情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

바이오 보안토큰을 이용한 프라이버시 보호형 사용자 인증기법*

신 용 녀,[1†] 전 명 근[2‡]
[1]한양사이버대학교, [2]충북대학교

A Privacy Preserving User Authentication Using Biometric Hardware Security Module*

Yong-Nyuo Shin,[1†] Myung Geun Chun[2‡]
[1]Hanyang Cyber University, [2]Chungbuk National University

요 약

바이오 보안토큰은 바이오 인식 센서와 바이오인식 정보를 처리할 수 있는 MCU, 보안토큰으로 구성된 USB 형태의 하드웨어 기기로서, 기기 내부에서 바이오인식 센서로 가입자의 바이오인식 정보를 추출하여 보안토큰에 안전하게 저장하며, 사용자 인증시 바이오인식 센서로 부터 취득된 바이오인식 정보와 저장되어 있는 바이오인식 정보를 기기 내부 MCU에서 매칭하여 사용자를 인증하는 독립된 하드웨어 보안모듈이다. 기존의 보안토큰이 제공하는 개인인증기법이 ID/패스워드에 기반한 방법이므로 이의 유출로 인해 생길 수 있는 피해를 최소화하고, 고의적인 공인인증서의 오용을 막을 수 있도록 높은 수준의 사용자인증기법을 제공한다. 이에 본 논문에서는 공개키기반구조(PKI: Public Key Infrastructure)를 연동한 바이오보안 토큰의 이용에 있어서 사용자의 바이오인식 정보를 보호하면서 바이오인식 정보를 이용하여 보안 수준이 높은 사용자 인증이 가능한 기법을 제시한다.

ABSTRACT

A biometric hardware security module is a physical device that comes in the form of smartcard or some other USB type security token is composed with biometric sensor and microcontroller unit (MCU). These modules are designed to process key generation and electronic signature generation inside of the device (so that the security token can safely save and store confidential information, like the electronic signature generation key and the biometric sensing information). However, the existing model is not consistent that can be caused by the disclosure of an ID and password, which is used by the existing personal authentication technique based on the security token, and provide a high level of security and personal authentication techniques that can prevent any intentional misuse of a digital certificate. So, this paper presents a model that can provide high level of security by utilizing the biometric security token and Public Key Infrastructure efficiently, presenting a model for privacy preserving personal authentication that links the biometric security token and the digital certificate.

Keywords: Biometric Hardware Security Module, Biometrics, Personal Identifiable Information, Privacy

접수일(2012년 3월 3일), 게재확정일(2012년 4월 12일)
* 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(한국연구재단 -2011-0026223)
† 주저자, ynshin@hycu.ac.kr
‡ 교신저자, mgchun@chungbuk.ac.kr

I. 서 론

보안토큰(Hardware Security Module)은 전자서명생성키 등 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기로서, 마이크로프로세서, 운영체제, 보안 모듈, 메모리 등을 자체적으로 갖추고 특정 트랜잭션을 처리할 수 있도록 집적회로 칩으로 구성되어 있으며 피싱·해킹으로부터 공인인증서의 유출을 방지하는 기능을 제공함으로써 안전한 인터넷 환경을 구축하는데 사용되는 하드웨어 모듈이다[1].

바이오 보안토큰(Biometric Hardware Security Module; BHSM)은 바이오 인식 센서와 바이오인식 정보를 처리할 수 있는 MCU(Microcontroller Unit), 스마트카드로 구성된 USB 형태의 하드웨어 기기로서, 기기내부에서 바이오인식 센서로 가입자의 바이오인식 정보를 추출하여 보안토큰에 안전하게 저장하며, 사용자 인증 시 바이오인식 센서로부터 취득된 바이오인식 정보와 저장되어 있는 바이오인식 정보를 기기내부 MCU에서 매칭하여 사용자를 인증하는 독립된 하드웨어 보안모듈이다. 바이오 보안토큰은 기존의 보안토큰이 제공하는 개인인증 기법이 ID/패스워드에 기반한 방법이므로 이의 유출로 인해 생길 수 있는 피해를 최소화하고, 고의적인 공인인증서의 오용을 막을 수 있도록 높은 수준의 보안 및 사용자인증기법을 제공할 수 있다[2].

