금융환경을 위한 공개키 기반구조 및 응용에 관한 연구

서문석*, 김광조*, 윤이중**
*한국정보통신대학원대학교 **한국전자통신연구원

Electronic Fund Transfer Protocol over the Financial Public Key Infrastructure

Moonseog Seo*, Kwangjo Kim* and Leejung Yun**
*Information and Communications University
**Electronics and Telecommunications Research Institute

요 약

불특정 다수의 고객이 인터넷과 같은 개방형 네트워크 접속을 통해 금융 서비스를 이용하기 위해서는 금융거래에 대한 기밀성 및 인증의 확보가 필수적이며, 이를 위해서는 공개키 암호 이용을 가능하게 하는 공개키 기반구조(PKI : Public Key Infrastructure)의 구축이 선결되어야 한다. 공개키 기반구조가 확립될 경우 이를 이용한 인증서 기반의 다양한 금융 서비스가 제공될 수 있을 것이다. 본 논문에서는 공개키 기반구조가 구축될 경우 금융환경에 적용 가능한 공개키 기반 구조를 살펴보고 인증서를 이용한 전자자금이체 프로토콜을 제안하여 금융환경의 공개키 기반구조의 활용 가능성에 대해 알아본다.

1. 개 요

전자상거래의 활성화로 인터넷과 같은 개방형 네트워크 상에서의 전자지불시스템에 대한 요구가 증대하고 있다. 이러한 개방형 네트워크 상에서의 지불과 같은 금융거래의 안전한 처리를 위해서는 금융거래에 대한 기밀성 확보 및 통신 상대방의 인증과 같은 보안 서비스 이용이 필수적이다. 이러한 보안 서비스를 제공하기 위해서는 전자서명 기술을 포함하고 있는 공개키 암호화 기술이 적용되어야 하고 공개키에 대한 신뢰기관의 인증도 필요하다. 지역적으로 널리 분포해 있는 불특정 다수 고객의 공개키 인증을 위해서는 공개키 인증서의 사용을 통한 자동화된 공개키 관리가 가능한 공개키 기반구조의 구축이 필수적이다. 공개키 기반구조하에서는 다수의 신뢰기관들이 존재할 수 있으며 이들간의 인증구조(신뢰구조)의

확립이 무엇보다 선결되어져야 한다. 특히 거래의 안전을 위해서 인증 및 기밀성 확보가 필수적으로 요구되는 개방형 네트워크 상에서의 금융 서비스 제공을 위해서는 금융기관의 금융서비스 제공에 적합한 공개키 기반구조의 구축이 요구된다.

금융환경에 적합한 공개키 기반구조 하에서 전자자금이체, 전자수납 등과 같은 다양한 응용 프로그램들이 개발되어질 때 안전한 금융거래를 토대로 하는 전자상거래의 활성화가 본격화 될 수 있을 것이다. 본 논문에서는 전자지불시스템 등과 같은 금융거래에 적용되어질 공개키 기반 구조의 구축과 관련하여 적합한 인증구조, 인증기관의 역할 등에 대해 연구해 보고, 공개키 인증서를 이용한 응용프로그램의 예로 은행내 개설된 계좌를 이용한 전자자금이체 프로토콜을 구성해 봄으로써 금융환경 공개키 기반구조의 적용 가능성을 알아보고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 금융 환경에 공개키 기반구조를 적용해야 할 필요성을 살펴보고 3장에서는 신용카드 지불시스템인 SET에서 적용하고 있는 인증구조를 알아보고 4장에서는 공개키 기반 구조의 구축 시 고려되어져야할 구성요소들의 요구사항을 살펴본다. 5장에서는 금융 환경에 적용 가능한 공개키 기반 구조에 대해 살펴보고 6장에서는 금융환경 공개키 기반 구조를 이용한 응용의 예로써 공개키 인증서를 이용한 전자자금이체 프로토콜을 구현해 보고자 한다. 7장에서는 결론과 차후 과제를 기술한다.

2. 금융환경에 공개키 기반구조 적용의 필요성

현재 대부분의 금융기관이 인터넷에 접속하여 제공하는 정보는 단순 홍보차원의 정보 제공에 그치고 있다. 은행이 금융거래를 위해 인터넷과 같은 개방형 네트워크에 접속이 불가능한 이유는 인터넷상에서 전달되는 정보는 외부에 노출될 가능성이 많고, 네트워크에 접속되어 있는 시스템이 주로 개방형 시스템으로 해킹의 위협에 노출되어 있기 때문이다. 특히 금융거래의 특성 상 정보의 누출은 금전적인 손실과 직결되기 때문에 완벽한 기밀성과 인증기술이 보장되지 않으면 개방형 네트워크에 접속은 요원한 것이다. 이와 같이 개체의 인증과 정보의 기밀성 확보는 암호기술을 근간으로 하여 제공될 수밖에 없으며 불특정 다수의 서비스 이용을 가능하게 하는 중요한 기술로 공개키 암호 시스템을 이용할 경우 공개키와 사용자인 개체를 연결시켜주는 신뢰할 수 있고 자동화된 메커니즘이 필요하다. 이를 구체화하여 활용할 수 있는 것이 공개키 기반구조라 할 수 있다. 아직 국가적인 차원에서 공개키 기반 구조가 확립되어 있지 않으나 다양한 응용분야별로 연구가 계속되고 있으며, 조만간 이의 적용이 가능할 것으로 생각되며 전자서명법의 발효에 즈음하여 99년도 7월부터는 공적인 공개키 기반구조와 관계된 인증기관의 서비스가 제공되고 있다.[1][2][3][4]

