情 報 保 護 學 會 誌
第18卷 第4號, 2008. 8

JTC1 SC27 바이오 정보보호 국제표준화 동향

문 지 현*

요 약

ISO/IEC JTC1 SC27은 IT 정보보호 및 보안에 관한 국제표준 제정 활동을 하는 국제기구이다. SC27은 다섯 개의 WG으로 구성되어 있는데, 이들 중 WG3와 WG5에서 총 3건의 바이오인식 관련 정보보호 표준화 작업을 수행하고 있다. 19792 바이오인식 보안 평가(Security Evaluation of Biometrics), 24761 바이오인식 인증 컨텍스트(Authentication Context for Biometrics), 24745 바이오 템플릿 보호(Biometric Template Protection)의 세 건이 바로 그것이다. 바이오인식 관련 전문가들의 활동이 적은 SC27에서 바이오인식 기술에 관한 국제표준화가 함께 진행될 수 있었다는 점은 놀라운 일이며, SC37 바이오인식 관련 국제표준 전문가들의 많은 관심을 통해 SC27에서의 바이오인식 관련 국제표준화 활동이 조속한 결실을 맺을 수 있도록 함께 노력해 나가야 할 시점에 있다 하겠다. 본 고에서는 바이오인식 기술의 관점에서의 SC27 국제표준화 활동 내용을 소개하고 현재까지의 진행상황과 앞으로의 일정 및 추진 방향 등을 분석, 정리하여, 관련 전문가들로 하여금 SC27에서의 바이오인식 관련 표준화 활동에 보다 많은 관심을 가질 수 있도록 하는 계기를 마련하고자 한다.

Ⅰ. 서 론

ISO/IEC JTC1 SC27(IT Security Techniques)은 ISO와 IEC가 공동으로 설립한 JTC1의 27번째 위원회로서, 암호화 기술의 국제표준을 담당하던 SC20 (Cryptographic Techniques)의 표준화 기능을 확대 계승하여 만들어진 것이다. 1989년 JTC1 총회에서 설립이 결정되어 1990년 4월 스웨덴에서의 창립총회를 통하여 범위, 조직 등이 갖추어졌다. 일본 도쿄에서의 제2회 회의를 시작으로, 매년 2회의 WG회의와 1회의 총회를 개최하고 있다. 현재 SC27은 36개국의 P-member와 13개국의 O-member들이 활동하고 있으며, 우리나라 전문가들은 1992년부터 P-member로서 SC27-Korea 전문위원회를 통해 활동을 계속해 오고 있다[1].

2005년 이래 SC27은 다섯 개의 WG 체제로 국제표준화를 진행해오고 있다. 그 중 보안 평가 기준을 다루는 WG3와 ID 관리 및 프라이버시 관련 기술을 다루는 WG5에서 바이오인식 보안 평가, 바이오인식 인증 컨텍스트 및 바이오 템플릿 보호의 세 가지 표준화 작업을 진행 중에 있다. 이들 세 가지 표준안은 바이오인식 기술과 밀접한 관계를 가지고 있으며, 따라서 SC37에서 진행하고 있는 용어 및 기술 표준들을 따르고 있는 부분들이 많다.

본 고는 SC27의 바이오인식 관련 세 가지 표준안들의 내용을 기술적인 관점에서 간략히 요약하고 현재까지의 표준화 진행 현황과 앞으로의 방향 등에 대하여 정리하여, 많은 관련 전문가들이 SC27에서의 바이오인식 관련 표준화 활동에 관심을 가질 수 있게 한다.

Ⅱ. 19792 바이오인식 보안 평가(Security Evaluation of Biometrics)[2]

이 국제표준은 표준에 적합한 바이오인식 시스템의 보안 평가 시 다루어져야 될 주제들에 대하여 설명하고 있다, 즉, 바이오인식 시스템 각각의 보안 평가 과정에서 고려되어야 하는 바이오인식에 특화된 특성과 원칙들을 다루고 있는 것이다. 이 표준은 바이오인식 시스템의 보안 평가를 위한 구체적 방법론의 정의를 목적으로 하지 않는 대신 따라야 하는 주요한 요구사항들에 초점을 맞추고 있다. 따라서 이 표준에 있는 요구사항들은 어떠한 구체적인 평가 또는 인증 방법과도 무관하다.

