TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx 제정일: 2019년 12월 11일

정보분할에 의한 바이오인식 정보 보호

Biometric reference protection using information splitting

한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 바이오인식 프로젝트그룹(PG505)

표준안 심의 위원회 정보 보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	전명근	충북대	교수	PG505 부의장	TTAx.xx-xx.xxxx
	조래성	㈜와임	대표이사		TTAx.xx-xx.xxxx
표준 초안 작성자	전명근	충북대	교수	PG505 부의장	TTAx.xx-xx.xxxx
	조래성	㈜와임	대표이사		TTAx.xx-xx.xxxx
사무국 담당	김재웅	TTA	단장	사무국	
	문서연	TTA	선임	사무국	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2019.xx

서 문

1 표준의 목적

이 표준의 목적은 정보분할에 의한 바이오인식 정보의 보호를 위한 표준화된 기법을 제공하고자 하는 것이다. 정보분할 기법에 대해서는 랜덤 분할에 의한 기법과 암호학적 기법을 이용하는 경우를 나누어 기술한다.

2 주요 내용 요약

이 표준은 바이오인식 시스템을 구현함에 있어서, 다중 기관간의 바이오인식 정보 공유에 의해서 어느 한곳에서 불법으로 바이오인식 정보가 유출되더라도 대상자의 바이오인식 정보가 침해 당할 수 있는 경우를 배제하기 위한 기법을 기술한다. 다음과 같은 정보분할 기법에 의한 바이오인식 정보 보호 구현 방법과 응용모델을 기술한다.

1) 랜덤 분할에 의한 바이오인식 정보의 분할과 인증
2) 암호학적 기법을 이용한 바이오인식 정보의 분할과 인증

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

- 해당사항 없음

3.2 인용 표준과 본 표준의 비교표

- 해당사항 없음

Preface

1 Purpose

The purpose of this standard is to provide a standardized method for the protection of biometric reference by information splitting. For the information splitting technique, the cryptographic technique and the random splitting technique are described separately.

2 Summary

This standard describes a scheme for protecting a subject's biometric reference even if his/her biometric reference is illegally leaked from one place due to the sharing of biometric reference among multiple parties in implementing the biometric recognition system. The implementation method and application model of biometric reference protection by the following information splitting techniques are given.

1) biometric reference splitting and authentication scheme using random techniques
2) biometric reference splitting and authentication scheme using cryptographic techniques

3 Relationship to Reference Standards

3.1 Relationship of Reference Standards

- None

3.2 Differences between Reference Standard and this Standard

- None

목 차

정보분할에 의한 바이오인식 정보 보호
(Biometric reference protection using information splitting)

1 적용 범위

정보분할에 의한 바이오인식 정보 보호를 위한 표준화된 기법을 제공한다. 정보분할 기법에 대해서는 암호학적 기법을 이용하는 경우와, 랜덤 분할에 의한 기법을 나누어 제시한다.

2 인용 표준

3 용어정의

3.1 바이오인식 정보(biometric reference: BR)
비교를 위해 개인 식별 대상자에 대해서 추출한 속성으로 하나 또는 다수의 저장된 바이오인식 샘플, 바이오인식 템플릿, 바이오인식 모델 등을 나타냄.

3.2 개인식별 정보(identity reference: IR)
주어진 응용영역에서 개인을 나타내는 특징이나 이들의 조합. 예를 들이, 이름, 전화번호, 주민등록번호, 여권번호, 이메일주소 등도 여기에 해당된다.

3.3 개인 인증(Personal authentication)
개인이 정보 자산에 접근을 요청할 때 본인임을 인식하는 과정. 주민등록번호나 패스워드와 같이 본인만이 아는 것, 스마트카드나 메모리 카드와 같이 본인만이 가지고 있는 것, 지문이나 음성, 생체신호 등 본인만의 신체적 특징을 이용하는 방법 등이 사용됨.