개방형 네트워크 상에서 금융거래의 적용을 위해서는 효율적인 금융서비스 제공에 적합한 공개키 기반구조를 가지는 것이 필요하다. 특히 전자상거래의 활성화로 다양한 응용서비스가 제공되어 질 수 있으며 이러한 전자상거래의 마지막 단계에는 대금결제를 위한 금융시스템과의 연결이 필수적이다. 결국 전자상거래의 활성화를 위해서는 대금결제를 위한 안전하고 효율적인 전자지불시스템의 구축에 달려 있으며 전자지불시스템의 중심에 은행 및 신용카드사와 같은 금융기관이 위치하고 있다.[5][13]

기존에 금융거래와 관련한 공개키 기반구조의 인증구조로는 신용카드 기반의 전자지불시스템에 적용 가능한 SET(Secure Electronic Transactions)의 인증구조 및 SSL(Secure Socket Layer)에 이용되는 인증구조가 있다. 그러나 이러한 인증구조들은 금융기관의 다양

한 업무에 적용될 수 없고, 국내에 신뢰할 수 있는 인증 서비스를 제공하는 인증기관이 없는 경우에 인증 서비스를 받기 위해서는 외국의 인증 서비스 제공 기관에 높은 사용료를 내고 이를 이용할 수밖에 없는 실정이다. 이에 따라 각국에서도 인터넷과 같은 개방형 네트워크 상에서 전자상거래에 적용 가능한 공개키 기반구조의 구축에 박차를 가하고 있으며, 이미 외국에서는 VeriSign, GlobalSign, Thawte 등과 같이 실용화 단계까지 접어든 인증 시스템들도 있다.[7][8][9]

전자상거래의 활성화로 전자지불시스템의 개발이 필수적으로 요구되는 시점에서 이를 원활히 수행하기 위한 공개키 기반구조의 확립은 무엇보다도 우선적으로 필요하다고 할 수 있다.

3. SET의 인증구조[7]

본 장에서는 금융거래 중의 하나인 신용카드에 의한 전자지불시스템에 활용되고 있는 SET에서 채택하고 있는 인증구조에 대해 살펴보고자 한다.

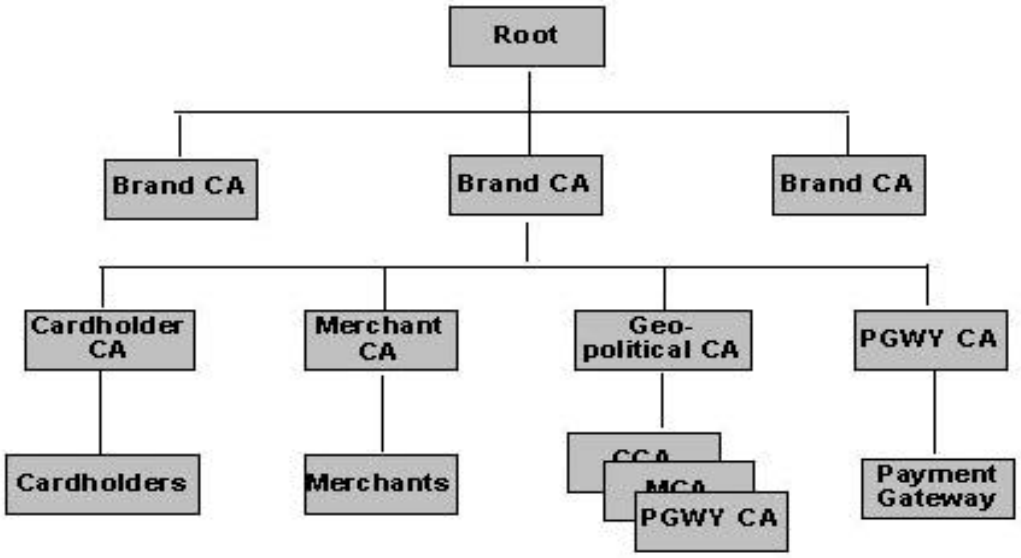
SET 환경에서의 구성원은 VISA혹은 MasterCard와 같은 신용/직불카드를 발급해주는 카드 발급기관(Issuer) 및 상점의 거래 내역을 처리해주는 서비스를 제공해 주는 매입기관(Acquirer)이 있으며 이러한 역할은 보통 은행 및 신용카드사가 수행한다. 또한 발급기관으로부터 카드를 발급 받은 카드소지자(Cardholder), 상품이나 서비스를 판매하는 상점(Merchant) 그리고 상점에 온라인 전자 상거래 서비스를 제공해 주는 시스템 혹은 기관인 지불 게이트웨이(Payment Gateway)로 구성된다. 서비스가 원활히 이루어지도록 상점 및 카드 소지자에게 공개키 인증서를 발행해 주는 인증기관도 구성원으로 포함되어 진다.

SET에서 공개키 암호기술을 이용하여 제공하고 있는 서비스로는 발급기관의 공캐키 인증서를 이용하여 고객의 카드 번호가 노출되지 않도록 하는 기밀성 서비스, 고객이 상품이나 서비스의 대가 지불 시에 자신의 전자서명에 의한 인증 서비스, 카드소유자나 매입기관에 대한 상점의 인증, 발급기관 및 매입기관의 인증 서비스 등을 제공할 수 있다. 또한 개방형 네트워크인 인터넷 상에서 거래 정보의 무결성 확보가 가능하다.