바이오인식 정보 중에서 임베디드화가 가장 용이하고 가장 널리 사용되고 있는 지문인식이 채택되고 있다. 그러나 휴대폰을 이용한 얼굴이나 홍채 영상 취득이 용이해 짐에 따라, 보안토큰과 접목하여 다양한 바이오인식 기법이 사용될 수 있으리라 생각된다. 행정안전부에서는 공인인증서 저장 및 보관방법을 위한 개선책을 마련하여, 공인인증서는 원칙적으로 PC하드디스크에 보관하지 않고 USB 등 휴대용 저장장치에 보관될 수 있도록 보안토큰의 이용을 강화하고 있다.

이렇듯 어느 때 보다도 공인인증서와 연계된 보안토큰에 대한 관심이 높으며, 앞으로서 그 수요는 계속하여 증가할 것으로 예상된다. 그러나 이와 더불어 보안토큰에서의 단순한 패스워드 기반의 사용자 인증으로 인하여 공인인증서를 악의적으로 사용하기 위하여 고의적으로 패스워드를 특정인에게 노출한다든지, 부주의나 해킹 등에 의해서 패스워드가 노출되어 개인정보 등이 누출되는 등의 원하지 않는 위험이 발생할 수 있기 때문에 바이오 보안 토큰에 대한 사회적 요구는 커지고 있다[2].

이와 관련하여 바이오 보안 토큰과 공인인증서의 연계 모델을 제시함으로써, 바이오보안토큰과 공인인증서의 효율적 활용을 통한 확장성을 제공할 수 있는 정책적 방안을 제시한 연구가 있었다[3]. 다양한 유형의 바이오인식기반 임베디드 시스템 도입에 대비한 OID(Object Identifier)를 활용하는 방안을 제시하였으며, X.509 Qualified Cirtificate 개인키, 공개키를 이용하여 바이오정보를 보호하고 장치를 활용한 바이오인증을 처리하고 있는 지 확인할 수 있도록 하여 바이오인증 결과를 활용해 개인키 사용을 통제할 수 있는 방안을 제시하였다. 그러나 구체적으로 바이오정보와 보안토큰내의 개인식별정보에 대한 결합 방법과 사용자 인증을 위한 구체적인 기법을 제시하지는 않고 있다.

한편, 최근에 제정된 바이오보안토큰에 관한 표준안에서는 PC 및 모바일 환경에서 바이오 보안 토큰 기반 공인 인증서를 이용하기 위한 응용 프로그램과 바이오 보안 토큰 간 인터페이스 기본 요구 사항과 바이오 보안 토큰을 이용함에 있어 필요한 기능적 요구 사항을 명시하고 있다[4]. 한편 [5]에서는 공인인증서내에 개인식별 정보를 프라이버시 보호 기능을 갖도록 저장하는 방법에 대해서 다루고 있으나 본 논문의 주제와 같은 바이오인식 정보 및 바이오보안 토큰에 대한 고려는 없다.

이에, 본 논문에서는 [3][4][5]가 갖는 한계를 극복하고 바이오보안 토큰을 이용하여 프라이버시 보호 기능을 가는 개인 인증 기법을 다루고 있다. 이를 위하여 바이오 보안 토큰에서 바이오정보와 공인인증서를 이용할 때의 보안 및 개인정보보호 요구사항을 알아보고 바이오 보안 토큰을 이용한 프라이버시 보호형 사용자인증 기법을 제시함으로써 바이오보안토큰과 공인인증서의 효율적 활용을 도모하도록 한다.

II. 바이오보안토큰과 요구사항

2.1 바이오인식과 바이오 보안토큰

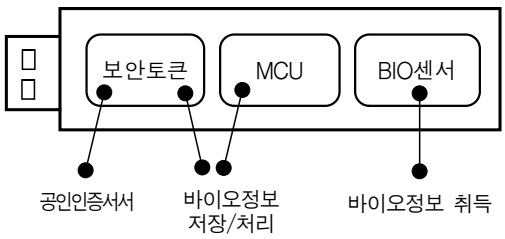
바이오인식 시스템은 인터넷 환경과 같이 비대면의 개인인증 환경에서 인증대상자가 제시한 개인의 신체정보나 서명과 같은 동적 특성의 특징정보를 제시함으로서 사전에 등록단계에서 미리 저장시켜 놓은 정보와의 비교를 통하여 확인 받고자 하는 개인의 신분을 확

인 하는 역할을 수행한다.

