情 報 保 護 學 會 誌
第17卷 第5號, 2007. 10

BIP, X.tsm 국제표준간 통합모델 제시

신용녀*, 김재성*, 최진영**

요 약

X.tsm은 템플릿 관리 위치와 바이오인식 인증 위치에 따라 9개의 모델을 제시한 바이오 인증 프로토콜로, 2006년 12월 제네바ITU-T SG17 Q.8 회의에서 First of Recomanda- tion 단계로 채택된 표준이다[1].

바이오인식 제품 응용 인터페이스(BioAPI)에 입각하여 6개의 모델을 제시한 BIP(BioAPI Interworking Protocol)은 2007년 1월 뉴질랜드 ISO/IEC JTC1 SC37 WG2 회의에서 FCD로 제정된 국제표준이다[5].

X.tsm과 BIP간의 중복성 문제가 제기됨에 따라 ITU-T SG17 Q8(Telebiometrics)에서 2006년 4월 제주에서 두 표준과제의 공통사항을 반영한 X.bip가 채택되어 표준화가 진행되고 있다. 이 논문에서는 바이오 주요 컴포넌트의 개념을 명확하고, 모델 간 중복성을 제거하기 위해 13개의 새로운 모델을 제안한다. 두 표준에서 새로운 모델을 공통적으로 수용하게 되면, 표준안을 준용하는 사용자 입장에서 구현을 용이하게 할 수 있다.

Ⅰ. 서 론

BioAPI[4]는 바이오인식기술 전 분야에 적용 가능한 응용프로그램 인터페이스를 제공하기 위해 2002년 2월 BioAPI 컨소시엄에서 BioAPI V1.1이 개발되었다. BioAPI 컨소시엄을 통하여 여러 가지 다양한 인터페이스 규격을 고려한 단체표준이 마련되었으며 NIST를 통하여 M1 표준으로 인정받아 ANSI 표준으로 제정되었으며, 그 이후에 ISO/IEC JTC1/SC37이 구성되는 시점에서 Fast Track으로 각 국의 의견을 종합하여 BioAPI V2.0(19784-1)이 2006년 5월에 IS(국제표준)으로 제정되었다. BioAPI 표준을 준용하는 제품이 생산되게 될 경우에는 그 제품의 구현이 제대로 된 것인가에 대한 적합성 시험이 필요하게 된다. 제품 개발 초기에 적합성 시험방법 및 절차 표준을 사용하여 표준 규격의 준용여부를 검사하고 개발한다면, 시간과 비용에서의 절감 효과뿐만 아니라 표준 규격을 준용한 제품이라는 신뢰성을 주게 된다. BIP(BioAPI Interworking Protocol)은 본질적으로 BioAPI 프레임워크 간 통신을 명세한 표준이다. BIP는 PC 내 수행되는 BioAPI 어플리케이션이 다른 PC에서 수행되고 있는 원격 BSP를 사용할 수 있게 한다. X.tsm(telebio- metrics system mechanism)은 9개의 인증 모델을 제시하여, 각 모델별 위협을 제시하고 이를 해결하기 위한 바이오인식기술과 데이터를 활용한 PKI 인증 모델과 TLS 프로토콜을 제시한 표준이다. 이 논문에서는 ISO/IEC JTC1 SC37에서 표준화 되고 있는 BIP와 ITU-T SG17 Q8 X.tsm 표준에서 제시하고 있는 모델에 대한 비교·분석을 통하여 새로운 모델을 제시하고자 한다.

Ⅱ. BIP 표준

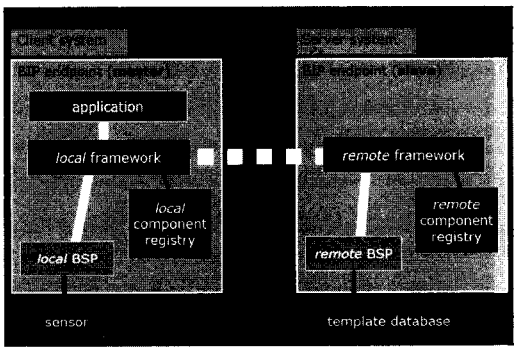
2.1. 개요

BioAPI 상호작용 프로토콜(BIP : BioAPI Interworking Protocol)은 ISO/IEC JTC1 SC37 WG2에서 CD(Committee Draft) 단계에 있는 표준이다. 바이오인식 제품 응용 인터페이스(BioAPI)에 입각하여 6개의 모델을 제시한 바이오

