게 되었다. 이러한 상호 인증은 인증기관과 인증기관사이에 또는 인증기관과 브릿지 CA사이, 또는 브릿지 CA와 브릿지 CA사이에 이루어진다.

상호 인증기관이 존재하지 않을 경우에는 인증서 발행기관을 따라 올라가면서 인증서 검증을 하면 되지만, 상호 인증기관이 존재하게 되면 인증기관들 사이에 다양한 인증 경로가 존재하게 되며, 이러한 PKI에서는 보다 효율적인 인증 경로 탐색이 필요하다. 여기서 효율적인 인증 경로 탐색이란 사용자가 탐색한 인증 경로를 통해 얼마나 빠르게 인증서를 검증 할 수 있는지를 뜻한다.

지금까지 발표된 인증 경로에 관한 프로토콜에는 OCSP(Online Certificate Status Protocol)가 있다. 온라인 상에서 인증서 상태 정보를 조회하는 OCSP v1은 사용자에게 인증서의 폐기 유무를 알려주는 기능을 수행한다. 현재 표준화가 진행 중에 있는 OCSP v2는 사용자가 인증 경로를 탐색하고 검증하는 부담을 덜어주기 위해 전용 서버를 제안했는데 아직까지 구현되어 있지 않다.[10]

본 논문에서는 다양한 인증 경로가 존재하는 Enterprise PKI에서 고속의 인증 경로를 탐색하는 알고리즘을 제안하고자 한다. 이를 위해 고속 인증 경로 탐색의 기준이 되는 CA topology라는 개념을 도입하고, CA topology의 구성 요소와 CA topology 획득 방법에 관해 살펴보겠다. 또한 고속인증 경로 탐색 서버를 구현하여 고속 인증 경로 알고리즘을 검증하였다.

II. PKI간의 상호 연동 방법

PKI간의 상호 연동시 가장 중요한 사항은 인증 경로 구축에 소요되는 시간이다.

현재 다양한 구조의 PKI가 존재하기 때문에 이종의 PKI간의 상호 연동은 매우 중요하다. 상호 연동을 위해서는 PKI에서 사용되는 프로토콜, 데이터 구조, 인증서 및 CRL 공유 방식 등의 기술적인 측면을 만족해야 한다. 또한 전자서명과 관련된 법적 효력과 보안 정책, 인증 업무 준칙, PKI 체계 및 관련 정책도 만족 해야한다. 이종의 PKI간의 상호 연동을 위해서 다음과 같은 방법들이 연구되고 있다.[4,5]

① 상호 인증

각각의 PKI 영역들에 대해 다른 인증기관에서 인증서를 발행하는 방법이다. 이 경우에 발급되는 인증서를 상호 인증서라고 한다.

이 연동 방법의 목적은 두 인증기관 간에 신뢰 관계를 구축하는 것이다. 계층적 구조의 경우에는 인증 경로의 길이를 줄일 수 있으나, 원하지 않는 상호 인증의 확장이 발생할 수 있으므로 이를 방지하기 위해서 인증서의 확장자를 이용하거나 정책 제한, 이름 제한, 경로 길이 제한 방식을 사용한다.

② 브릿지 CA

브릿지 CA는 하나의 PKI 신뢰 영역을 다른 PKI 신뢰 영역에 소개하는 소개자의 역할을 수행한다. 각각의 신뢰 영역이 다른 영역과 양방향 상호 인증 협정을 체결할 필요가 없다. 단지 각 PKI 신뢰 영역은 하나 이상의 인증서 정책을 갖는 브릿지 CA와 상호 인증 협정을 체결하게 되며, 두 조직의 인증서 정책이 일치하면 브릿지 CA를 통해서 신뢰 경로가 생성된다.

③ 상호 인정

상호 인정 방식을 이용한 상호 연동 방법은 APEC 통신 워킹 그룹에서 고려하고 있는 개념이다. 상호 인정 방식은 하나의 PKI 도메인 응용이 다른 PKI 도메인의 주체를 인증하기 위해서 다른 PKI 도메인의 인증기관 정보를 사용할 수 있게 하는 방식이다.

이 방식이 상호 인증과 다른 점은 인증기관간의 상호 인증을 위한 별도의 협정이 존재하지 않는다는 것이다. 단지 외부의 독립적인 인가 기관이 각 인증기관을 허가했다는 개념에 바탕을 두고 있다.

④ 인증서 신뢰 목록

사용자가 자신이 신뢰하는 여러 개의 루트 CA의

목록을 만들어 가지고 있는 방식이다. 현재 웹브라우져에서 사용하는 방식이다.

