PKI 다중 서명 알고리즘의 연동 방법

고혜원*0 임복희* 서창호**
*전남대학교 정보보호 협동과정, **공주대학교 응용수학과
{suni135@naver.com0, bim@chonnam.ac.kr, chseo@kongju.ac.kr}

A Multiple signature algorithm interoperability on Public Key Infrastructure

Hyewon Ko*0 Bokhee Im* Changho seo**
Dept. of Information Security, Chon-nam National University
Dept. of Application Mathematics, Kong-ju University

요 약

인터넷 사용자의 증가와 더불어 보안의 중요성이 확산됨에 따라 공개키 기반구조(Public Key Infrastructure)하에서의 상호 인증 기술이 정보보호 기반기술의 중요요소로 논의되고 있다. 전자 상거래환경의 각종 응용분야에 대한 정보보호 서비스를 위하여 PKI 환경구축이 선진국들을 중심으로 광범위하게 추진되고 있다. 그러나, 개별적으로 추진되고 있는 다양한 형태의 PKI 환경은 상호 연동성이 보장되어야 한다. 따라서, 본 논문에서는 상호 연동을 위하여 고려해야 하는 서명 알고리즘의 상호 연동성 방안을 제안하였다.

1. 서 론

최근 통신기술의 발달과 전 세계적인 규모의 통신 기반인 인터넷은 전자상거래라는 새로운 경제 패러다임을 창출하고 있다. 전자상거래는 기존 상거래의 시간적 공간적 제약을 극복하며 유통, 물류 비용 등의 상거래 비용을 절감하고 탄력성 있는 기업/경제활동이 가능하도록 하여 다양하게 기존 상거래를 대체하고 있으며 최근 급속하게 확장하고 있다[1,2].

전자상거래의 안전성과 신뢰성을 확보하기 위해서 반드시 필요한 요소로 부각되는 것이 인증기술이다[1,3].

미국을 중심으로 한 세계 각 국에서는 이미 인증 서비스가 실험단계를 거쳐 상용화 단계에 이르고 있다. 국내에서도 공인인증체계가 구축되어 본격적인 전자 상거래 및 인증 서비스를 위한 환경이 갖추어졌다고 할 수 있다.

공인인증체계와 같은 인증서비스의 기반을 구성하는 것이 공개키 기반구조 (PKI: Public Key Infrastructure)이다. 공개키 기반구조는 선진국들을 중심으로 광범위하게 추진되고 있으나, 개별적으로 추진되고 있어 다양한 형태를 가지고 있으므로 사용자 그룹과 각 국의 실정에 맞는 융통성 있는 상호 연동 정책이 요구되고 있다.

본 논문에서는 다양한 형태를 가지고 있는 서명 알고리즘의 상호 연동 방안을 제안하고 비교 검토하였다.

2. 관련연구

2.1 인증 방식

PKI에서 정의하고 있는 상호인증은 다음 세 가지이다.

①계층형 상호 인증서(Hierarchical Cross-Certificates) 계층형 상호 인증서는 루트 CA에 대한 계층형 인증 경로와 동일하다. 이러한 상호 인증서는 클라이언트가 언제나 Federal CA에서 발급된 어떠한 인증서에 대해서라도 그 인증 경로를 찾을 수 있도록 하기 위해 사용된다.

② 일반적 상호 인증서 (General Cross-Certificates)
일반적 상호 인증서는 인증 계층(certification hierarchy)을 제공하여 더 짧은 인증 경로들을 사용할 수 있도록 한다. 하위 CA들간의 일반적 상호 인증서는 상호인증의 검증 경로를 짧게 하고 자주 사용되는 인증 경로의 효율을 증대시키고자 할 때 적당하다.

③ 특수 상호 인증서(Special Cross-Certificates)
특수 상호 인증서는 루트 CA로부터의 경로들에 계층적으로 부과된 제약들을 따를 필요가 없는 인증 경로를 제공한다.

2.2 서명 알고리즘

전자서명 알고리즘은 서명자로 하여금 전자서명을 생성할 수 있도록 하고, 검증자에게는 서명의 진위여부를 확인할 수 있게 해준다.

