생체정보와 해시함수를 이용한 인증서 보안 강화 방법

이 경 환*

An Security Hardening Method for the Certificate using Bio-Information and Hash Function

Kyeong-Hwan Lee*

요 약

공인인증서가 폐지되었지만 관공서 및 금융거래 등에 인증서는 사용되고 있고, 보안 강화의 필요성이 여전히 존재한다. 본 논문에서는 최근에 다양하게 활용되고 있는 생체인식 기술 및 해시함수를 이중 비대칭키와 접목하여 이러한 문제를 해결하고자 한다. 공인인증서 발급시 생체정보 특징값의 해시값을 이용하여 개인키2를 암호화하여 사용자측에 보관하고, 공인기관에는 이 특징값을 이용하여 이중 암호화된 개인키1을 보관한다. 사용자는 생체 인식을 통하여 개인키2를 복호화하고 이를 이용하여 인증기관에 보관된 개인키1를 전송받아 복호화하여 사용하므로써, 분실이나 해킹 상황에서 위험을 줄이고 재발급시 개인키2만 변경하면되므로 이전에 암호화한 문서를 사용할 수 있게 하였다.

Abstract

The certificate is still much used in financial transactions and public service. So new security hardening methods are necessary for safely using the cerificate. In this paper, we are going to solve the problem using the bio-information technolodgy and the hash function with the two pairs of asymmetric keys. Private-key2 and encrypted private-key2 are encrypted by the hash result from bio-characteristics and stored at the user part and the certification authority respectively. Because the user are firstly recognized by the hash result and use the private-key1 decoded by the private-key2, we can reduce the risk of the loss or hacking, and only change the private-key2 when a reissue.

* 위덕대학교 경찰정보보안학과 (Department of Police and Information Security, Uiduk University)

Ⅰ. 서 론

공인인증서는 비대칭 암호화 및 해시함수 등 많은 정보보안 기술들을 기반으로 개발되었고, 우리나라는 1999년 전자서명법이 재정되면서 인증계층구조 즉 공개키 기반 구조(PKI, public key infrastructure)를 구축하게 되어, 인터넷상에서 금융거래 및 전자상거래, 그리고 공공기관 등에서 신원 증명서로 사용되었다.[1-3]

또한 2000년대 모바일 시대가 시작되어 개인이 모바일기기를 항상 휴대하여 사용하면서 대부분의 온라인 접속이 이를 통해 이루어지게 되면서, 공인인증서는 모바일기기로 복사되어 사용되는 것이 필수적으로 되었다.[4]

그러나 공인인증서는 보관이나 재발급시에 발생하는 많은 문제점이 있어 이에 대한 개선책도 많이 연구되었다. 통신기술이 발달하면서 실시간으로 인증을 하는 여러 가지 방법들이 공인인증서를 대신하여 사용되었지만, 우리나라의 경우 법으로 정하여 공공기관 등 대부분의 시스템이 공인인증서를 기반으로 하였기에 다른 인증시스템을 사용하기 어려웠다.[5-6]

생체인증은 개인의 홍체, 지문 등 생체정보에서 고유한 특징데이터를 추출하여 단말기의 데이터베이스에 패턴으로 저장하고 이를 비교하여 인증 및 식별을 하는 방법으로 기존의 ID/PW를 활용한 단순한 인증방법에 비해 기억할 필요가 없으며 크래킹이 매우 어려우므로, 데이터의 해킹 등 보안문제만 해결되면 매우 유용하며 인증번호나 OTP 등 복합적인 인증을 통해 기존의 인증서를 대치할 수 있는 기술로 주목 받았다. 이를 활용하여 생체 데이터를 통한 키생성 기법, 공동인증서와 연동하여 인증하는 방법, 공동으로 기관들이 생체정보를 활용하는 '바이오체인' 기법들이 제안되고 있다.[7-11]

또한 2020년 5월 전자서명법 개정안이 국회를 통과하면서 공인인증서가 폐지되었고, 민간영역에서는 인증서 대신 생체인증 등을 활용한 다른 인증 방법들이 사용되고 있지만, 공공기관이나 은행 등에서는 여전히 공동인증서라는 이름으로 사용되고 있고, 모바일기기에서는 기기 내부의 생체인증 데이터와 결합하여 앱에서 사용되고 있으며, 웹브라우저 등의 암호화 통신에서 인증서는 여전히 사용되고 있다.