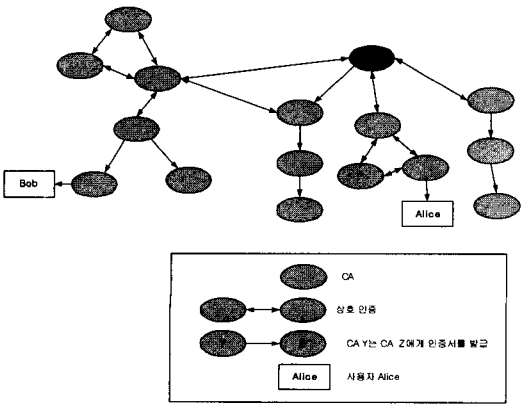
⑤ 위임된 인증 경로 발견 및 검증 방법

인증서의 경로를 찾고 인증서의 유효성을 검증하는 기능을 가진 별도의 서버를 두고, 그 서버에게 해당 인증서에 대한 신뢰 여부를 질의하면 서버가 그 질의에 대한 결과를 사용자에게 통보하는 방식이다.

Ⅲ. 고속 인증 경로 탐색 알고리즘 제안

〔그림 1〕에서 Alice가 Bob의 인증서를 검증하기 위해서는 Alice의 인증기관으로부터 Bob까지 인증서 연결구조를 구성해야 하며 이때 다양한 인증 경로가 존재하게 된다.[6]

계층적 구조만으로 이루어진 PKI 구조에서는 하나의 인증 경로가 존재하나, 메쉬 구조나 상호 인증 기관이 존재하게 될 경우에는 다양한 인증 경로가 존재하게 된다. 각 인증 경로 별로 인증서 연결구조의 길이와 인증서 획득에 걸리는 시간이 다르므로 고속의 인증 경로를 탐색하는 과정이 필요하다. 여기서 고속의 개념은 다양한 척도의 기준을 비용으로 환산했을 경우에 최저 비용이 드는 경로를 말한다. 최저 비용이란 인증 경로를 구성하는 인증기관의 수가 최소인 것이 아니라 각 인증기관에서 인증서 및 CRL 획득에 걸리는 시간이 최소인 것을 말한다. 본 논문에서는 인증 경로를 구성하는데 사용되는 여러 요소들을 비용의 개념으로 환산하여 CA topology 비용이라는 용어를 사용하였다. CA의 topology 비용에 대해 Dijkstra 알고리즘을 적용하여 최소 비용이 소요되는 경로를 찾는다.



〔그림 1〕 복잡한 PKI 구조에서의 인증 경로 설정

본 논문에서는 인증 경로 탐색 서버(DS: delegated server)를 이용하여 고속 인증 경로 탐색의 문제를 해결하고자 한다. 인증서 검증을 위해 사용자가 인증 경로 설정을 DS에게 요청하면 인증 경로를 탐색하여 이를 사용자에게 알려준다.

DS는 사용자의 인증 경로 설정 요구에 응답하기 위해서 PKI를 구성하고 있는 인증기관의 정보(인증기관간의 상호 인증 관계, 인증기관의 CRL size등)를 알아야 한다. 이러한 인증 경로 탐색에 필요한 정보를 CA topology라 하고 이를 다시 비용화 하여 고속 인증 경로를 탐색하는데 사용한다.

3.1 CA topology 비용

고속 인증 경로 탐색 알고리즘에서는 CA topology의 구성 요소를 선택하는 것이 중요하다. CA topology의 구성 요소에 따라서 탐색된 인증 경로가 달라질 수 있기 때문이다.

○ CA topology 비용을 산정 하는 구성 요소를 살펴보면 다음과 같다.

가. CRL size

인증서를 검증하기 위해서는 CRL 또는 delta-CRL의 검증이 필수적이다. 인증기관에서 발급한 인증서의 수가 많을수록 폐기되는 인증서도 많을 것이며, 그만큼 CRL 크기도 커지게 된다. 따라서 CRL의 크기가 클수록 사용자가 다운로드 하는데 걸리는 시간이 많이 소요되며, 다운로드한 인증서 폐기 목록에서 특정 인증서 검색시 더 많은 시간이 소요될 것이다.[7]

또한 사용자가 많을수록 디렉토리 서버에서 사용자의 요청에 대한 서비스 응답 시간이 지연되기 때문에 해당 디렉토리 서버의 인증서 수 및 CRL size는 인증 경로 탐색시 부여되는 비용의 중요한 요소이다.[8]

나. 회선 속도(Bandwidth)

회선 속도는 디렉토리 서버가 연결되어 있는 링크의 전송 능력을 의미한다. 인증서 검증을 위해 CRL 또는 delta-CRL을 다운로드 할 경우, 다운로드 할 CRL size 만큼 회선 속도도 커다란 영향을 미친다.

일반적으로 파일 전송 능력은 10-Mbps의 이더

넷이 64Kbps 전용선보다 높다. 따라서 고속의 회선을 사용하는 디렉토리 서버일수록, CRL 또는 delta-CRL을 빨리 다운로드 할 수 있고 그만큼 인증서를 빨리 검증할 수 있다.

다. 경로 수(Hop count)

홉 수는 인증 경로를 구성하는 인증서 수를 의미한다. 모든 디렉토리 서버의 다른 비용이 같을 경우에는 가장 적은 인증서를 가진 경로가 최상의 경로로 선택될 것이다.

라. 사용량(Load)

각 CA 디렉토리 서버에 대한 자원 사용 비율을 의미한다. 자원이란 CPU 처리속도, 메모리 크기, 네트워크 처리 속도 등을 들 수 있다.

