의료 보안 PKI 표준의 인증서 요구사항에 관한 연구

박근호*, 김성진*, 손태식**
*아주대학교 컴퓨터공학과
**아주대학교 사이버보안학과
e-mail : happyrjsgh@ajou.ac.kr

A Study on Certificate Requirement of Health Informatics Public key infrastructure Standard

Keunho Park*,Sungjin Kim*,Taeshik Shon**
*Dept. of Computer Engineering, Ajou University
**Dept. of Cyber Security, Ajou University

요 약

보건의료 산업에서 보건의료제공자와 의료 단체들은 국가와 국가간 환자의 정보를 교환한다. 이 때 교환되는 환자의 정보를 보호하기 위한 수단으로 공개키 기반 구조와 전자 인증서 기술을 사용해야 한다. 하지만 국가마다 전자인증서를 사용하기 위한 인증기관과 등록기관의 정책이 일치하지 않으므로, 여러 나라들과 기관이 신뢰하고 사용할 수 있는 프레임워크가 필요하다. 이러한 프레임워크를 구축하기 위한 국제 표준 문서가 ISO 17090 이며, 본 고에서는 ISO 17090 에 명시된 인증서 요구사항과 암호화 알고리즘에 대한 개선방안을 제시한다.

1. 서론

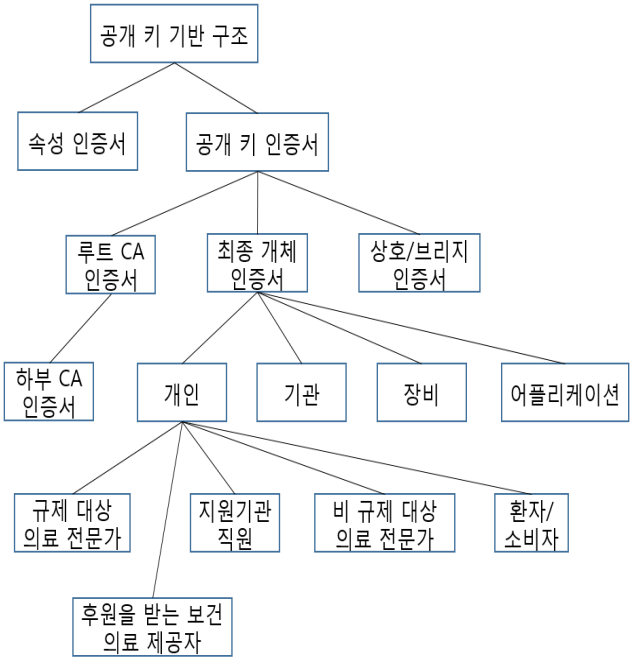
현대의 보건의료산업은 종이 문서기반에서 자동화 기기를 이용한 환자 정보 관리로 이동하는 추세이다. 이에 따라 보건의료 서비스 제공자와 여러 의료 단체들은 전자메일, 원격 데이터베이스 접속과 같은 전자자료 교환 방법으로 보건의료정보를 교환하고 있다. 하지만 이런 방법을 통한 보건의료정보 교환은 권한이 없는 접근을 통한 환자의 사생활 침해, 보건의료정보 조작과 같은 보안 위협에 쉽게 노출되어 있다.

환자의 진료 기록과 같은 개인정보는 개인정보보호법 제 23 조에 의해 보호받는 정보로 한번 노출이 되면 회복이 불가능한 민감정보이다. 이러한 정보를 보호하기위한 수단으로 공개 키 기반 구조와 전자인증서의 사용이 불가피한데, 국가와 국가간에 환자의 정보를 교환할 경우 인증기관(CA)과 등록기관(RA)의 정책과 절차가 일치하지 않기 때문에 여러 나라와 기관들이 신뢰하고 사용할 수 있는 보건의료산업만의 프레임워크가 필요하다. 이러한 프레임워크를 구축하기 위해 ISO 17090 은 보건의료산업에서, 전자인증서를 사용하여 국가간 환자 정보의 교환을 보호하는데 필요한 일반적인 기술적, 운영적, 정책적 조건에 관하여 명시하고 있다[1].

가짜 인증서를 사용한 보안 위협이 빈번한 요즘, 보건의료산업에서도 인증서에 관한 규제를 강화해야 한다. 그러므로 본 고에서는 ISO 17090 에 정의된 내용 중, 인증서에 관한 내용을 간략하게 정리하고, 인증서의 보안상 취약점이 우려되는 부분을 지적한 뒤 개선방안을 제시한다.

2. 인증서의 종류와 공통 필드

ISO 17090 에 따르면, 보건의료산업에서는 인증서가 쓰이는 대상 마다 필요한 정보가 다르기 때문에 여러 종류의 인증서를 사용한다. 아래의 (그림 1)은 이러한 인증서들의 유형과 상호관계를 나타낸다.