이 국제표준은 바이오인식 시스템의 보안 평가에 사

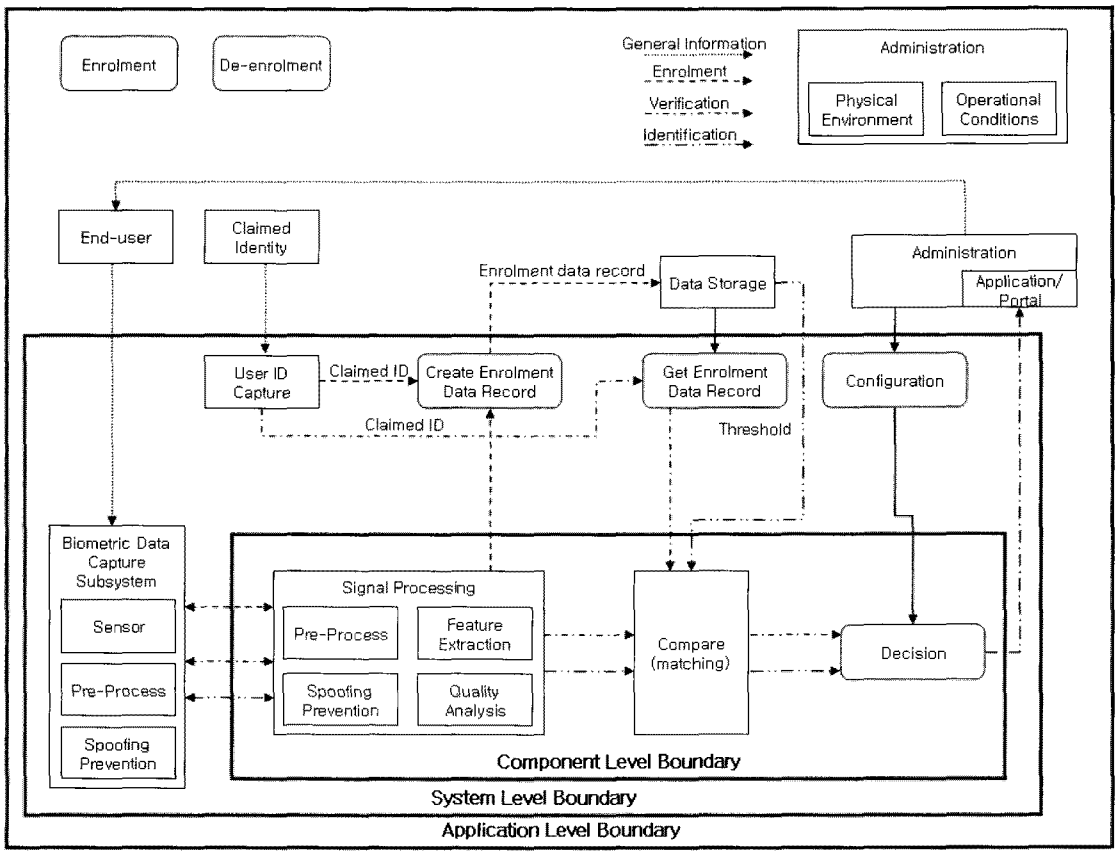
* 한국바이오인식포럼 사무국 간사, 한국정보보호진흥원 보안성평가단 선임연구원 (jhmoon@kisa.or.kr)

용된 용어 정의, 유의어들 전부를 개관한다. 바이오인식 시스템 보안 평가를 위한 전반적인 개념도 소개하고 있으며, 보안에 관련된 에러율의 통계학적 특성, 바이오인식 시스템의 취약성 평가 방법론 및 프라이버시 특성 평가에 대한 내용을 다룬다. 이와 같은 내용들 바탕으로, 이 표준은 평가자들을 위한 일반적인 요구사항들을 정의하고 바이오인식 시스템 보안 평가를 수행하기 위한 가이드라인을 제공하며, 보안 평가를 준비하는데 필요한 바이오인식 보안 평가를 위한 요구사항들을 개발자들에게 알려준다.

특히, 보안 평가를 위해 필요한 것 이외의 내용이 이 표준의 범위에 들어 있지 않기 때문에, 바이오인식 성능 시험 및 보고에 대한 ISO/IEC JTC1 SC37 (Biometrics)의 관련 표준들을 인용하여 사용한다. 이러한 표준들은 바이오인식 보안 평가의 특정 요구사항들을 위하여 필요할 경우 채택되기도 하였다.

[그림 1]은 이 표준에서 사용되고 있는 바이오인식 시스템의 레퍼런스 구조를 보여준다. 이 표준에서 바이오인식 시스템은 하드웨어와 소프트웨어 구성요소들의 모음으로 이루어진다. 운영 환경은 공간, 온도, 습도, 조명 등의 물리적 요인들뿐만 아니라 절차적 특성들 및 시스템 사용자들로 포함하는 것으로 되어 있으며, 시스템 사용자는 운영자, 관리자, 등록자 등과 같이 시스템과 상호작용 할 수 있는 모든 등급의 사람들로 정의된다.

