산업기술연구(강원대학교 산업기술연구소 논문집), 제21권 B호, 2001.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 21 B, 2001.

공개키 기반 구조에서의 고속 인증 경로 탐색 서버의 설계 및 구현

Design and Implementation of High-Speed Certification Path Discovery Server on Public Key Infrastructure

이 주 남* 유 종 덕* 이 구 연**
Lee, Ju-Nam Yu, Jong-Duk Lee, Goo-Yeon

Abstract

In the field of secure information systems including electronic commerces, 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 require 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. We designed and implemented the high-speed certification path discovery algorithm. Also, we investigated the feature of operation of the system.

키워드 : *공개키, 상호 인증, 고속 인증 경로*
Keywords : *pubkic key infrastructure, cross certifications, high-speed certification paths*

1. 서론

고도의 정보화 사회가 도래하면서 인터넷을 비롯한 정보 통신 기술은 급속한 발전을 이루었다. 이로 인해 인터넷을 이용한 전자 상거래와 같은 상업적 서비스가 널리 사용되면서 정보 보호의 중요성이 점차 증대되고 있다. 전자상거래는 서비스 주체나 사용자 모두 인터넷을 기반으로 가상공간에서 정보를 교환하는데 이때 발생하는 여러 형태의 위험을 극복하기 위해서는 end-to-end 개념의 복합적이고 세밀한 수준의 보안 기술이 적용되어야 한다. 또한 사이버 공간에서 교환되는 정보의 내용과 커뮤니케이션 자체를 입증해 주고 중재해 줄 수 있는 공공성을 지닌 서비스가 필요하개 되었다.[1][9]

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 과정이 필요하다. 공개키 사용자가 원하는 인증서와 인증기관 이름 그리고 관련 정보 등을 서명한 인증기관의 검증된 공개키를 가지고 있지 않을 경우 그 공개키를 획득할 수 있는 추가적인 인증서 체인이 필요한데, 이는 특정 인증기관에서 서명한 공개키 소유자의 인증서와 다른 인증기관에 의하여 서명된 인증기관의 인증서들로 구성된다. 이렇게 인증기관의 인증서로 구성된 인증서 체인을 인증 경로라 한다.[6][7]

각 국가 및 기관에서 서로 다른 인증기관을 운영함에 따라 다른 도메인에 속한 인증기관끼리의 인증 과정이 필요하게 되었다. 이러한 상호 인증은

* 강원대학교 컴퓨터정보통신공학과 석사과정
** 강원대학교 컴퓨터정보통신공학과 교수

인증기관과 인증기관사이에 또는 인증기관과 브릿지 CA사이, 또는 브릿지 CA와 브릿지 CA사이에 이루어진다.[5]

상호 인증기관이 존재하지 않을 경우에는 인증서 발행기관을 따라 올라가면서 인증서 검증을 하면 되지만, 상호 인증기관이 존재하게 되면 인증기관들 사이에 네트워크가 형성되어 사용자가 신뢰하는 인증기관과 수령한 인증서 사이에 다양한 인증 경로가 존재하게 되며, 다양한 인증 경로가 존재하는 PKI에서는 보다 효율적인 인증 경로 탐색이 필요하다. 효율적인 인증 경로 탐색이란 탐색한 인증 경로를 통해 얼마나 빠르게 인증서를 검증할 수 있는지를 뜻한다.

본 논문에서는 다양한 인증 경로가 존재하는 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 인증 경로 탐색 서버를 구현하여 고속 인증 경로 알고리즘을 검증하였다.

2. PKI간의 상호 연동 방법

PKI 영역간 상호 연동시 가장 중요하게 고려되는 사항은 사용자가 다른 영역의 인증기관으로부터 인증 경로를 구축하고, 인증서를 검증하는 과정에 소요되는 시간이라고 할 수 있다. 이러한 관점에서 본 장에서는 이종의 PKI 간의 상호 연동방안에 대해서 알아보겠다.

현재 다양한 구조의 PKI가 존재하기 때문에 이종의 PKI간의 상호 연동은 매우 중요하다. 상호 연동을 위해서는 각각의 PKI 구조가 PKI에서 사용되는 프로토콜, 데이터 구조, 인증서 및 CRL(Certficate Revocation Lists) 공유 방식 등의 기술적인 측면을 만족해야 하고, 또한 전자서명과 관련된 법적 효력과 보안 정책, 인증 업무 준칙, PKI 체계 및 관련 정책도 만족 해야한다.[2]

이종의 PKI간의 상호 연동을 위해서 다음과 같은 방법들이 연구되고 있다.