SET에서 사용하고 있는 인증구조는 (그림 1)에서와 같이 하향식 계층구조(Top-Down Hierarchical Structure)를 가지고 있으며 이러한 하향식 계층구조는 전체의 인증구조가 하나의 응용인 카드거래에 적용되도록 국한하고 있어 다른 인증구조와의 연동 없이 단일 인증서 만을 채택하여 위협요소를 최소화할 수 있다. 결국 현재 SET의 인증구조 하에서 발급되는 인증서는 신용카드 거래에 국한하여 이용될 수 있는 것으로서 이의 사용을 위해서는 복잡한 소프트웨어의 개발 및 인증 획득이 필요하다.

SET의 인증구조를 일반적인 금융거래를 위한 인증구조로 그대로 채택하기란 불가능할 것으로 판단된다.

한편, 전자쇼핑몰들이 기밀성 및 인증 서비스 이용을 위해 SSL을 설치하여 이용하는 경우 일반 인증기관에서 발행하는 서버의 인증서가 필요하기 때문에 외국의 인증기관으로부터 인증서 발급 서비스를 이용하고 있다. 미국의 VeriSign사의 경우 SSL 서버용 인증서 수수료가 1년에 서버 1대 당 $249이다. 현재 국내에는 인증기관 서비스를 상업적으로 운영하는 업체가 없는 관계로 대부분의 전자쇼핑몰들이 외국의 인증기관을 이용하는 상태이므로 많은 외화가 손실되고 있다.[10][13]



(그림 1) SET의 공개키 인증구조

4. 공개키 기반구조(PKI) 구축을 위한 구성요소별 요구사항[6]

PKI구축을 위해 필요한 요구사항들을 PKI를 구성하는 구성요소별로 정리하였다.

가. 전반적인 기반구조에 대한 요구사항

PKI 전반에 걸쳐 적용되어질 수 있는 요구사항들로 다음과 같은 것들이 있다.

- 신뢰(Trust) : PKI 자체 및 그들의 구성요소들은 신뢰할 수 있는 개체이어야 한다. PKI는 자신의 신뢰성을 보안정책을 확립함으로써 증명할 수 있는 데 보안정책은 사용자 인증 및 식별을 위한 절차, 키의 생성 및 배포방법, 안전하고 신뢰할 수 있는 방법으로 인증서를 생성하는 방법을 서술하고 있다. PKI의 구성요소들도 PKI가 이러한 기능들을 올바로 수행하고 있다는 것을 납득할 수 있도록 보안 대응책을 구현할 필요가 있다.
- 사용의 편리성(Ease of Use) : PKI의 구성 및 기능이 전자서명을 이용하는 응용에 짐이되거나 사용이 어려워지도록하는 요소로 작용해서는 안된다.
- 상호 운용성(Interoperability) : PKI는 다른 PKI와 상호 운용될 수 있어야 한다.
- 명명법(Naming Convention) : PKI는 각 개체들의 이름이 유일하도록 하는 명명법을 지지고 있어야 한다.
- 확장성(Scalability) : PKI의 구축은 사용자와 그들과 관련된 인증서의 수가 증가함에 따라 이를 수용할 수 있도록 확장 가능하여야 한다.
- 융통성(Flexibility) : PKI의 구축은 기술의 변화와 향상을 수용하고 서로 다른 구현들이 상호 잘 작동할 수 있도록 융통성이 있어야 한다.
- 표준 적응성(Standard Compliance) : PKI 구성요소들은 적용되어지고 있는 국제 표준과 잘 호응되어져야 한다.
- 저장(Archiving) : PKI는 전자 서명된 문서 저장을 위한 지원을 제공해야 한다.

나. 인증기관(CA) 요구사항

- 신뢰성(Trust) : CA가 생성한 인증서가 사용자로부터 신뢰받을 수 있도록 하기 위해 PKI내의 CA들은 올바로 기능해야 하고 특정 보안정책을 구현하고 있어야 하며, 사용자와 사용자의 공개키 간의 연결을 유지할 수 있어야 한다.
- 가용성(Availability) : 최소한 PKI내의 CA들은 정상적 영업시간동안 모든 서비스를 제공할 수 있어야 한다. 보안 정책에 따라 CA는 상시 키 침해보고 메커니즘을 제공할 필요도 있다.
- 서비스 및 기능(Services and Functions)
  - 사용자 식별 및 인증(Identification and Authentication) : PKI내의 CA들은 그들의 사용자를 식별하고 인증해야 한다. PKI는 다른 강도의 인증방법이 그들의 CA들에 의해 사용되어질 수 있도록 허용해야 한다.
  - 인증서 생성(Certificate Generation) : PKI내의 CA들은 인증서를 생성해야 한다.
  - 인증서 분배(Certificate Distribution) : PKI내의 CA들은 디렉토리에 인증서를 분배해야하고 관련된 사용자들에게 인증서를 분배할 수 있다.
  - 인증서 저장 및 조회(Certificate Storage and Retrieval) : PKI내의 CA들은 인증서를 저장하고 조회할 수 있다. CA들은 인증서가 만료되거나 철회될 때, 이를 사용자에게 알리는 것과 같은 인증서에 대한 관리 기능을 수행해야하며 이를 위해 CA는 자신이 생성한 인증서들을 저장하고 조회할 수 있어야 한다.
  - 인증서 철회보고(Certificate Revocation Report) : PKI내의 CA들은 인증서 철회보고를 접수하고 이를 인증해야 한다.
  - 인증서 취소 목록 생성 및 유지(CRL Generation and Maintenance) : PKI내의 CA들은 CRL을 생서해야 하고 그들이 가장 최신의 정보가 포함하도록 CRL을 관리해야 한다.
  - 인증서 취소 목록 분배(CRL Distribution) : PKI내의 CA들은 CRL을 디렉토리에 분배해야 한다.
  - CRL 저장 및 조회(CRL Storage and Retrieval)
  - 감사(Auditing) : CA의 신뢰성을 부가적으로 더욱 보장하기 위해 그리고 내부감사를 위한 정보를 제공하기 위해 각 CA들의 행위들은 감사되어질 수 있어야 한다.
  - 저장(Archiving) : CA들은 인증서 생성과 철회에 대한 로그를 저장해야 한다.

