情 報 保 護 學 會 誌
第17卷 第4號, 2007. 8

전자거래 신뢰구조를 위한 공개키 기반구조 도메인간 상호인정 방안에 관한 연구

김정덕* · 최광희**

요 약

전자거래 환경 하에서 거래 당사자들간의 신분 확인 및 신뢰 구축은 매우 중요한 문제이다. 이러한 문제에 가장 현실적, 효과적 해결책으로 제시되고있는 것이 PKI기반의 신뢰구조이다. 그러나 기존의 계층적 신뢰구조는 광범위한 전자거래환경의 요구조건을 만족시키지 못하고 있다. 이러한 문제를 해결하기 위하여 각국에서는 상호인증과 상호인정 관련 많은 연구와 대안을 제시하고 있다. 그러나 지금까지의 연구는 신뢰 구조의 형성과 CA간의 상호 연동에만 치중하였을 뿐 최종 사용자의 신뢰의 판단이나 요구사항의 실시간 확인과 같은 의사결정에 직접 관련된 문제에는 소홀히 하였다.

여기에서는 최종사용자의 에이전트와 중계에이전트를 사용하여 실시간 확인기능의 제공과 신뢰보드를 이용하여 상호인정관련 신뢰구조의 확립을 제공하고자 한자. 이는 상호인증과 상호연동의 정책적, 기술적 장벽을 해소하는데 많은 도움을 제공할 것이다.

Ⅰ. 서 론

공개키 기반구조(PKI: Public Key Infrastruc-ture)는 각 나라마다 전자정부 프로젝트, 전자거래 활성화, 개인정보의 보호, 기업기밀 누출방지 문제 등과 맞물려 빠르게 확산되고 있다. 국가별 또는 특정목적의 단체나 조직 대부분은 PKI 신뢰구조 중 가장 단순한 형태의 인증기관(CA) 구성인 계층적 형태의 구조를 구축하고 있다. 계층적 구조의 PKI 인증체계에서는 부속된 모든 인증기관(CA) 및 사용자들을 하나의 루트인증기관(Root CA)하에 두게되는 방식이다. 루트인증기관은 그 도메인 내에서 모든 신뢰당사자들을 위한 신뢰의 정점으로 인정된다. 이러한 계층구조는 루트CA가 하위CA에 인증서 정책의 준수를 요구할 수 있다. 이는 도메인내의 인증서 정책의 일관성을 유지하게 해준다. 또한 상위의 CA가 도메인간 인증을 통제할 수 있고 인증서 경로설정이 용이하다. 따라서 구축이 용이하다는 장점을 가지고 있다.[1][4]

그러나 전자거래가 활성화되면서 국가 간 거래나 다른 성격의 PKI 도메인에 속하여 있는 최종 사용자들간의 거래가 증가되고 있다. 기존의 계층적 방식으로는 이러한 요구를 만족시키기에는 다음과 같은 문제가 발생한다.[6]

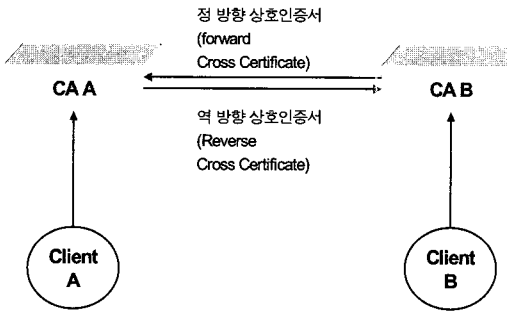
- 전 세계를 통합하는 하나의 루트 인증기관이 필요
- 루트인증기관에 과도한 시스템 부하 발생
- 다양한 서비스를 하나의 시스템으로 구축하기 어려움

따라서 각국마다 이러한 문제를 해결하기 위하여 또한 자국의 PKI체계가 신뢰구조의 종속이나 고립이 되지 않게 하기 위하여 다양한 도메인간 연결방안이 제시되고 있다.