본 논문에서는 공동인증서에 생체정보 데이터의 해시값과 이중 비대칭키를 이용하여 보안을 강화시키는 방법을 제안한다. 공동인증서 발급시 공개키와 개인키를 1쌍이 아니라 공개키1, 개인키1, 공개키2, 개인키2의 2쌍을 부여받게되며, 사용자는 이중 공개키1과 개인키2를 보관하고 공인기관에는 공개키1, 공개키2, 그리고 공개키2로 암호화한 개인키1을 보관하게 된다. 이때 문서의 암호화와 복호화에는 공개키1, 개인키1이 사용되면 공개키2와 개인키2는 키들의 보안에 관여하게 된다. 사용자가 개인키1을 보관하지 않으므로 해킹 등 보안 문제에서 자유로우며, 재발급시에는 공개키2와 개인키2만 교체하면 되므로 영구히 사용할 수 있는 구조가 된다. 더 나아가서 생체정보 데이터의 해시값으로 사용자가 보관하는 개인키2에 홍채 특징값을 이용하여 대칭 암호화 하고, 공인기관에서 보관하는 개인키1 부분에도 이를 이용하여 대칭 암호화함으로써 공동인증서의 보안문제를 해결할 수 있다. 제안한 방법으로 비밀 문서 암호화 및 전자서명, 부인방지에 활용하여 좋은 결과를 보였다.

Ⅱ. 공동인증서 기술 및 활용

1. 암호화와 공개키 기반 기술

문서를 암호화할 때와 복호화할 때 동일한 키를 사용하는 대칭키(symmetric key) 방식이 제안되었다. 여기에 사용되는 키를 비밀키(secret key)라고 부르며, 키 교환이나 보관의 문제가 있어 해킹에 취약한 단점이 있다.

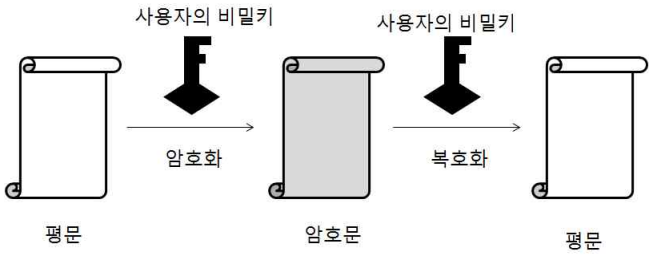

그림 1. 대칭키 암호화 및 복호화 알고리즘

이러한 문제점을 해결하기 위해 비대칭키(asymmetric key) 방식이 제안되었으며, 이에는 공개키(public key)와 개인키(private key)의 2개의 키가 사용된다. 이를 이용하여 암호화와 복호화시 동일하지 않는 키를 사용한다. 즉 공개키로 암호화한 암호문은 개인키로만 복호화할 수 있고, 개인키로 암호화한 암호문은 공개키로만 복호화할 수 있다.

비대칭키 알고리즘을 사용하면 모든 사용자는 자신만의 공개키와 개인키를 가진다. 공개키는 말 그대로 다른 모든 사용자에게 공개된 키이고, 개인키는 절대 공개되면 안되는 소유자만이 가지는 키이다. 이를 이용하면 대칭키에서 문제가 되는 키 교환 및 보관의 문제가 발생하지 않는 장점이 있다.

이를 이용하여 상대방의 공개키로 암호화한 문서를 전달하면 상대방은 그 문서를 자신의 개인키로만 복호화할 수 있으므로 기밀성을 보장할 수 있다. 또한 사용자 자신의 개인키로 암호화한 문서는 그 사용자의 공개키만으로만 복호화되므로 전자서명 및 부인방지에 활용할 수 있다.