마. 회선 신뢰도(Reliability)

회선 신뢰도는 각 링크의 비트-에러율을 나타낸다. 회선 신뢰도가 좋을수록 동일한 회선 속도를 가지는 링크에서 보다 빨리 데이터를 전송 할 수 있다.

위의 5가지 정보 외에도 네트워크 패킷 전송에 영향을 미치는 요소들이 CA topology 비용으로 산정 될 수 있다. DS 운영자는 위의 정보를 이용하여 다음과 같은 경로 비용 테이블을 구성한다.

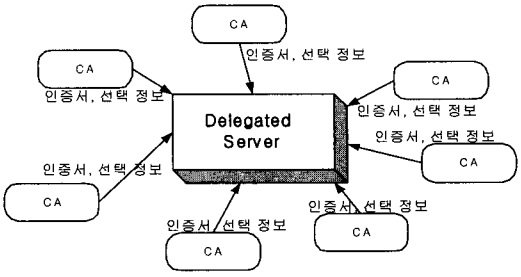
〔표 1〕 CA의 topology 정보

	CA 1	CA 2	...	CA N
CRL size				
회선 속도				
경로 수				
사용량				
회선 신뢰도				

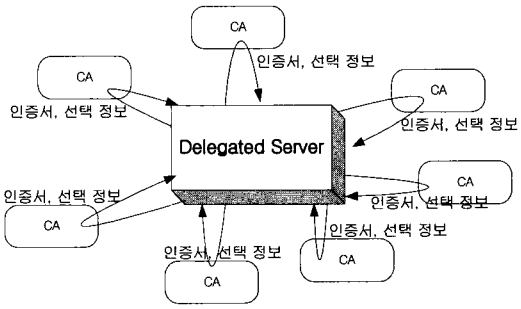
3.2 CA topology 비용 획득 방법

3.1절에서 CA topology를 구성하는 여러 가지 기준 요소에 대해서 알아보았다. 본 절에서는 이러한 CA topology 정보를 획득할 수 있는 방법에 대해서 알아보겠다. 본 논문에서는 다음과 같은 4가지 방법을 같이 제시한다.

가. 〔그림 2〕는 모든 인증기관이 자신과 인접한 인증기관의 CA topology 정보를 유지하고 있다.



〔그림 2〕 CA는 정보 저장, DS에게 정보 제공



〔그림 3〕 CA는 정보 저장, DS가 직접 엑세스

각각의 인증기관은 DS에게 보유하고 있는 정보를 주기적으로 알려준다. 이러한 방법이 DS 입장에서는 가장 이상적이나 현재 운영되고 있는 CA는 이런 기능이 구현되어 있지 않다.

나. 모든 인증기관은 자신과 인접한 인증기관의 CA topology 정보를 유지하고 있으나 자체적으로 DS에게 알려주지는 않는 경우이다. 이 경우는 DS가 직접 인증기관을 접근하여 정보를 수집해야 한다. 가의 경우와 마찬가지로 현재의 CA는 topology 정보를 가지고 있지 않기 때문에 실질적으로 사용하기에는 적합하지 않다.

다. 위의 두 경우처럼 인증기관에게 CA topology 정보 수집 기능을 추가적으로 부여하는 것과는 달리 DS가 모든 CA의 인증서를 직접 획득하여 인증서 정보를 바탕으로 PKI의 전체 구조를 인지하고 CA의 topology 정보를 직접 획득한다. 이는 기존의 CA에 별도의 기능 추가 없이 사용할 수 있다는 장점이 있으나 DS가 정보를 얻는 과정에서 많은 overhead가 발생된다.

라. DS 운영자가 모든 CA에 대한 정보를 직접 입력

하여 테이블을 생성하는 방법이다. 이 경우 DS 운영자는 전체 PKI 구조와 각 인증기관의 CA topology 정보를 알고 있어야 하는 단점을 가지고 있지만, 현재 운영되고 있는 CA의 수가 적고, CA마다 topology를 저장하는 기능이 없기 때문에 현실적으로 가장 적합한 방법이다. 따라서 본 논문에서는 이 방법을 선택하였다.

3.3 인증 경로 탐색시 우선 순위 부여

DS는 PKI 구조와 CA topology 정보를 이용하여 사용자로부터 입력받은 인증기관과 end-entity에게 인증서를 발급한 인증기관 사이의 인증 경로를 탐색한다.

인증 경로 탐색 과정은 먼저 입력받은 인증기관의 상위 인증기관이나 상호 인증기관을 탐색한다. 탐색된 인증 경로에 대하여 basic constraints와 policy constraints의 유효성을 검사한 후, 유효한 경로에 대해서 다시 우선 순위를 부여한다.

인증 경로에 대한 유효성 검사와 우선 순위 부여는 다음과 같은 과정을 거친다.