Ⅱ. 도메인간 신뢰연결 방안

도메인간 신뢰의 연결을 제공하기 위한 다양한 방법들이 제시되고 있다. 상호인증, 가교 인증기관, 교차인정, 인증서 신뢰목록, 지정된 인증서, 엄격한 계층구조, 위탁 경로 검증 등 그러나 어떠한 방식도 모든 상황에 적용되지는 못한다. 각 도메인구조나 요구되는 서비스

본 연구는 중앙대학교 교내연구비의 지원을 받아 수행되었습니다.
* 중앙대학교 정보시스템학과 교수(jdkimsac@cau.ac.kr)



〔그림 1〕 상호인증(Cross Certification)

상황에 따라 적절한 방안이 혼합되어 사용되어 질 수 있다. 여기서는 대표적인 세 가지 방식만을 고려해본다.

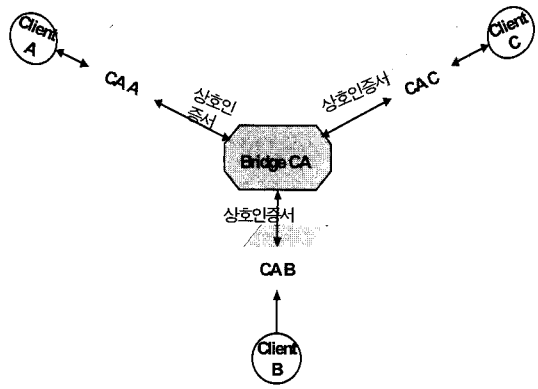
2.1. 상호인증(Cross Certification)

상호인증은 하나의 CA가 다른 CA에게 인증서를 발급하는 행위를 말하며 이때 인증서를 상호인증서라 한다. 이 인증서를 통하여 도메인간 신뢰구조가 연결이 된다.[1]

상호인증이 가지는 장점은 동일한 도메인에서와 같은 원활한 인증서 검증과 일 방향 인증이 가능하다. 즉, A가 B에게 인증서를 발행한다고 해서 꼭 B가 A에게 인증서를 발행할 필요는 없다. 이러한 점은 정책적 문제에서 협상 시 유연성을 제공할 수 있다. 그러나 상호인증의 단점으로는 첫째, 사용자자가 만족하는 서비스수준을 제공하기 위해서는 세밀한 부분까지 완벽한 연동이 필요하다. 그러나 실제 정책적, 정치적 문제와 어플리케션상의 문제로 같은 도메인 내에서도 상호인증은 용이하지 못하다. 둘째, 상호인증 방법의 가장 심각한 문제는 상호인증이 필요한 CA이 수가 늘어날 경우 필요한 상호인증서의 갯수가 급격히 증가한다는 문제점(최악의 경우 n2개의 인증서)[1] 가지고 있다.[1][2][4][8]

2.2. 가교 인증기관(Bridge CA)을 이용한 방법

가교 인증기관(BCA)은 "hub and spoke" 형태의 신뢰모델에 그 이론적 기반을 두고 있다. 이는 양방향 상호인증에서 급격히 증가되는 상호인증의 문제를 해결할 수 있는 방식이다. 각각의 조직이나 CA는 가교 인증기관과 하나 이상의 인증서 정책에 기반 하여 상호인증 협정을 가질 수 있다. 이때 가교 인증기관은 다른 조직이나 CA



〔그림 2〕 가교 인증기관을 이용한 신뢰구조

들간에 인증서 정책상의 일치되는 부분에 한하여 신뢰경로를 제공한다. 이로 인하여 각 조직은 다른 모든 조직과 양방향 상호인증을 수행할 필요가 없어지게 된다.