(그림 1) 인증서의 유형

보건의료산업에서 공개 키 기반 구조는 크게 속성 인증서와 공개 키 인증서로 나뉜다. 공개 키 인증서는 다시 루트 CA 인증서와 상호/브리지 인증서, 최종 개체 인증서로 나뉜다.

루트 CA 인증서의 경우, 루트 CA 인증서 밑에 하위 CA 인증서로 나뉘는데, 루트 CA 인증서는 자가 서명을 하여 신뢰 당사자 또는 하부 CA 들에게 인증서를 발행하여 준다. 하부 CA 인증서의 경우, 자기 자신이 아닌 다른 CA 에 의해 인증을 받은 CA 로 인증 계층 구조에서 자기 자신보다 아래에 있는 CA 또는 최종 개체에게 인증서를 발행한다. 상호/브리지 인증서는 다른 관할구역의 최상위 계층의 CA 를 신뢰할 수 있도록 교차 인증해 주는 인증서이다. 최종 개체 인증서는 인증서를 최종적으로 사용하는 개체에게 발행이 된다.

마지막으로 속성 인증서는 인증서 보유자의 소속, 권한 정보, 역할 등의 속성을 포함하고 있다. 속성 인증서의 보유자와 속성의 연결성은 전자 서명을 통해 확인한다. 보건의료산업에서 의료전문가의 역할, 의료전문가 관리 기관과 신원 확인 기관의 분리를 고려할 때 속성 인증서를 사용하는 것이 바람직하다.

이러한 인증서들은 ISO 17090 에 명시된 공통된 요소들을 따라야 하는데, 이러한 요소는 공개키 인증서 표준인 X.509 표준 문서의 버전 3 을 기반으로 하였다. 공통된 요소로는 버전, 식별 번호, 발행자, 유효성, 대상 등이 있다. 아래의 (그림 2)는 보건의료산업에서 쓰이는 인증서들의 공통 요소와 공통 요소들의 파라미터를 나타내고 있다.

```
Certificate  ::=  SIGNED { SEQUENCE {

version                  [0]   Version DEFAULT v1,
serialNumber                   CertificateSerialNumber,
signature                          AlgorithmIdentifier,
issuer                                 Name,
validity                               Validity,
subject                                Name,
subjectPublicKeyInfo           SubjectPublicKeyInfo,
issuerUniqueIdentifier   [1]   IMPLICIT UniqueIdentifier OPTIONAL,
subjectUniqueIdentifier  [2]   IMPLICIT UniqueIdentifier OPTIONAL,
extensions               [3]   Extensions MANDATORY,
```

(그림 2) 인증서의 공통 필드

3. 인증서 보안 요구사항

ISO 17090 에 의하면 CA 인증서 키의 크기는 RSA 알고리즘을 기준으로 2,048 비트를 사용하는 보안 강도를 지녀야하고 FIPS(Federal Information Processing Standard 의 약자로, 미국 정부의 컴퓨터 보안 표준이다. 이는 암호화 모듈의 보안 등급을 제공하는데 사용된다.) 140-2 Level 2 를 준수할 것을 권장하고 있다.

반면, 최종 개체 인증서와 상호/브리지 인증서와 같이 CA 가 아닌 인증서 키의 크기는 RSA 알고리즘을 기준으로 1,024bit 의 보안 강도를 가져야하고, FIPS 140-2 Level 1 을 준수할 것을 권장하고 있다.

(그림 2)의 인증서 공통 필드 요소의 서명 필드의 경우 아래의 < 표 1>의 전자 서명 알고리즘 목록 중 하나를 사용할 것을 권장한다.

<표 1> 서명 필드에 사용되는 알고리즘

순번	알고리즘
1	md5WithRSAEncryption (1.2.840.113549.1.1.4)
2	sha1WithRSAEncryption (1.2.840.113549.1.1.5)
3	dsa-with-sha1 (1.2.840.10040.4.3)
4	md2WithRSAEncryption (1.2.840.113549.1.1.2)
5	ecdsa-with-SHA1 (1.2.840.10045.4.1)
6	ecdsa-with-SHA224 (1.2.840.10045.4.3.1)
7	ecdsa-with-SHA256 (1.2.840.10045.4.3.2)
8	ecdsa-with-SHA384 (1.2.840.10045.4.3.3)
9	ecdsa-with-SHA512 (1.2.840.10045.4.3.4)
10	id-RSASSA-PSS (1.2.840.113549.1.1.10)
11	sha256WthRSAEncryption (1.2.840.113549.1.1.11)
12	sha384WithRSAEncryption (1.2.840.113549.1.1.12)
13	sha512WithRSAEncryption (1.2.840.113549.1.1.13)