바이오인식 시스템은 크게 3가지의 역할로 나누어서 생각해 볼 수 있다. 첫 번째로 등록(enrollment) 과정이다. 이 기능은 제시되는 대상자의 바이오정보로부터 개인식별(identification)과정이나 개인인증(verification)과정에서 필요로 하는 바이오인식정보(Biometric reference)를 생성하고 저장하는 과정을 의미한다. 개인식별과정은 주어진 바이오인식정보에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 모든 바이오인식정보와의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 한편, 개인인증과정은 대상자가 본인의 바이오인식정보와 함께 개인식별정보(Identity Reference)를 제시하게 되는데, 이는 주어진 바이오인식정보에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 사용된다. 이때 바이오인식시스템은 저장장치내의 해당 식별정보의 바이오인식정보와의 비교를 통하여 대상자의 인증여부를 결정하게 된다. 바이오보안 토큰을 이용하는 경우는 토큰의 소유자, 혹은 공인인증서의 소유자가 본인인지의 여부를 확인하는 개인인증 과정이라고 볼 수 있다.

바이오 보안토큰은 바이오 인식 센서와 바이오인식 정보를 처리할 수 있는 MCU 등으로 구성된 바이오인식 모듈과, 보안토큰으로 구성된 임베디드 형태의 하드웨어 기기로서, 기기 내부에서 바이오인식 센서로 가입자의 바이오인식 정보를 추출하여 저장한 후, 사용자 인증시 바이오인식 센서로 부터 취득된 바이오인식 정보와 저장되어 있는 바이오인식 정보를 기기내부 MCU에서 매칭하여 사용자를 인증하는 하드웨어 보안모듈로서 보통 그림 1과 같은 임베디드 형태로 구성된다.

바이오인식 정보(biometric reference; BR)는 비교를 위해 개인식별 대상자에 대해서 추출한 속성으로 하나 또는 다수의 저장된 바이오인식 샘플, 바이오인식 템플릿, 바이오인식 모델 등을 의미한다. 한편, 한 개인의 신원을 나타내는 개인식별정보(identity reference; IR)는 그 사람이 신원 확인하기를 바라는 상황에서 대상자와 관련된 모든 속성이라고 할 수 있다. 바이오보안 토큰의 경우에는 보안 토큰내에 저장되는 주민등록 번호 등과 같은 민감한 개인정보 등이 될 수 있다. 넓게 보면 바이오인식 정보도 개인 식별정보(identity reference; IR)의 일종으로 볼 수 있다. 그러나 통상 바이오 인식 시스템에서는 개인식별정보를 바이오인식 정보와 분리하여 생각하는데 [8], 본 논문에서도 이와 같은 관점으로 바이오인식 정보와 개인식별 정보를 분리하여 기술하고자 한다. 개인식별정보와 바이오인식 정보가 동시에 사용되는 바이오 보안토큰에서 프라이버시 보호기법이 무엇보다도 필요하다.



[그림 1] 바이오 보안토큰의 구성

2.2 바이오인식과 바이오 보안토큰

먼저, 다음과 같이 [5]에서 사용된 기호들을 확장하여 바이오보안 토큰을 위한 암호학 및 관련 기호들을 정의한다.

- h( ) 암호학적으로 안전한 해쉬 알고리즘
- E( ) 암호화 알고리즘
- D( ) 복호화 알고리즘
- IR ISO 24745 국제표준[6]에 정의된 주민등록번호, 신용카드번호 같은 개인식별정보(Identity Reference).
- BR ISO 24745 국제 표준에 정의된 지문이나 얼굴인식을 위한 템플릿 등과 같은 바이오인식 정보(Biometric Reference)
- R RA에 의해 생성된 난수

PBID 해쉬 알고리즘과 난수에 의해 발급되는 재발급성을 갖는 개인식별 정보. 개인의 고유한 바이오인식 정보를 포함하고 있지 않는 형태(Pseudo Biometric Identity)

- pk 공개키
- sk 개인키

바이오 보안토큰이 사용되어질 환경에 대해서 다음과 같이 가정한다.