* 한국정보보호 진흥원 (ynshin@kisa.or.kr), (kimjs@kisa.or.kr)
** 고려대학교 (choi@formal.korea.ac.kr)

정보 통신 프로토콜로, BioAPI에 적합한 어플리케이션이 다른 PC에서 작동하고 있는 BSP를 사용하기 위해 메시지들을 정의하고 있다. 바이오인식데이터블럭(BDB), 바이오인식정보레코드(BIP), 매칭 알고리즘, 보안메커니즘 정의, 바이오인식 시스템 분류, 바이오인식 시스템 측정, 바이오인식 시스템상의 요구사항은 해당사항이 없다. BIP 모델은 [Figure 3]과 같은데, BIP endpoint는 Master도 될 수 있고, Slave도 될 수 있다.

BIP 표준에서는 BIP 구현물에 대한 적합성 시험을 적합성 레벨과 역할에 따라 구분하는 기준을 [Table 1]과 같이 제시하고 있다.



[Figure. 1]. 기본 BIP 모델

Table 1 – Conformance classes

		Conformance level	
		level 1 (generic BIP entity)	level 2 (BIP-enabled framework)
Role capability class	master-role-capable	master-role-capable generic BIP entity	master-role-capable BIP-enabled framework
	slave-role-capable	slave-role-capable generic BIP entity	slave-role-capable BIP-enabled framework
	dual-role-capable	dual-role-capable generic BIP entity	dual-role-capable BIP-enabled framework

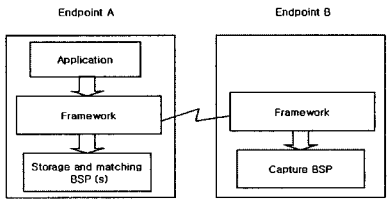
Level 1은 프레임워크가 없는 경우를 말한다. 예를 들어, BIP endpoint가 있는데 이 endpoint는 센서만 달려있고, 센서를 구동하는 드라이버 같은 소프트웨어에 프레임워크가 하는 기능이 포함되고 BIP 통신하는 모듈이 들어있는 경우를 말한다. Level 2는 BioAPI 프레임워크가 있는 경우를 말한다. Level 2에 대해서는 모델만 제시되어 있고 실제 구현된 모델에 대해서는 제시되어 있지 않다. 역할구분(Role capability class)은 Master 역할을 하는지, Slave 역할을 하는지 아니면 두 역할을 다하는 건지를 구분 하는것을 말한다. 예를 들어, Slave-role-capable generic BIP entity는 적합성 테스트를 한다면, BIP 기능이 있는 제품인데 네트워크 기능이 되고 BioAPI 프레임워크 설치 안해도 되는 제품에 대해서 이 제품이 slave 역할에 필요한 메시지 생성이나 기능을 하는지를 테스트 하는 것이다.

Table 2 – Conformance testing

Conformance class	BioAPI API	BioSPI API	Messaging interface
master-role-capable generic BIP entity			X
slave-role-capable generic BIP entity			X
dual-role-capable generic BIP entity			X
master-role-capable BIP-enabled framework	X		X
slave-role-capable BIP-enabled framework		X	X
dual-role-capable BIP-enabled framework	X	X	X

[Table 2]에서는 [Table 1]의 적합성 분류에 따라 시험에 필요한 항목을 보여주고 있다. 메시징 인터페이스는 BIP 메시지 생성 및 전송에 필요하기 때문에 클래스(Class) 별 시험에 다 포함된 것이다. master-role-capable BIP-enabled framework에 BioAPI API가 포함되는 것은 적합성 시험에 BioAPI 프레임워크가 포함되고, 프레임워크의 상위 응용계층에서 BioAPI API 호출하는 것이 포함되기 때문이다. Master 기능을 시험할 때는 BSP를 호출하는 BioSPI를 호출하는 경우는 표준에 없다. 마찬가지로 slave-role-capable BIP-enabled framework에는 slave 기능에서 BioAPI 프레임워크 상부의 응용이 BioAPI API를 호출하는 경우가 없어서 포함되어 있지 않다. dual-role-capable인 경우는 Master, Slave 기능을 다 수행해야 하므로 BioAPI와 BioSPI가 다 포함된다.