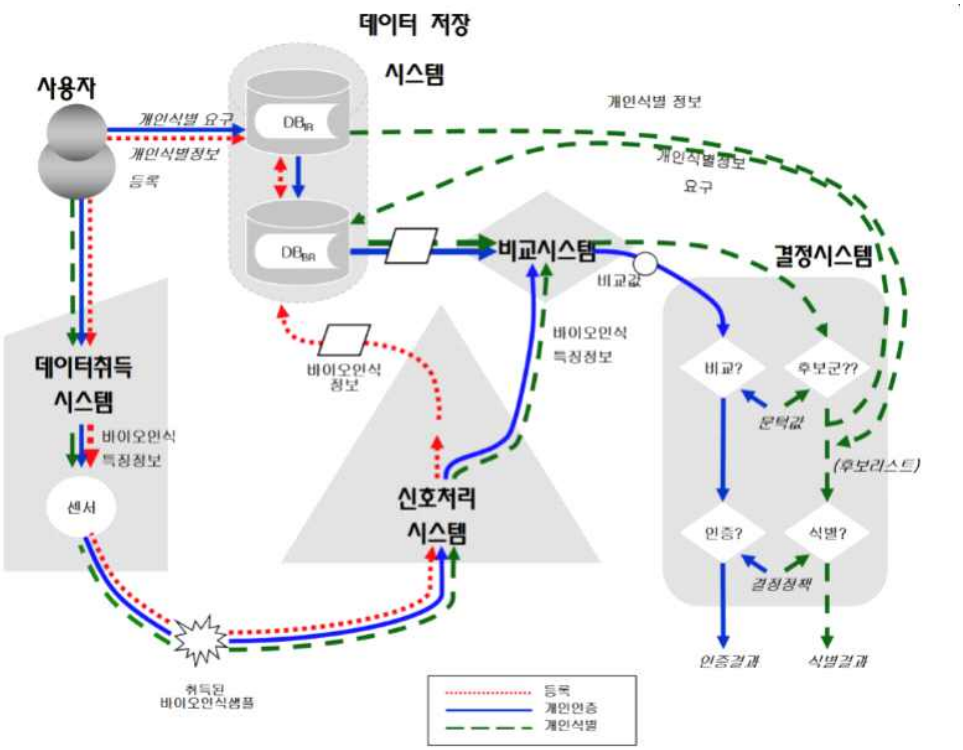
4 약어 및 기호

BR Biometric Reference
CI Common Identifier
IR Identity Reference
K_b^s 바이오인식 정보 암·복호화를 위한 개인키
K_b^p 바이오인식 정보 암·복호화를 위한 공개키
K_i^s 개인식별 정보 암·복호화를 위한 개인키
K_i^p 개인식별 정보 암·복호화를 위한 공개키

5 바이오인식 정보와 개인식별 정보 보호

바이오인식 시스템은 개인의 신체적 또는 행위적 특징에 기반한 개인식별 방법의 일종이라고 할 수 있다. 인터넷 환경과 같이 비대면의 개인 인증 환경에서 인증대상자가 제시한 개인의 신체정보나 서명과 같은 동적 특성의 특징정보를 제시함으로서 사전에 등록 단계에서 미리 저장시켜 놓은 정보와의 비교를 통하여 확인 받고자 하는 개인의 신분을 확인 하는 역할을 수행한다.

그림 5-1에서 볼 수 있듯이 바이오인식 시스템은 크게 3가지 역할로 나누어서 생각해 볼 수 있다. 첫 번째로 등록(Enrollment) 과정이다. 이 기능은 제시되는 대상자의 바이오인식 정보로부터 개인식별(Identification) 과정이나 개인 인증(Verification) 과정에서 필요로 하는 바이오인식 정보(Biometric reference)를 생성하고 저장하는 과정을 의미한다. 개인 식별 과정은 주어진 바이오인식 정보에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식 시스템은 저장장치 내의 모든 바이오인식 정보와 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 한편, 개인 인증 과정은 대상자가 본인의 바이오인식 정보와 함께 개인식별 정보(Identity reference)를 제시하게 되는데, 이는 주어진 바이오인식 정보에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 사용된다. 이때 바이오인식 시스템은 저장장치 내의 해당 식별정보의 바이오인식 정보와의 비교를 통하여 대상자의 인증여부를 결정하게 된다.



(그림 5-1) 바이오인식 시스템의 구성도

개인식별 정보는 어떠한 형태가 되었든 그 정보를 소유하고 있는 사람을 식별할 수 있는 정보라고 볼 수 있다. 바이오인식 정보만 있는 경우에는 특정 개인을 판별하는 정보로

사용하기가 용이하지 않다. 그러나 이러한 바이오인식 정보가 개인식별 정보와 결합되었을 경우에는 매우 민감한 개인정보로 간주할 수 있다. 따라서 이들 각각에 대해서 개인정보 보호에 준하는 기술적 보호 대책뿐만 아니라, 이들은 결합과정에 있어서도 개인의 프라이버시 침해 방지를 위한 별도의 대책을 필요로 한다.

