

[정보보호] 텔레바이오인식의 원격의료서비스 응용

스위스 제네바에서 ITU-T/SG 17 회의의 2009 - 2012 회기의 첫 회의가 지난 2월에 개최되었으며, 종전에 WP2/Q.8이었던 텔레바이오인식(Telebiometrics)은 WP2/Q.9으로 번호만 변경되었다. 라포처는 김학일 교수(인하대)가 유임하는 동시에 한국정보보호진흥원 및 한국전자통신연구원의 전문가들이 계속 활동함으로써 한국이 지속적으로 주도할 것으로 예상되는 가운데, 스위스, 프랑스, 일본, 중국, 영국 등이 계속 참여하고 있다. 여덟 건의 제안된 표준규격 가운데 여섯 건을 승인했던 지난 회기와 비교하여, 이번 회기에는 지난 회기에 연기되었던 두 건의 제안규격(X.tsm-2, X.tpp-2) 이외에 한국이 제안한 X.ott 및 X.tif가 새로이 제안되어 연구될 것이며, 스위스에서 제안한 X.th가 6개의 multi-part 형태로 진행될 예정이다.

특히 이번 회기에 새로이 진행된 표준안들은 원격의료(Tele-health 또는 Tele-medicine) 서비스들을 대상으로 환자뿐만 아니라 의사, 병원의 관리자 등의 신원확인을 위한 텔레바이오인식 기술 및 정보보호 기술에 관한 표준들이어서 원격의료 서비스 분야의 전문가들의 관심을 끌 것으로 기대된다. 본 보고서는 현재 제안 단계에 있는 새로운 텔레바이오인식 표준안들의 기술적인 내용들을 분석하고, 향후 개발 방향을 예측한다.