BIP 프로토콜을 사용하여 가능한 시스템 구성을 [Figure 2]에서 볼 수 있다. BIP 표준에서는 6개의 모델을 제시하고 있다. EndPoint A에서 어플리케이션은 원격의 Capture 기능을 하는 BSP와 통신한다. 이를 제외한 모든 기능들은 endpoint A에서 수행된다.



[Figure. 2] BIP로 가능한 시스템 구성 예

1. EndPoint A에서 어플리케이션은 원격의 캡처 기능을 하는 BSP와 통신하는 경우
2. EndPoint A에서 어플리케이션은 저장 BSP를 호출하고 캡처와 매칭을 위해서는 원격 BSP와 통신하는 경우
3. 저장을 위한 BSP만을 원격으로 통신하고, 모든 다른 기능은 EndPoint A에서 수행하는 경우
4. Endpoint A에 로컬 센서가 구동되고, 저장과 매칭 BSP는 원격으로 수행하는 경우
5. 저장과 매칭 기능을 제공하는 것과 캡처를 제공하는 두 원격 BSP와 통신하는 경우
6. 저장을 제공하는 것과 캡처와 매칭을 제공하는 두 원격 BSP와 통신하는 경우

2.2. BIP 구조

BIP의 중점은 BIP-enable 프레임워크, BIP 메시지, BIP endpoint, BIP 링크, Master/Slave endpoint 그리고 전송 프로토콜 바인딩의 개념이며, 거기에 BSP나 로컬 응용과 같은 BioAPI 개념이 추가된다. BIP의 목적 중 하나는 BioAPI 응용을 로컬 BSP와 같은 방식으로 원격 BSP를 사용하는 것이다. 로컬 BSP는 BioAPI 프레임워크의 BioAPI API를 통해 등록된 컴포넌트를 모두 사용할 수 있지만, 원격 BSP는 원격 BioAPI 프레임워크의 등록된 컴포넌트에서 제공하는 스키마만을 사용할 수 있다. 로컬 프레임워크의 BioAPI API를 통한 원격 BSP의 접근은 불가능 하지만, BIP를 사용하면 가능하다. BIP 메시지는 두 개의 BIP-enabled 프레임워크 사이의 교환되는 메시지의 집합, BioAPI 함수 호출, callback 사이의 관계에 있어 메시지의 생성과 처리에 대한 정확한 규칙을 나열한 것이다. 최상계층에는 요청, 응답, 알림, 승인의 선택적인 메시지가 있으며, 네 종류의 메시지는 링크번호와 응답번호 또는 알림의 순서 번호를 가지고 있다. BIP에 있어 링크번호와 순서번호의 목적은 응답과 승인을 쉽게 하기 위함이다. BIP endpoint은 개념적인 실시간 소프트웨어 개체이며, BIP endpoint는 BIP 링크를 통해 다른 BIP endpoint로 BIP 메시지를 전송한다.

BIP 메시지의 교환을 제공하는 실행중인 두 BIP-enabled 프레임워크 사이의 논리적 연결이 BIP 링크이다. 이 표준에 있어 '전송' 은 BIP endpoint(전송자)로부터 전송 endpoint와 수신 endpoint 사이의 BIP 링크까지 BIP 메시지의 개념적 전송을 의미하고, '수신'의 의미는 BIP 링크에서 수신 BIP endpoint까지 BIP 메시지의 개념적 수신을 의미한다. 메시지가 전송되면 수신의 결과로서 링크에서 제거된다. master endpoint는 요청 BIP 메시지만 보낼 수 있고, acknowledgement BIP 메시지는 링크를 거치며, slave endpoint는 응답 BIP 메시지만 보낼 수 있고, notification BIP 메시지는 링크를 통과한다. BIP 링크는 항상 BIP endpoint에 의해 생성된다. 전송 프로토콜 바인딩은 링크 채널의 물리적 현실화이다.

BIP 링크는 요청/응답 채널을 가지고 있으나 통지(notification)/수락(acknowledgement) 링크 채널은 가지거나 그렇지 않을 수 있다.