취약성 평가는 개별적 구성요소의 취약성 조사를 포함하여 순차적 방식으로 수행되어야 한다. 그러나 평가자는 다른 시스템 구성요소들 사이에서 일어나는 상호작용에 대한 고려 없이 구성요소의 취약성 평가 결과를 논할 수 없다. 바이오인식 시스템은 시스템 구성요소 사이의 상호작용에 의해 발생되는 크고 작은 본질적 취약성들에 노출이 되기 쉽다. 따라서 평가자는 개별 구성요소의 취약성을 면밀히 살펴야 하며, 이들이 전체 시스템의 취약성 결과에 어떤 영향을 미치는지를 파악하기 위하여 구성요소들 간 상호작용들을 이해하는 것이 필요



〔그림 1〕 19792 Security Evaluation of Biometrics에서의 일반적인 바이오인식 시스템[2]

한 것이다.

이 표준은 바이오인식 시스템에 특화된 보안 평가의 특성들만을 강조한다. 바이오인식 기술 역시 IT 기술의 하나로 분류될 수 있으므로, 바이오인식 시스템의 보안 평가는 분명 IT 보안 평가의 특성을 포함하게 될 것이다. 그러나 그러한 광범위한 특성들은 다루지 않으며, 바이오인식과 관계없는 시스템 보안 평가에 대하여는 Common Criteria(CC)와 같은 다른 IT 보안 평가 표준들과 방법론들을 참고하도록 하고 있다.

이 표준의 7절에서는 바이오인식 시스템 보안 평가에서의 보안 관련 에러율 시험에 관한 개념을 소개한다. 통계학적 에러율은 바이오인식 알고리즘 또는 사용자가 데이터 획득 구성요소의 센서로부터 직접 바이오인식 샘플을 제공받을 수 있는 시스템을 대상으로 계산된다. 바이오인식 알고리즘 시험 시의 에러율은 흔히 다른 알고리즘과의 성능을 비교하는데 사용되며, 알고리즘 개발에 따른 성능 변화를 정량화 하는데도 사용된다. 알고리즘 시험은 보안 평가에서는 제한적일 수밖에 없는데, 그 이유는 알고리즘 에러가 전체 바이오인식 시스템에서 발생 가능한 에러들 중 단지 한 가지일 뿐이기 때문이다. 보통은 시나리오 시험을 통하여 실제 대상자들로부터 취득한 바이오인식 샘플들을 이용한 바이오인식 시스템의 통계학적 에러 측정법을 사용하는 것이 필요하지만, 알고리즘의 통계학적 시험은 바이오인식 시스템의 최대 에러율을 생성하는 시도를 찾거나 시험을 준비하는데 필요한 바이오인식 시스템의 이해에 도움이 될 수 있다.

8절에서는 취약성 평가를 위한 가이드라인을 제공한다. 기술적인 취약성들은 이론적으로 고려되어야 할 사항들과 실제 경험을 기반으로 바이오인식 시스템의 잠재적 취약성에 대응되는 항목에서 다루어진다. 잠재적 취약성의 개발은 전형적으로 다수의 구성요소들을 포함하게 될 것이다. 예를 들면, 위조 가공물이 센서에 의해 수용되어야 할 경우가 생길 것이다. 위조 방지방책들을 다 통과하고 품질 분석 단계로 지나가고 성공적으로 전처리 되어서 특징이 추출되고 계속되는 품질 제어 검사를 통과할 것이다. 이와 같은 단계들은 보통 하나 이상의 시스템 구성요소를 포함하게 될 것이다.

Ⅲ. 24761 바이오인식 인증 컨텍스트(Authentication Context for Biometrics, ACBio)[3]

원격지에서의 바이오인식 검증 과정은 위조한 레퍼런스(reference), 날조된 원시자료, 신뢰성 없는 바이오인식 기기 등과 같은 많은 위험에 노출되어 있다. 어떻게 하면 확인자가 원격지에서 수행되는 바이오인식 검증 과정의 신뢰성을 확인할 수 있을까?

일반적으로, 바이오인식 검증 과정 결과의 신뢰성은 수행된 과정의 보안 레벨과 사용된 바이오인식 기기의 기능적 성능 레벨에 의존한다. 더 좋은 성능 레벨을 가진 기기가 사용된다면 그 결과는 더욱 신뢰성을 갖게 될 것이다. 기기가 안전하지 않거나 과정이 안전하지 않은 환경에서 수행되었다면 그 결과는 신뢰성을 가질 수 없게 될 것이다.

인터넷 환경에서는 보통 바이오인식 검증 과정의 확인자가 사용되는 바이오인식 기기나 원격지에서 사용된 과정들에 대해 직접적으로 알지 못한다. 사용된 바이오인식 기기의 기능적 성능 레벨, 원격 시스템의 보안 레벨, 시스템 내 수행되고 있는 과정이 안전한지 등의 신뢰성 관련 정보를 획득함으로써 확인자는 해당 바이오인식 검증 결과에 더 많은 신뢰도를 부여할 수 있게 된다.

바이오인식 인증 컨텍스트(Authentication Context for Biometrics, ACBio)에 관한 이 국제표준은 사용된 기기와 원격지에서 실행된 과정들에 대한 정보를 확인자에게 보냄으로써 위와 같은 문제에 대한 해결책을 제공한다.