공개키 기반 기술은 이러한 비대칭키 알고리즘을 공인기관과 연계하여 구축한 복합적인 보안 시스템 환경을 말한다. 여기에는 공개키에 대한 인증서를 발급하는 '인증기관', 사용자들의 인증서 신청시 인증기관 대신 그들의 신분과 소속을 확인하는 '등록기관', 인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서 취소 목록 등을 저장·검색하는 장소인 '디렉토리', 또한 다양한 응용에서 공개키를 이용하여 전자서명을 생성하고 검증하며 데이터에 대한 암호, 복호를 수행하는 사용자 등이 포함된다. 이를 활용하면 온라인상에서 기밀성 보장, 부인방지, 전자서명, 전자봉투 등의 다양한 보안 통신을 행할 수 있다.

공개키 기반 기술에 의하여 개인이 자신임을 인증하거나 문서를 암호화하기 위해 보유하는 키 등은 공동인증서라고 하는 파일 형식으로 부여받는다. 즉 공동인증서는 공개키와

공개키의 소유자를 연결시켜주는 전자문서로, Kohn Felder가 1978년 처음 제안했다. 공동인증서는 신뢰할 수 있는 인증기관(CA)이 전자서명하여 생성되며 인증기관이 공개키를 공증해준다고 생각하면 된다. 오늘날 사용되는 대부분의 인증서는 X.509 V3를 표준으로 따르고 있다.

공동인증서를 발급받으면 원하는 곳에 파일로 저장되는데, 주로 NPKI라는 폴더와 하위에 인증기관, 사용자의 폴더를 만들고 내부에 2개의 파일이 생성된다. 이 중 확장자 'der'인 파일은 사용자의 공개키 등이 담겨있는 인증서 파일이고, 확장자 'key'인 파일은 사용자의 개인키이다. 공개키 기반 구조에서 사용자는 이러한 공인인증서를 이용하여 암호화 및 개인 인증을 할 수 있게 된다.

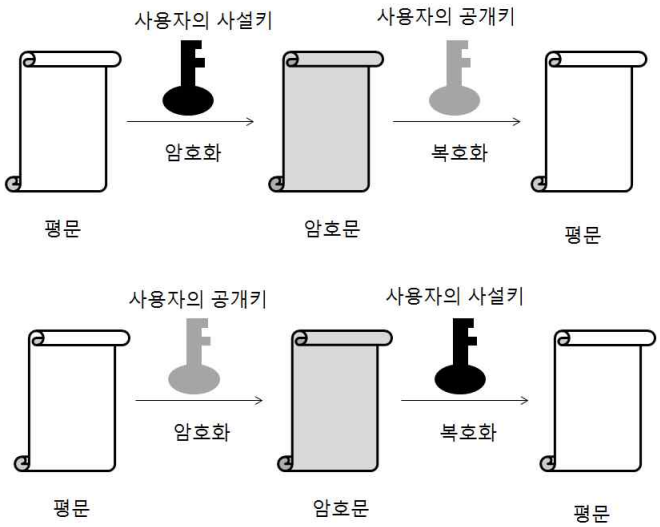

그림 2. 비대칭키 암호화 및 복호화 알고리즘

2. 공동인증서의 활용

기밀성(confidentiality) 보장은 암호화의 기본 기능으로 평문을 암호화하여 암호문으로 바꾸고, 암호문을 복호화하여 평문으로 복원하는 것을 말한다. 비대칭 암호화 방식에서는 송신측 사용자가 누구나 획득할 수 있는 수신측 사용자의 공개키로 암호화하여 전송하고, 수신측에서는 개인만 가지고 있는 사설키를 이용하여 복호화하므로 키전달의 필요가 없고, 대칭키 암호화에 비해 키의 개수도 크게 줄어드는 장점이 있다.