BIP 링크는 BIP-enabled 프레임워크에 의해 생성된다. BIP의 생성은 두 가지 관점에서 발생한다. 하나는 전송계층 연결이 전송 프로토콜 바인딩에 따라 새로운 BIP 링크의 각 채널을 정하는 것이고, 두 번째는 master 프레임워크가 addMaster 요청 BIP 메시지를 slave endpoint에 보낼 때이다.

BIP 링크의 파괴 또한 두 가지 관점에서 발생한다. 첫 번째는 deleteMater 요청 BIP 메시지를 mater에 따른 MasterEndpoints 테이블 개체의 삭제가 발생한 것으로부터 slave에 의해 수신될 때이며, 두 번째는 master가 링크의 채널에 따라 전송계층 연결을 파괴할 때이다.

Ⅲ. X.tsm 표준

3.1. 개요

X.tsm(telebiometrics system mechanism)은 telecommunication 시스템에 프로파일과 바이오인증 프로토콜을 제공한다. 개방형 네트워크상에서 불특정 다수의 사용자와 서비스 제공자를 위한 바이오 인증 프로토콜을 정의하고 있다. 템플릿 관리 위치와 바이오인식 인증 위치에 따라 9개의 모델을 제시한 바이오 인증 프로토콜로, ITU-T SG17 Q.8에서 First of Recommendation 단계에 있는 표준이다. 빠르고 광범위하게 보급된 인터넷은 다양한 네트워크 서비스들이 제공하고 있다. 인터넷뱅킹, 인터넷쇼핑, 인터넷거래 등과 같은 고부가가치 서비스들은 피싱에 의해 얻어진 PIN에 의해 불법적 거래가 현실화 되었다. 그러므로 바이오인식과 같은 고도의 보안인증 메커니즘이 필요하게 되었다.

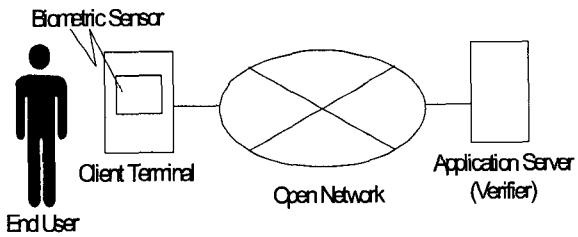
인터넷 상의 바이오인증 표준은 아래와 같은 문제점들이 있다.

- 사용자측 바이오인식 장치, 보안레벨, 작동방법 등의 정보가 서비스제공자들에게 없음
- 각 바이오인식제품의 정확성(FAR)은 자체 threshold 변수에 따라 결정되기에 서비스제공자는 통일된 정확도를 제공할 수 없음
- 바이오인증의 정확도는 바이오인식이 신체의 형태를 이용하기 때문에 사용자의 연령에 따라 변화함

이러한 문제점의 해결책으로 개방형 네트워크에서 사용자와 서비스제공자간에 데이터포맷 전제조건(템플릿, 입력장치인증 등)의 프로파일과 바이오인증 프로토콜이 필요하다.

3.2 범위

X.tsm은 비대면 개방형 네트워크에서 사용자 인증인 바이오 보안메커니즘을 위한 권고안이다. X.tsm에서는 개방형 네트워크를 [Figure. 3]과 같이 정의하고 있다.



〔Figure. 3〕 개방형 네트워크

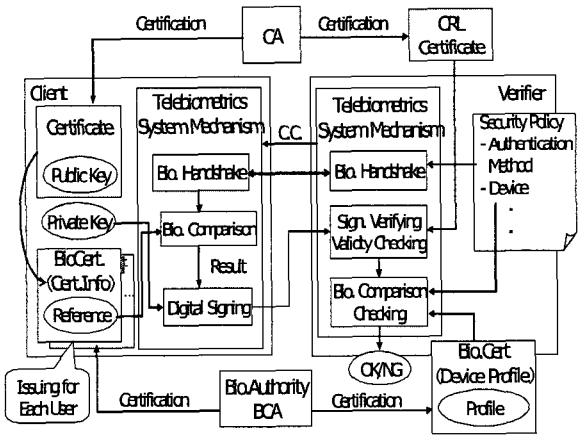
- 불특정다수 검증기(verifier)는 네트워크에 연결되어 있고 다양한 형태의 바이오인식 방법들을 사용
- 불특정다수의 사용자 또한 네트워크에 연결되어있고, 바이오인증을 통해 신원을 확인받으며 고부가가치, 효과적인 정부, 온라인 쇼핑 서비스 제공자에게서 서비스를 제공받음

바이오인증의 사용 요점은 각 검증기에 의해 결정되며, 검증기의 위험/가치 또한 다르다. 검증기는 각기 다른 인증 보안 정책, 수용성 그리고 개인정보 보호정책을 가지고 있다.