○ Basic constraints 유효성 검사

Basic constraints는 인증서의 주체가 인증기관인지 end-entity인지 구분하며, 인증 경로를 구성하는 인증서의 수를 제한한다.[9]

Basic constraints는 인증서의 pathLenConstraint 필드를 이용하여 인증 경로를 제한한다. pathLenConstraint 필드는 CA가 true로 설정되어 있을 때만 의미를 지닌다. 이러한 경우, 현재 인증 경로 다음에 올 수 있는 CA의 인증서 최대 수를 제한한다. 0은 인증 경로에 end-entity 인증서 만이 올 수 있음을 나타낸다. pathLenConstraint 필드가 있을 경우, 반드시 0 이상의 값을 가져야만 한다. pathLenConstraint가 나타나지 않을 경우, 인증서 경로의 길이 제한은 없다. 본 인증 경로 탐색 알고리즘에서는 인증 경로 탐색시 basic constraints를 체크하여 다음 인증서가 pathLenConstraint를 만족하지 못한다면 인증 경로 설정시 과다한 비용을 부여하여 인증 경로에 선정되지 못하도록 하였다.

○ Policy constraints 유효성 검사

Policy constraints는 inhibitPolicyMapping 필드와 requiredExplicitPolicy 필드를 이용하여 인증 경로를 제한한다. policy constraints는 위의 두 필드를 이용하여 정책 매핑과, 인증 경로 내의 인증서가 특정 정책만을 허용하도록 할 수 있다.

inhibitPolicyMapping 필드가 있다면 그 값은 인증 경로 내의 정책 매핑이 허용되지 않을 때까지의 정책 매핑이 허용되는 인증서 수를 나타낸다. 예를 들어 1값은 정책 매핑이 현 인증서의 주체에 의해서 발행된 인증서 내에서 처리될 수 있지만, 경로내의 다른 인증서에서 처리 될 수 없음을 나타낸다.

requiredExplicitPolicy의 값은 명시적인 정책이 요구되기 전까지 경로 내에 나타날 수 있는 추가적인 인증서 수를 나타낸다. 여기서 명시적인 정책이란 수용 가능한 정책 식별자나 정책 매핑을 통해 동등하다고 선언된 정책의 식별자를 뜻한다. 인증기관은 적어도 하나의 inhibitPolicyMapping 필드나 requiredExplicitPolicy 필드가 반드시 있어야 한다. requiredExplicitPolicy 필드를 사용하여 policy constraints을 적용 할 경우에는 다음 인증서의 certificate policy 필드를 체크하여 특정 정책 식별자가 존재하지 않을 경우는 과다한 비용을 부여하여 인증 경로 설정에서 제외시킨다.

○ 그 밖의 인증 경로 설정 시 경로에 대한 우선 순위 부여 기준은 다음과 같다.

가. 발행자 algorithm의 OID(Object Identifier)와 주체자 algorithm OID가 동일한 경로에 우선 순위를 둔다.

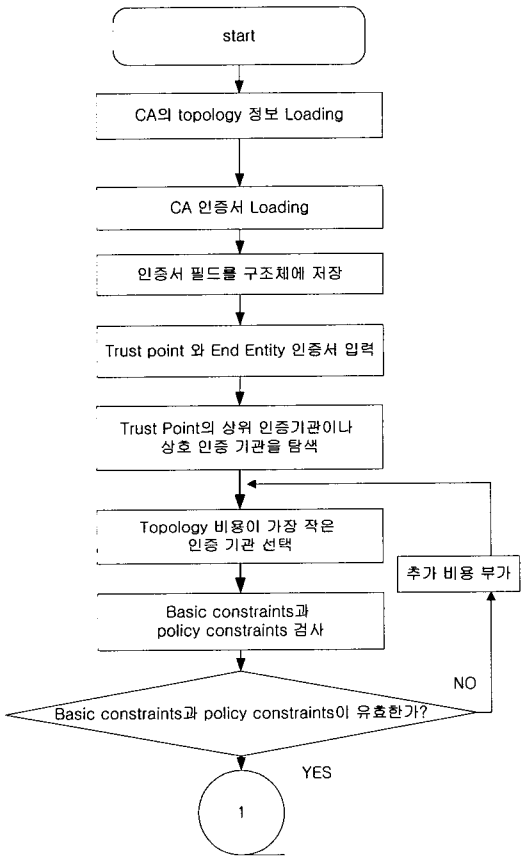
인증서 signature 필드는 인증기관의 서명 알고리즘을 나타내는데 이는 인증기관이 인증서를 서명하기 위해서 사용하는 암호 알고리즘의 식별자를 포함한다. 또한 subjectPublicKeyInfo 필드는 인증서의 공개키 알고리즘을 식별하는데 이용된다. 여기서 발행자 algorithm의 OID와 subject algorithm OID가 동일하다는 것은 인증 경로 상에 있는 인증기관의 서명 알고리즘과 subject의 공개키 생성 알고리즘이 동일하다는 것을 뜻한다.