다. 등록기관(RA:Registration Authority) 요구사항

- 신뢰성(Trust) : RA는 정확한 인증 요구 및 정확한 인증 철회 요구를 CA에 전달하는 것에 대해 신뢰되어 질 수 있어야 한다.
- 가용성(Availability) : CA에 준하는 가용성 요구조건을 만족하여야 한다.
- 서비스 및 기능(Services and Functions)

  RA는 사용자와 CA사이에서 중재자 역할을 수행하며 주요 기능은 CA를 위한 사용자 인증 기능을 수행한다.
  - 사용자 식별 및 인증(Identification and Authentication) : PKI내의 RA들은 그들의 상위 CA에 의해 사용되는 동일한 방법으로 그들의 사용자를 식별하거나 인증할 수 있어야 한다.

- 인증서 요구(Certificate Request) : 사용자를 인증한 후에 RA는 해당 CA로 인증서를 위한 서명된 요구를 전송한다.
- 인증서 수령(Certificate Receipt) : PKI내의 RA들은 CA로부터 새로운 인증서를 받을 수 있다.
- 새로운 인증서의 배달(Delivery of New Certificate) : PKI내의 RA들은 새로운 인증서를 인증서 내에 명명된 사용자에게 전달할 수 있어야 한다.
- 인증서 철회 보고(Certificate Revocation Report) : PKI내의 RA들은 인증서 취소 요구를 수신 및 인증할 수 있어야 하고 이러한 요구를 해당 CA로 전송할 수 있어야한다.
- 감사(Auditing) : RA는 감사 수행 능력을 가져야 한다.
- 저장(Archiving) : RA는 인증서 생성(방법) 및 철회 요구를 위한 로그를 저장하고 있어야 한다.

라. 인증서에 대한 요구사항

- 다중 인증서(Multiple Certificates) : PKI는 하나의 개체에 대한 용도별 다중의 인증서를 지원해야 한다
- 조직 인증서(Organizational Certificates) : PKI는 조직에 대한 인증서를 지원할 수 있어야 한다.
- 익명 인증서(Anonymous Certificate) : 가명의 개인 식별정보를 이용하는 인증서 지원이 가능하여야 한다.
- 인증기관 인증서(CA Certificate) : PKI내에서 CA를 위한 인증서는 개인 사용자나 조직과 관련된 인증서와 구분되어야 한다.
- 인증서 양식(Certificate Format) : PKI 전반에 걸쳐 자신의 인증서를 위해 공통된 양식을 사용해야 한다.

5.금융환경에 적용 가능한 공개키 기반 구조(FPKI)[5][6][7][9]

개방형 네트워크를 통해 이용 가능한 금융거래로는 잔액조회, 전자화폐 자금 인출, 자금이체 등 기존의 금융서비스들이 대다수 적용되어질 수 있다. 특히 자금이체의 경우 현재 전화 및 PC를 이용한 전자자금이체가 전용선 및 전화망 등의 폐쇄형 네트워크를 통해서 단일 은행 내 및 은행간 거래 형태로 이루어지고 있다. 신용카드의 경우에는 전자지불시스템의 일환으로 인터넷상에서 이용할 수도 있다. 본 장에서는 다양한 금융거래를 위해 적용 가능하고 각 구성요소들의 요구조건을 만족할 수 있는 금융환경 공개키 기반구조(FPKI : Financial PKI)의 인증구조, 구성요소들의 역할 등을 살펴보기로 한다.