가교 인증기관을 이용한 방식의 문제점은 다중 상호협상을 위해서 명백한 정책 협상방안이 요구되다. 또한 원하지 않은 신뢰구조의 생성으로 인한 취약성이 발생될 수 있으며 인증서 폐지 목록의 처리에 어려움이 있다. 마지막으로 누가 가교인증기관의 수행주체결정은 각 도메인간의 이익과 관련된 해결하기 어려운 문제로 남아 있다.[1][4][5][8]

2.3. 교차인정(Cross Recognition)

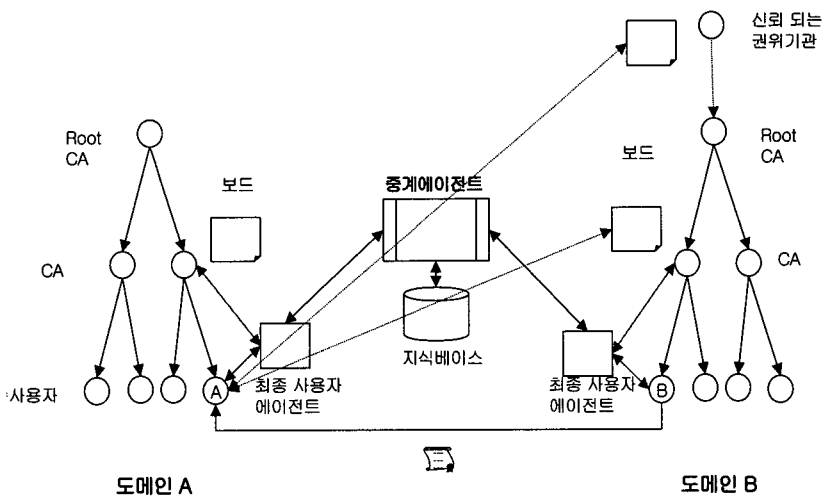
교차인정은 APEC TEL 작업그룹에서 고려되고 있는 개념으로 교차인정의 개념은 다음과 같이 정의한다. "한 도메인의 신뢰당사자가 다른 도메인의 인증서 주체(Subject)[2]를 인증하기 위한 방법으로 인증서 주체가 속해 있는 도메인내의 권위 있는 정보를 이용할 수 있도록 하는 상호연동 협정이다"[1][7]

교차인정은 상호인정과 다음과 같은 점에서 차이가 있다. 첫째, CA들 사이에 상호 또는 단방향의 인정이 없다. 즉 교차인정은 인증기관간의 상호인정이 아니라 국가 간 혹은 PKI 도메인간 상호 인정한 신뢰기관에 의해 상대 인증기관이 허가, 지정, 감리등을 받았다는 개념에 근거를 둔다. 둘째, 신뢰 당사자가 CA을 대신하여 신뢰 여부를 결정한다는 것이다.[1][3][4][8]

교차인정의 가장 큰 장점은 상호인증 협정이 필요하지 않다는 것이다. 그러나 여기에는 신뢰당사자가 어떻

1) n은 상호인증을 필요로 하는 CA의 수

2) 인증기관에서 인증서를 발급 받은 측



〔그림 3〕 중계에이전트를 이용한 신뢰 모형

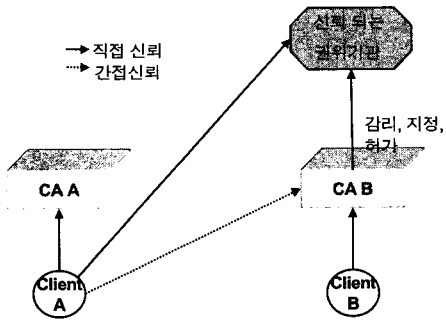
게 의사결정 정보를 가져올 것이지 방법이 제시되지 못한 문제점을 가지고 있다.[7]

도메인간 상호신뢰구조를 만든다는 것은 어려운 문제다. 특히 도메인별로 상이한 도메인의 구조와 어플리케이션이 운영 중이라면 CA간의 연동은 더욱더 세밀한 부분까지의 연동준비작업이 필요하다. 따라서 현재 기술수준과 각각의 도메인별 운영상황을 고려 해보면 상호인정이 현실적 접근이 가능한 방식이다. 이는 CA에 상호인증을 위한 부담을 줄여주며 도메인간 서비스를 요구하는 최종사용자의 기대에 부흥할 수 있다.[2]

Ⅲ. 중계에이전트를 이용한 도메인 간 상호연결 모형

3.1. 신뢰모형

상호인정방안에서는 인증서 신뢰의 여부의 결정은



〔그림 4〕 상호인정을 통한 신뢰구조

신뢰당사자(Relying Part)[3]에게 달려있다. 따라서 어떠한 정보를 제공하여야 신뢰당사자가 충분히 신뢰여부를 결정할 수 있으며 어떠한 방식으로 이러한 정보를 제공할 것이냐가 관건이 된다.