3.3 X.tsm 전제조건

X.tsm은 [Figure 4]과 같은 전제조건을 만족해야한다[3][4].

- TTP(Trusted Third Party)는 사용자의 공개키를 인증할 수 있어야 하며, 인증서를 발급할 수 있어야 한다.
- TTP는 인증을 위해 각 바이오인식 기술의 threshold와 평가결과의 정확성을 인증할 수 있어야 하며, 인증을 위해 서명이 필요하다.
- TTP는 CC에 근거하여 안전한 평가가 이루어졌는지 인증할 수 있어야 하며, 인증을 위해 서명이 필요하다.
- 모델에 따라 TTP는 바이오인식 등록 정보를 관리할 필요가 있다.
- 모델에 따라 TTP는 바이오인식 비교 기능을 수행할 필요가 있다.



〔Figure. 4〕 X.tsm의 전제조건

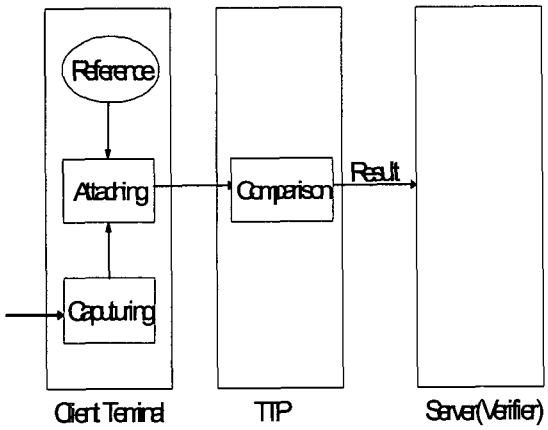
3.4. X.tsm 9 모델

[Table 3]에서는 클라이언트, 서버, TTP별로 바이오 참조 템플릿 관리 위치 및 비교 위치에 대해 인증 모델을 제시하고 있다. Local 모델에서는 클라이언트 측에서 캡처한 데이터와 참조 데이터간의 비교를 수행해 서버 측으로 결과 값을 넘겨준다.

Download 모델은 참조 데이터를 클라이언트 측으로 다운로드 받아 캡처한 데이터와 비교를 수행해 서버 측으로 결과 값을 넘겨준다. [Figure. 5]은 Client 모델에 의한 비교 아웃소싱을 보여준다.

〔Table 3〕 인증 모델

Management / Comparison	Client	Server	TTP
Client	Local	Download	Reference management on TTP for Client comparison
Server	Attached	Center	Reference management on TTP for Server comparison
TTP	Comparison Outsourcing by Client	Comparison Outsourcing by Server	Storage & comparison Outsourcing