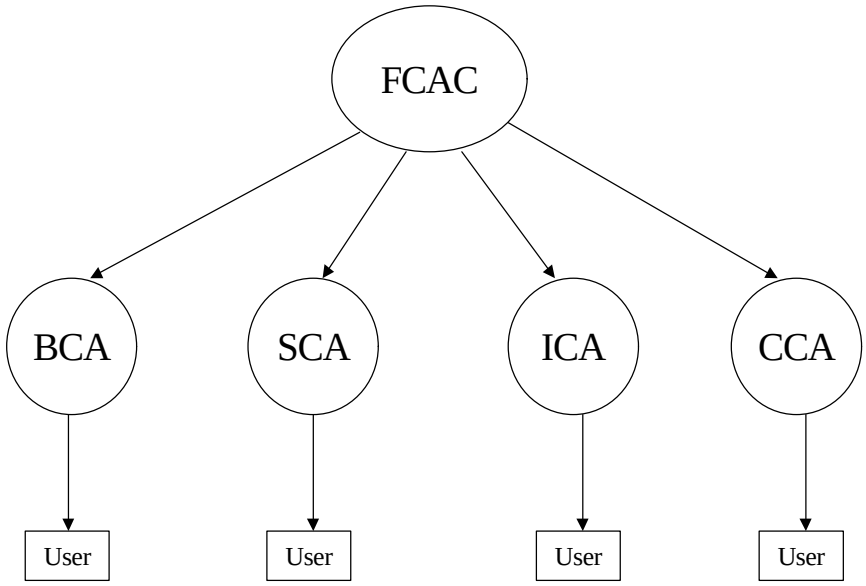
가. 계층구조에 기반한 FPKI

(그림 2)에서 보는 바와 같이 계층구조에 기반한 FPKI에서는 은행, 증권 보험등 동질의 업무(Community of Interest)를 수행하고 있는 금융권 별로 공동 전산 서비스를 제공하고 있는 기업이 보안정책을 수립하거나 고객 인증업무를 수행하고 각각의 인증기관을 금융공동인증센터인 FCAC(Financial Certificate Authority Center)가 인증해 주는 2계층의 인증구조를 이루고 있다. 이러한 인증구조 하에서 고객은 자신의 주요 거래 금융기관에 따라 해당 인증기관으로부터 인증서를 발급받고 인증기관은 금융공동인증센터로 부터 인증서를 발급받

게 된다. 그림에 나타난 화살표는 신뢰가 형성되는 관계를 나타내고 있는 것으로 화살표 방향에 있는 기관이 인증을 받는 기관에 해당된다.

이러한 인증구조는 초기 인증서 사용자의 수가 적은 경우 효율적으로 구성될 수 있으며 인증경로의 길이도 짧아 효율적인 인증 메커니즘을 제공할 수 있다. 현재 은행, 증권 등 금융권간의 거래가 활성화되어 있지 못한 환경 하에서는 이들 간의 상호인증은 그다지 중요한 요소로 작용하지 않을 것이다.

<표 1>에서는 이러한 계층구조에 기반한 FPK내의 CA들을 그 기능별로 구분하여 정리한 것으로 FCAC와 CA들로 구성되어 있으며 서로 계층을 이루는 구성요소이기도 한다.



(그림 2) 계층 FPKI

<표 1> 계층구조 하에서의 CA별 담당기관 및 주요 역할

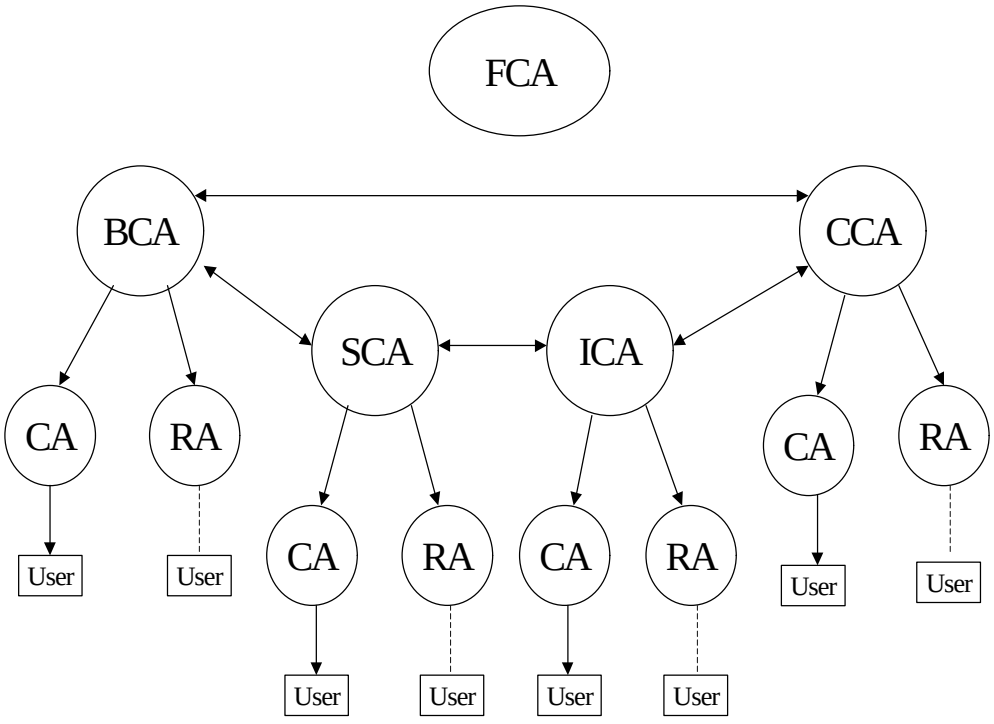
명 칭		담당기관	주요 역할
FCAC (Financial Certificate Authority Center)		금융정책 입안 및 승인 기관	보안 정책 승인 및 CA 인증
CA	BCA(CA for Bank)	금융기관 부문별 공동 전산 서비스 제공 기관	보안 정책 수립 및 고객 인증
	SCA(CA for Stock Institute)		
	ICA(CA for Insurance Company)		
	CCA(CA for CreditCard Company)		

나. 중계CA간 상호 인증에 기반한 FPKI

전자상거래가 활성화되고 이용고객이 증가될 경우 개방형 네트워크 상에서의 안전한 금융거래의 성취를 위한 암호 서비스 제공을 위해 개별 금융기관들은 자신의 고객요구조건을 만족시키고 자사의 필요에 따라 인증기관을 구축할 수 있다. 동종의 업무를 수행하는 금융기관별로 해당 금융기관을 인증해 주는 중계 인증기관으로써 은행들을 위한 BCA, 증권사들을 위한 SCA, 신용카드사들을 위한 CCA등이 구축되어 질 수 있다. 또한 이러한 중계 CA들은 금융권별 고유의 보안 정책을 수립하고 중계 CA들간의 상호 인증을 통해 금융권간 거래에 대한 인증 서비스를 제공할 수 있다.