대칭키와는 달리 공개키와 사설키을 사용하는 공개키 기반 방법에서는 기밀성 보장 외에 부인방지 및 전자서명 기능에 적용할 수 있다. 부인방지(non-repudiation) 기능은 '자신이 작성한 문서를 작성하지 않았다고 하지 못한다.'는 것으로, 오프라인에서 인감도장이나 친필싸인이 되어있는 문서와 같음을 뜻한다. 사용자A가 작성한 문서를 A의 사설키로 암호화하였을 경우, 사용자A의 공개키만 이를 복호화할 수 있기 때문에 가능하다. 이를 이용하면 전자서명(digital signature)파일을 만들 수 있느데, 문서를 해시한 값을 사용자의 사설

키로 암호화하여 문서에 첨부하여 보냄으로써, 이 문서가 사용자가 작성한 것이 확실하다는 보장을 하는 개념이다. 이러한 두가지 기능을 이용하여 보안 영역에서 중요한 문서의 무결성(integrity)을 확보할 수 있다.

Ⅲ. 생체인증 및 해시함수

1. 생체인식의 원리 및 처리절차

생체인증 및 인식을 하기 위해서는 얼굴모양, 홍채, 망막, 정맥, 지문 등 다양하며, 모바일 기기 등은 이미지 센서 및 전용 프로그램을 이용하여 신체 특징데이터를 검출하여 데이터베이스에 등록한다. 이를 사용하는 방법은 사용자 자신이 자신임을 확인하는 인증(verification)과 데이터베이스에 등록된 여러 사용자 중 특정 사용자를 찾아내는 인식(identification)으로 나누어진다.

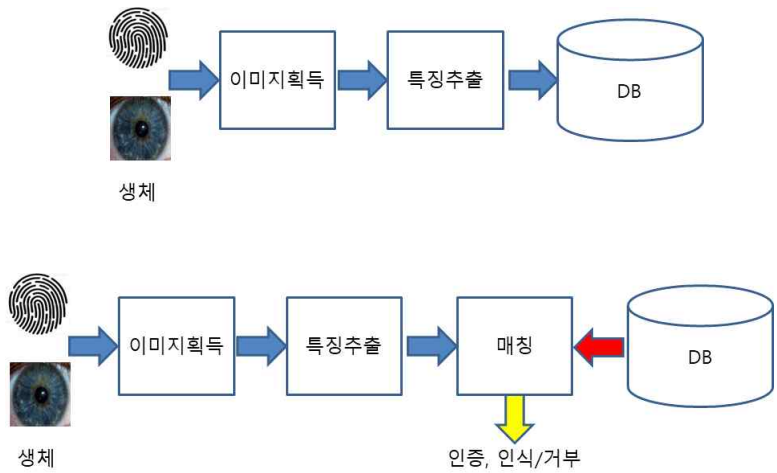

그림 3. 사용자 생체 등록, 인증, 인식 과정

2. 해시함수

해시함수(Hash Function)는 암호학 측면에서 보면 복호화 과정이 없이 암호화 과정만 존재하고 암호화키가 없는데, 암호문 즉 해시함수값(해시값)은 입력값에 상관없이 출력값으로 짧은 비트열을 생성하며 128비트를 가지는 MD5, 160비트와 256비트를 생성하는 SHA-1, SHA-256 등이 널리 사용된다. 좋은 해시함수는 다른 입력값이 같은 출력값을 가지게 되는 충돌(collision)의 확률이 작으며, 입력값이 한 비트만 변경되어도 해시값의 모든 비트에서 변동이 일어나서 입력값의 추정이 힘들게 되는 혼돈(confusion) 및 확산(diffusion)의 특성이 있어야 한다.

해시는 디지털포렌식에서 증거의 무결성을 유지하거나, 블록체인 기술의 핵심으로 사용

되는 등 현재 많은 분야에서 중요한 기술로 자리잡고 있다. 그림 4에서는 128비트의 해시값을 만드는 MD5 해시함수의 사용 예를 나타내고 있는데, 용량이 큰 문서와 간단한 문자열, 그리고 지문 특징데이터들이 모두 128비트의 해시값으로 표현됨을 알 수 있다.