- Alice: 공인인증서와 바이오 정보를 담고 있는 바이오 보안토큰 소유자

- Bob: 사용자인 Alice가 바이오 보안토큰 등록시의 본인이 맞는지를 요구하는 신뢰당사자
- Eve: Alice의 바이오보안 토큰을 획득한 공격자
- RA: Alice가 자신의 바이오정보를 최초 한번 공개하여 BR을 등록해야만 하는 등록기관(Register Authority)
- CA: Alice의 바이오 보안 토큰을 발급하는 인증기관(Certificate Authority)

프라이버시 보호 기능을 포함하면서 기존의 공인인증서 체계를 이용할 수 있도록 하기 위한 다음과 같은 운영요구사항을 제시한다.

운영요구사항 1. CA는 기존의 PKI를 이용하여 바이오보안 토큰을 운용함에 있어서 X.509 확장 필드를 이용함으로서 기존의 X.509에 대해서 별도의 수정을 요구하지 않는다.

운영요구사항 2. 사용자 확인을 위한 X.509 확장 필드를 사용함에 있어서 사용자의 프라이버시 보호를 위하여 Alice의 개인식별 정보 IR을 직접적으로 사용하지 않아야 한다.

운영요구사항 3. 바이오인식정보를 이용함에 있어서 ISO 24745 국제표준에서 제시한 바이오 프라이버시 보호를 위한 비가역성(irreversibility), 비연결성 (Unlinkability), 기밀성(confidentiality)를 만족해야 한다.

운영요구사항 4. 바이오인식 프라이버시 보호를 바이오인식 정보 BR은 운영중에 오직 바이오보안 토큰내에서만 사용됨으로서 바이오정보에 대한 자기 통제가 보장되어야 한다.

위와 더불어 다음과 같은 보안 요구 조건도 만족하여야 한다.

보안요구사항 1. Alice는 Bob에게 자신의 바이오 보안토큰을 이용하여 RA에 등록된 사용자가 본인 임을 증명할 수 있다.

보안요구사항 2. Eve가 Alice의 인증서로부터 바이오인식 정보 BR을 알아내기 위해서는 막대한 양의 작업 시간을 요구한다.

III. 바이오 보안토큰의 발급과 사용자인증

3.1 바이오 보안토큰의 발급절차

PBID 생성을 포함하는 바이오 보안 토큰의 등록 과정은 그림 2와 같이 나타낼 수 있다. 일반적인 공인인증서 발급을 포함한 공개키 기반 구조(PKI)에 관한 설명은 참고문헌[7]에 자세히 기록되어 있다.

(a) Alice는 RA를 방문하여 자신의 바이오인식 정보 BR을 제공한다. 이때, RA는 등록시의 바이오인식 정보의 위변조등을 방지하기 위한 조치들을 취해야한다.

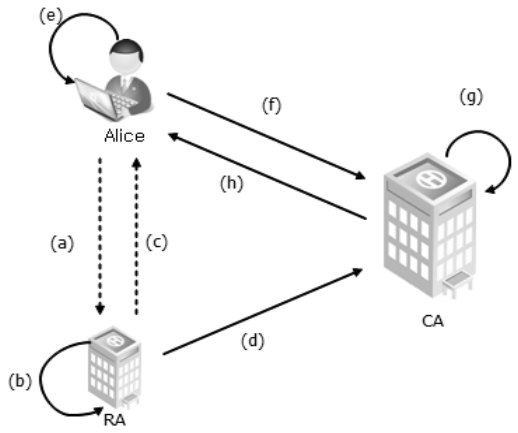
(b) RA는 Alice의 바이오정보 RA와 더불어 PBID를 생성하는데 필요한 난수 R을 발생시킨다.

(c) RA는 발생된 난수 R과 Alice의 바이오인식 정보 BR을 바이오보안 토큰에 담아서 Alice에게 전달한다.

(d) RA는 Alice의 BR과 난수 R을 이용하여 다음식을 이용하여 PBID를 만들어서 CA에게 전송한다.

PBID=h(h(R || BR))

(e) Alice는 바이오보안토큰을 이용하여 자신의 개인키와 공개키쌍을 발생시킨다. 이는 공인인증서를 위한 전자서명 등에 사용되게 된다. 바이오 보안토큰내에 저장되어 있는 난수 R과



[그림 2] 바이오 보안토큰의 등록과정

BR를 가지고 본인의 PBID를 만들기 위하여 h(R || BR)를 만든다. CA에의 전송시 정보 보호를 위해서 CA의 공개키로 암호화 하여 EPBID= E(h(R || BR))의 형태를 만든다.