나. 발행자 DN(Distinguished Name)에서 보다 적은 RDN(Relative Distinguished Name) 구성 요소를 갖는 인증서 경로에 우선 순위를 둔다.

issuer 필드는 인증서를 서명하고 발행한 인증기관을 구분한다. DN은 RDN의 조합으로 구성되어지며, DN은 인증서 마다 각기 다른 값을 갖는다. RDN은 country, organization, state 또는 province name, 그리고 common name의 표준 속성 타입을 나타낸다. 따라서 발행자 DN에서 보다 적은 RDN 구성 요소를 갖는 인증서는 도메인 상에서 보다 상위의 인증기관에 의해 발행된 인증서이다.

다. 주체 DN과 발행자 DN사이에 일치하는 RDN 이 많을수록 우선 순위를 둔다.

subject DN과 issuer DN 사이에 일치하는 RDN 이 많다는 것은 인증서를 발행한 인증기관과 인증서를 발급 받은 인증기관이 동일 도메인 상에 있거나 동일 도메인이 아니더라도 인증서 발급한 인증기관의 도메인과 인증서를 발급 받은 인증기관의 도메인이 서로 관련성 있는 그룹에 속해 있음을 의미하는 것이다.

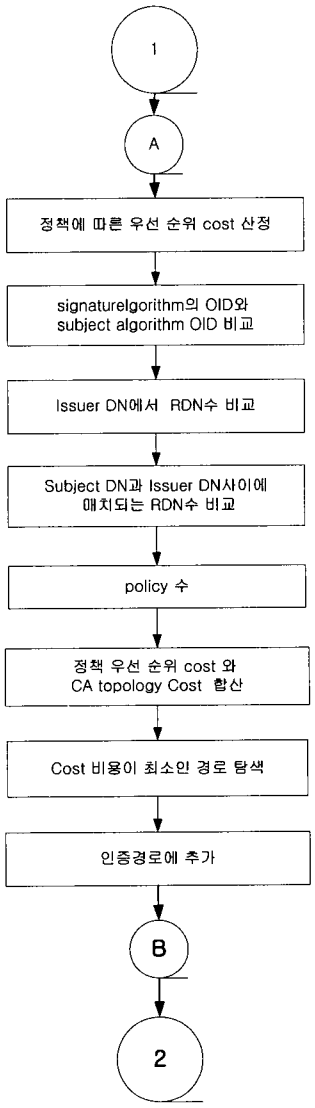


(a)

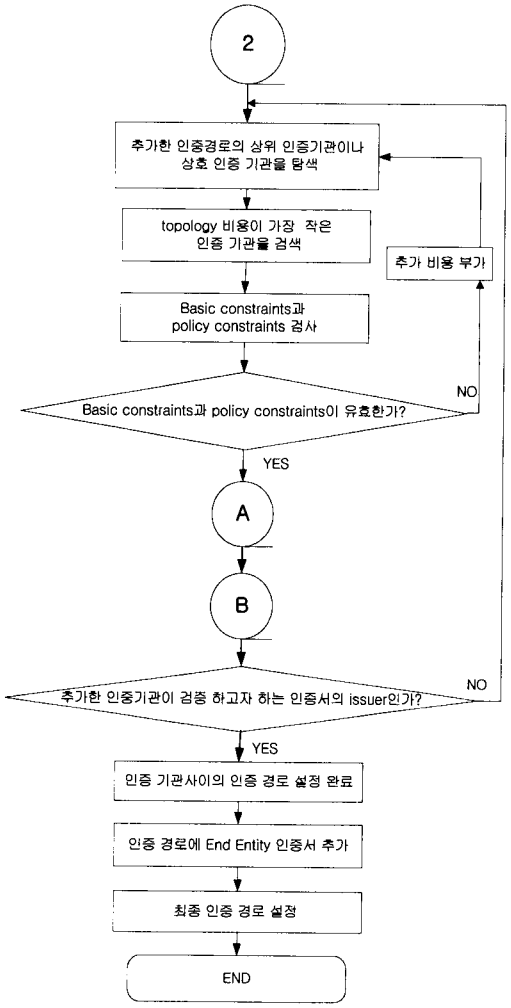
라. 정책이 없는 인증서 보다는 정책이 있는 인증서에 우선 순위를 둔다.

certificate policy 필드는 인증기관이 사용하고 있는 정책에 관한 정보를 나타낸다. 인증 정책 영역은 하나의 인증기관이 여러 개의 인증 정책을 가지는 것을 허용한다. 따라서 정책이 없는 인증서 보다는 정책이 있는 인증서에 우선 순위를 주며, 두 인증서가 모두 정책을 가지고 있을 경우에는 더 많은 정책을 가지고 있는 인증서에 우선 순위를 부여한다.

위에 제시한 여러 가지 기준에 의하여 본 논문에서 구현한 DS의 인증 경로 탐색 알고리즘의 구현 흐름도는 아래 그림과 같다.