먼저 신뢰여부를 결정할 정보를 살펴보면 다음과 같다.

- 충분히 권위 있는 기관의 신뢰정보
  - 신뢰당사자가 신뢰할 수 있는 기관 예를 들어 국가기관이나 누구나 신뢰할 수 있는 국제조직, 단체가 지정하고 관리 감독하는 인증기관이라면 신뢰당사자는 신뢰할 수 있다.
- 인증서의 유효성
  - 신뢰 당사자가 제공받은 인증서가 신뢰결정 당시에 유효하다면 이를 통해 인증서 주체의 신원과 신뢰를 검증 받을 수 있다.

그러나 도메인간 신뢰연결구조가 없는 상황에서 신뢰당사자가 인증서를 받은 경우 수신된 인증서와 관련된 정보를 획득할 수 없다. 따라서 신뢰당사자가 신뢰할 수 있는 기관까지 신뢰관계를 추적, 신뢰여부를 결정하는 것은 불가능하다. 또한 수신된 인증서에서 인증서 주체와 관련된 정보를 획득, 신뢰당사자가 사용하려면 해당 도메인에서 사용되는 응용프로그램이 있어야 가능하다. 물론 현재 유명 인터넷 탐색기에는 인증서 정보를 제공해주는 기능이 있으나 이는 특정 도메인과 형식에

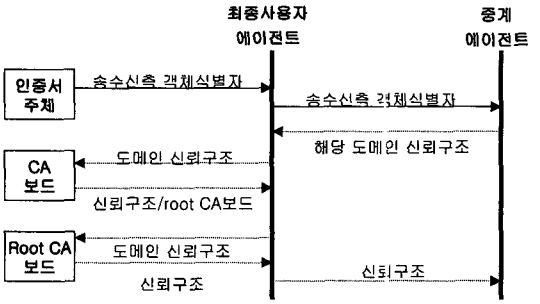
3) 신뢰당사자(Relying Part)는 인증서를 다른 주체로부터 받은 수신자를 의미한다.

한정되어 있으며 최종사용자가 인증서 수신사실의 인식과 수신된 인증서의 위치와 형식에 대한 폭넓은 지식이 있어야 한다. 이것을 전자거래의 편리함을 제공하려고 제안된 인증서 방식이 도메인간 거래에서 오히려 사용자를 어렵게 만들고 있는 것이다.

따라서 최종사용자에게 상이한 도메인으로부터 인증서 수신사실과 해당도메인의 신뢰되는 권위기관이 제공해주고 정보와 인증서의 유효성을 통합해서 제공되어야만이 최종사용자는 수신된 인증서의 신뢰여부를 결정할 수 있다. 또한 최종사용자를 PKI관련지식으로부터 자유롭게 해주기 위해서는 일련의 PKI관련 작업을 대행해 줄 최종사용자 에이전트와 도메인간 신뢰정보를 최종사용자 에이전트에게 전달하고 연결정보를 유지 갱신할 중계에이전트가 필요하다. 이러한 에이전트의 작용으로 최종사용자는 상이한 도메인간 인증서의 사용이나 어플리케이션의 사용이 가능하며 다수의 도메인간 신뢰구조의 연결이 가능하다.