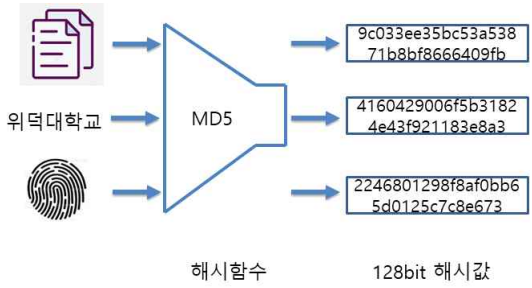

그림 4. MD5 해시함수의 사용예

Ⅳ. 제안한 생체정보와 해시함수를 이용한 공동인증서 보안 강화

1. 이중키를 활용한 인증서 보안 강화 방법

인증서를 발급받는 프로세서를 살펴보면, 인증기관은 개인키를 발급만 할 뿐 보관하지 않으며, 사용자의 개인키는 비밀번호로 대칭암호화하여 원하는 미디어에 폴더를 생성하여 보관하므로 이를 분실하거나 해킹당했을 경우 심각한 문제가 발생한다. 인증서는 한번 폐기되면 더 이상 사용할 수 없도록 인증서 폐기 목록(CPL, Certification Revocation List)으로 인증기관에 보관된다. 인증기관은 사용자의 개인키를 보관하고 있지 않으므로 동일한 인증서를 재발급하지 않고, 재발급시 적절하게 폐기하고 다시 새로운 개인키를 가진 인증서를 발급해준다.

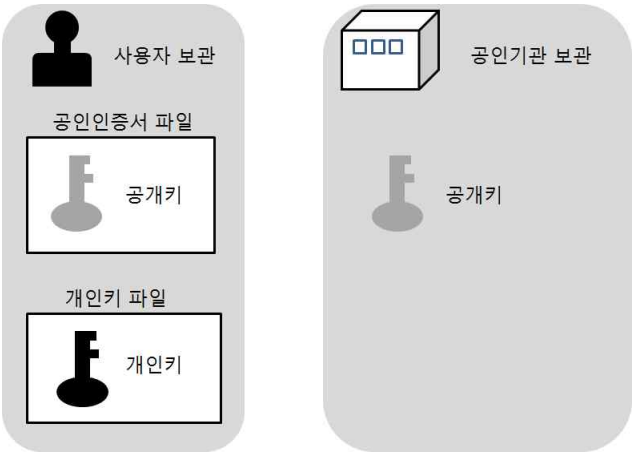

그림 5. 기존의 인증키 보관 방식

이러한 인증서 구성에는 공개키와 개인키 파일이 들어있어, 분실이나 해킹을 당했을 경우 이들을 폐기하고 재발급받아야 하므로 키가 모두 바뀌는 문제가 있다. 따라서 이전에 공인인증서의 공개키로 암호화한 기밀성이 보장된 문서나, 개인키로 암호화된 부인방지 및 전자서명이 된 문서도 모두 쓸모가 없어지는 문제점이 존재한다.

본 논문에서는 이런 단점을 보완하기 위해 공개키와 개인키를 2개씩 쌍으로 사용한다. 인증서를 발급하는 인증기관은 사용자에게 공개키1, 공개키2, 개인키1, 개인키2의 4가지 키를 만들어 사용자의 인증서에는 공개키1과 개인키2를 발급하고, 인증기관에 공개키1, 공개키2, 그리고 공개키2로 암호화한 개인키1을 보관한다. 그리고 인증서 정책대로 개인키들을 절대 보관하지 않는다.

사용자가 문서의 암호화 및 복호화에 사용하는 키는 공개키1과 개인키1이다. 기밀성을 보장하기 위해 사용자의 문서는 먼저 개인키2로 인증기관으로 연결하여 공개키2로 암호화한 개인키1을 받아와서, 개인키2로 복호화하여 개인키1로 암호화한다. 이 문서를 복호화하는 상대방은 기존의 방법대로 사용자나 공인기관으로부터 획득한 사용자의 공개키1로 복호화 하면 평문의 문서를 볼 수 있다.