4. 제안하는 인증서 보안 요구사항

한국인터넷진흥원(KISA)에서 발간한 '국내 암호 이용 현황 및 암호 구현 가이드'에 따르면 개인정보 암호화에 적용되는 단 방향 해시 함수 중 MD5 와 SHA1 의 사용을 권고하지 않는다[2]. 또한 Stevens Marc 가 저술한 "First Collision Attack on MD5"와 Xiaoyun Wang 이 저술한 "Collision Search Attack on SHA1"에 따르면 MD5 와 SHA1 은 이미 취약하다는 것이 증명이 되었다. 그러므로 해당 해시 함수를 사용해 생성된 문자열을 RSA 알고리즘을 사용해 개인키로 서명할지라도 해시 충돌을 일으켜 키 값을 유추할 수 있기 때문에 보안에 대한 위험이 여전히 존재한다[3][4]. 이러한 이유로 본 고에서는 <표 1>의 순번 1 에서 5 까지를 사용하지 않는 것을 제안한다.

ISO 17090 에 의하면 보건의료산업에서 CA 인증서가 아닌 다른 인증서에 쓰이는 공개 키 쌍의 경우, RSA 알고리즘의 1,024 비트의 키를 사용하는 것과 같은 보안 강도를 준수 하라고 권고하고 있다. 하지만 NIST(미국 국립표준기술 연구소)에 의하면 개인의 신원 보장, 부인 방지의 목적으로 전자 인증서를 사용할 경우, RSA 알고리즘을 기준으로 2,048 비트의 키를 사용하라고 권고하고 있다[5]. 뿐만 아니라 전 세계 OS 시장의 70% 이상을 점유한 회사인 마이크로소프트사의 공식 홈페이지에 따르면 1024 비트 미만의 RSA 키를 사용한 인증서는 짧은 시간 안에 파생될 수 있으며, 공격자가 인증서를 복제하고 부당한 방법으로 이용하여 콘텐츠를 스푸핑하거나 중간자 공격을 수행할 수 있다고 한다. 이러한 이유로 윈도우 OS 의 인증서 탑재 정책을 바꾸어, 2011 년부터 1,024 비트 인증서의 사용을 금지하였다. 따라서 CA 가 아닌 인증서를 사용할 때 RSA 알고리즘을 기준으로 1,024 비트의 키를 사용하면 더 이상 인증서 보안을 보장하지 못한다. 그러므로 인증서의 키 길이를 1,024 비트에서

2,048 비트로 상향 조정해야 하며, 이 경우 공격자가 전자서명 키를 알아내기 위해 연산해야 하는 양이 2^{1024} 번에서 2^{2048} 으로 증가된다. 현재의 컴퓨팅 파워를 감안했을 때 무어의 법칙에 따라 2030 년까지 안정성을 확보할 수 있을 것이다.

5. 결론

본 고의 목적은 보건의료산업에서 환자의 정보를 안전하게 교환하기 위한 목적으로 제정된 표준문서인 ISO 17090 의 인증서 요구사항 부분의 보안이 우려되는 부분을 지적하고 안전한 방법을 제안하는 것이다. 그러므로 본 고에서는 ISO 17090 이 제정된 시기를 고려하여 현재에는 보안에 취약하다고 판명된 MD5 와 같은 암호화 알고리즘과 짧은 RSA 알고리즘의 키 길이를 지적하였고, 그 대안으로 SHA256, SHA384 와 같은 알고리즘을 쓸 것을 제안하였다. 보건의료정보는 재사용이 가능하고 참조하는 사람이 있는 한 영구히 보존될 수 있다는 특성을 고려하였을 때, ISO 17090 에 명시된 보안의 수준을 현재 수준보다 더 높여야 할 필요가 있다.

추후에는 본 고에 제안된 인증서 알고리즘과 RSA 키 보안등급을 실제 환경에 적용하여, 암호화 등급을 높인 비용 대비 효율이 충분한지에 관한 연구가 필요하다.

참고문헌

[1] ISO 17090:2008 “Health informatics – Public key infrastructure” ISO, 2008.

[2] 한국인터넷진흥원 “국내 암호 이용 현황 및 암호 구현 가이드” 2011.

[3] Stevens, Marc. "Fast Collision Attack on MD5." *IACR Cryptology ePrint Archive* 2006.

[4] Wang, Xiaoyun, Yiqun Lisa Yin, and Hongbo Yu. "Collision search attacks on SHA1." 2005.

[5] Elaine Barker, Quynh Dang “Recommendation for Key Management Part 3: Application-Specific Key Management Guidance” NIST Special Publication,2015.

[6] CA/Browser Forum “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.2.3” CA/Browser Forum, 2015.