일반적으로, 바이오인식 등록 과정은 데이터 획득, 중간 신호 처리, 최종 신호 처리, 저장과 같은 세부 과정들로 구성된다. 바이오인식 검증 과정은 데이터 획득, 중간 신호 처리, 최종 신호 처리, 저장소 검색, 비교, 결정의 세부 과정들로 구성된다. 보통 세부 과정들은 하나 이상의 바이오인식 프로세싱 단위(Biomertic Processing Unit, BPU)에서 실행되며 각각의 BPU는 고유의 균일한 보안 레벨을 가진다. 몇몇 세부 과정들은 바이오인식 검증 과정에 포함되지만, 저장소 검색을 위한 세부 과정의 보안은 바이오인식 등록 과정에 포함된 세부 과정들과도 관련이 있다.

ACBio는 확인자로 하여금 바이오인식 검증 과정 결과의 신빙성 정도를 결정하는데 도움을 주는 BPU에 대한 인증된 정보를 제공하기 위하여, 센서, 스마트카드, 비교기 등 BPU에 의해 생성되는 보안 데이터를 위한 데이터 포맷을 정의한다. ACBio는 PKI 기술과 PKIX를 기본으로 하며, 신뢰성 확보와 부인방지를 위하여 전자서명을 사용한다. ACBio는 데이터 프라이버시 관련 지역법과 규정에 따르고 동의해야 하는 바이오인식 요

소들의 저장에 관련된 프라이버시 요구사항들을 인정한다. 따라서 ACBio는 요구자로부터 획득한 바이오인식 샘플 또는 비교에 사용되는 바이오인식 레퍼런스와 같은 사적 데이터의 수령 없이도 확인자가 바이오인식 검증 과정의 결과를 확인할 수 있음을 보장한다.

이 표준에서 말하는 ACBio 인스턴스란 XML 인코딩 룰(XER) 또는 흔히 암호용 툴킷 제공업체들로부터 제공되는 ASN.1 기본 인코딩 룰(BER)을 이용하여 인코딩된 보고서이다. 구문은 알고리즘 독립적이며, 데이터 무결성과 데이터 원본 인증을 지원한다. SC27에 명시된 암호화 알고리즘들이 추천되지만 사용에 적합하다면 어떠한 알고리즘도 사용이 가능하다.

ACBio는 BPU 인증기관에서 발급된 BPU 인증서들과 BR 인증기관에서 발급된 BR 인증서들을 사용한다. BR 인증서는 데이터베이스 혹은 스마트카드에서의 바이오인식 레퍼런스 생성 보유에 대해 발급되는 것이다.

3.1 바이오인식 등록 및 검증 과정 모델과 BPU

ACBio의 설계는 다음과 같은 바이오인식 검증 세부 과정들을 기반으로 한다.

3.1.1 데이터 획득(data capture)

이 세부 과정에서는 요구자로부터 바이오인식 정보를 획득하여 이를 원시 바이오인식 샘플로 전환한다. 원시 바이오인식 샘플은 다음 처리를 위하여 중간 신호 처리 세부 과정으로 전송된다.

3.1.2 중간 신호 처리(intermediate signal processing)

이 세부 과정에서는 원시 바이오인식 샘플을 받아 중간 바이오인식 샘플로 변환한다. 중간 바이오인식 샘플은 다음 처리를 위하여 또 다른 중간 신호 처리 세부 과정 또는 최종 신호 처리 세부 과정에 전송된다.

3.1.3 최종 신호 처리(final signal processing)

이 세부 과정은 중간 바이오인식 샘플을 받아 처리된 바이오인식 샘플로 변환한다. 처리된 바이오인식 샘플은 검증을 위한 비교 세부 과정 또는 등록을 위한 저장 세부 과정 중 하나로 전송된다.

3.1.4 저장(storage)

이 세부 과정은 원시 바이오인식 레퍼런스, 중간 바이오인식 레퍼런스 또는 처리된 바이오인식 레퍼런스의 세 가지 중 하나의 형태로 바이오인식 레퍼런스를 저장한다. 이렇게 저장된 바이오인식 레퍼런스는 검증을 위해 바이오인식 샘플과 비교될 것이다.

3.1.5 비교(comparison)

이 세부 과정에서는 요구자로부터 획득한 바이오인식 샘플과 (처리를 했거나 하지 않은 상태의) 바이오인식 레퍼런스를 받는다. 이 세부 과정은 바이오인식 샘플과 처리된 바이오인식 레퍼런스를 비교하여 (소위 비교 점수라 불리는) 유사도를 계산한다. 비교 점수는 판단 세부 과정에 전송된다.