부인방지 기능도 이와같이 사용할 수 있다. 사용자는 개인키2로 공인기관으로부터 공개키2로 암호화된 개인키1을 획득하여, 이를 개인키2로 복호화한 후에 이 개인키1으로 문서를 암호화하여 전송하면, 수신측은 이를 사용자의 공개키1으로 복호화하여 성공할 경우 사용자의 부인방지 처리가 가능하다.

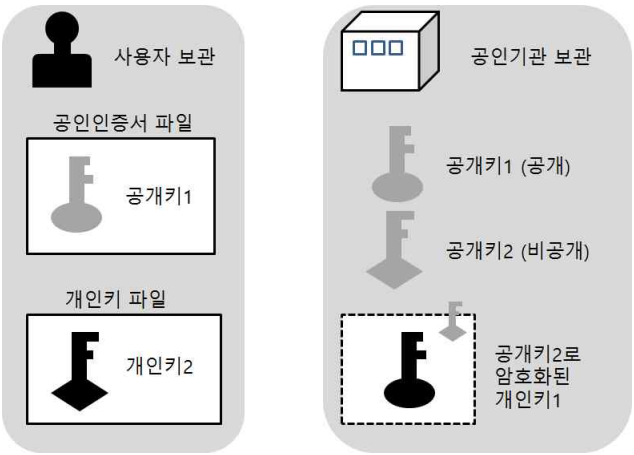

그림 6. 이중 비대칭키 공인인증의 키 보관 방식

2. 인증서의 등록 및 키 보관 방법

본 논문에서는 생체 정보와 이중키를 이용하여 공인인증서의 보안을 더욱 강화시키는 방법을 제안한다. 현재 인식률을 향상시킨 생체인식 알고리즘의 개발과 실시간에 활용할 수 있는 정보통신 기술의 발달이 이루어져, 홍체 및 지문, 얼굴인식 등의 경우 모바일 기기의 카메라 및 센서를 통해 특징값을 추출하여 내부 데이터베이스의 패턴과 비교에 의한

개인 인식이 보안 장치로 활용되고 있다.

이러한 데이터베이스에 저장된 생체정보 특징값은 기존의 비밀번호를 대치하거나 보완할 수 있으며, 이는 인증서 비밀번호를 대치할 수 있으며, 보안 수준을 매우 크게 향상시킬 수 있다. 공인인증서를 분실하더라도 홍채인식으로 본인 인증이 이루어지지 않으면 재발급 받을때까지 해킹의 우려가 거의 없다고 볼 수 있다.

데이터베이스에 저장된 생체정보 특징값의 해시값을 취하여 이를 비밀번호로 사용하는데, 해시함수로는 128비트 해시값이 나오는 MD5를 그리고 암호화는 이 해시값을 암호화키로 사용하는 대칭암호화인 AES(Advanced Encryption Standard) 암호화를 사용한다. 제안한 방법에서는 이중 비대칭키로 공개키1, 개인키1, 공개키2, 개인키2의 키들이 사용되며, 그림 11에서와 같이 사용자 측에는 공개키1을 포함한 공인인증서 파일 및 사용자의 생체정보 해식값으로 암호화한 개인키2 파일을 보관하게 된다. 또한 공인기관에는 사용자의 공개키1과 공개키2를 가지게 되는데 공개키2의 경우 다른 사용자에게 공개되지 않는다. 그리고 공개키2로 비대칭 암호화한 후 생체정보 해시값으로 대칭암호화한 개인키1을 가지게 된다.