2.2.1 RSA

이 방식은 큰 소수의 곱으로 이루어진 합성수의 소인수 분해는 계산하기가 매우 어렵다는 수학적 방식을 기반으로 개발된 전자서명 알고리즘이다.

[키 생성]

①두 개의 (서로 다른) 큰 소수 p와 q를 임의로 생성한다.

② $n=pq$와 $\Phi=(p-1)(q-1)$를 계산한다.

③ $\gcd(e,\Phi)=1$인 정수 $e(1<e<\Phi)$을 임의로 선택한다.

④확장된 유클리드 알고리즘을 사용하여 $ed\equiv 1 \pmod{\Phi}$인 유일한 정수 $d(1<d<\Phi)$를 계산한다.

⑤ 공개키 : (n, e)
비밀키 : d

[서명 생성 과정]

① $h(M)$을 구한다. (M은 서명할 메시지)

② 서명 $S=h(M)^d \pmod{N}$ 을 구한다.

③ (M, S)를 수신자에게 전송한다.

[서명 검증 과정]

① $h(M)$을 구한다.

② $V=S^e \pmod{N}$을 계산한다.

③ $V=h(M)$을 만족하면 서명이 유효하다.

2.2.2 KCDSA (Korean Certificate-based Digital Signature Algorithm)

KCDSA는 이산대수 문제의 어려움에 기반을 둔 전자서명 알고리즘으로서, 한국통신정보보호학회의 주관 하에 우리나라의 주요 암호학자 들이 주축이 되어 1996년 11월에 개발하였으며, 이후 지속적인 수정 및 보완 작업을 거쳐 1998년 10 월 TTA에서 단체 표준으로 제정되었다.

[KCDSA 서명 생성]

메시지 m에 서명하는 signer는 메시지 m에 대한 서명 $\{r \| s\}$를 다음과 같이 생성한다.

① 난수 $k \in Z_q^* = \{1, 2, \cdots, q-1\}$ 선택

② $w = g^k \pmod p$ 계산

③ $r = h(w)$를 계산

④ $e = r \oplus h(z \| m) \pmod q$ 계산

⑤ $s = x(k-e) \pmod q$ 계산

⑥ 만일 $s = 0$이면 위의 과정을 다시 수행함

[KCDSA 서명 검증]

메시지와 서명 $\{m \| r \| s\}$을 받으면 다음과 같이 검증한다.

① 서명자는 Certificate의 Validity를 확인

② 서명자의 Certificate의 Certdata를 이용해 $z = h$(Certdata) 계산

③ r, z의 값이 $0 \le r < 2^{|q|}$, $0 < s < q$인지 확인

④ $e = r \oplus h(z \| m) \pmod q$ 계산

⑤ $w' = h^y g^e \pmod q$ 계산

⑥ $r = h(w')$인지 확인

3. 상호 연동

3.1 서명 알고리즘 (Signature Algorithm)

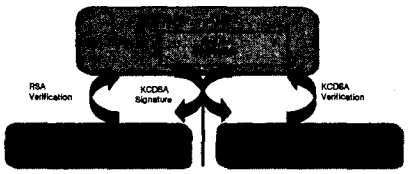
다음의 선택 사항들은 KCDSA를 사용하는 사용자들과 RSA 암호 시스템을 사용하는 사용자들 사이의 상호 연동성을 위해 고려되는 방법들이다.

- 종단 시스템이 두 암호 시스템으로부터의 서명을 검증하도록 한다.
- RSA를 사용하는 도메인에 등록된 사용자와 통신하기를 원하는 행정 사용자에게 RSA와 KCDSA 인증서를 모두 발행한다.
- 믿을 수 있는 게이트웨이를 사용한다.
- 일반 사용자들에게 KCDSA를 사용하기 쉽도록 한다.

3.1.1 종단 시스템 검증 (End System Verification)

종단 사용자가 다른 암호 시스템 알고리즘으로 만들어진 서명들을 검증하기 위해서는 외부 인증서를 신뢰할 수 있어야 한다. 이를 위해, FPKI의 CMA는 RSA CMA에게 인증서를 발급할 것이다. 연방 CMA는 연방 CMA의 KCDSA 비밀키를 사용하여 RSA CMA의 RSA 공개키에 서명을 할 것이다. 또한 RSA CMA는 RSA CMA의 RSA 비밀키를 사용하여 연방 CMA의 KCDSA 공개키에 서명할 것이다.