① 상호 인증

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

이 연동 방법의 목적은 두 인증기관간에 신뢰 관계를 구축하는 것이다. 계층적 구조의 경우에는 인증 경로의 길이를 줄일 수 있으나, 원하지 않은 믿음의 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 없고 단지 각각의 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

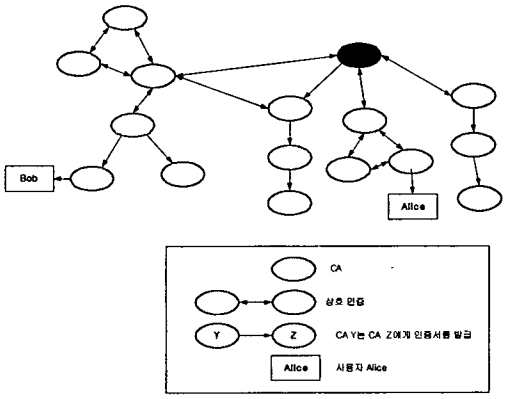
사용자가 자신이 신뢰하는 여러 개의 루트 CA의 목록을 만들어 가지고 있는 방식이다. 현재 웹 브라우저에서 사용하는 방식으로 웹브라우저는 인증서 신뢰 목록을 가지고 있다.

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 통보하며, 인증서의 신뢰 여부는 신뢰 당사자가 결정하게 된다.

3. 고속 인증 경로 탐색 알고리즘 제안

그림1에서 Alice가 Bob의 인증서를 검증하기 위해서는 Alice의 신뢰 기관으로부터 Bob까지의 인증서 체인을 구성해야 하며 위와 같은 복잡한 PKI 구조에서는 다양한 인증 경로가 존재하게 된다.[3][4][5]



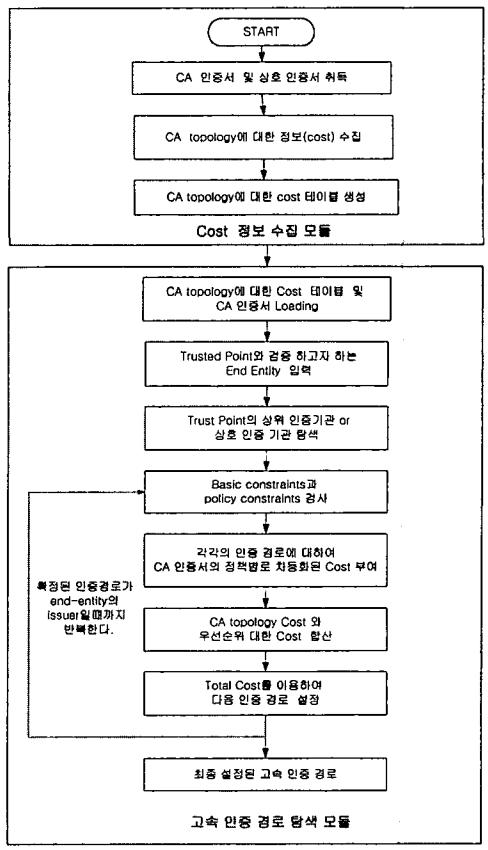
[그림 1] 복잡한 PKI 구조에서의 인증 경로 설정

계층적 구조만으로 이루어진 PKI 구조에서는 하나의 인증 경로가 존재하나, 메쉬 구조나 상호 인증기관이 존재하게 될 경우에는 인증기관 사이에 네트웍이 형성되므로 사용자의 신뢰기관으로부터 검증 대상까지 다양한 인증 경로가 존재하게 되며, 각각의 인증 경로 별로 구성되는 인증서 체인의 길이나 인증서 획득에 걸리는 시간이 각각 다르다. 따라서 다수의 인증 경로중 가장 빠른 고속의 인증 경로를 탐색하는 과정이 필요하다. 여기서 고속의 개념은 다양한 척도의 기준을 비용으로 환산했을 경우에 가장 적은 비용이 드는 경로를 말한다. 즉 고속 인증 경로 탐색이란 다수의 인증 경로중 최저의 비용이 요구되어지는 경로 탐색으로 변환될 수 있다. 최저 비용이란 단순히 인증 경로를 구성하는 인증기관의 수가 최소인 경우로 볼 수 있으나, 보다 실질적인 경우로서 각 인증기관에서 관리하는 디렉토리에서의 인증서 획득 시간 및 CRL 획득 시간 등을 고려하여 비용을 산정 할 수 있다. 각각의 인증 경로 별로 책정된 비용을 Dijkstra 알고리즘을 적용시켜서 최저 비용의 고속 인증 경로를 탐색한다.