(f) Alice는 CA에 대해서 인증서 요청을 위해 IETF RFC 2511 표준인 CRMF(Certificate request message format) 또는 RSA사의 표준인 PKCS#10인증서 요청 형식(Certificate request syntax standard)으로 CA에 전달한다[7][12].

(g) 인증서 발급을 위해서 CA는 수신된 인증서 요청 메시지에서 EPBID를 추출하여 기관의 개인키를 가지고 다음과 같은 복호화과정을 거친다.

h(R || BR) = D(EPBID)

이런 후에, 위의 값과 미리 정해진 해쉬함수를 이용하여 다음과 같은 값을 구해 본다.

PBID′ = h(h(R || BR))

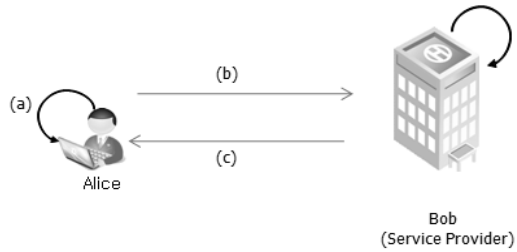
이 값은 등록 단계에서 RA로부터 받아 놓은 PBID와 비교하여 일치하면, 비로서 인증서 발급단계에서의 사용자 인증이 완료 되게 되며, CA는 X.509 인증서의 확장 필드 중 소유자대체 명칭(subjectAltName)에 PBID를 주입한 후, Alice의 공인인증서를 생성한다.

(h) CA는 생성된 X.509 공인인증서를 Alice에게 전송하고, 이는 Alice의 바이오보안 토큰에 저장되게 된다.

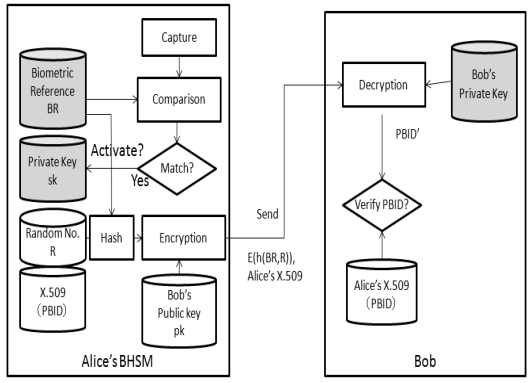
3.2 바이오 보안토큰을 이용한 사용자 인증

신뢰당사자 Bob은 공인인증서를 통하여 통상적인 사용자 접근 통제 및 부인 방지 서비스를 수행하지만, 이와 더불어 바이오인식 정보를 이용하여 강력한 사용자 인증을 수행함에 있어서, 개인의 바이오인식 프라이버시를 보호할 수 있도록 PBID를 이용하여 그림 3과 같이 각 단계별로 수행 할 수 있다.

(a) Alice가 바이오보안토큰의 바이오인식 모듈을 이용하여 자신의 바이오인식 정보를 입력하면, 바이오인식모듈내에서 매칭을 수행하면 바이오보안 토큰에 대한 접근이 허용되게 된다.



[그림 3] 바이오 보안토큰을 이용한 사용자인증



[그림 4] 바이오 보안토큰을 이용한 사용자인증

(b) 접근이 허용되면, 바이오인식 모듈내에 저장되어 있던 BR과 보안토큰 내에 저장되어 있던 R을 이용하여, 이를 직접 노출함이 없이 h(R || BR)의 형태와 X.509 공인인증서를 Bob에게 넘긴다.

(c) Bob은 수신된 h(R|| BR)를 이용하여 PBID′=h(h(R || BR)를 구한 후, 인증서 내에 있는 PBID 값과 비교하여 값이 같은지 검증한다. 이를 통해 Alice가 바이오보안토큰 발급 당시의 당사자임을 인증한다.

지금까지의 과정을 정리하여 Alice와 Bob사이의 개인인증을 위한 바이오보안토큰내의 정보와 Bob사이의 데이터 흐름은 다음의 그림 4와 같다.