3.2. 최종사용자 에이전트(EndUser Agent)

인증서를 보내는 인증서 주체측 최종사용자 에이전트(End User Agent)역할을 살펴보면, 에이전트는 송신자의 인증서 송신을 감지 이 사실을 중계에이전트에 보낸다. 이때 송신측의 IP어드레스와 같은 송신측 정보[4], 수신대상 정보를 중계에이전트에 보낸다. 또한 중계에이전트와 상호작용을 통하여 해당 도메인의 구조를 중계에이전트에 전송하게 된다. 즉 중계에이전트에서 해당 도메인의 구조를 사전에 알고 있다면 도메인 구조관련 정보는 전송할 필요가 없을 것이다. 그러나 최종사용자 에이전트 포함되어 있는 도메인이 중계에이전트와 처음 상호 작용을 할 경우는 해당 도메인의 신뢰구조를 전송하게 될 것이다. 또한 사전에 중계에이전트에 보관중인 송신측 도메인 구조에 변화가 생길 경우 이에 대한 전송 또한 발생할 것이다. 이러한 도메인 구조의 정보 획득을 위해 최종 사용자 에이전트는 송신자의 인증서에 서명한 CA와 지속적 상호 작용을 통하여 도메인 구조 정보를 최신의 것으로 갱신하게 될 것이다.



〔그림 5〕 인증서 주체측 에이전트

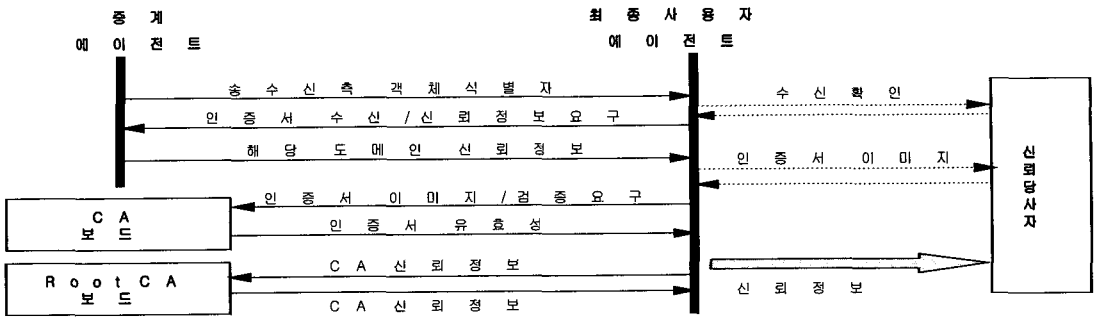
수신측의 최종사용자 에이전트의 역할을 살펴보면 중계에이전트로부터 인증서 송신 사실을 통보 받는다. 또한 송신자의 객체 식별자와 관련된 정보를 중계에이전트로부터 전송 받아 수신된 식별정보와 비교 송신자의 일치여부를 확인하게 된다. 또한 직접적 상호 인증구조가 확립되어 있지 않는 경우(수신측의 신뢰경로내에 송신측과 상호인증의 관계가 없을 경우) 신뢰여부를 판단하기 위한 중계에이전트에 요구하게 된다. 이때 수신측 최종사용자 에이전트는 중계에이전트로부터 송신측 인증기관의 보드정보(위치 및 접근 방법)를 수신하고 또한 인증서 발행 인증기관의 신뢰여부를 결정할 정보를 획득하기 위한 해당 도메인의 Root CA의 신뢰보드 정보도 함께 수신한다. 이 정보를 통하여 수신측 최종사용자 에이전트는 CA신뢰보드에 수신된 인증서 이미지[5]를 보내어 유효성 여부를 검증 받는다. 또한 Root CA신뢰보드에서 해당 신뢰정보를 획득한다.

3.3. 중계에이전트

중계에이전트는 송신측의 최종사용자 에이전트를 통하여 송수신측의 IP어드레스나 정보를 확인하고 인증서 송신사실을 수신하여 수신측 최종사용자 에이전트와 동기화를 위한 준비를 한다. 송신측 최종사용자 에이전트와 작용을 시작하면 우선 도메인구조 정보를 중계에이전트의 지식베이스의 정보와 비교하는 작업을 한다. 이를 통하여 처음 시도되는 도메인이라면 송신측 최종사용자 에이전트에 해당 도메인 신뢰구조를 요구하면 획득하게된다. 이미 저장된 도메인 구조라면 최신정보의 일치성 여부의 확인과 갱신 작업을 한다.