본 논문에서는 인증 경로 탐색 서버(DS: delegated server)를 이용하여 고속 인증 경로 탐색의 문제를 해결하고자 한다. 인증서 검증을 위해 사용자가 인증 경로설정을 DS에게 요청하면 DS는 고속 인증 경로 탐색 알고리즘을 이용하여 최적의 인증 경로탐색하여 이를 사용자에게 알려준다.

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

DS는 크게 CA topology를 취득하는 cost 정보 수집 모듈과 cost 정보를 이용하여 고속의 인증 경로를 탐색하는 모듈로 나눌 수 있다.



[그림 2] 고속 인증 경로 탐색 모듈별 흐름도

3.1 CA topology 비용

고속 인증 경로 탐색 알고리즘에서 가장 중요한 것은 CA topology의 구성 요소를 선택하는 것이다. CA topology의 구성 요소에 따라서 탐색된 인증 경로가 달라질 수 있기 때문이다.

고속 인증 경로 탐색 알고리즘은 사용자가 인증서 검증을 위해 특정 인증기관 디렉토리 접근에 필요한 시간을 cost화하여 CA topology 비용을 구성한다.

이때 각 인증기관의 디렉토리 접근에 필요한 시간은 CA topology의 구성 요소에 따라서 각각 달라 질 수 있다.

○ CA topology의 경로 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 인증서를 검색할 때도 더 많은 시간이 소요될 것이다.

또한 사용자가 많을수록 디렉토리 서버에서의 사용자의 요청에 대한 서비스 응답 시간이 지연되기 때문에 해당 디렉토리 서버의 인증서 수 및 CRL 크기는 인증 경로 탐색시 부여되는 cost의 중요한 요소이다.

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 목록의 크기 만큼 회선 속도도 커다란 영향을 미친다.

일반적으로 파일 전송 능력은 10-Mbps의 이더넷이 64Kbps 전용선보다 높다. 따라서 고속의 회선을 사용하는 디렉토리 서버일수록, 인증서 검증을 위해 CRL 또는 delta-CRL을 빨리 다운로드 할 수 있고 그만큼 인증서를 빨리 검증할 수 있다.

다. 경로 수(Hop count)

하나의 홉은 하나의 디렉토리 서버를 access하는 것을 의미한다. 홉 수는 인증 경로 구성에 필요한 인증서 개수를 의미한다. 따라서 모든 디렉토리 서버의 다른 비용이 같을 경우에는 가장 적은 경로 수를 가진 경로가 최상의 경로로 선택될 것이다.

라. 사용량(Load)

회선 사용량은 링크와 같은 네트워크 자원이 얼마나 많이 사용되는지를 보여준다. 사용량은 CPU 사용량, 초당 패킷 처리량과 같은 다양한 측정에 의한 동적인 요인이다. 이러한 값들을 주기적으로 살펴봄으로써 네트웍 자원의 사용 경향을 살펴볼 수 있다.

마. 회선 신뢰도(Reliability)

회선 신뢰도는 각 링크의 비트-에러율을 참조한다. 어떤 네트웍 링크들은 다른 네트웍 링크 보다 더 자주 나빠질 수 있고, 어떤 링크는 나빠졌다가 다른 것보다 더 빨리 좋아질 수도 있다. 회선 신뢰도가 좋을수록 동일한 회선 속도를 가지는 링크에서 보다 빨리 데이터를 전송 할 수 있다. 따라서 회선 신뢰도라는 항목도 CA topology 경로 비용 선정 기준의 하나가 될 수 있다.

위의 5가지 정보 외에도 네트워크 패킷 전송에 영향을 미치는 요소들이 경로 비용으로 산정 될 수도 있다. 기본적으로 위의 정보를 모든 인증기관이 유지하고 있다고 한다면, DS는 위의 정보를 이용하여 다음과 같은 경로 비용 테이블을 구성할 수 있다.