다음 그림에서는 종단 시스템 검증 방식을 사용하여 연방 사용자와 비 연방 사용자간의 서명을 생성/검증하는 과정을 나타내고 있다. (각 사용자는 검증을 위하여 RSA와 KCDSA 알고리즘을 모두 사용할 수 있다.)

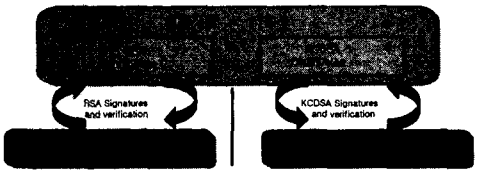


[그림 1] 서명 검증을 위한 종단 시스템 검증

[그림 2] 종단 시스템 검증에 의한 디지털 서명의 상호 연동

3.1.2 다중 인증 경로 (Multiple Certificate Paths)

KCDSA를 사용하는 연방 정부와 RSA를 사용하는 다른 공개키 암호 시스템사이의 불일치를 해결하기 위한 두 번째 방법은 RSA 사용자들과 통신하는 것을 필요로 하는 연방 사용자에게 RSA 인증서들을 발급해주는 것이다. RSA와 KCDSA 인증서는 FPKI내에 있는 모든 CMA에게 발급되어져야 할 것이며, 각 연방 사용자들은 KCDSA 인증서를 받을 것이다. 또한, 연방 사용자는 만일 RSA 사용자와 통시하기를 원한다면 RSA 인증서를 받을 것이다. 이때, RSA 인증서는 적절한 CMA의 RSA 키를 사용하여 서명될 것이다.



[그림 3] 서명 검증을 위한 다중 인증 경로

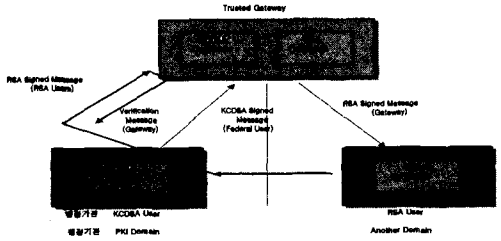
[그림 4] 다중 인증 경로에 의한 디지털 서명의 상호 연동

3.1.3 신뢰 게이트웨이

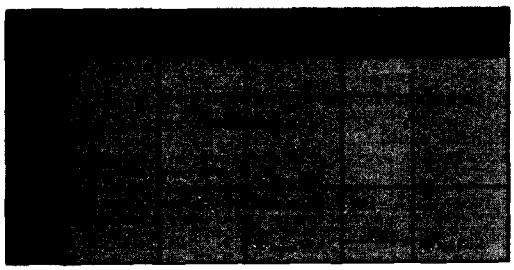
신뢰 게이트웨이 대책에서, FPKI는 전체 연방 사용자 집단에서 신뢰된 게이트웨이를 배치할 것이다. 연방 사용자가 RSA 사용자로부터 메시지를 받을 때, [그림 5]과 같이 검증을 위해서 그 메시지들을 게이트웨이에 보낸다. 게이트웨이는 RSA와 KCDSA 서명과 검증 기능을 가지고있을 것이다. 게이트웨이는 게이트웨이의 KCDSA 서명과 함께 응답을 사용자에게 보낸다. 이와 같이, 연방사용자는 게이트웨이를 통하여 RSA 사용자에

재 메시지를 보낼 것이다. 게이트웨이는 연방 사용자의 서명을 검증하고 RSA를 사용하여 서명을 하여 메시지를 RSA 사용자에게 보낼 것이다.

[그림 5]과 [그림 6]는 신뢰할 수 있는 게이트웨이를 통하여 연방 사용자들이 상호간에 서명 검증을 수행하는 절차를 나타내고 있다.