3.1.6 판단(decision)

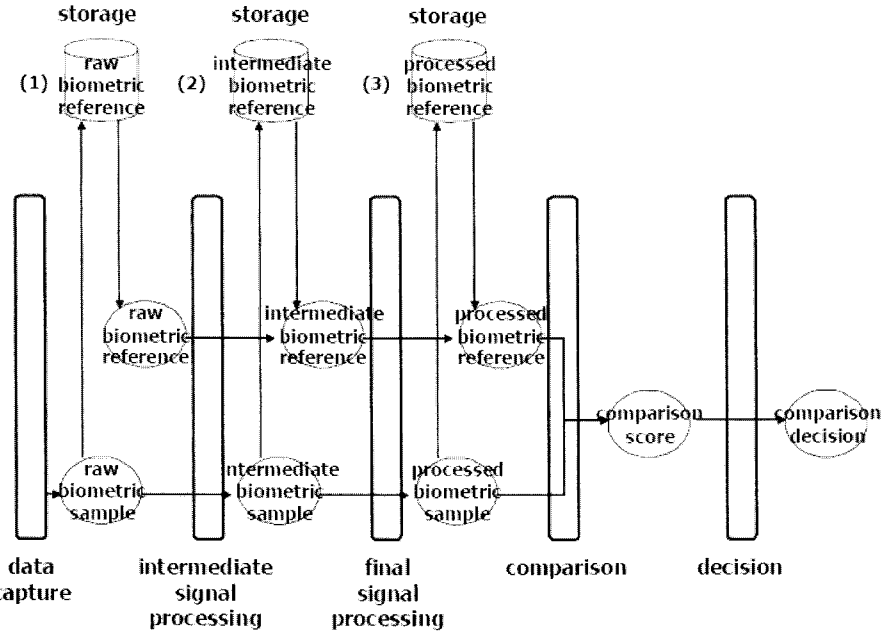
이 세부과정은 비교 세부 과정으로부터 비교 점수를 받아, 사용되고 있는 보안 정책에 의해 결정된 룰에 따라 그 점수를 평가하고, 요구자 신원의 유효성을 결정하고, 비교 결과 및 정합/부정합 등의 결과를 확인자에게 보여준다.

다음의 [그림 2]는 저장 세부 과정에서 무엇을 저장하는지- 원시 바이오인식 샘플, 중간 바이오인식 샘플, 최종 바이오인식 샘플 중 하나가 될 것이다. -에 따른 세 가지 바이오인식 검증 과정 모델들을 보여준다.

ACBio는 확인자에게 바이오인식 검증 과정의 신뢰성 레벨에 관한 정보를 준다. 이 절에서는 비교 결과를 보여주는 BPU 생산 과정과 바이오인식 레퍼런스를 생산하는 BPU 등록 과정에서 준비되어야 할 것들에 대하여 설명하고, ACBio 인스턴스가 이러한 과정들에서 어떻게 만들어지며 바이오인식 검증이 어떻게 확인되는지에 대하여 정리한다.

3.2 ACBio 활용을 위한 준비

ACBio를 이용한 바이오인식 검증 과정 확인을 위하여, 요구자의 바이오인식 레퍼런스를 획득하고 저장하는 것 이외의 준비가 필요하다. ACBio 사용을 위한 일

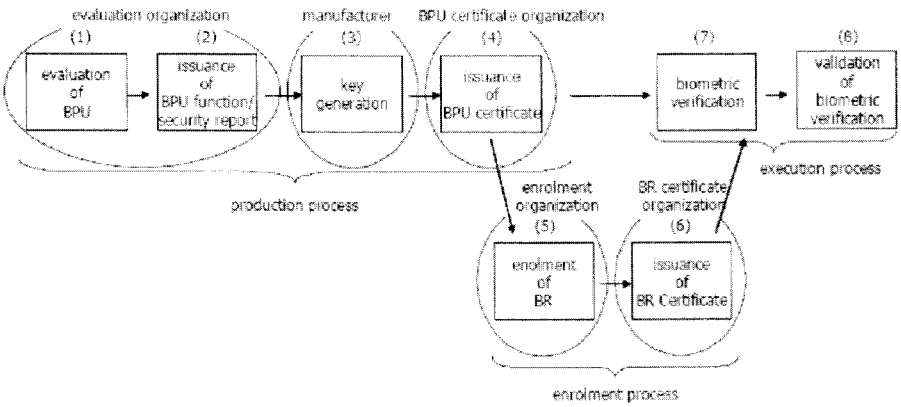


〔그림 2〕 24761 Authentication Context for Biometrics에서의 바이오인식 검증 과정 모델[3]

련의 준비 작업들은 [그림 3]과 같으며 생산/등록 과정과 뒤이어 일어나는 검증 과정으로 나뉘어 진다.