(b)

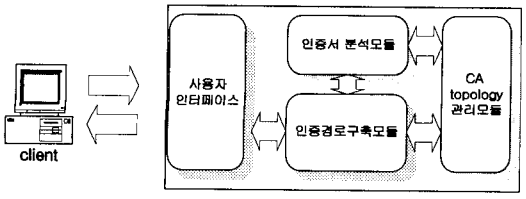


(c)

〔그림 4〕 고속 경로 탐색 알고리즘 순서도

Ⅳ. 고속 인증 경로 탐색 서버 구현

DS의 구성을 살펴보면 〔그림 5〕와 같이 사용자 인터페이스, CA topology 관리 모듈, 인증서 분석 모듈, 인증 경로 구축 모듈로 구성된다.



〔그림 5〕 고속 인증 경로 탐색 서버의 구성

가. 사용자 인터페이스

사용자의 접속을 대기하고, 사용자로부터 경로 설정 요청을 받고, 탐색된 인증 경로를 사용자에게 반환한다.

나. CA topology 관리 모듈

인증 경로 구축 모듈이 인증 경로 구축에 사용하는 정보를 수집하는 모듈로써, CA의 topology 정보와 인증기관의 인증서 정보를 수집한다. 본 논문에서는 CA topology 관리 모듈의 기능을 파일을 통해 입력받는다.

다. 인증서 분석 모듈

인증 경로를 구축하기 위해서는 인증서 정보를 분석해야 한다. 인증 기관의 정책 제한이나 기본 제한의 사용 유무 등을 분석하여 인증 경로 설정에 적용시킨다. 그 외에도 인증 경로 우선 순위에 따라서 비용을 부과하여 고속 인증 경로를 탐색한다.

라. 인증 경로 구축 모듈

사용자 인터페이스로부터 인증 경로 구축을 위한 사용자의 인증기관과 end-entity의 인증기관을 입력받은 후, 이를 기반으로 CA topology 정보를 이용하여 인증 경로를 구축한다. 인증 경로 구축시 인증서 분석 모듈을 통해서 얻은 정보를 함께 적용시켜 최적의 고속 인증 경로를 구축한다.

Ⅴ. 고속 인증 경로 탐색 서버 동작 과정

〔그림 4〕에 나타난 고속 인증 경로 탐색 서버의 동작 과정을 살펴보면 다음과 같다.

① CA topology 비용 및 PKI 정보를 시스템에 loading 한다.
② DS는 사용자의 인증기관과 사용자가 검증 하고자 하는 end-entity의 인증기관을 입력 받는다.
③ CA topology 정보를 이용하여 사용자 인증기관의 상위 인증기관과 상호 인증기관을 탐색한다.
④ 사용자 인증기관으로부터 경로 설정이 가능한 모든 인증기관에 대해 basic constraints와 policy constraints의 유효성을 검사한다.
⑤ 유효성을 위배하는 경로에 대해서 과다한 비용을 부여한 후, 인증 경로 별로 우선 순위를 비교하

여 우선 순위에 따른 비용을 부여한다.

⑥ 초기의 CA topology 비용과 인증 경로 우선 순위 비용을 합하여 dijkstra algorithm 적용, 비용이 최소가 되는 인증 경로를 확정한다.

⑦ 새로 확정된 인증기관에 대해 상위 인증기관과 상호 인증기관을 탐색한다.

⑧ ④번과 ⑤번, ⑥번의 경로 탐색 과정을 거쳐 다음 인증 경로를 확정한다.

⑨ 마지막 인증 기관이 end-entity의 인증기관이 될 때 까지 위의 방법을 반복한다.

⑩ 인증 경로가 확정이 되면 인증서 연결구조 리스트를 구성하여 사용자에게 알려준다.

Ⅳ. 고속 인증 경로 탐색 서버 테스트

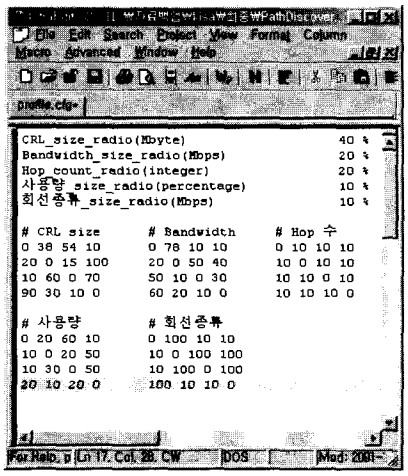
고속 인증 경로 탐색 알고리즘의 검증을 위하여 다음과 같은 테스트를 실시하였다. 테스트 베드에 사용된 PKI 구조는 4개의 인증기관이 각각 상호 인증을 하고 있으며, 각 인증기관 인증서는 자가 인증서를 비롯하여 총 16개의 인증서를 사용하였다.

○ 테스트 베드에서 사용된 개발 환경은 다음과 같다.

- PC: Pentinum Ⅲ 800MHz
- OS: Window 2000 Server
- 개발 tool: Visual Studio 6.0
- Netscape Directory Server 4.2

○ CA topology 비용 구성 요소와 구성 비율은 다음과 같다.

