情 報 保 護 學 會 誌
第22卷 第4號, 2012. 6

프라이버시 관점에서의 바이오인식 국제표준화 동향

신 용 녀*, 전 명 근**

요 약

ISO/IEC JTC1 SC27 WG 5의 프라이버시 프레임워크 표준에서는 바이오인식 정보를 그 정보만으로 개인을 식별하는 유일 정보로 규정하고 있고, 이는 이름과 주소등과 같이 그 자체가 식별정보는 아닌 정보와 구별하고 있다. 바이오정보는 한번 유출될 경우 개인의 프라이버시 침요요소가 매우 크기 때문에 국가 인프라 구축에 활용되기 위해서는 많은 기술적 문제점들이 고려되어야 한다. 프라이버시 프레임워크 표준등과 같이 프라이버시 정보와 바이오 정보가 함께 사용될 때 개인 식별정보에 대한 다양한 표준들이 바이오인식 프라이버시와 정보보호 관점에서 논의되고 있다. 본 논문에서는 프라이버시 관점에서의 바이오인식 표준화 동향을 소개하고, 향후 추진해야할 중점 표준화 항목을 도출한다.

Ⅰ. 서 론

바이오인식 정보의 상업적 이용의 증가와 정보통신 시스템의 복잡도 증가는 기업으로 하여금 그들 고객의 바이오인식 정보를 보호하고 다양한 프라이버시 규정을 준수하기가 어려워지고 있다. 경제적이고 기술적 관점에서 바이오인식 표준화에 대한 요구는 계속하여 증대되고 있다. 전자상거래에 있어서 신뢰를 구축하는 것은 바이오정보를 포함한 소비자의 개인정보가 프라이버시 관련 규정을 준수할 수 있게끔 처리하고 다루어 질 수 있도록 보장하는 것으로만 이루어지는 것이 아니라 심지어 개인의 자기정보 통제권이 행사 될 수 있도록 적절한 기술적 기능을 제공해 줄 수 있어야 한다.

ISO/IEC JTC1 워킹그룹(Working Group) 5에서는 이러한 개인의 기본권인 프라이버시 보호를 위한 표준화 작업에 착수하여, 프라이버시 프레임워크(Privacy Framework) 와 프레임워크 구현을 위한 프라이버시 레퍼런스 아키텍쳐(Privacy Reference Architecture)에 대한 표준화에 주력하고 있다. 국내에서도 개인정보보호법이 시행되어 개인정보보호 시장이 크게 확대되고 있다. 개인의 프라이버시 보호에 대한 이러한 발전추세에는 국내외 표준화기구를 통한 활발한 표준화작업이 밑바탕이 되고 있으며, 프라이버시에 대한 관심은 더욱 높아지고 있다. 정보통신기술의 발전과 더불어 대두되고 있는 정보보호 기법의 표준화에 대한 요구에 부응하여, 암호화 기법 등을 이용한 정보보호기법과 이들 기술에 대한 평가 등을 담당하였던 SC27이 개인정보보호와 관련이 있는 프라이버시 분야, 바이오정보보호, 신원(identity) 관리 분야로 그 영역을 넓혀나가는 것은 우리나라를 포함하여 각국에서 대두되고 있는 프라이버시 및 개인정보보호 관련 사회적 이슈를 해결하는데 크게 도움이 되리라 생각된다. 관련법에서는 바이오인식 정보를 민감정보 및 고유식별정보 처리제한으로 규정하고 있으나, 정보주체에게 별도 동의를 얻거나, 법령에서 구체적으로 허용된 경우에 한하여 예외적으로 처리를 허용하고 있다. 그러나 바이오인식 정보의 안전성 및 편이성으로 인해 이러한 예외적 처리가 필요한 경우가 다수 발생될 것으로 예상된다.