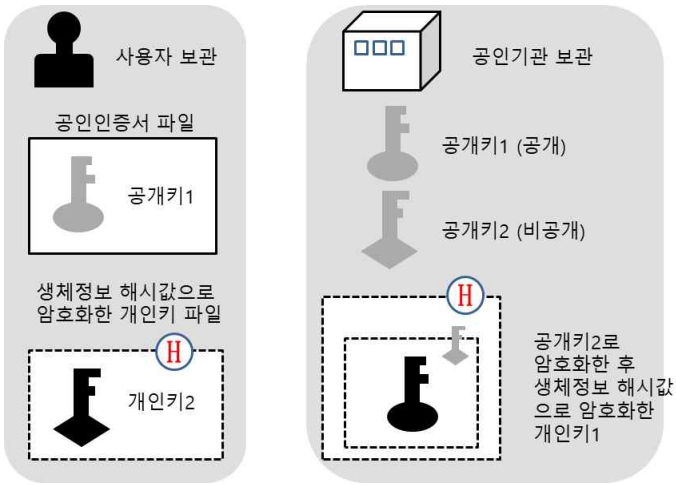

그림 7. 제안한 생체정보와 해시함수를 이용한 키 보관 방식

3. 인증서의 활용 방법 및 보안상 장점

(1) 문서 암호화

제안한 방법으로 문서를 암호화하는 방법은 다음과 같다. 예로 사용자A가 사용자B에게 암호화된 문서를 전달하려면, 사용자A는 공인인증기관이나 사용자B로부터 받은 사용자B의 공개키1으로 문서를 암호화해서 보낸다. 사용자B는 생체 인식을 통해 특징값의 해시값을 얻어 이를 통해 개인키2를 복호화한다. 또한 사용자B는 이 생체정보 해시값을 공인기관으로 보내게 되는데, 공인기관에는 '공개키2로 암호화한 후 생체정보 해시값으로 암호화한 개인키1'이 있는데, 전송한 해시값과 일치할 경우 이를 복호화하여 수신하게 된다. 이렇게

수신한 '공개키2로 암호화한 개인키1'은 이전에 복호화한 개인키2에 의해 복호화되어 결국 개인키1을 얻게 된다. 최종적으로 이 문서는 공개키1으로 비대칭 암호화되어 있으므로 개인키1으로 복호화하게 되는데, 기존의 방식에 비해 매우 뛰어난 기밀성을 보장하게 된다.

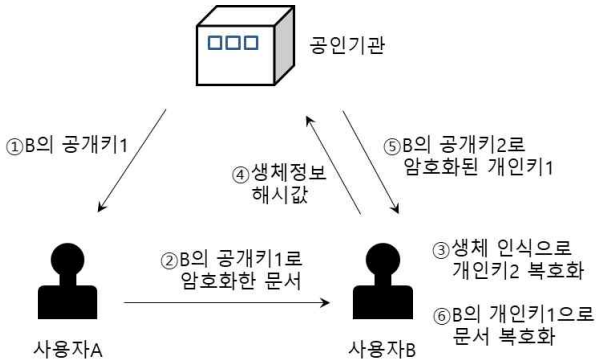

그림 8. 제안한 방법으로 문서의 기밀성을 보장하는 방법

(2) 전자서명 및 부인방지

제안한 방법으로 문서의 전자서명 및 부인방지를 하는 방법은 다음과 같다. 예로 사용자A가 전자서명을 하기 위해서는, 먼저 사용자A는 생체 인식을 통해 특징값의 해시값을 얻게되고 공인기관에 이를 전송하여 보관된 '공개키2로 암호화한 후 생체정보 해기값으로 암호화한 개인키1'에서 특징값이 본인이 맞다면 이를 복호화하여 '공개키2로 암호화한 개인키1'를 수신받게된다. 사용자A는 생체정보 해기값으로 보호화한 개인키2를 이용하여 이를 복호화하여 개인키1을 획득하게된다.

사용자A는 이 개인키1로 문서를 암호화하여 발송하면 사용자B이든 누구든 이 문서를 보기위해서는 반드시 사용자A의 공개키1로만 복호화되는 것을 보게되며 이는 사용자A가 작성한 문서임을 입증하는 것으로 전자서명 및 부인방지에 활용할 수 있다.