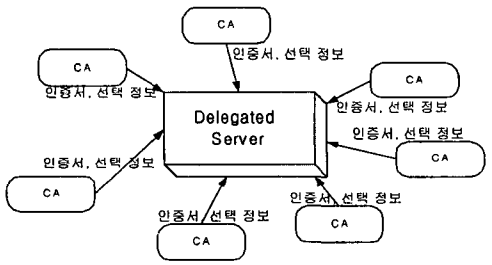
	CA 1	CA 2	...	CA N
CRL size				
회선 속도				
경로 수				
사용량				
회선 신뢰도				

[그림 3] CA의 topology 정보

3.2 CA topology 비용 획득 방법

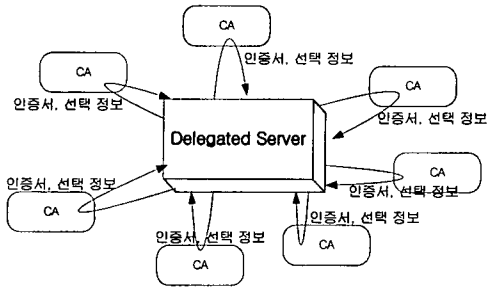
3.1절에서 CA topology를 구성하는 여러 가지 기준 요소에 대해서 알아보았다. 본 절에서는 이러한 CA topology 정보를 획득할 수 있는 방법에 대해서 알아보겠다. 본 논문에서는 다음과 같은 4가지 방법을 같이 제시한다.

가. 그림 4의 경우처럼 모든 인증기관은 자신과 인접한 인증기관의 CA topology 정보를 유지하고 있다. 각각의 인증기관은 DS에게 보유하고 있는 정보를 주기적으로 알려준다.



[그림 4] CA는 정보 저장, DS에게 정보 제공

나. 모든 인증기관은 자신과 인접한 인증기관의 CA topology 정보를 유지하고 있으나 자체적으로 DS에게 알려주지는 않는 경우이다. 이런 경우는 DS가 직접 인증기관을 access하여 정보를 수집해야 한다.



[그림 5] CA는 정보 저장, DS가 직접 엑세스

다. 위의 두 경우처럼 인증기관에게 CA topology 정보 수집 기능을 추가적으로 부여하는 것과는 달리 DS가 모든 CA의 인증서를 직접 획득하여 인증서에 있는 정보를 바탕으로 PKI의 전체 구조를 인지하고, 또한 CA의 topology 정보도 직접 획득한다.

라. DS 오퍼레이터가 모든 CA에 대한 정보를 직접 입력하여 테이블을 생성하는 방법이다. 이 경우 DS 오퍼레이터는 전체 PKI 구조와 각 인증기관의 CA topology 정보를 알고 있어야 한다.

본 논문에서 이용한 전체 PKI 구조와 CA topology 정보 획득 방법으로는 라의 경우를 사용한다. DS의 오퍼레이터가 각 CA의 인증 관계와 함께 CA topology 정보를 파일의 형태로 서버에 입력하는 형식을 갖는다.

3.3 인증 경로 탐색시 우선 순위 부여

DS는 PKI 구조와 CA topology 정보를 이용하여 사용자로부터 입력받은 신뢰기관과 end-entity의 인증기관 사이의 실질적인 인증 경로를 탐색한다.[8][10]

인증 경로 탐색 과정은 먼저 신뢰기관의 상위 인증기관이나 상호 인증기관을 탐색한다. 그리고 연관된 상호 인증기관 중 basic constraints나 policy constraints의 유효성을 검사한 후, basic constraints나 policy constraints에 위배되는 경로는 과다한 cost를 부여하여 인증 경로 설정시 제외되게 만든다. 그리고 basic constraints나 policy constraints이 유효한 경로 중에서 이미 책정된 CA topology 비용과 정책적 우선 순위에 따른 차등화 된 비용을 합하여 최소 비용의 경로를 설정한다.

인증 경로에 대한 유효성 검사와 우선순위 부여는 다음과 같은 과정을 거친다.

o Basic constraints 유효성 검사

Basic constraints는 인증서의 주체가 인증기관인지 end-entity인지 구분한다. 그리고 인증기관을 통한 인증서 경로가 얼마나 깊은지를 구분한다.