이에, 본 논문은 프라이버시 관점에서의 바이오인식과 관련된 표준화 워킹그룹(Working Group) 5의 주요 표준화 동향에 대하여 간략하게 소개하고자 한다. 본 논문의 구성은 다음과 같다. 본 논문의 2장에서는 정보보호 분과인 ISO SC27워킹그룹(Working Group) 표준화 동향에 대해 살펴보고, 3장에서는 프라이버시 관점에서의 바이오인식 표준화동향에 대해 살펴보고, 4장에서 본 논문의 결언을 맺는다.

본 논문은 지식경제부 산업융합원천기술개발사업(10039149)으로 지원된 연구결과입니다
* 한양사이버대학교 컴퓨터공학과(ynshin@hycu.ac.kr)
** 충북대학교 전자공학부(mgchun@chungbuk.ac.kr)

Ⅱ. ISO SC27 WG5 표준화 동향

WG5는 ID 관리(Identity management)와 프라이버시 기술(Privacy technologies)에 대해 표준화 하고 있으며, Published 된 표준은 일본에서 주도한 ACBio (Authentication Context for Biometrics)와 한국 주도의 Biometric Information Protection, 이탈리아 주도의 ID 관리-part1, 독일주도의 프라이버시 프레임워크이다.

〔표 1〕 WG5 (ID 관리 및 프라이버시 보호) 표준화 추진 현황

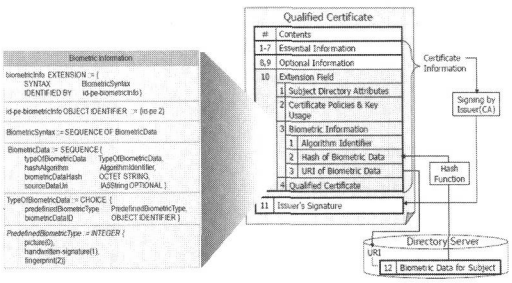
표준화 상태	표준 번호	표준명	에디터 (국가)	비고
IS	24745	Biometric Information protection	전명근 한국	
IS	24761	Authentication context for biometrics	Yamada Asahiko 일본	
IS	24760	part1 : Technology and Concept	Christophe Stenuit (이탈리아)	A framework for identity management
WD (3rd)		part2 : Reference Frameworke and Requirements	Edward de Jong, José Fernando Carvajal	
WD (2nd)		part3 : Practice	Edward de Jong, José Fernando Carvajal	
IS	29100	Privacy framework	Stefan Weiss (독일)	
CD (6th)	29101	Privacy reference architecture	Hans Hedbom 미국	co-editor : Dan Bogdanov
FDIS	29115	Entity authentication assurance	Brackney 미국	ITU-T SG17 Q.6 공동 추진 (X.eaa)
WD (6th)	29146	A framework for access management	José Fernando Carvajal Vion 스페인	co-editor Yasuo Miyakawa 일본
DIS	29191	Requirements on relative anonymity with identity escrow	Kazue Sako 일본	

[표 1]는 ID리 및 프라이버시관련 WG5의 표준화 추진화 현황이다[1].

Ⅲ. 프라이버시관점에서의 바이오인식 표준화

3.1 바이오인식 인증 컨텍스트(ACBio)

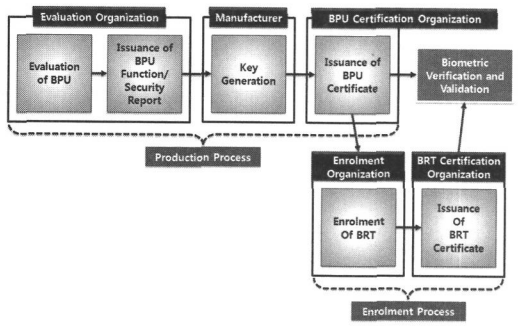
바이오인식 인증 컨텍스트(ACBio, Authentication Context for Biometrics)는 ISO/IEC 24761[4] (Information technology－Security techniques－Authentication context for biometrics)에 정의된 메커니즘으로, 바이오인식이 사용된 장치와 원격지에서 실행된 과정들에 대한 정보를 확인자에게 보냄으로써 원격에서의 바이오인식 검증함으로서 발생할 수 있는 문제에 대한 해결책을 제공해 준다[5]. ACBio는 확인자가 바이오인식 검증 과정 결과의 신빙성 정도를 결정하는데 도움을 주는 BPU (BPU, Biomertic Processing Unit)에 대한 인증된 정보를 제공하기 위하여, 센서, 스마트카드, 비교기 등 BPU에 의해 생성되는 보안 데이터를 위한 데이터 포맷을 정의한다.