3.2.1 생산 과정에서의 준비

단일 BPU 내 각 기능의 보안 레벨과 기능적 성능 레벨은 하나 또는 그 이상의 평가 기관에 의해 평가되며, 평가기관으로는 해당 제품-BPU를 구성하는 소프트웨어 또는 하드웨어를 말한다.-의 생산자를 포함할 수 있다. 평가 후에는 평가기관으로부터 BPU 기능보고서와 BPU 보안보고서가 발급되는데, 이 두 가지 보고서가 합쳐져서 BPU 보고서를 구성한다. BPU를 구성하는 제품의 생산자는 BPU에 따른 키(쌍), 대칭 암호화 시스템의 키 또는 비대칭키 암호화 시스템의 키를 각 BPU에 대하여 생성해야 한다. 키는 인증 받은 것이어야 하며, BPU 인증서는 BPU 인증기관에 의해 발급된 것이어야 한다. BPU 보고서 또는 그에 대한 레퍼런스, BPU 인증서 또는 그에 대한 레퍼런스, 그리고 키는 BPU 결과가 전달되기 전에 각각의 BPU 보고서 안에 저장되어야 한다. 각 BPU는 전자서명 또는 메시지 인증 코드를 생성



〔그림 3〕 ACBio 사용을 위한 준비와 바이오인식 검증 실행 과정[2]

할 수 있는 수단을 가지고 있어야 하며, 이로써 확인자는 ACBio 인스턴스의 무결성을 확인할 수 있게 된다.

3.1.2 등록 과정에서의 준비

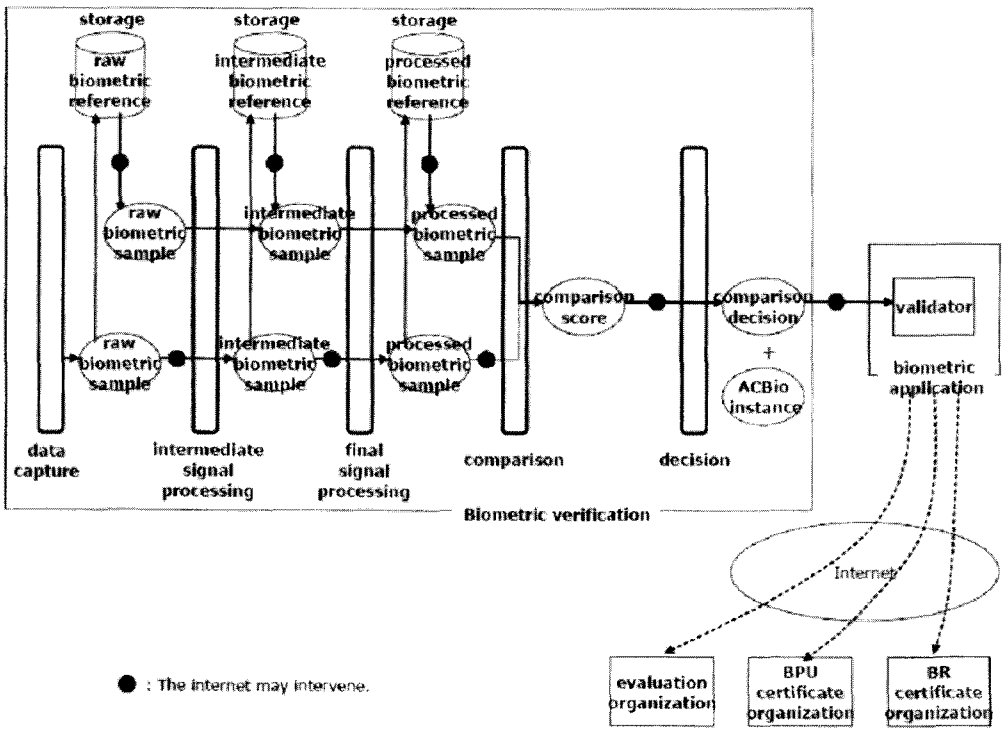
바이오인식 검증을 위하여, 바이오인식 레퍼런스는 등록 기관에 앞서 등록이 되어 있어야 하며, 바이오인식 검증 과정의 유효성 검사를 위한 ACBio 사용을 위하여, 바이오인식 레퍼런스 인증서(BR 인증서)가 BR 인증기관으로부터 발급되어야 한다. BR 인증서 또는 그에 대한 레퍼런스는 인증된 바이오인식 레퍼런스가 저장되는 BPU 내에 저장되어야 한다.

3.3 바이오인식 검증과 ACBio

[그림 4]는 [그림 3]의 (7)과 (8) 부분을 자세히 나타낸 것이다. 바이오인식 검증 과정에서 각각의 BPU는 BPU 인증서 정보, BPU 보고서 정보 및 BR 인증서 정보를 담은 ACBio 인스턴스를 채워야 한다. ACBioContentInformation이라는 데이터 타입은 확인자로부터의 값인 제어값과 BPU를 통한 입출력 바이오인식 데이터를 해쉬한 값을 포함해야 한다. ACBioContentInformation 값은 확인자로 하여금 BPU 간의 바이오인식 데이터 전송의 일관성을 확인할 수 있게 해 준다. ACBioContentInformation에 BPU 키를 이용한 전자서명 또는 메시지 인증 코드 등을 추가함으로써 하나의 ACBio 인스턴스가 생성된다.