전체 금융권은 작게는 2개에서 많게는 4~5 개의 공동체로 나눠 질 수 있으므로 금융인증기관(FCA)이 중계CA들을 인증할 필요 없이 중계CA들 간의 상호 인증구조 만으로도 효율적인 인증구조를 확립할 수 있다. FCA는 중계CA들이 수립한 보안 정책을 승인해 주는 역할만을 수행하고 있어 이러한 인증구조 하에서 인증경로의 가능한 최대 길이는 3으로 동일한 형태의 계층구조에 비해 상대적으로 짧다. 다만 상호인증으로 인한 인증경로 탐색의 어려움등 기술적으로 해결되어져야 하는 문제들은 별도로 고려되어져야 한다.

금융권이 세분화 될 경우는 상호 인증의 어려움으로 인해 FCA에 의한 중계CA들의 인증을 수행하는 계층구조도 고려할 수 있다. (그림 3)에서는 중계CA간의 상호인증에 바탕을 둔 인증구조를 나타내고 있으며 이러한 FPKI를 구성하는 CA들의 담당기관 및 주요역할을 구분하여 <표 2>에 정리하였다.



(그림 3) 상호 인증기반 FPKI

<표 2> 상호인증구조 하에서의 CA별 담당기관 및 주요 역할

명 칭		담당기관	주요 역할
FCA(Financial Certificate Authority)		금융정책 입안 및 승인 기관	보안 정책 승인
중계 CA	BCA(CA for Bank)	금융기관 부문별 공동 전산 서비스 제공 기관	보안 정책 수립 및 CA 인증
	SCA(CA for Stock Company)		
	ICA(CA for Insurance Company)		
	CCA(CA for CreditCard Company)		
CA(Certificate Authority)		대규모 금융기관	고객 인증
RA(Registration Authority)		소규모 금융기관	등록 업무

다. FPKI 구축관련 기타 사항

FPKI구축과 관련하여 고려되어져야 할 중요 요소로써 인증서, 인증서 취소 목록의 구조 및 디렉토리 서비스 등은 앞의 4장에 정의한 구성요소별 요구사항을 만족하는 형태의 국제 표준을 채택함으로써 이용 가능하고, 인증서 취소 목록의 갱신 주기, 키의 생성 및 분배 등과 같은 내용에 있어서는 그 응용 및 법적인 환경 등을 고려하여 이에 적합한 방법 및 메커니즘에 대한 연구가 더욱 필요한 부분이다.

6. 인증서 기반 전자자금이체 프로토콜[7][11][12]

인터넷과 같은 개방형 네트워크 시스템을 이용한 전자자금이체시스템의 구현을 위해서는 기밀성 및 인증 서비스의 이용이 가능해야 하며 이는 신뢰할 수 있는 인증기관에 의해 발행된 인증서를 근간으로 하는 공개키 암호기술을 이용할 때 가능하다. 여기서는 이러한 공개키 기반구조가 이미 수립되어 있고 인증서의 신뢰정도는 거래의 안전성 확보를 위해 인증기관에 의해 적절한 개체 확인 절차에 의해 발급된 것으로 가정한다. 정보의 전달 수단으로는 기존에 인터넷상에서 가장 많이 이용되고 있는 개인간 정보전송 수단인 전자우편시스템을 사용한다. 이러한 전자우편 시스템을 이용하여 예약이체 등과 같은 일괄(Batch) 처리형(예를 들어 오전 수신 내역을 오후 2시에 일괄처리, 오후 수신 내역은 익일 오전 10시에 처리) 전자자금이체 프로토콜을 구성하여 인증서에 기반한 전자자금이체 프로토콜의 적용 가능성을 검증하고자한다.

가. 은행내 전자자금이체 프로토콜

단일 은행내에서 이루어지는 계좌간 자금이체 업무에 대해서 개략적으로 살펴보면 다음과 같다. 인터넷상에서 전자자금이체를 하고자하는 사람은 먼저 인증기관으로부터 자신의 인증서를 발급 받고 거래 은행의 인증서를 얻는다. 다음으로 자신의 출금 계좌번호, 해당 계좌의 비밀번호등으로 구성된 메시지를 생성하고 자신의 비밀키로 서명한 서명문을 생성한 후 메시지 및 서명문 전체를 거래 은행의 공개키로 암호화하여 거래은행으로 전송한다.

은행은 주기적으로 수신한 우편을 확인하여 적정 시간 대에 수신한 전자우편에 대해 자금이체 업무를 수행한다. 은행 내에서의 처리 순서는 먼저 자신의 비밀키로 우편을 복호화하

여 메시지와 서명문을 생성하고, 수신된 인증서의 정당성을 검증한 후 정당하게 검증된 경우 이체 의뢰자의 공개키를 이용하여 메시지에 대한 서명 검증하고 메시지 내용대로 은행내 시스템을 이용하여 자금이체를 수행한다. 처리결과는 자신의 비밀키로 서명하여 고객의 이체의뢰 전자우편에 대해 응답하여 이체결과를 고객이 알 수 있도록 통지한다.