4) X.509인증서에서는 주체의 대체이름으로 rfc822name, DNS, IP, URI, ediPartyname, Drectory Name등이 사용된다.

5) 인증서는 복제가 불가능하게 되어있다. 그러나 CA가 인증서의 신속한 복원을 위해 이미지를 백업하는 서비스를 제공하기도 한다.



〔그림 6〕 신뢰 당사자측 에이전트

상호인증에서 제시된 문제점과 같이 많은 수의 도메인이 상호연결을 원한다면 하나의 중계 에이전트가 모든 도메인의 신뢰구조를 확보하고 수많은 최종사용자 에이전트와 지속적 작용을 하기 어렵다. 이러한 문제를 해결하기 위해 다수의 중계에이전트가 필요하다. 중계에이전트간의 상호 작용을 통하여 수신측의 정확한 위치를 확인할 수 있으며 해당 최종사용자 에이전트와 동기화가 가능하게 된다. 중계에이전트간에 상호작용은 중계에이전트별로 유지 되어야할 지식베이스의 정보의 양을 급격히 줄여줄 수 있으며 많은 CA의 연결이 가능하게 해준다.

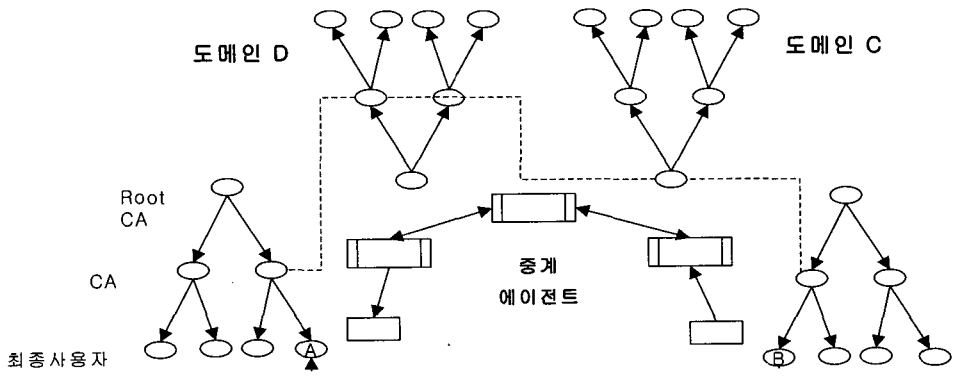
중계에이전트간의 상호작용의 활용은 기존의 상호인증에서 인증서 정책문제로 발생할 수 있는 신뢰의 수준저하를 막기 위해 사용되는 인증서 확장필드의 제한을 좀더 유연하게 해준다.

3.4. 신뢰보드

상호인정(Cross Recognition)에서 최종사용자의 신뢰여부의 결정을 위해서는 두 가지 정보의 제공이 요구된다. 첫째, 인증서를 발행한 CA가 해당도메인에서 신뢰당사자인 최종사용자가 신뢰 할만한 기관이나 조직으로부터인가를 받았다는 정보. 둘째, 수신된 인증서의 유효성 검증 정보. 그러나 기존의 디렉토리 시스템의 경우 최종사용자가 인증서나 PKI관련 지식이 필요로 하며 인증서 주체에 관한 정보와 디렉토리의 접근법에 대한 정보를 알고 있어야 한다.

신뢰보드는 이러한 디렉토리의 문제해결을 위해 신뢰당사자의 에이전트와 통신을 하면 접근은 인증서 이미지와 송수신측의 개체식별정보를 사용하게 된다. 신뢰보드의 종류는 크게 인정기관이나 Root CA에서 사용되는 경우와 CA에서 사용되는 경우로 나누어 볼 수가 있다.