〔그림 1〕 X.509 QC 인증서 포맷

ACBio는 PKI(Public Key Infrastructure) 기술과 PKIX(X.509, Public Key Infrastructure)를 기본으로 하며, 신뢰성 확보와 부인 방지를 위하여 전자서명을 사용한다. ACBio를 이용한 바이오인식 검증과정 확인을 위하여, 요구자의 바이오인식 레퍼런스를 획득하고 저장하는 것 이외의 준비가 필요하다. [그림 1]과 같이 ACBio 사용을 위한 일련의 준비 작업들은 생산/등록과정과 뒤이어 일어나는 검증 과정으로 나누어진다.이러한 ACBio 프레임워크를 통하여, 확인자는 비교결과, 바이오인식 검증 결과 뿐 만아니라 수행된 바이오인증 검증 결과의 유효성을 확인할 수 있는 ACBio 인스턴스도 얻을 수 있다. 바이오인식 검증 과정에서 각각의

BPU는 BPU 인증서 정보, BPU 보고서 정보 및 BR 인증서 정보를 담은 ACBio 인스턴스를 채워야 한다. ACBio 인스턴스란 XML 인코딩룰(XER, XML Encoding Rules) 또는 흔히 암호용 툴킷 제공업체들로부터 제공되는 ASN.1 기본 인코딩룰(BER, Basic Encoding Rules)을 이용하여 인코딩된 것으로, 구문은 알고리즘 독립적이며, 데이터 무결성과 데이터 원본 인증을 지원한다. 확인자는 BPU 인증서에 있는 전자서명 혹은 메시지인증코드를 확인함으로써 ACBio 인스턴스의 확실성과 무결성을 확인할 수 있다. 확인자는 BPU 보고서에 따라 BPU의 보안 레벨과 기능적 성능 레벨을 알 수 있고, BRT(Biometric Referece Template) 인증서에 따라 바이오인식 검증 과정에서 사용된 바이오인식 레퍼런스의 확실성도 알 수 있게 된다. [그림 2]와 같이 ACBio를 사용할 경우, BPU의 개인키에 의해 계산된 전자 서명을 사용해야 하므로, 현존하는 PKI 인프라의 많은 수정이 불가피 하다.



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

2012년 5월 스웨덴 스톡홀름 회의에서는 ACBio이 국제 표준 제정 후 3년이 경과되어 첫 번째 정기 리뷰(Periodical pre-review) 기간을 가졌다. 이 경우 각국은 confirmed, revised, declared as stabilized or withdrawn 중에서 하나를 선택하는 투표기간을 가져야 하는데, 4개국 이상이 confirm으로 투표 하였다. 일본에서는 ACBio를 구현하는 사업을 도시바 솔루션에서 진행하고 있는데, 이를 프로그램화 하는 과정에서 표준에 있는 몇 개의 오류를 발견하여 이번 회의를 통하여 Technical corrigendum을 발간하기로 하였다. 이 경우 corrigendum에 대해서 한 번의 투표를 거쳐서 승인 받는 절차를 밟게 된다. ACBio를 구현하기 위해서는 BPU(Biometric Processing Unit)에 대한 인증서 발급기관, BRTCertificate 발급기관 등 추가적으로 필요한 기관들이 요구되므로, 우리나라와 같이 PKI에 기반한 인증시스템에서는 바로 적용하는데 한계가 있다. 이러한 한계에 대해서 이번 회의를 통하여 활발하게 토론하였으며, 현재 우리나라가 국제표준화를 추진하고 있는 X.bhsm을 이용할 경우 더욱 효율적으로 원격 바이오인증을 수행 할 수 있음을 설득 하였다. 이에 일본에서도 X.bhsm이 ACBio와 융합하여 사용될 수 있음에 인식을 같이하여, 향후 표준안 개발에 동참하기로 의견을 모았다.