3.4 ACBio를 이용한 바이오인식 검증 과정의 유효성 검사

이러한 ACBio 프레임워크를 통하여, 확인자는 비교 결과, 바이오인식 검증 결과뿐만 아니라 수행된 바이오인식 검증 결과를 유효성을 확인할 수 있는 ACBio 인스턴스도 얻게 된다. 확인자는 BPU 인증서에 있는 전자서명 혹은 메시지 인증 코드를 확인함으로써 ACBio 인스턴스의 확실성과 무결성을 확인할 수 있다. 확인자는 BPU 보고서에 따라 BPU의 보안 레벨과 기능적 성능 레벨을 알 수 있게 되고, BR 인증서에 따라 바이오인식 검증 과정에서 사용된 바이오인식 레퍼런스의 확



[그림 4] 바이오인식 검증 과정 및 그의 유효성 검사[3]

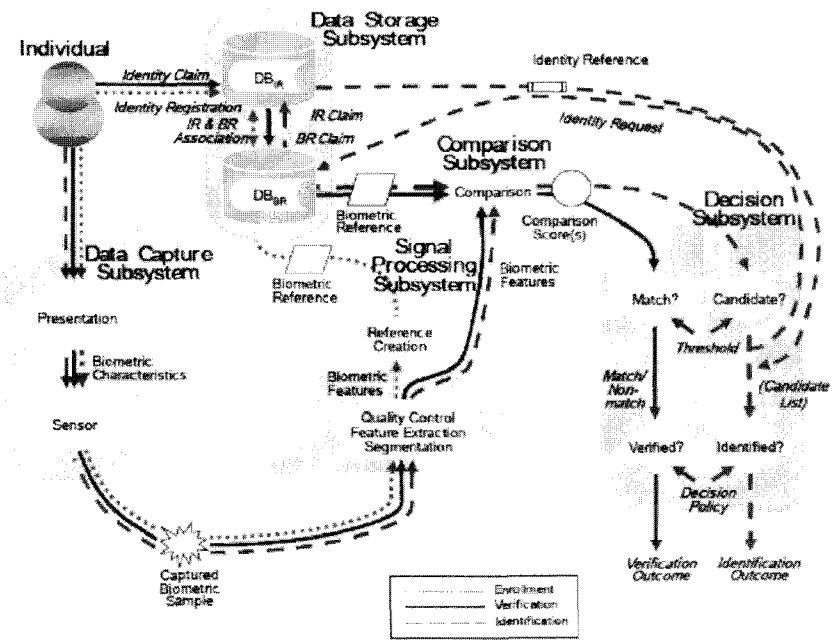
실성도 알 수 있게 된다. 또한, 확인자는 바이오인식 프로세스 블록과 ACBio 인스턴스 내의 제어값을 각각 확인함으로써 BPU 간 및 확인자와 바이오인식 검증 과정 간 통신의 일관성을 확인할 수 있다. 이러한 모든 것들을 통하여, 확인자는 해당 바이오인식 검증 결과의 신뢰도 레벨을 결정할 수 있게 된다. 필요한 경우, 확인자는 BPU 인증기관, 평가기관, BR 인정기관 등의 유관기관과의 연계가 가능하다.

Ⅳ. 24745 바이오 템플릿 보호(Biometric Template Protection)[4]

이 표준은 바이오인식 템플릿(Biometric Template)을 사용하는 바이오인식 시스템에서 템플릿을 보호하기 위하여 필요한 보안 특성을 정의한다. 또한, 바이오인식 레퍼런스가 개인정보와의 관계에서 발생 가능한 보안상 취약성들을 분석하고, 바이오인식 시스템 활용에 있어서의 바이오 템플릿 프라이버시에 대하여 설명한다. 아직 WD 단계이기 때문에 용어의 정의와 바이오 정보 보호를 위한 전체적인 프레임워크가 확고히 세워지지 않은 표준안으로, SC27에서의 표준화 목적에 맞게 내용의 일부가 수정 또는 변경 되어야 하는 작업이 필요한 문건이다. 24745 표준안은 다루고자 하는 바이오인식 시스템의 개요를 시작으로, 바이오인식 템플릿 사용 시 보안상 취약점이 발생할 수 있는 시스템적 요소들을 분석하는 방향으로 내용을 전개하고 있다. 또한 바이오인식 레퍼런스와 바이오인식 템플릿을 구분하면서, 각각이 담고 있는 정보의 특성에 따른 보안상 고려해야 될 사항들을 자세히 설명하고 있다. [그림 5]는 이 표준에서 다루고자 하는 바이오인식 시스템 개념도이다. SC37에서의 기본적 바이오인식 시스템 개념도를 정보보호의 관점에서 재해석하여 본 표준의 목적에 맞게 다시 그린 것이라 할 수 있다.