1) 상세 프로토콜

참여자 및 사용도구

고객 : A

은행 : B

$Cert$: 공개키 기반 구조하에서 인증서

$Sign_A(\bullet)$: A에 의한 서명 생성 알고리즘

|| : 메시지 연접

$E_A(\bullet)$: A에 의한 공개키 알고리즘을 이용한 암호화

$D_A(\bullet)$: A에 의한 공개키 알고리즘을 이용한 복호화

$h(\bullet)$: 해쉬 알고리즘

사전준비

- 고객 및 은행의 인증서 획득 : $Cert_A, Cert_B$
- 이체정보 생성 : $M =$ **출금계좌번호‖비밀번호‖이체금액‖입금계좌번호‖날짜‖일련번호**

이체 프로토콜

(1) 고객은 $s = Sign_A(h(M))$를 생성한 후 $e = E_{Bank}(M \| s)$를 계산하여 $e, Cert_A$를 은행으로 전송한다.

(2) 은행은 수신한 $Cert_A$의 정당성을 검증한 후 $D_{Bank}(e) = M \| s$를 복원하여 $Cert_A$의 공개키로부터 s의 정당성을 검증한다.

(3) 은행은 복원된 M을 이용하여 날짜와 일련번호를 이용하여 중복 전송 여부를 검사한 후 M의 내용에 따라 은행내 자금이체를 수행한다.

(4) 은행은 $r = Sign_{Bank}($**이체결과**$)$을 생성하여 $($**이체결과**$, r)$을 고객 A에게 전송한다.

(5) 고객 A는 수신한 $($**이체결과**$, r)$을 영수증으로 사용할 수 있다.

2) 안전성 검증

이러한 인증서 기반 전자자금이체 프로토콜이 만족하고 있는 안전성은 다음과 같다.

- 기밀성 확보 : 고객의 이체의뢰 내용은 은행의 공개키에 의해 암호화되어 있으므로 해당 거래은행만이 고객의 계좌 비밀번호 등과 같은 비밀정보를 알아낼 수 있으므로 고객 정보에 대한 기밀성이 확보된다.
- 인증 및 무결성 : 이체 의뢰 정보에 대해 고객의 인증서와 연결된 개인키에 의해 서명이 이루어짐으로써 은행은 메시지 송신자에 대한 인증을 확보할 수 있을 뿐만 아니라 수신한 메시지의 무결성도 결정할 수 있다.
- 부인방지 : 이체 의뢰 정보에 대한 고객의 서명은 이체 결과에 대한 고객의 이체 의뢰 부

인 방지를 위해서도 이용될 수 있다.
- 중복 전송 방지 : 공격자가 프로토콜을 중복 수행하는 경우 은행은 메시지 내의 날짜 및 일련번호를 이용하여 중복전송을 검출해 낼 수 있다.
- 영수증 처리 : 처리결과에 대한 은행의 통보 내용은 처리은행의 개인키에 의해 서명되어 있으므로 전자자금이체 거래 당사자간의 영수증으로도 사용이 가능하다.
- 인증서의 안전성 : 인증서를 이용할 경우 이용시점에서 매번 인증서 철회 목록(CRL : Certificate Revocation List)을 검사함으로써 인증서의 안전성을 확보할 수 있다.

나. 은행간 전자자금이체 프로토콜

개방형 네트워크 상에서 은행간 자금이체를 하고자하는 사람은 먼저 인증기관으로부터 자신의 인증서를 발급 받고 자신의 거래은행(출금은행)의 인증서를 얻는다. 다음으로 출금정보 및 입금정보 등으로 구성된 메시지를 생성하고 자신의 비밀키로 서명하여 서명문을 생성하여 메시지와 서명문을 출금은행의 공개키로 암호화한 후 출금은행으로 전송한다.

출금은행은 주기적으로 수신한 우편을 확인하여 적정 시간대에 수신한 전자우편에 대해 출금처리 업무를 수행한다. 출금은행은 메시지 내용 중 입금은행을 확인하여 메시지에 대해 자신의 비밀키를 이용하여 서명한 후 입금은행의 공개키를 이용하여 암호화한 결과 및 자신의 인증서를 입금은행으로 전송한다.

입금은행은 자신의 비밀키를 이용하여 전자우편을 복원한 후 수신한 인증서를 검증하여 정당성이 입증되면 메시지의 서명을 검증하고 해당 입금계좌로 입금업무를 수행한다. 입금은행은 처리결과를 출금은행의 입금의뢰 우편에 대해 응답하여 입금결과를 출금은행에게 알리고 출금은행은 입금은행으로부터 우편을 수신한 후 처리결과에 따라 고객의 이체 의뢰 우편에 응답하여 처리결과를 통지한다. 출금은행의 경우 고객의 이체의뢰정보가 잘못된 경우 더 이상의 처리를 진행하지 않고 고객의 이체 의뢰 우편에 대해 즉각 응답할 수도 있다.

1) 상세 프로토콜

참여자 및 사용도구

고객 : A

출금은행 : BW

입금은행 : BD

사용도구는 은행 내 자금이체 프로토콜에서 사용한 도구와 동일하다.

사전준비

- 고객 및 출금은행의 인증서 획득 : $Cert_A, Cert_{BW}$
- 이체정보 생성 : $M =$ **출금계좌번호‖비밀번호‖이체금액‖입금은행‖입금계좌번호‖날짜‖일련번호**

이체 프로토콜

(1) 고객은 $s = Sign_A(h(M))$를 생성한 후 $e = E_{BW}(M \| s)$를 계산하여 $e, Cert_A$를 출금은행으로 전
송한다.