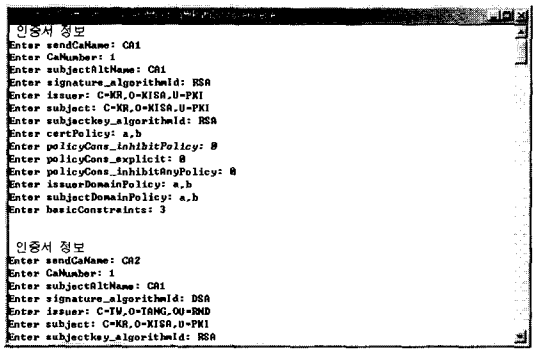
본 테스트 베드에서는 CA topology 비용 구성 요소로써 CRL size, 회선 속도, 경로 수, 사용량, 회선 신뢰도를 사용하였다. CA topology 비용 구성 요소는 CA가 속한 네트워크의 상태에 따라 다르게 책정할 수 있지만, 네트워크라는 개념에 비추어 위와 같이 책정하였다. 또한 구성 비율은 인증 경로 탐색을 요구한 사용자의 요청에 따라서 운영자가 그 비율을 재조정하면 된다. 본 테스트에서 CA topology 구성 비율은 CRL size 40%, 회선 속도 20%, 경로 수 20%, 사용량 10%, 회선 신뢰도가 10%를 차지하도록 구성하였다.



〔그림 6〕 Topology 구성 값

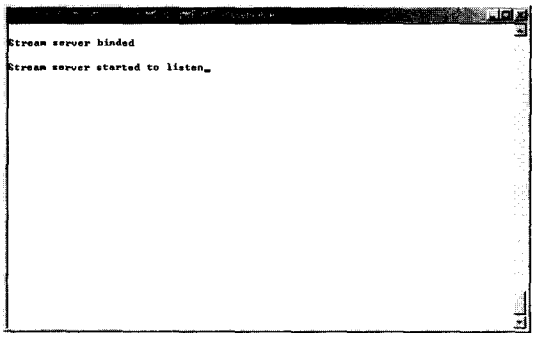
○ 고속 인증 경로 탐색 서버의 테스트 과정은 다음과 같다.

① DS는 파일로부터 각 인증기관에 대한 인증서 정보와 CA topology 정보를 loading 한다.



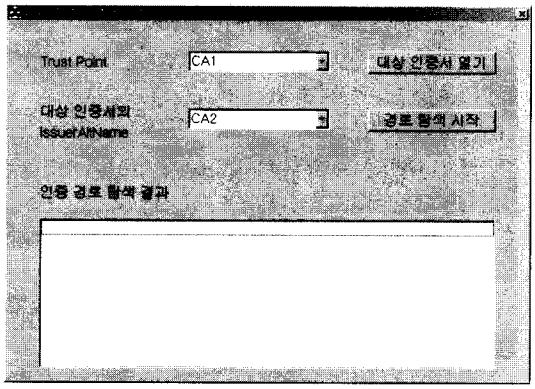
〔그림 7〕 테스트 1

② DS는 사용자의 요청을 기다린다.



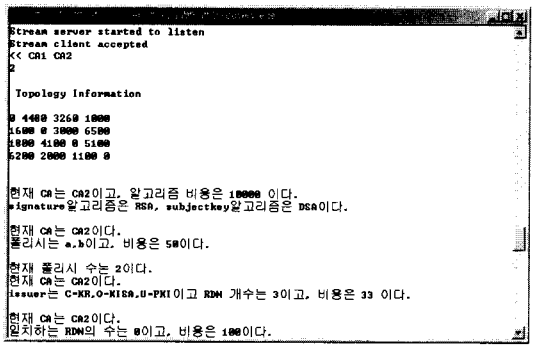
〔그림 8〕 테스트 2

③ 사용자가 인증 경로 설정을 DS에게 요구한다.



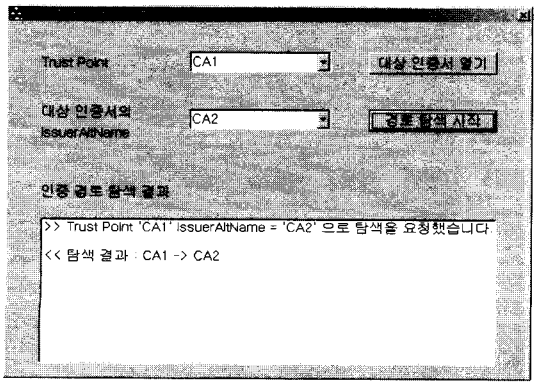
〔그림 9〕 테스트 3

④ DS가 고속 인증 경로 탐색 알고리즘을 이용하여 인증 경로를 탐색한다.



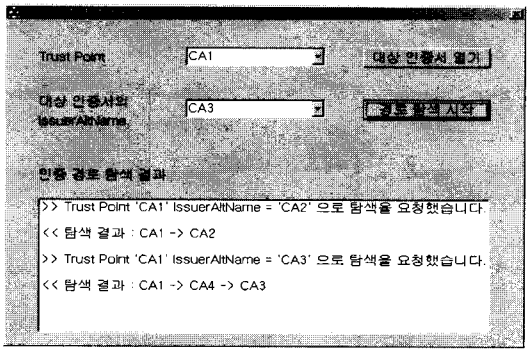
〔그림 10〕 테스트 4

⑤ DS는 사용자에게 탐색된 인증 경로를 알려준다.