3.2 바이오인식 템플릿 보안

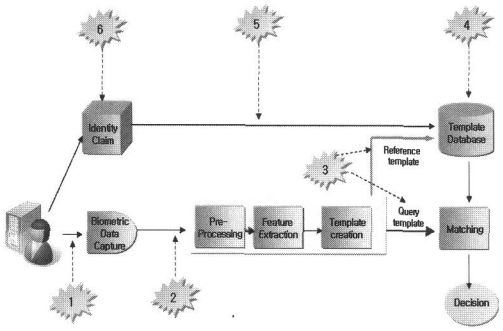
바이오인식 시스템의 각 구성 부분에서 언급되고 있는 것이 바로 바이오인식 템플릿이다. 국제 표준(ISO)에 따르면 바이오인식 템플릿을 정의하기 위해서는 다음과 같은 몇가지 용어에 대한 정의가 필요하다[7].

- 바이오인식 샘플(biometric sample): 바이오인식 특징점이 추출되기 전의 바이오인식 특징의 아날로그 및 디지털 표현으로 바이오인식 취득 디바이스나 바이오인식 데이터취득부에서 얻어 지는 것. 예를 들면 얼굴영상이나 취득된 지문영상이 여기에 해당된다.
- 바이오인식 특징(biometric feature): 바이오인식 샘플로부터 추출된 숫자나 레이블로 비교를 위해 사용된다. 예를 들면 얼굴영상에서 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값 등의 모임이 여기에 해당된다.

바이오인식 템플릿은 다음과 같이 정의된다.

- 바이오인식 템플릿(biometric template): 인식하고자하는 바이오인식 샘플의 바이오인식 특징에 직접적으로 필적하는 저장된 형태의 바이오인식 특징점 집합. 예를 들면 얼굴영상에서 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값 등이 비교부를 위해서 보통 사용자 ID 정보 등과 함께 저장부에 저장되어 있는 것을 말한다.

바이오인식시스템에서 템플릿에 대한 공격위험이 있



[그림 3] 바이오인식 시스템에서의 템플릿 주요 공격 지점[6]

는 주요 지점을 나타내면 [그림 3]과 같다.

AT_P1: 가짜 바이오정보(Spoofing biometric identifier)에 의한 공격. 위조지문이나 복사된 얼굴사진 등을 통한 바이오정보의 등록이나 타인을 사칭하는 행위

AT_P2: 취득된 바이오인식 샘플의 변경. 바이오인식 데이터의 취득부로부터 얻어진 샘플을 임의로 변경

AT_P3: 만들어진 템플릿을 저장부에 이송 중에 변경

AT_P4: 저장되어진 템플릿에 대한 변경

AT_P5: 개인인증과정에서 ID에 대한 고의적 오차 삽입. 조작된 ID나 잘못된 ID로의 변경

[표 2] 바이오인식시스템에서의 공격과 대책

위협	공격의 예	공격위치	
위조 바이오인식 샘플	모조지문, 얼굴사진, 홍채사진	AT_P1	R1
날조된 바이오인식 템플릿	저장부에 저장되어 있거나, 등록시의 제공되어 생성되는 바이오인식 템플릿을 날조	AT_P1 AT_P4	R2
바이오인식 데이터/템플릿 전송위협	등록이나 데이터 전송시의 바이오인식 템플릿 가로채기	AT_P2 AT_P3	R3
사용자식별자	개인인증을 위해 제공되는 식별자의 가로채기나 변조	AT_P5 AT_P6	R4
등록이나 관리 사용상의 위협	등록, 관리, 사용상의 바이오인식샘플 변경	AT_P1 - AT_P6	R5
유사한 바이오인식 특징을 가진 사용자에 의한 공격	합법사용자와 유사한 바이오인식특징을 가진 비합법사용자의 인증시도	AT_P1	R6
무작위 공격	침입자가 시스템을 속이기 위해 계속적인 시도	AT_P1	R7
바이오인식 템플릿의 소실	하드 디스크나 하드웨어의 소실	AT_P4	R8