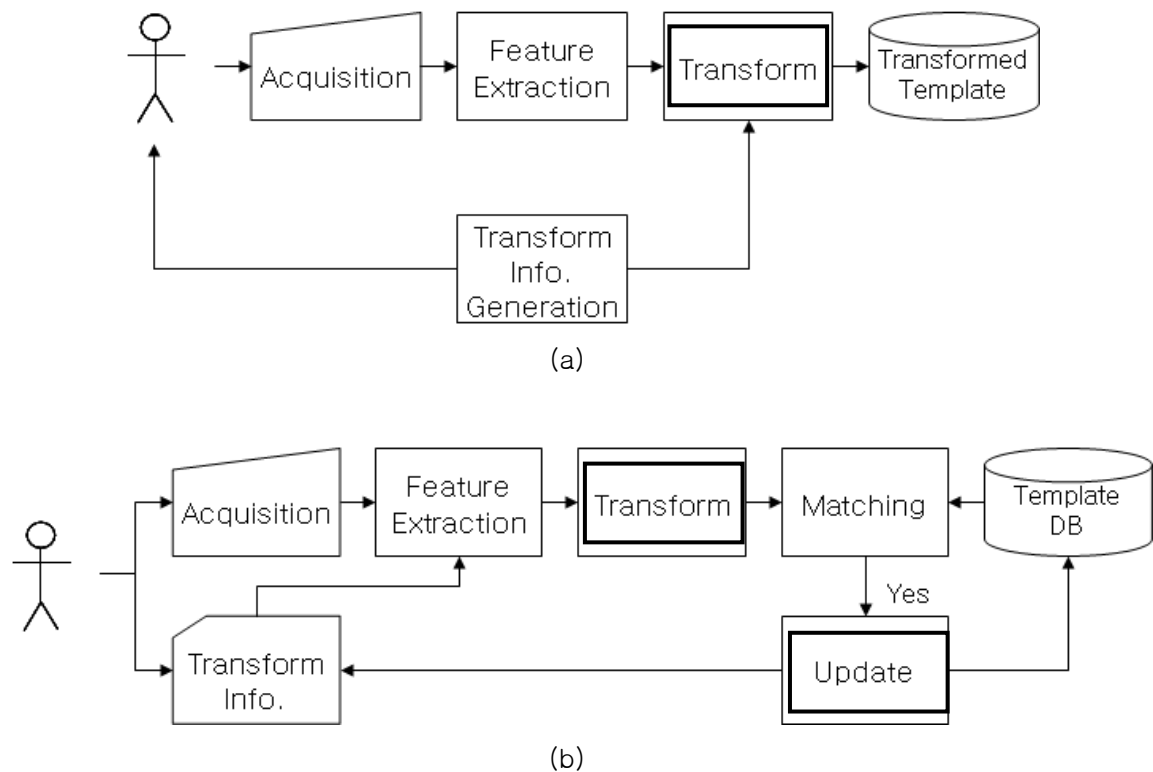
텔레바이오인식 신규 표준안

• X.ott

본 표준 규격안은 한국전자통신연구원과 한신대가 공동 개발하고 있는 표준안으로서, “Replay attack”과 같은 바이오인식 템플릿에 대한 위협으로부터 템플릿 데이터를 보호하기 위하여 일회용 바이오인식 템플릿을 이용한 사용자 인증 프레임워크를 정의한다. 단, 본 규격안은 일회용 템플릿(OTT)을 생성하는 변환 방법을 다루지는 않는다. <그림 1>은 일회용 템플릿을 이용한 등록 과정과 인증 과정을 설명하고 있으며, 기존의 바이오인식 등록, 인증 과정과 다른 점은 추출된 바이오인식 특징들이 변환되어 저장되고, 정합된다는 점이다. 본 규격안은 OTT를 이용한 인증 프레임워크를 정의하면서 특히 Synchronization model과 Update model을 제공하며, 이와 더불어 안전한 인증을 위한 요구사항들을 제시할 것이다.

<표 1> ITU-T/SG17 WP2/Q.9 신규 표준안

규격 명칭	제목	에디터 그룹	승인 예정
X.ott (X.1090)	Authentication Framework with One-time Telebiometric Template	이용진, 정윤수, 문기영 (이상 ETRI), 이형우 (한신대)	2011 년 9 월
X.tif (X.1091)	Integrated framework for telebiometric data protection in telehealth and world-wide telemedicine	신용녀 (KISA), 이용준 (LG-CNS), 김학일 (인하대)	2012 년 9 월
X.th (X.1092 ~ X.1097)	Generic Telecommunications Protocol for Telebiometrics related to health	J.P. Lemaire (프랑스)	2010 년 4 월
	Telebiometrics related to physics		
	Telebiometrics related to chemistry		
	Telebiometrics related to biology		
	Telebiometrics related to culturology		
	Telebiometrics related to psychology		



<그림 1> 일회용 템플릿을 이용한 등록과정 (a), 인증과정 (b)

• X.tif

본 표준 규격안도 한국정보보호진흥원 및 LG-CNS, 인하대 등의 전문가들이 산학연으로 협력하여 공동 개발하고 있는 표준안이며, 지난 회기에 이미 제정된 X.tsm - part 1 (Telebiometrics system mechanism - Part 1: General biometric authentication protocol and system model profiles on telecommunication systems)과 X.tdk (Telebiometrics digital key - A framework for biometric digital key generation and protection)를 기반으로 텔레바이오인식을 원격의료 서비스에 활용하기 위한 “통합된 프레임워크 (Integrated framework)”를 정의한다.

제안된 프레임워크는 유무선 통신을 이용한 원격의료 서비스에서 환자, 의사, 시스템관리자 등의 사용자 식별 및 인증을 위한 텔레바이오인식 활용 모델을 정의함으로써 개인 의료정보를 보호함을 목적으로 한다. 더불어 이러한 민감한 정보들을 전송함에 있어 주요 위험들과 이에 대한 대응 방안을 제시한다. <그림 2>는 원격의료 서비스의 구성요소를 개념적으로 표시하고 있고, <그림 3>은 바이오인식 기반의 개인인증 기능을 갖는 원격의료 서비스의 통합 모델을 보여주고 있다. 여기서 보는 바와 같이, 주요 정보들은 프라이버시 보호를 요하는 매우 민감한 의료 정보 및 개인 식별 정보이며, 개인 인증은 의료기관의 중앙 서버에 데이터베이스를 갖추고 이루어 질 수도 있지만, 원격으로 떨어져 있는 터미널에서도 이루어 질 수 있도록 되어 있다.

• X.th series

X.th는 IEC/TC25에서 ITU-T X.1082 표준규격을 기반으로 여섯 개의 멀티파트 표준안으로 제안 하여 X.th1부터 X.th6까지 구성되게 되었다. X.th1은 X.th의 모든 표준을 위한 ASN.1 정의를 제시하며, X.th2부터 X.th6까지는 다섯 가지 과학분야, Physics, Chemistry, Biology, Culturology, Psychology 등의 센서장치 모달리티(Modality)에 따라 원격의료의 입력신호를 정의하고자 한다.