〔Figure. 5〕 Client 모델에 의한 비교 아웃소싱 모델

Ⅳ. BIP와 X.tsm 비교

4.1. 개요

BIP는 네트워크상의 상호작용을 위한 BioAPI 프레임워크를 확장한 것으로, 개별적 노드와 프로세스간의 원격 BSP간의 통신 및 상호작용을 보여주고 있다. 그에 반해 X.tsm은 암호화기술을 위해 X.509 프레임워크와 통합으로, telebiometric 시스템을 위해 바이오인식 명세를 제공한다. BIP는 메시지 생성, 처리, 전송, 수신 등의 BioAPI 프레임워크의 구조의 확장을 명세하였으나, Biometric Data Block이나 BIR은 포함하고 있지 않다. X.tsm에서는 9가지 TSM 모델을 제시, 각 모델에 대한 위험분석, TLS상의 telebiometric 시스템 내 데이터 프로토콜과 Flow를 정의, 서버와 클라이언트 정책 사이의 협상을 위한 바이오인식 핸드세이크, 바이오 인식시스템이 PKI와 연계하기 위한 템플릿 포맷을 정의 등을 포함하고 있다. BIP에는 보안 매커니즘은 정의되어 있지 않으나, BIP endpoint간 안전한 정보 전송을 위한 SOAP/HTTP와 같은 바인딩이 명세 되어 있다. TSM은 개방형 네트워크상의 클라이언트 단말과 응용서버 사이의 용자 인증을 위한 보안과 바이오 인식 기술에 초점을 두고 있다. BIP은 SI(System Integration) 프로그램에서 필수적이며, BIP는 BioAPI 프레임워크하의 원격 BSP간의 통신을 제공한다. 그에 반해, TSM은 SI 프로그램에서 필수적이 아니며, 다양한 응용 서버에서 공유할 수 있는 메커니즘으로 볼 수 있다. 또한, 개방형 네트워크상의 바이오 인식 시스템 인증을 위한 PKI에 기반하고 있다. BIP의 메시지들은 BioAPI 프레임워크를 사용하는 원격 BSP의 운영을 위한 것인데 반해, TSM의 메시지들은 클라이언트 정책과 서버 정책 간의 협상을 위한 메시지로 볼 수 있다. 즉, BIP에서는 BioAPI 함수의 입•출력 데이터를 위한 메시지를 정의하는데 반해, TSM은 TLS 확장 메시지들을 정의한다.

〔Table 4〕 표준 간 용어 비교

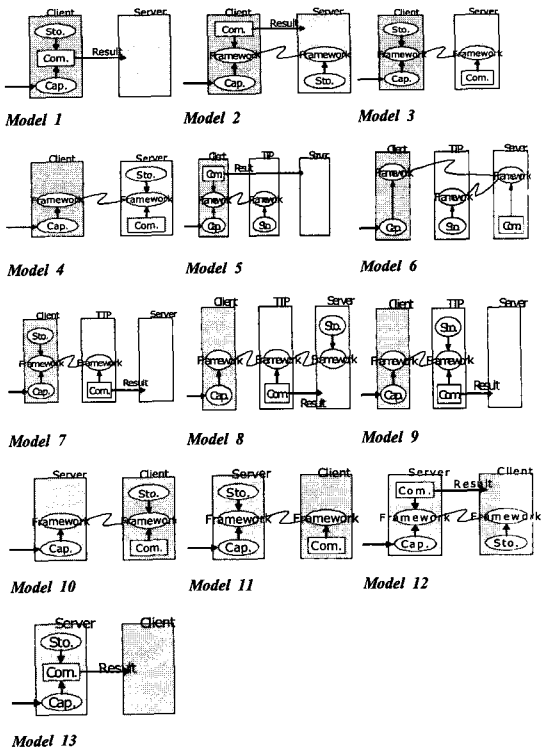
	BIP	X.tsm	통합모델
Biometric Data Capture	Capture	Capturing	Capture
Template Database	Storage	Template	Storage
Capturing Date& Template DB Matching	Matching	Matching	Comparison

BioAPI는 확장성을 위한 선택적인 기능들을 포함하며 생체인식 방법에 대한 접근은 BioAPI에서 정의된 표준 BioAPI 프레임워크를 통하여 이루어기 때문에, 제안하는 모델은 이 프레임워크를 기반으로 한다. 제안하는 모델에서는 Capture, Storage, Comparison으로 X.BIP과 X.tsm에서 혼용되고 있는 용어를 [Table 4]와 같이 통일하였으며, [Figure. 6]와 같이 비교될 수 있다. [Figure. 7]과 같은 통합 모델을 X.BIP과 X.tsm에서 수

용할 경우 각 표준안에서 혼용되고 있는 바이오 주요 컴포넌트의 개념을 명확히 할 수 있으며, 모델 간 중복성을 제거함으로써 표준안을 준용하는 사용자 입장에서 구현을 용이하게 할 수 있다.