3.3 운영 및 보안 요구사항의 수용여부 분석

제시된 기법이 앞의 2.2에서 언급된 운영 및 보안 요구사항들을 만족하는지 다음과 같이 분석하였다.

<운영요구사항 1>

3.1에 설명된 바와 같이 CA는 X.509 확장 필드 "SubjectAltName"에 포함된 하나의 부가 이름으로서 PBID를 처리한다. 따라서 기존의 X.509에 대해서 별도의 수정을 요구하지 않는다.

<운영요구사항 2>

PBID를 생성하고 X.509 확장 필드에 해쉬화된 h(R || BR)을 이용할 뿐 직접적으로 Alice의 개인 식별 정보 IR을 사용하지 않는다.

<운영요구사항 3>

바이오 정보를 이용함에 있어서 해쉬화된 h(R || BR)와 공개키에 기반한 암호화 기법을 사용하기 때문에 ISO 24745 표준에서 제시한 바이오인식 프라이버시 요구조건인, 비가역성(irreversibility), 비연결성(Unlinkability), 기밀성(confidentiality)를 만족한다.

<운영요구사항 4>

사용자는 USB타입의 바이오 보안 토큰을 사용함으로 자신의 바이오 인식정보가 밖으로 유출되지 않고 자신의 통제하에 사용될 수 있어 프라이버시 침해요소를 최소화 할 수 있다

<보안요구사항 1>

Alice는 Bob에게 자신의 바이오보안토큰을 이용하여 RA에 등록된 사용자가 본인 임을 3.2의 과정을 통하여 증명할 수 있다.

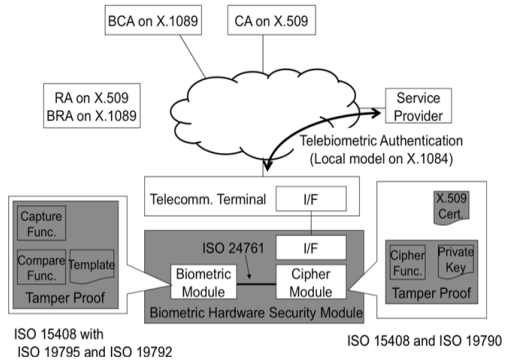
<보안요구사항 2>

Eve가 Alice의 인증서에 있는 PBID를 통해서 BR를 알아낼 수 있다고 한다면, Eve는 해쉬함수 h( )의 역상 공격이 가능한 공격자임을 의미한다. 해쉬함수의 일방향성에 의해서 PBID로부터 BR를 알아내는 방법은 해쉬함수 h( )의 역상 공격을 수행하는 만큼의 막대한 작업시간이 필요하다.

IV. 바이오보안토큰 활용을 위한 표준환경

4.1 바이오보안 토큰을 위한 표준환경

바이오 보안 토큰이 국가인프라에 구축·보급되기 위해서는 그림 5와 같은 다양한 종류의 표준이 고려되



[그림 5] 바이오보안 토큰과 관련된 국제표준

어야 한다. ISO/IEC 24761[13]은 PKI(Public Key Infrastructure) 기술과 PKIX(X.509, Public Key Infrastructure)를 기본으로 하며, 신뢰성 확보와 부인 방지를 위하여 전자서명을 사용한다. X.1089[14]는 바이오인증서 구조를 정의하고 CBEFF(Common Biometric Exchange File Format) 기반 바이오 인식 정보들에 대해 정의하였다. ISO/IEC 19795[15]는 바이오인식시스템의 인식성능에 대한 평가를 다루고 있는데, 바이오 보안 토큰을 이용하는 응용에 있어서도 Alice 본인을 제대로 인식 못하는 오류와 타인을 Alice로 잘못 인식하는 오류에 대한 고려가 필요하며 이에 대한 설명은 상기 표준에 자세히 나와 있다.

제안된 PBID 기법은 PKI 환경을 이용하면서 사용자의 바이오인식 정보에 대한 프라버시를 보호 할 수 있는 구조를 가지고 있으므로 기존의 표준과 연계되어 널리 이용될 수 있는 구조를 가지고 있다[16][17].