AT_P6: 등록이나 인증단계에서 변조된 ID의 제공

바이오인식시스템에서 바이오인식 템플릿은 인증을 요구하는 대상자가 실제로 해당 식별 ID을 가진 본인인지의 여부를 가리는데 매우 중요한 역할을 하는 것을 알 수 있다.

상기의 8가지 위협에 대한 대책을 살펴보면 다음과 같다.

(I) 일반적인 정보보안 정책에 의한 위협방지의 대책이 될 수 있는 것: R5, R7, R8

(II) 하나의 바이오인식 정보가 아닌 여러개의 바이오인식 정보를 이용하는 다중 생체인식 기법을 이용한 대책: R1, R6

(III) 바이오정보의 취득대상인 살아있는(Liveness)지의 여부로 위조나 사진 등의 복제를 검출하는 대책: R1

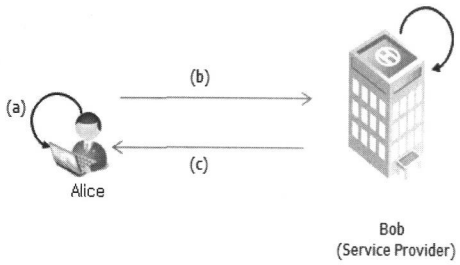
(IV) 암호와 전자서명 등의 보안 기법에 기반한 대책: R2, R3, R4

3.3 바이오 보안 토큰

바이오인식 정보는 개인을 고유하게 식별할 수 있는 개인정보이기 때문에 이에 대한 프라이버시 침해 우려로 인한 적용상의 제한이 있어 왔다. ISO 24745 국제표준에서는 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 PC하드디스크에 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 바이오 보안토큰을 이용한 프라이버시 친화형 개인 인증기법은, 스마트폰을 이용해 취득한 얼굴이나 홍채와 같은 바이오인식 정보와 스마트폰 내의 공인인증서가 결합되는 개인인증기법에도 다양하게 응용될 수 있다.

바이오 보안토큰을 이용한 사용자 인증은 신뢰당사자 Bob은 공인인증서를 통하여 통상적인 사용자 접근통제 및 부인 방지 서비스를 수행하지만, 이와 더불어

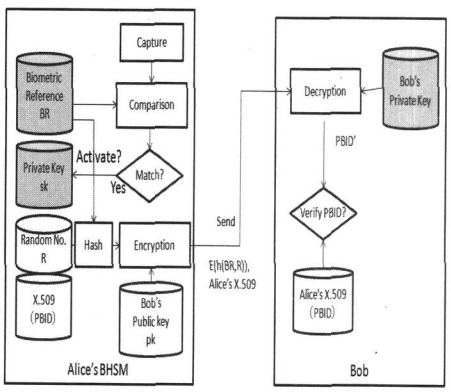
바이오인식 정보를 이용하여 강력한 사용자 인증을 수행함에 있어서, 개인의 바이오인식 프라이버시를 보호할 수 있도록 PBID를 이용하여 [그림 4]와 같이 각 단계별로 수행 할 수 있다[8][1].



[그림 4] 바이오 보안토큰을 이용한 사용자인증

(a) Alice가 바이오보안토큰의 바이오인식 모듈을 이용하여 자신의 바이오인식 정보를 입력하면, 바이오인식모듈내에서 매칭을 수행하면 바이오보안 토큰에 대한 접근이 허용되게 된다.
(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, 인증서내에 있는 PBID 값과 비교하여 값이 같은지 검증한다. 이를 통해 Alice가 바이오보안토큰 발급 당시의 당사자임을 인증한다.