Proposal Model	X.tsm Model	BIP Model
Model 1	Local	-
Model 2	Download	Remote storage BSP (Model 3)
Model 3	Attached	-
Model 4	Center	Remote storage and matching BSP (Model 4)
Model 5	Reference management on TTP for Client comparison	Model 6
Model 6	Reference management on TTP for Server comparison	-
Model 7	Comparison Outsourcing by Client	-
Model 8	Comparison Outsourcing by Server	-
Model 9	Storage & comparison Outsourcing	Model 5
Model 10	-	Remote capture BSP (Model 1)
Model 11	-	-
Model 12	-	Remote capture BSP with remote matching (Model 2)
Model 13	-	-

(Figure. 6) 제안된 모델과 기존 표준간의 비교표



(Figure. 7) X.tsm and BIP 13개 통합모델

Ⅳ. 결 론

개방형 네트워크상에서 불특정 다수의 사용자와 서비스 제공자를 위한 바이오 인증 프로토콜을 정의하고 있는 X.tsm은 템플릿 관리 위치와 바이오인식 인증 위치에 따라 9개의 모델을 제시한 바이오 인증 프로토콜로, ITU-T SG17 Q.8에서 First of Recomandation 단계에 있는 표준이다. 그러나 이 표준은 PKI 모델에 대한 구체적 언급이 없고, 기존 TLS 프로토콜을 바이오 인증과 결합하는 내용이 효율적으로 증명되어 있지 않다.

바이오인식 제품 응용 인터페이스(BioAPI)에 입각하여 6개의 모델을 제시한 BioAPI 상호작용 프로토콜(BIP : BioAPI Interworking Protocol)은 BioAPI에 적합한 어플리케이션이 다른 PC에서 작동하고 있는 BSP를 사용하기 위한 메시지들을 정의하고 있다.

ITU-T SG17회의에서 핫이슈로 부상한 X.tsm(PKI 기술을 이용한 클라이언트-서버간 9개 모델을 제시한 바이오정보 통신 프로토콜)과 ISO/IEC JTC1 SC37 WG2에서 추진 중인 BioAPI Interworking Protocol간의 중복성 문제가 제기됨에 따라 ITU-T SG17 Q8(Telebiometrics)의 신규과제로 두 표준과제의 공통사항을 반영한 X.bip가 채택되어 표준화가 진행되고 있다. 이 논문에서 제시한 모델을 X.bip과 X.tsm에서 공통적으로 수용할 경우 각 표준안에서 혼용되고 있는 바이오 주요 컴포넌트의 개념을 명확히 할 수 있으며, 모델 간 중복성을 제거함으로써 표준안을 준용하는 사용자 입장에서 구현을 용이하게 할 수 있다.

참고문헌

[1] ITU-T SG17 Q.8, TD 2444, Revised draft Recommendation X.tsm-1 (Revision 2)

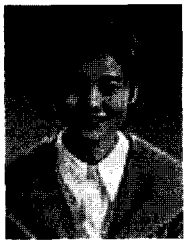
[2] ITU-T Recommendation X.681 (2002) | ISO/IEC 8824-2 : 2002, Information technology - Abstract Syntax Notation One (ASN.1) : Information object specification.

[3] IETF RFC3739 : Internet X.509 Public Key Infrastructure Qualified Certificates Profile, S. Santesson, M. Nystrom, T. Polk, Network Working Group

[4] ISO/IEC 19784-1, Information Technology-Biometric application program interface - part1 : BioAPI Specification

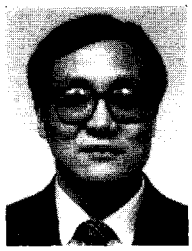
[5] ISO/IEC FCD 24708, BioAPI Interworking Protocol

〈著者紹介〉



신 용 녀 (Yong Nyuo Shin)
정회원
1999년 2월 숭실대학교 컴퓨터학과 학사
2001년 9월 고려대학교 컴퓨터학과 석사
2007년 8월 동대학원 박사과정 수료
2002년 1월 ~ 현재 한국정보보호진흥원 산업지원팀 연구원
<관심분야 : 바이오인식, 정형기법, 정보보호>

김 재 성(jason Kim)
정회원
1986년 2월 인하대학교 전산학과 학사
1989년 2월 동대학원 석사
2005년 8월 동대학원 박사
1996년 7월~ 현재 한국정보보호진흥원 산업지원팀 팀장
<관심분야 : 바이오인식, 인지과학, 정보보호>



최 진 영 (Jin-Young Choi)
정회원
1982년 2월 서울대학교 컴퓨터학과 학사
1986년 2월 Drexel 컴퓨터학과 석사
1993년 2월 Pennsylvania 컴퓨터학과박사
1996년 2월 ~ 현재 고려대학교 컴퓨터학과 부교수
<관심분야 : 정형기법, 정보보호>