Ⅴ. 결 론

19792 바이오인식 보안 평가 표준은 2003년 WD가 제출된 이후 지금까지 꾸준히 작업이 진행되어, 2008년 현재 2nd FCD 단계에 접어들었다. 가장 최근에 있었던 2008년 4월 교토회의에서는 특별히 별도의 editorial session을 만들어서 회의가 진행되었다. 가장 길게 논의가 되었던 부분은 SC37에서의 liaison 의견과 용어들을 수정, 반영하는 것이었다. SC27은 정보보호나 암호화에 관련된 전문가들이 대부분이어서 바이오인식 기술과 그의 표준화 현황에 대한 전문가의 활동이 많지 않은 실정이다. 이와 같은 어려운 조건에서도 이 국제표준은



[그림 5] 24745 바이오 템플릿 보호에서의 바이오인식 시스템 개념적 구조도[4]

5년 이상의 긴 시간을 작업한 끝에 이제 곧 FDIS 단계를 눈앞에 두고 있다.

24761 바이오인식 인증 컨텍스트 표준은 2008년 4월 교토회의 결과 FDIS로 상태가 상향되었다. 이제 곧 IS로의 완료를 눈앞에 두고 있는 것이다. 19792 바이오인식 보안 평가 표준의 에디터가 SC27의 SC37 liaison officer인 것과 마찬가지로, 24761 표준의 에디터 역시 SC37 WG2에서 CBEFF 관련 표준화 활동을 병행하고 있다. 24761 표준의 IS 완료를 끝으로 SC37에서의 표준화 활동에 전념하겠다는 에디터를 2008년 7월 SC37 부산회의에서 다시 만날 수 있었다.

24745 바이오 템플릿 보호 표준은 2004년 NWI으로 제안된 이래 지금까지 그 진행이 미진했었다. 최초의 표준화 목적을 약간 벗어났다가[5], 올해 4월 교토회의에서 원래의 표준화 목적과 추진 범위를 살려 다시 진행할 것을 확인하였다. 24745 표준은 특히 세 에디터 모두 한국대표들로 구성되어 있다는 점을 주목할 만하다. 교토회의 이후 세 번째 WD가 제출되어 있는 상태이며, 9월 중순까지 검토의견을 수렴하여 차기 회의에서 수정, 반영될 예정이다.

이와 같이, 바이오인식 기술이 개인인증을 위한 수단일 뿐만 아니라 개인의 민감함 정보를 보호하고 현존하는 인증기반을 대체할 수 있는 중요한 기술로 여겨지고 있는 지금, 많은 융합기술 및 응용기술들에서 다양한 방법으로 접목되어 사용되고 있는 것이 현실이다. 전자여권을 위한 국제표준에서도 바이오인식 기술에 관한 부분을 다루고 있으며, HCI 로봇과 같은 응용분야에서도 바이오인식 기술을 이용한 다양한 제품들이 속속 선을 보이고 있다. 따라서 이제는 바이오인식 기술 자체의 개발 및 표준화뿐만 아니라 보다 다양하고 개발 가능성이 큰 융합기술 중 하나로서의 바이오인식 기술의 표준화에 대하여도 관심을 가질 필요가 있다. 이는 바이오인식 기술의 무한한 발전 가능성과 응용 잠재력을 부각시켜, 관련 산업을 발전시킬 수 있는 긍정적인 원동력이 될 수 있다는 점에서 그 중요성이 크다 하겠다.

참고문헌

[1] ISO/IEC JTC1 SC27 Standardization Activities, http://www.iso.org/

[2] ISO/IEC FCD 19792, Information Technology - Security techniques - Security evaluation of biometrics, SC27N6652 FCD 19792 Jun2008.zip

[3] ISO/IEC FCD 24761, Information Technology - Security techniques - Authentication context for biometrics, SC27N6590 FCD 24761 Apr2008.zip

[4] ISO/IEC 3rd WD 24745, Information Technology - Security techniques - Biometric template protection, SC27N6755 3rdWD 24745 20080630.zip

[5] Status Report on project 24745 on "Biomtric template protection", SC27N6539 Late KR comm status report 24745 N6314.pdf

〈著者紹介〉

문 지 현 (Ji-Hyun Moon)
정회원

1999년 2월 : 인하대학교 항공우주·자동화공학군 졸업
2007년 2월 : 인하대학교 정보통신공학과 대학원 박사
2007년 1월~현재 : 한국정보보호진흥원 보안성평가단 선임연구원
2004년 6월~현재 : SC37(바이오인식) 한국대표단
2006년 1월~현재 : TTA IT 국제표준전문가
2007년 1월~현재 : 한국바이오인식포럼 사무국 간사
2008년 4월~현재 : SC27 24745 co-editor
<관심분야> 바이오인식, 정보보호, 국제표준화활동