인정기관이나 Root CA에서 사용하는 신뢰보드의 구조와 역할은 첫 번째로 인정기관에서 인정한 CA의 목록을 제공해 줄 수 있다. 둘째, 제3의 신뢰할 수 있는 기관(감리기능의 조직)에서 감리결과나 일정기간내의 운영상의 결과를 공시하여 열람을 원하는 사용자에게 신



〔그림 7〕 중계에이전트간 연결모형

뢰에 관련된 정보를 제공해 줄 수 있다. 이것을 최종사용자가 생소한 CA에 대한 신뢰 여부를 판단할 때 많은 도움을 제공할 수 있을 것이다.

CA에서 사용되는 경우를 생각해 보면 각각의 CA에서는 독립적인 신뢰보드를 운영할 수 있고 또한 공동의 신뢰보드를 운영할 수도 있다. 두 경우 모두 제공되는 정보는 우선 CA의 공개키와 CRL, 인정관련 정보, 독립된 제3의 기관(감리기능의 조직)에서 제공하는 감리결과를 함께 제공할 수 있다. 이 신뢰보드는 최종사용자의 에이전트와 상호작용이 가능하면 최종사용자가 해당 인증서의 인코딩이나 키값의 사용을 요구할 경우 해당 기능의 어플리케이션을 제공할 수 있다.

Ⅳ. 결 론

최종사용자들은 특수한 경우를 제외한(최고수준의 보안을 요구하는) 대부분 최종사용자간의 신분확인과 인증서 유효성의 확인을 원한다. 중계에이전트와 최종사용자 에이전트를 이용한 도메인간 상호인정모델은 최종사용자를 PKI나 인증서 관련지식으로부터 자유롭게 한다. 또한 CA는 상호인증이나 상호연동에 대한요구를 특정서비스로 한정시켜줄 수 있으며 상호연동이나 상호인증을 위한 기술적, 정책적 요구에 좀더 유연성을 제공할 수 있다. 물론 이러한 에이전트를 이용한 방안이 절대적 방법이 아니며 다른 연결모형과 보안적 관계에 있으며 함께 사용되어 질 수 있을 것이다.

후속 되는 연구에서는 실질적 구현을 위한 기술적인 문제(특히 신뢰보드의 보안문제와 인증서이미지 처리, 송수신자 에이전트의 동기화 등)를 심도 있게 다루게 될 것이다.

참고문헌

[1] CA-CA Interoperability, PKI Forum, http://www.pkiforum.org

[2] PKI Interoperability Framework, PKI Forum, http://pkiforum.org

[3] APEC TEL WG, http://www.apii.or.kr/apec/main_apii.html

[4] John Linn, "Trust Models and Management in Public-key Infrastructure", RSA Laboratories, November 2000.

[5] http://www.entrust.com/news/appendices/fbca.htm

[6] 최용락외, "전자상거래를 위한 상호인증 메커니즘", 한국정보보호진흥원, 1999년 8월.

[7] 이상영, "전자서명 상호인정", 한국정보보호진흥원, http://www.kisa.org

[8] Steve Orlowski, "전사서명의 국가간 상호인증을 위한 제언", 정보보호21C, pp.87-98, 2001년 5월.

〈著者紹介〉

김 정 덕 (Kim, Jungduk)
정회원
1979년 연세대학교 정치외교학과, 학사
1981년 연세대학교 경제학과 대학원, 석사
1986년 University of S. Carolina, MBA
1990년 Texas A&M University, Ph.D. in MIS
1991년 - 1993년 한국전산원, 선임연구원
1993년 - 1995년 원광대학교, 조교수
1995년 - 현재 중앙대학교, 교수
관심분야 : 정보보호 거버넌스, 정보보호 관리, IT 감사, 정보시스템의 전략적 응용 등

최 광 희 (Choi, Kwanghee)

1997년 중앙대학교 정보시스템학과, 학사
2002년 중앙대학교 정보시스템과 대학원, 석사
2006년 전남대학교 정보보호협동과정 대학원, 박사 수료
2002년 - 현재 한국정보보호진흥원 선임연구원
관심분야 : 정보보호 거버넌스, 정보보호 관리, Web 20의 신뢰체계