(1) X.th1은 원격의료 활동의 구조를 설명하고, 의료정보를 지원하는 오브젝트 클래스용 ASN.1

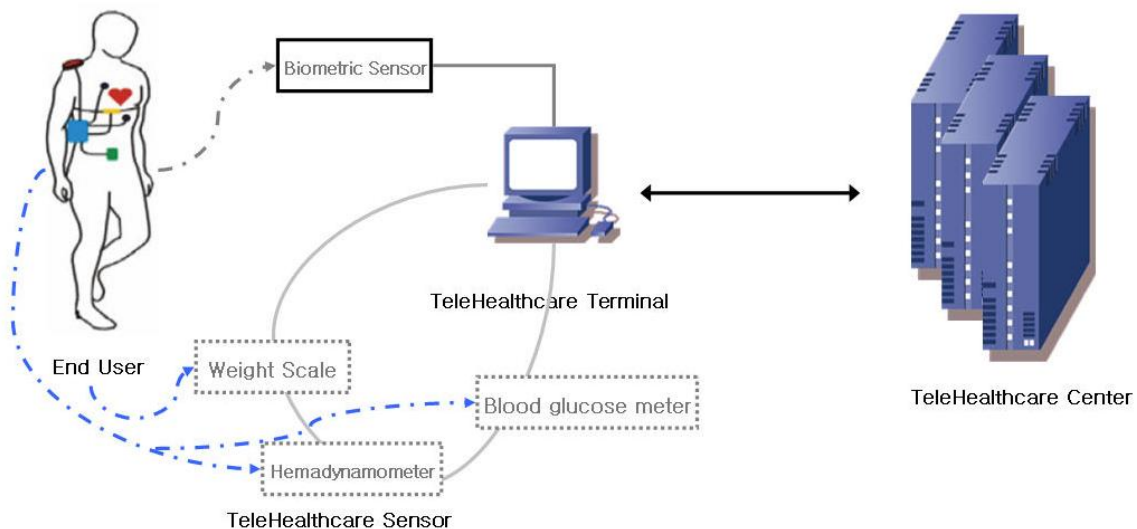
프로토콜과 SOAP을 이용한 서비스 프로토콜을 규정하고, 이러한 프로토콜을 위한 integrity와 encryption 메커니즘을 규정하고 있으며, 본 규격안이 정의하는 프로토콜을 ITUTHP 프로토콜로 명명할 계획이다.

(2) X.th2 ~ X.th6은 다양한 지역 (동일한 나라뿐만 아니라 여러 나라를 포함하여)에서 사용되는 각기 다른 의료 진단 및 치료 방법들이 준수해야 할 정보들의 내용을 센서의 종류에 따라 정의하고 있는데, 각 센서의 종류는 그 원리에 따라 Physics (X.th2), Chemistry (X.th3), Biology (X.th4), Culturology (X.th5), Psychology (X.th6) 등으로 구분하고 있다. 의료 진단 및 치료와 관련하여 제공되어야 할 정보들은 현재 다음과 같이 나열되어 있으며, 본 규격안이 발전되면서 더욱 구체적인 정보들이 포함될 것으로 기대한다:

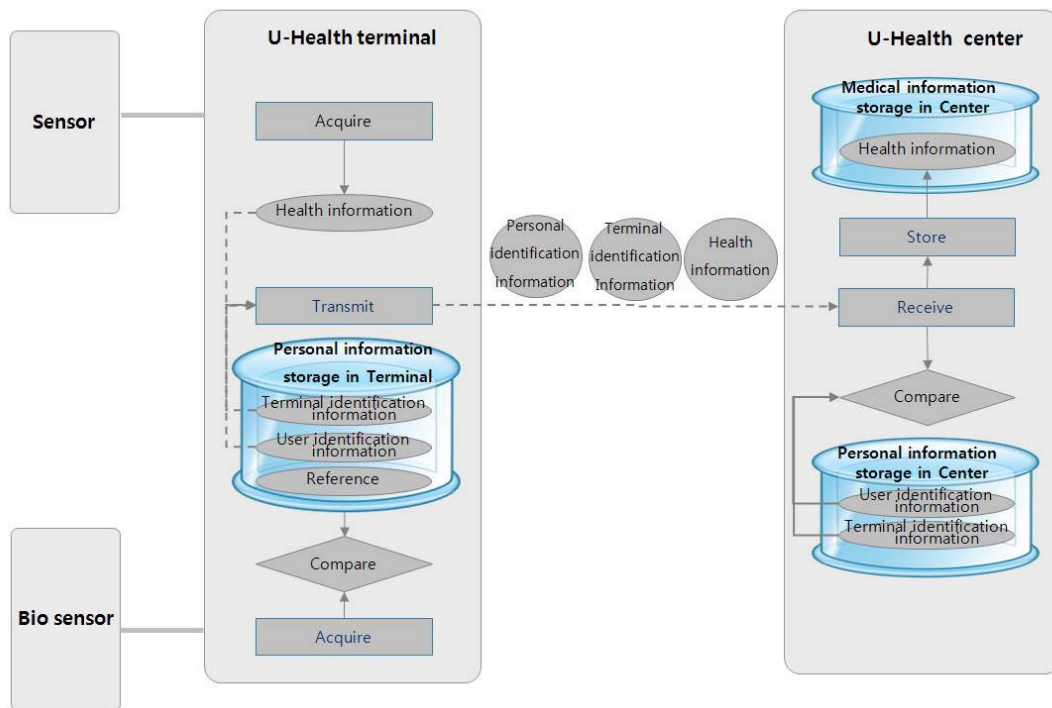
- 의사의 판단을 도와주기 위해 사용될 의료 센서들에 관한 정보
- 최종 진단을 내리기 위해 더 많은 조사나 자료가 필요한 지 여부
- 환자에게 적용 가능한 중간 단계의 치료 방법
- 환자에게 사용 가능한 치료제 및 예상 효용성

전 회기에서 연기된 표준안

2005~2008 회기에서 미제정 되어 이번 회기로 연기된 표준안은 두 건이 있다. 첫째, X.tsm-2 (Telebiometrics system mechanism - Part 2: Protection profile for client terminals)는 일본의 히타치(주)와 한국정보보호진흥원이 공동으로 개발하고 있는 표준안으로서, 그 승인이 연기된 이유는 본 표준안이 참조로 하고 있는 ISO/IEC JTC1/SC27의 19792 표준안이 현재 FCD 단계이기 때문에 FDIS 단계로 발전하여 안정화 된 후에 추진하기로 결정했기 때문이다. 둘째, X.tpp-2 (Telebiometrics protection procedures - part 2: A guideline for data protection in multibiometric systems)는 한국전자통신연구원이 제안한 표준안으로서 X.tpp-1을 기반으로 특별히 다중 바이오인식 데이터의 보호를 위한 가이드라인을 규정하고 있는데, 이미 제정된 X.tpp-1과 기술적 측면에서 일관성을 유지해야 할 필요성이 지적되어 아직 개발 중이다.



<그림 2> 원격의료 서비스의 구성 요소



<그림 3> 바이오인식 기반 원격의료 통합 정보시스템 모델

맺음말

유무선 환경에서 바이오인식을 이용한 개인 인증 기술에 관한 텔레바이오인식 기술의 표준화는 지난 회기 동안에 주로 일반적인 위협과 이에 대한 보안 대응기술의 메커니즘과 프로토콜, 시스템 및 데이터 보호 절차를 규격화 하였고, 이번 회기 동안에는 프라이버시 보호가 가장 높이 요구되는 원격의료 분야에 있어서 바이오인식을 이용한 원격 개인인증 기술에 초점을 맞추고 있다. 이러한 표준들은 바이오인식 데이터뿐만 아니라 의료정보 자체에 대한 보호에도 활용될 수 있어 관련 분야의 전문가들의 주의가 필요하다 하겠다.

따라서, 현재 국내에서는 한국전자통신연구원, 한국정보보호진흥원과 같은 정보통신 분야의 연구기관과, 유사 분야의 업계, 학계 전문가들이 활동을 하고 있지만, 원격의료 분야의 연구소 및 산학 전문가들의 참여가 요구된다.

김학일 (인하대학교 정보통신공학부 교수, hikim@inha.ac.kr)