[그림 5] 서명 검증을 위한 Trusted Gateway 접근



[그림 6] 신뢰 게이트웨이에 의한 디지털 서명의 상호 연동

3.1.4 KCDSA와 RSA 하나의 알고리즘 채택

KCDSA 채택은 상업적 부분에서 RSA암호 시스템이 설치된 기반이 형해되고 있다. RSA의 채택은 현존하는 FPKI 요소 즉, MISSI에 상당한 비용을 요구한다. 이 경우 서명 알고리즘의 관점에서 상호 연동성에 대해 고려할 필요가 없다.

4. 비교 검토

<표 1> 서명 알고리즘 상호 연동성 대책들의 비교

대안	장점	단점
종단 시스템 검증	· 확장 가능 · 산업체들은 적은 추가 비용으로 RSA와 KCDSA를 함께 사용 · 상업적 응용 프로그램은 RSA를 사용	· 연방 사용자들은 RSA검증 소프트웨어가 필요 · RSA사용자들은 KCDSA검증 소프트웨어가 필요
trusted gateway	· 다른 지역들에서 gateway는 상호 연동성을 가능하게 함	· 추가적으로 안전한 gateway의 구축 필요 · 확장성 없고 매우 비쌈 · 연방 PKI영역과 다른 영역에 의해서 신뢰받아야 함 · 부인 봉쇄를 약화시킴 · gate를 위한 강제의 FIPS 포기를 요구할 수 있음 · 사업적 응용 프로그램의 사용자들에게 RSA인증서를 발행해야 함
다중 인증 경로	· 확장 가능 · RSA 사용자에게 영향 없음 · RSA 기반의 상업적 응용 프로그램 사용할 때 상호 연동성을 고려할 필요 없음	· 추가된 기반구조 비용 · FPKI에 있는 사용자들과 CMA들은 다중인증서 필요 · FIPS의 변경이나 포기가 필요 · 연방 사용자는 RSA 서명 및 검증 소프트웨어 필요 · 연방 사용자와 소프트웨어는 서명을 위해 어떤 인증서를 사용 할 것인가를 결정해야 함
RSA	· 상업 분야와 상호 연동 · 하나의 인증서 · 종단 시스템에 대한 하나의 암호학적 알고리즘 · RSA에 기반을 둔 상업적 응용프로그램에 대한 상호 연동성을 고려할 필요 없음 · 유리한 특허 상황	· FIPS로의 변화를 요구 · KCDSA와 다른 기술 기반 계층들과 연동성이 없음 · MISSI에 대하여 상당한 비용을 요구 · FPKI를 하나의 기술에 고착시킴

5. 결론 및 향후 과제

본 논문에서는 광범위하고 개별적으로 추진되고 있어 다양한 형태를 가지고 있는 서명 알고리즘의 상호 연동성 방안을 제안하고 비교 검토하였다. 전자 정부, 전자 상거래, 전자 금융의 활성화되면서 정부 각 부처는 민간부문과 연계 부분이 증대되고 민간 부문에서는 국제적인 교류를 위하여 다양한 알고리즘의 사용을 요구하고 있다. 따라서 특별히 정부 각 부처에서 사용하고 있는 KCDSA와 민간 부문에서 주로 사용하고 있는 RSA를 비교함으로써 다중 서명 알고리즘의 상호 연동 대책들을 연구 분석하였다.

향후 PKI의 개발자는 최소 상호 연동 규격을 맞추어야 할 뿐 아니라 이에 기반한 PKI 서명 알고리즘의 상호 연동에 따른 시험 후 검증이 요구될 것이다. 다중 서명 알고리즘의 키 분배 방안이 본 논문의 추후 연구 사항이다.

6. 참고문헌

[1] W.Ford, M.S.Baum, "Secure Electronic Commerce", prentice Hall, 1997

[2]권용진, 김정선, "전자상거래의 보안" 한국통신학회지, Vol.16 No. 11, pp.29-45, 1999

[3] J. Feghhi, P. Williams, J. Feghhi, "Digital Certificate : Applied Internet Sedurity", Addison Wesley, 1998

[4] W. Stallings, " Cryptography and Network Security: Principles and Practice", Prentice Hall, 1998

[5] 이만영, 김지홍, 류재철, 송유진, 영홍열, 이임영, " 전자상거래 보안 기술", 생능 출판사, 1999

[6] NIST PKI Program web site, http://csrc.nist.gov/pki