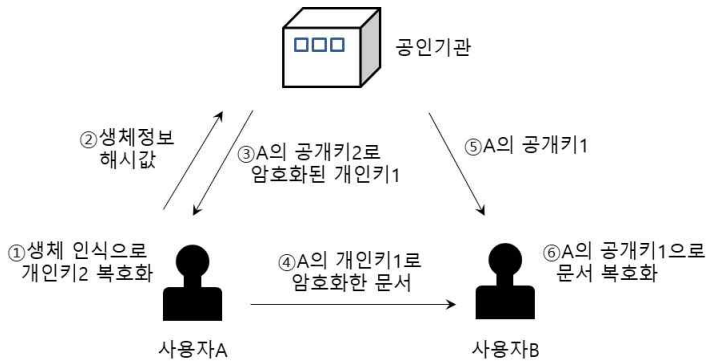

그림 9. 제안한 방법으로 전자서명 및 부인방지하는 방법

Ⅴ. 결 론

본 논문에서는 생체정보 특징값의 해시값과 이중 비대칭키를 이용하여 공인인증서의 보안 강화 방법을 제시하였다. 사용자가 공인인증서를 발급받은 때 생체정보 해시값으로 첫번째 개인키를 암호화 하고, 공인기관에는 이 생체정보 해시값으로 암호화한 최종 두번째 개인키를 저장함으로써 비밀문서의 암호화나 전자서명, 부인방지 등에 안전하게 사용할 수 있는 방법을 제안하였다.

제안한 방법을 이용하면, 인증서 사용시 생체정보 특징값을 전송하면서 한번더 접속이 이루어져야하는 단점이 있지만, 인증서 개인키 파일을 분실이나 해킹되었을 때 홍채 인식과정에 의해 개인키를 복호화 할 수 없으므로 매우 강력한 보안을 가질 수 있으며, 이중키 방식이므로 인증서 재발급시에도 이전에 암호화한 문서를 계속 사용할 수 있는 등 편의성을 보장할 수 있으므로 향후 다양한 적용분야에 사용될 수 있을 것이다.

참고 문헌

[1] 정보보호진흥원 암호인증기술팀, 전자서명 인증서 프로파일 기술규격[V1.10], 정보보호진흥원, 2004.

[2] R. Hunt, “PKI and Digital Cerfification Infrastructure,” Ninth IEEE International Conference on Networks(ICON’01), Oct., 2001.

[3] 인터넷 해킹과 보안: 양대일, 김경곤 공저, 한빛미디어, 2012년.

[4] 강필용, “모바일 혁명시대의 공인인증서 이용 현황 및 정책 방향,” 정보보호학회지, pp. 51-55, 제21권 제1호, 2011년 2월.

[5] 최윤성, 이영교, 이윤호, 박상준, 양형규, 김승주, 원동호, “삭제된 공인인증서 복구 및 개인키 암호화 패스워드의 검출,” 정보보호학회논문지, pp. 41-54, 제17권 제1호, 2007년.

[6] 정기석, “전자금융거래시 공인인증서 의무사용 개선방안에 관한 연구,” 융합보안논문지, pp. 25-33, 제13권 제6호, 2013년.

[7] 바이오정보 보호 가이드라인: 방송통신위원회, 한국인터넷진흥원, 2017년 12월.

[8] 이형우, 윤성현, 문기영, 정윤수, “바이오정보 기반 전자서명 및 디지털 키생성 기법,” 한국콘텐츠학회지, pp. 32-44, 제5권 제1호, 2005년.

[9] 임철수, 박병섭, “홍채인식 시스템을 위한 임베디드 시스템의 설계 및 구현,” 한국콘텐츠학회논문지, pp. 47-54, 제3권 제3호, 2003년.

[10] 이현석, 김혜진, 양대헌, 이경희, “생체 정보와 다중분류 모델을 이용한 암호학적 키 생성 방법,” 정보보호학회논문지, pp. 1427-1437, 제28권 제6호, 2018년 12월.

[11] 김선종, “스마트폰 환경에서 공인인증서 사용시 소유 및 생체인증 연동 방법,” 정보보호학회지, pp. 13-17, 제25권 제6호, 2015년 12월.