Basic constraints는 인증서의 pathLenConstraint 필드를 이용하여 경로 검증을 제한한다. pathLenConstraint 필드는 CA가 true로 설정되어 있을 때만 의미를 지닌다. 이러한 경우, 이 필드는 인증 경로에서 현재 인증 경로의 다음에 올 수 있는 CA의 인증서의 최대 수를 정한다. 0 값은 경로에서 end-entity 인증서 만이 올 수 있다는 것을 나타낸다. pathLenConstraint 필드가 있을 경우, 반드시 0 이상의 값을 가져야만 한다. pathLenConstraint가 나타나지 않을 경우, 인증서 경로의 길이 제한은 없다. 본 인증 경로 탐색 모듈에서는 인증 경로 탐색시 인증서의 basic constraints를 체크하여 만일 인증 경로 체인을 이루는 인증서의 pathLenConstraint 값이 조건을 만족하지 못한다면 basic constraints를 위배하므로 인증 경로 설정시 과다한 cost를 부여하여 인증 경로에 선정되지 못하도록 하였다.

o Policy constraints 유효성 검사

Policy constraints는 inhibitPolicyMapping 필드와 requiredExplicitPolicy 필드를 이용하여 경로 검증을 제한한다. policy constraints는 위의 두 필드를 이용하여 정책 매핑을 금하거나, 인증 경로 내의 각 인증서가 수용할 수 있는 정책 식별자를 가지도록 요구할 수 있다.

inhibitPolicyMapping 필드가 있다면 그 값은 경로 내의 정책 매핑이 더 이상 허용되지 않을 때까지의 추가적인 인증서의 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.

requiredExplicitPolicy 필드가 있다면 인증서는 수용 가능한 정책 식별자를 반드시 포함해야 한다. requiredExplicitPolicy의 값은 명시적인 정책이 요구되기 전까지 경로내에 나타날 수 있는 추가적인 인증서 수를 나타낸다. 수용 가능한 정책 식별자이거나 정책 매핑을 통해 동등하다고 선언된 정책의 식별자이다.

프로필을 따르는 인증기관은 적어도 하나의 inhibitPolicyMapping 필드나 requiredExplicitPolicy 필드가 반드시 있어야 한다.

requiredExplicitPolicy 필드를 사용하여 policy constraints을 적용 할 경우에는 인증 경로 설정시 다음 경로를 확정하고자 할 때 현재 인증서의 requiredExplicitPolicy 필드의 값이 다음 경로 인

증서의 certificate policy 필드를 체크하여 특정 정책 식별자가 존재하지 않을 경우는 과다한 cost를 부여하여 인증 경로 설정에서 제외시킨다.

또한 inhibitPolicyMapping 필드를 사용하여 policy constraints을 적용 할 경우에는 인증 경로를 설정 하고자 할 때 현재 인증서가 inhibitPolicyMapping가 금지하고 있는데 policy mapping을 통하여 두 인증서 사이의 정책을 매핑할 경우에는 과다한 cost를 부여하여 인증 경로 설정에서 제외시킨다.

o 그 밖의 인증 경로 설정시 경로에 대한 우선순위 부여 기준은 다음과 같다.

가. 발행자 algorithm의 OID와 주체자 algorithm OID가 동일한 경로에 우선순위를 둔다.

인증서 signature 필드는 인증기관의 서명 알고리즘을 나타내는데 이는 인증기관이 인증서를 서명하기 위해서 사용하는 암호 알고리즘의 식별자를 포함한다. 또한 subjectPublicKeyInfo 필드는 인증서의 공개키를 운반하고 공개키를 이용하는 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 DN에서 보다 적은 RDN 구성 요소를 갖는 인증서 경로에 우선순위를 둔다

issuer 필드는 인증서를 서명하고 발행한 인증기관을 구분한다. issuer 필드는 비어있지 않은 DN(distinguished name)을 반드시 가져야 한다. DN은 RDN(relative distinguished name)의 조합으로 구성되어지며, DN은 인증서 마다 각기 다른 값을 갖는다.

RDN은 conutry, organization, organization unit, state 또는 province name, 그리고 common name의 표준 속성 타입을 나타낸다. 따라서 발행자 DN에서 보다 적은 RDN 구성 요소를 갖는 인증서는 인증기관이 도메인 상에서 보다 상위의 인증기관임을 알 수 있다.

다. 주체 DN과 발행자 DN사이에 매치되는 RDN이 많을수록 우선 순위를 둔다.

subject DN과 issuer DN 사이에 일치하는 RDN이 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.