(2) 출금은행은 수신한 $Cert_A$의 정당성을 검증한 후 $M \| s = D_{Bank}(e)$를 복원하여 $Cert_A$의 공개

키로부터 s의 정당성을 검증한다.

(3) 출금은행은 날짜와 일련번호를 이용하여 중복전송을 검사한 후 출금업무를 수행하고, 복원된 M으로 부터 입금은행을 확인한 후 $\bar{s} = Sign_{BW}(h(M))$와 $\bar{e} = E_{BD}(M \| \bar{s})$를 생성하여 $\bar{e}, Cert_{BW}$를 입금은행으로 전송한다.

(4) 입금은행은 수신한 $Cert_{BW}$의 정당성을 검증한 후 $M \| \bar{s} = D_{BD}(\bar{e})$를 복원하여 $Cert_{BW}$의 공개키로부터 $\bar{s}$의 정당성을 검증한다.

(5) 입금은행은 날짜와 일련번호를 이용하여 중복전송을 검사한 후 복원된 M을 이용하여 입금업무를 수행한다.

(6) 입금은행은 $r = Sign_{BD}(M \| \textbf{입금결과})$을 생성하여 $(\textbf{입금결과}, r)$를 출금은행으로 전송한다.

(7) 출금은행은 입금결과에 따라 필요한 처리를 한 후, $\bar{r} = Sign_{BW}(\textbf{이체결과})$를 생성하여 $(\textbf{이체결과}, \bar{r})$를 고객에게 전송한다.

(8) 고객은 수신한 $(\textbf{이체결과}, \bar{r})$을 영수증으로 사용할 수 있다.

2) 안전성 검증

은행간 전자자금이체의 경우도 은행내 전자자금이체에서와 동일한 방법에 의해 안전성을 확보할 수 있다. 또한 은행간 정보 전송 시에도 출금은행은 자신의 개인키로 서명하고, 입금은행의 공개키로 암호화하여 정보를 전송함으로써 은행간 전송에서도 기밀성 및 인증성을 확보할 수 있다. 다만, 출금은행은 출금정보에 대한 내용의 기밀을 유지하기 위해 입금정보만을 입금은행으로 송신함으로 자행 고객의 비밀정보는 타 은행으로 노출하지 않을 수도 있다.

7. 결 론

본 논문에서는 금융환경에 적용 가능한 공개키 기반구조 수립을 위한 두 가지 인증구조를 제시하고 있다. 두 인증구조는 상호 보완적인 성격을 가지고 있는 것으로서 업무(관심)의 동질성, 각 금융권간 정보의 상호 교환 정도 및 수용해야될 사용자 규모 등에 따른 비용분석 및 효율성 검토 등을 통해 구축되어진 CA들 간의 신뢰를 형성하기 위한 방법으로 선택되어질 수 있다. 사용자가 비교적 적을 것으로 예상되는 초기에는 단순한 계층구조 기반으로 확장이 용이한 FPKI를 구축하고 향후 이용자 확대 등으로 FPKI의 확장이 요구될 때 중계CA간의 상호 인증에 기반한 FPKI로 발전해 나가는 것이 타당할 것으로 판단된다.

또한, FPKI의 구축을 위해서는 이러한 인증구조의 확립과 더불어 인증구조에 적합한 인증 정책, 인증서 발급 및 취소 등과 같은 관리 방법 등에 대해서도 세부적인 기술 검토가 병행되어질 필요가 있다.

인증서에 기반한 전자자금이체 프로토콜의 구성에서는 정보의 전송 수단으로 전자우편 시스템을 이용하여 일괄처리형 전자자금이체 프로토콜을 제시하였으나 활용도를 높이기 위해서는 실시간 전자자금이체 거래에 적용 가능한 프로토콜의 설계가 필요할 것으로 생각된다.

참고문헌

[1] 한국정보보호센터, “공개키 기반구조 기술 관련 표준화 동향”, ‘97 정보보호기술 표준화 현황, 1997.12.

[2] 신홍식, 김지용, “전자상거래에서의 PKI 구축 사례 연구”, 개방형보안기술과 정보보호응용 워크샵, 제2회, 1998.11.

[3] 이강석 외 5명, “공개키 기반구조와 응용 및 국제동향”, 개방형보안기술과 정보보호응용 워크샵, 제2회, 1998.11.

[4] 최명렬, “국방PKI에 대한 연구”, WISC '98, 1998.

[5] 한국증권전산(주)전산기술연구소, “한국증권전산 인증기관 인증실무준칙 Ver1.1”, 1998.11.2

[6] MITRE, “Public Key Infrastructure Study : Final Report”, NIST, 1994. 4

[7] SET(Secure Electronic Transaction) Specification Book 1 : Business Description, http://www.setco.org/set_specifications.html

[8] GlobalSign, "GlobalSign CPS", 1998

[9] VeriSign, "VeriSign CPS Version 1.2", 1997

[10] Digital ID Pricing, http://www.verisign.com/products/pricing.html

[11] W. Ford & M.S. Baum, Secure Electronic Commerce, Prentice Hall, 1997

[12] P.Waynel, Digital Cash, AP Professional, 1997

[13] Internet Shopping Security, http://www.visa.com/cgi-bin/vee/nt/ecomm/security/set.html?2+0