〔그림 11〕 테스트 5

⑥ DS는 사용자의 또 다른 인증 경로 설정 요구에 따라 인증 경로를 탐색하여 알려준다.



〔그림 12〕 테스트 6

인증 경로 탐색 서버는 전체 PKI 구조를 인지하고 있어 사용자로부터 인증 경로 구축 요청이 오면 저장된 정보를 기반으로 인증 경로를 구축하여 알려준다.

앞으로는 국가간의 PKI 연동과 각 PKI에서 다양한 정책들이 사용될 것으로 예상되며, 이러한 구조하에서 사용자가 인증서 검증을 원한다면 인증 경로 선택에 관한 문제가 발생될 것이다. 본 논문에서는 이러한 문제를 해결하기 위해 고속의 인증 경로 구축을 위한 알고리즘을 연구하였다. 이 알고리즘은 앞으로 많은 활용 가능성이 예상된다.

Ⅶ. 결 론

PKI 영역간의 상호 연동에서 고려해야할 문제는 영역간에 인증 경로를 구축하고, 인증서의 유효성을 검증하는데 소요되는 시간이다. PKI 영역들은 각각의 특성에 맞게 독립적인 구조로 구축되어 있기 때문에 연동되는 다른 PKI 영역에 대한 인증 경로를 구축하고 검증할 수 있는 방안이 필요하다. 현재 상호 연동 방안으로 인증서 신뢰목록, 상호 인증, 브릿지 CA등이 제시되어 사용되고 있지만 상호 연동된 PKI 영역까지 인증 경로를 구축하기 위해서는 PKI 사용자가 각각의 영역에 대한 인증 경로 구축과 인증서를 검증해야 하는 부담이 있다. 본 논문에서는 이러한 문제를 해결하기 위해 고속의 인증 경로 구축을 위한 알고리즘을 연구하였고, 연구한 알고리즘을 기반으로 고속 인증 경로 탐색 서버를 구현하였다. 인증 경로 탐색 서버는 인증 경로 구축의 범위를 미리

정하고 있고, 그 범위 안의 인증기관들에 대한 정보와 CA topology정보를 미리 기록하고 있어서 사용자로부터 인증 경로 구축요청이 오게 되면 미리 저장되어 있는 인증기관의 정보를 기반으로 인증 경로를 구축하게 된다.

앞으로 국가간의 다양한 PKI의 연동이 이루어질 것이 예상되고 또한 다양한 정책들의 상호연동이 예상되므로 본 논문에서 제안한 고속 경로 탐색 서버의 기능은 유용하게 활용될 것으로 사려된다.

참 고 문 헌

[1] Nash, Andrew, "Implementing and Managing E-Security", McGraw-Hill, 2001.

[2] Housley, Russ, "Best Practices Guide for Deploying Public Key Infrastructure", Wiley, 2001.

[3] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocol", IETF PKIX RFC2510, 2000.

[4] M. Myers, C. Adams, D. Solo, D. Kemp "Internet X.509 Certificate Request Message Format", IETF PKIX RFC2511, 2000.

[5] 염흥열, "PKI 도메인간 상호연동 방안", 제2회 전자서명인증워크샵, 2001.

[6] Russ Housley, Tim Polk, "Planning for PKI", Wiley Computer publishing.

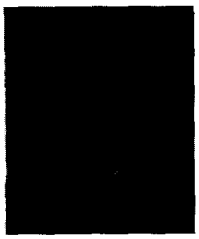
[7] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, 1999.1.

[8] S. Boeyen, T. Howes, P. Richard, "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2", RFC 2559, 1999.4.

[9] 이만영 외 5명, "전자상거래 보안 기술", 생능출판사, 2001.

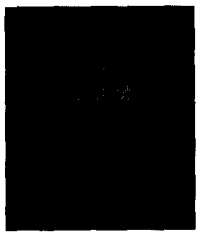
[10] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, 1999.6.

〈著者紹介〉



유 종 덕 (Jong-duk Yu)
2001년 2월 : 강원대학교 정보통신공학과 졸업
2001년 3월~현재 : 강원대학교 컴퓨터정보통신학과 석사과정
〈관심분야〉 PKI, 인터넷 보안, bluetooth

이 주 남 (Ju-nam Lee)
2001년 2월 : 강원대학교 정보통신공학과 졸업
2001년 3월~현재 : 강원대학교 컴퓨터정보통신학과 석사과정
〈관심분야〉 PKI, 인터넷 보안, wireless LAN



이 구 연 (Goo-yeon Lee)
1987년 : 서울대 전자공학과(공학사)
1989년 : 한국과학기술원 전기 및 전자공학(공학석사)
1992년 : 한국과학기술원 전기 및 전자공학(공학박사)
1997년~현재 : 강원대 컴퓨터정보통신학과 교수
〈관심분야〉 PKI, 인터넷 보안, 이동 통신, 데이터 통신, ATM, 광대역 통신망