Alice와 Bob사이의 개인인증을 위한 바이오보안토큰내의 정보와 Bob사이의 데이터 흐름은 다음의 [그림 5]와 같다.



[그림 5] 개인인증을 위한 바이오보안토큰내의 정보흐름

V. 결 론

Biometric Encryption을 사용하면, 바이오인식정보 샘플을 저장하는 대신에 바이오인식정보 샘플을 이용하여 PIN, 계좌정보, 암호화 키 와 같은 정보들을 암호화하거나 부호화할 수 있다. 이렇게 바이오정보를 이용하여 암호화된 코드만 저장하고 바이오인식정보 샘플은 저장하지 않는다. 이는 바이오인식정보를 데이터베이스에 저장할 필요성을 없애준다. 바이오정보 자체를 이용할 것이 아니라 바이오정보를 이용해 암호화된 개인정보를 사용하면 되기 때문이다. 따라서 데이터베이스에 집중되어있던 프라이버시와 보안관련 관심들이 해소될 수 있다. Biometric Encryption은 개인의 바이오인식정보 데이터를 다수의 다양한 식별자 (Identifier)를 제공함으로써 유출된(Compromised) 바이오인식 식별자에 대해 안전성을 보장한다.

ISO/IEC JTC1 SC27 WG 5의 프라이버시 프레임워크 표준에서는 바이오인식 정보를 그 정보만으로 개인을 식별하는 유일 정보로 규정하고 있다. 또한 국내 개인정보보호법에서는 바이오 정보를 민감정보 및 고유식별정보 처리제한으로 규정하고 있으나, 정보주체에게 별도 동의를 얻거나, 법령에서 구체적으로 허용된 경우에 한하여 예외적으로 처리를 허용하고 있다. 바이오정보는 한번 유출될 경우 개인의 프라이버시 침요요소가 매우 크기 때문에 국가 인프라 구축에 활용되기 위해서는 많은 기술적 문제점들이 고려되어야 한다. 이러한 기술적 문제점들을 해소하기 위하여 프라이버시 관점에서의 바이오인식분야 국제 표준화 동향을 파악하고 BHSM 등 바이오인식관련 프라이버시 분야 한국 주도 국제표준화 전략 수립이 필요하다.

참고문헌

[1] ISO/IEC JTC1 SC27 WG5 Resolutions, SC27 N1280, May. 2012.
[2] ISO/IEC JTC1 SC27 International Standard Privacy Framework, SC27.
[3] ISO/IEC JTC1 SC27 Privacy Reference Architecture, SC27 N9228, May. 2012.

[4] ISO/IEC 24761-Security techniques-ACBio, Authentication Context for Biometrics, 2009.
[5] Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, RFC3739, 2004.
[6] 신용녀, 권만준, 이용준, 박진일, 전명근, "개인식별정보와 바이오인식정보의 보호기법", 한국지능시스템학회 논문지 Vol. 19 No. 2, pp. 160-167, 2009년.
[7] ISO/IEC JTC1 SC27 International Standard 24745, "Biometric Information protection", 2011년.
[8] A. Carlisle, L. Steve, "Understanding PKI: Concepts, Standards, and Deployment Considerrations", 2nd Edition, Addison Wesley, 2003년.
[9] 신용녀, 김영진, 전명근, "바이오보안 토큰과 PKI 연계방안," 한국정보기술학회 논문지, Vol. 9, No. 5, pp. 207-216, 2011년.
[10] 신용녀, 권만준, 이용준, 박진일, 전명근, "개인식별정보와 바이오인식정보의 보호기법", 한국지능시스템학회 논문지 Vol. 19 No. 2, pp. 160-167, 2009년.
[11] 신용녀, 김학일, 전명근, "개인정보보호 참조 아키텍처와 국제표준화 동향", 정보보호학회지 Vol. 21, No. 5, pp. 12-20, 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
2011년~현재: TTA PG505 표준위원회 부의장
2007년~현재: ISO/IEC SC27 정보보호표준화전문위원
<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