4.2 PBID 구현을 위한 표준 포맷

표준에서의 데이터구조를 기술하는데 사용되는 ASN.1은 ITU-T 권고안 X.209 및 X.690에 정의되어 있다. 1988년에 처음 제정되어 1990년, 1994년 그리고 1997에 수정되어 있으며 오늘날에 이르고 있다[8][9]. 앞에서 제안된 PBID에 대한 표준포맷은 국내외 표준[10][11]과의 호환을 고려하여 다음과 같이 정의할 수 있다.

```
PBID ::= SEQUENCE  {
        hashAlg HashAlgorithm,
        vPBID [0] OCTET STRING }
```

```
HashAlgorithm ::=
AlgorithmIdentifier
HashContent ::= SEQUENCE {
BR PrintableString,
randomNum BIT STRING }
```

- hashAlg은 PBID를 생성하는데 사용된 해쉬 알고리즘 및 파라미터를 나타내고 있으며 알고리즘 파라미터는 해당 알고리즘에 따른다.
- vPBID은 3장에서 기술한 방식에 따라 계산된 값으로 HashContent 값을 2회 해쉬하여 계산한다.

HashContent 구조에서 사용되는 구성요소는 다음과 같다.

- BR은 바이오인식정보로 지문, 얼굴, 홍채 등 모달리티에 무관하게 정의할 수 있다. 이들은 숫자열로만 구성되도록 해야 한다.
- randomNum는 난수를 나타낸다.

PBID의 기밀성을 보호하기 위하여, 암호화된 PBID의표준 포맷은 다음과 같이 정의할 수 있다.

```
EncryptedPBID ::= SEQUENCE {
  bidHashAlg [0] PBIDHashAlgorithm
                    OPTIONAL,
  bidEncAlg [1] PBIDEncryptionAlgorithm,
  certID [2] IssuerAndSerialNumber,
  encryptedPBID [3] OCTET STRING }

PBIDHashAlgorithm ::= AlgorithmIdentifier
PBIDEncryptionAlgorithm ::=
                    AlgorithmIdentifier

IssuerAndSerialNumber ::= SEQUENCE {
 issuer Name,
 serialNumber CertificateSerialNumber }

EncryptContent ::= SEQUENCE {
   bid PBID,
   randomNum BIT STRING }
```

EncryptedPBID 구조에서 사용되는 구성요소는 다음과 같다.

- bidHashAlg는 PBID를 생성하는데 사용된 해쉬 알고리즘 및 파라미터를 나타낸다.
- bidEncAlg는 PBID를 암호화하는데 사용된 비대칭 암호알고리즘 및 파라미터를 나타내며 이는 공인인증기관의 인증서에 포함되어 있는 알고리즘과 동일한 알고리즘이어야 한다.
- certID는 PBID를 암호화에 사용된 공인인증기관의 인증서 식별자로 공인인증기관 인증서의 발급자와 공인인증기관 인증서의 일련번호로 구성된다.
- encryptedPBID는 EncryptContent 값을 공인인증기관의 공개키로 암호화한 결과를 나타낸다.

V. 결 론

바이오인식 정보는 개인을 고유하게 식별할 수 있는 개인정보이기 때문에 이에 대한 프라이버시 침해 우려로 인한 적용상의 제한이 있어 왔다. ISO 24745 국제 표준에서는 바이오인식정보 프라이버시 보호의 관점에서 사용자 개인의 통제하에 응용되는 것을 권고하며, 토큰 형태의 장치의 사용을 권하고 있다. 한편, 행정안전부에서는 공인인증서 저장 및 보관방법을 위한 개선책을 마련하여, 공인인증서는 원칙적으로 PC 하드디스크에 보관하지 않고 USB 등 휴대용 저장장치에 보관될 수 있도록 보안토큰의 이용을 강화하고 있다.

그러나 보안토큰에서의 단순한 패스워드 기반의 사용자 인증으로 인하여 부주의나 해킹 등에 의해서 패스워드가 노출되어 개인정보 등이 누출되는 등의 원하지 않는 위험이 발생할 수 있기 때문에 이로 인한 개인정보의 침해가 발생할 수 있다.

이를 극복하기 위해서 본 연구에서 제시한 바이오 보안토큰을 이용한 프라이버시 친화형 개인 인증기법은, 스마트폰을 이용해 취득한 얼굴이나 홍채와 같은 바이오인식 정보와 스마트폰 내의 공인인증서가 결합되는 개인인증 기법에도 다양하게 응용될 수 있으리라 생각된다.