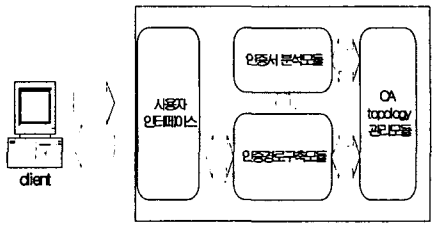
라. 정책이 없는 인증서 보다는 정책이 있는 인증서에 우선 순위를 둔다.

X.509v3 인증서에서 표준 확장의 certificate policy 필드에서는 인증서 정책 정보를 나타낸다. certificate policy 필드는 인증기관이 사용하고 있는 정책에 관한 정보를 가지며, 인증 실무 준칙과 매핑된 인증서 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.

4. 고속 인증 경로 탐색 서버 구현 및 동작 과정

DS는 사용자로부터 인증 경로에 대한 요청을 받으면 DS내에 구축되어 있는 CA topology 정보를 기반으로 인증 경로를 구축해서 알려주게 된다.

DS는 구성을 자세히 살펴보면 그림 6처럼 사용자 인터페이스, CA topology 관리 모듈, 인증서 분석 모듈, 인증 경로 구축 모듈로 구성된다.



[그림 6] 고속 인증 경로 탐색 서버의 구성

가. 사용자 인터페이스

사용자 인터페이스는 사용자로부터의 연결을 대기하고 있으며, 사용자로부터 경로 설정 요청을 받고, 또한 탐색된 인증 경로를 사용자로 반환하는 역할을 하게 된다.

나. CA topology 관리 모듈

인증 경로 구축 모듈이 인증 경로 구축시 사용하는 정보를 수집하는 모듈로써 CA의 topology 정보와 인증기관의 인증서 정보를 수집한다. 본 논문에서는 CA topology 관리 모듈의 기능을 파일을 통해서 입력받는 것으로 한다.

다. 인증서 분석 모듈

사용자로부터 입력받은 정보를 이용하여 고속 인증 경로를 구축하기 위해서는 인증 경로를 이루는 인증기관의 인증서 정보를 분석해야 한다. 인증기관의 정책 제한이나 기본 제한의 사용 유무 등

을 분석하여 인증 경로 설정에 적용시킨다. 그 외에도 인증 경로 우선 순위에 따라서 cost를 부여하여 고속 인증 경로를 탐색한다.

라. 인증 경로 구축 모듈

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

○서버 동작 과정

CA의 topology 비용과 정책에 따른 우선 순위 비용의 책정 모듈을 기본으로 하여 고속 인증 경로 탐색 서버의 동작 과정을 살펴보면 다음과 같다.

① CA topology 비용 및 인증서를 파일을 통해 시스템에 loading 한다.

② 사용자로부터 고속 인증 경로 탐색을 위해서 신뢰기관과 검증 하고자 하는 end-entity의 인증기관을 입력 받는다.

③ CA의 topology 정보를 이용하여 사용자의 신뢰기관의 상위 인증기관이나 상호 인증기관을 설정한다.

④ 설정된 인증기관까지의 인증 경로 확정을 위해 먼저 경로 설정이 가능한 모든 경로에 대하여 basic constraints와 policy constraints의 유효성을 검사한다. 이때 basic constraints나 policy constraints을 위배하는 경로에 대해서는 과다한 cost를 부여한다.

⑤ 인증 경로에 대한 basic constraints와 policy constraints의 유효성 검사후 각 인증 경로 별로 우선 순위를 비교하여 각각의 cost를 부여한다.

⑥ 이미 입력받은 CA topology 비용과 인증 경로 우선 순위 cost를 합하여 비용이 최소가 되는 다음 인증 경로를 확정한다.

⑦ 신뢰기관 다음으로 확정된 인증 경로에서 다시 상위 인증기관이나 상호 인증기관을 탐색한다.

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

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

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

5. 고속 인증 경로 탐색 서버 테스트

고속 인증 경로 탐색 알고리즘의 검증을 위하여 다음과 같은 테스트를 실시하였다.

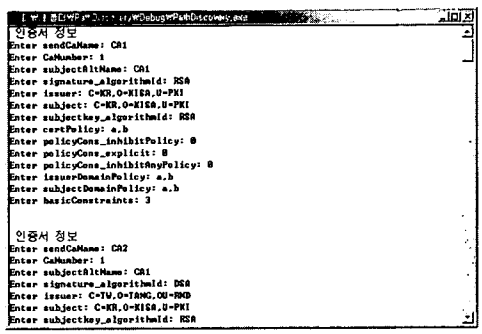
테스트 베드에 사용된 PKI 구조는 4개의 인증기관이 각기 상호 인증을 하고 있으며, 각 인증기관 인증서는 자가 인증서를 비롯하여 총 16개의 인증서를 사용하였다.