참고문헌

[1] 곽진, 홍순원, 이완석, "보안 토큰의 취약성/보안요구사항 분석 및 CC V3.1기반 보호 프로파일 개발," 정보보호학회논문지 18(2) pp. 139-150, 2008년.

〔2〕 전명근, "바이오 보안 토큰을 위한 표준안 개발," 정보통신표준기술력향상사업 최종보고서, 지식경제부, 방송통신위원회, 2011년.
〔3〕 신용녀, 김영진, 전명근, "바이오보안 토큰과 PKI 연계방안," 한국정보기술학회 논문지, 9,(5), pp. 207-216, 2011년.
〔4〕 한국정보통신기술협회, "바이오보안 토큰용 API: TTAK.KO-12.0165," 정보통신단체표준, 2011년.
〔5〕 이재일, 박종욱, 김승주, 송주석, "X.509 인증서에 포함된 프라이버시 보호기능을 가진 개인 식별 방법," 정보보호학회논문지, 16(5), pp. 59-66, 2006년.
〔6〕 ISO/IEC JTC1 SC27 International Standard 24745, "Biometric Information protection," 2011년.
〔7〕 A. Carlisle, L. Steve, "Understanding PKI: Concepts, Standards, and Deployment Considerrations," 2nd Edition, Addison Wesley, 2003년.
〔8〕 신용녀, 권만준, 이용준, 박진일, 전명근, "개인식별정보와 바이오인식정보의 보호기법," 한국지능시스템학회 논문지 19(2), pp.160-167, 2009년.
〔9〕 권만준, 신용녀, 송창규, 전명근, "재발급 가능한 바이오인식 정보를 이용한 개인인증용 표준 포맷 설계 및 구현," 한국정보기술학회 논문지 9(6), pp.177-188, 2011년.
〔10〕 한국인터넷진흥원, "식별번호를 이용한 본인확인 기술규격," V1.21, 2009년.
〔11〕 IETF RFC 4683, "Internet X.509 Public Key Infrastructure Subject Identification," 2006년.
〔12〕 RSA Laboratories PKCS#10 V1.7, "Certificate Request Syntax Standard," 2000년.
〔13〕 ISO/IEC JTC1 SC27 International Standard 24761- Security techniques-ACBio, Authentication Context for Biometrics, 2009년.
〔14〕 ITU-T International Standard X.1084 "Telebiometric system mechanism - part1 : General biometric authentication protocol and system model profiles for telecommunication systems," 2008년.
〔15〕 ISO/IEC 19795 -Information technology-Biometric performance testing and reporting, 2006년.
〔16〕 신용녀, 김학일, 전명근, "개인정보보호 참조 아키텍처와 국제표준화 동향," 정보보호학회지 21(5), pp. 12-20, 2011년.
〔17〕 한병진, 김학일, 신용녀, 전명근, "바이오인식 표준화 동향- 국제표준화기구를 중심으로," 정보보호학회지 21(2), pp. 61-69, 2011년.

〈著者紹介〉

신 용 녀 (Yong-Nyuo Shin) 정회원
1999년 2월: 숭실대학교 컴퓨터학과 졸업
2001년 9월: 고려대학교 컴퓨터학과 석사
2008년 2월: 고려대학교 컴퓨터학과 박사
2002년 1월~2009년 6월: 한국정보보호진흥원 주임연구원
2009년 7월~2010년 7월: 한국은행 전자금융팀 과장
2010년 9월~현재: 한양사이버대학교 컴퓨터공학과 교수
〈관심분야〉 바이오인식, 프라이버시, 정형기법

전 명 근 (Myung-Geun Chun) 종신회원
1987년 2월: 부산대학교 전자공학과 졸업
1989년 2월: KAIST 전기 및 전자공학과 석사
1993년 2월: KAIST 전기 및 전자공학과 박사
1993년~1996년: 삼성전자 자동화연구소 선임연구원
2000년~2001년: University of Alberta 방문교수
1996년~현재: 충북대학교 전자공학부 교수
2008년~현재: TTA PG505 표준위원회 의장
2007년~현재: ISO/IEC SC27 정보보호표준화전문위원
〈관심분야〉 바이오인식, 개인정보보호, 지능시스템