○ CA topology 비용 구성 요소와 구성 비율은 다음과 같다.

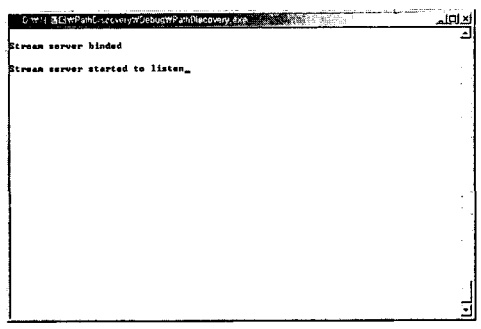
본 테스트 베드에서는 CA topology 비용 구성 요소로써 CRL size, 회선 속도, 경로 수, 사용량, 회선 신뢰도를 사용하였으며, CA topology 구성 비율은 CRL size 40%, 회선 속도 20%, 경로 수 20%, 사용량 10%, 회선 신뢰도가 10%를 차지하도록 구성하였다.

○ 고속 인증 경로 탐색 서버의 테스트 과정은 다음과 같다.

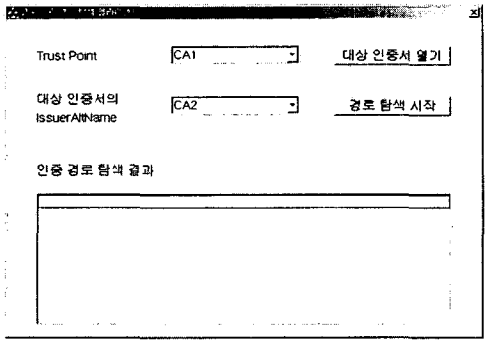
① DS는 파일로부터 각 인증기관에 대한 인증서 정보와 CA topology 정보를 loading 한다.



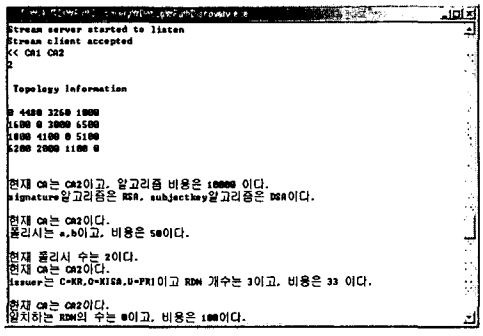
② DS는 사용자의 요청을 기다린다.



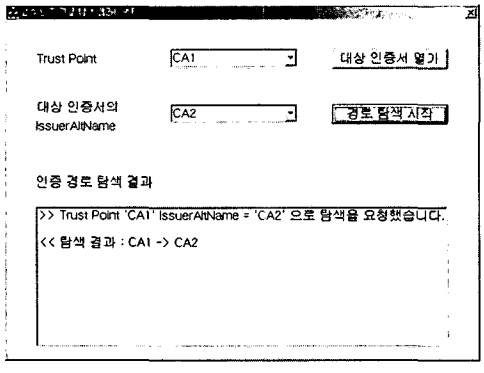
③ 사용자가 인증 경로 설정을 DS에게 요구한다.



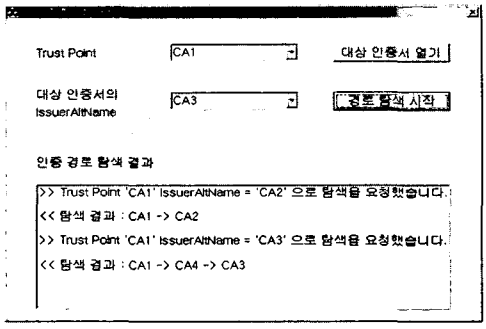
④ DS가 고속 인증 경로 탐색 알고리즘을 이용하여 인증 경로를 탐색한다.



⑤ DS는 사용자에게 탐색된 인증 경로를 알려준다.



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



6. 결론

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 위해서 고속의 인증 경로 구축을 위한 알고리즘을 연구하고, 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 사료된다.

참 고 문 헌

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

[2] Housley, Russ, "Best Practices Guide for Deploying", 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.