<표 5-1> 바이오 정보와 개인식별 정보

개인식별 정보(Identity reference)	바이오인식 정보(Biometric reference)
이름	지문 영상 정보
주민등록번호(생년월일)	얼굴 영상 정보
여권 번호	홍채 영상 정보
휴대폰 번호	손정맥 영상 정보
운전면허증 번호 등	지정맥 영상 정보 등

6. 정보분할에 의한 바이오인식 정보보호

6.1 랜덤 분할에 의한 바이오인식 정보의 분할과 응용

6.1.1 랜덤 분할에 의한 개인식별 정보의 분할

개인식별정보 IR은 IR_1과 IR_2의 2개의 조각으로 정보를 랜덤하게 분할하는 경우 다음과 같이 표시된다.

$$IR = IR_1 \| IR_2 \tag{1}$$

$$Help_{IR} = Help^{1_{IR}} \| Help^{2_{IR}} \tag{2}$$

위에서, 두 개의 랜덤 데이터로 나눈 관련 정보는 $Help_{IR}$에 저장되는데, 이것 역시 $Help_{IR}^1$와 $Help_{IR}^2$의 두 개의 정보로 분리된 후 각각 저장함으로서, 두 개의 정보가 동시에 주어져야만, 원래의 개인식별 정보 IR을 복구 할 수 있다. 이와 같이 랜덤한 방식에 의해 개인식별 정보분할을 수행하는 경우, 충분한 무작위성을 보장하여 각각의 정보 조각에서 원래의 정보 IR을 복구하거나 알아낼 수 없어야 한다.

6.1.2 랜덤 분할에 의한 바이오인식 정보의 분할

유사하게 바이오인식 정보 BR은 BR_1과 BR_2의 2개의 조각으로 정보를 랜덤하게 분할하는 경우 다음과 같이 표시된다.

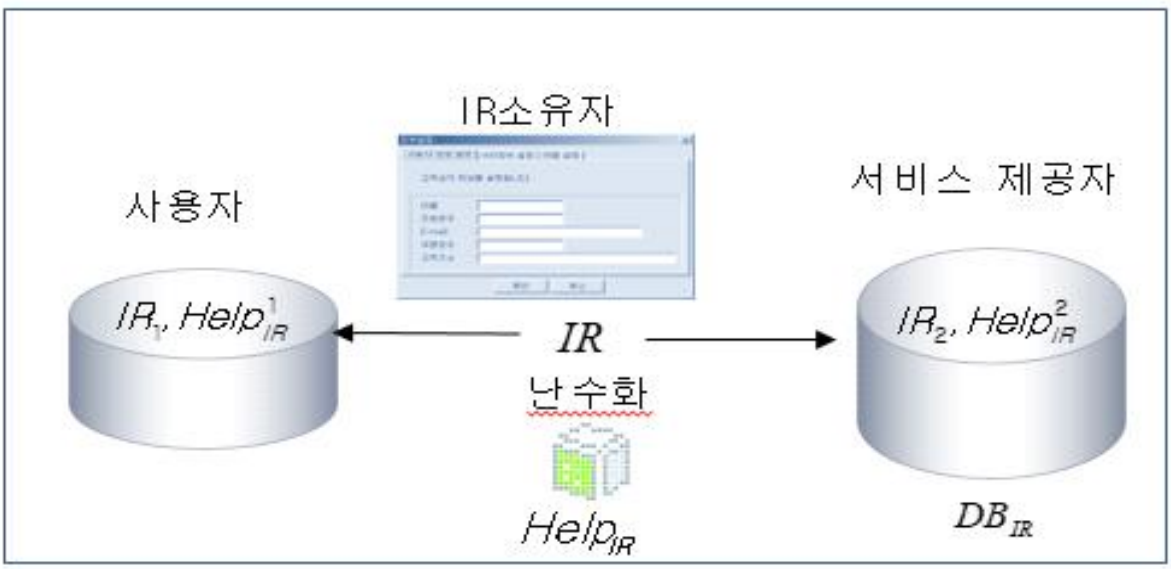
$$BR = BR_1 \| BR_2 \quad (3)$$

$$Help_{BR} = Help_{BR}^1 \| Help_{BR}^2 \quad (4)$$

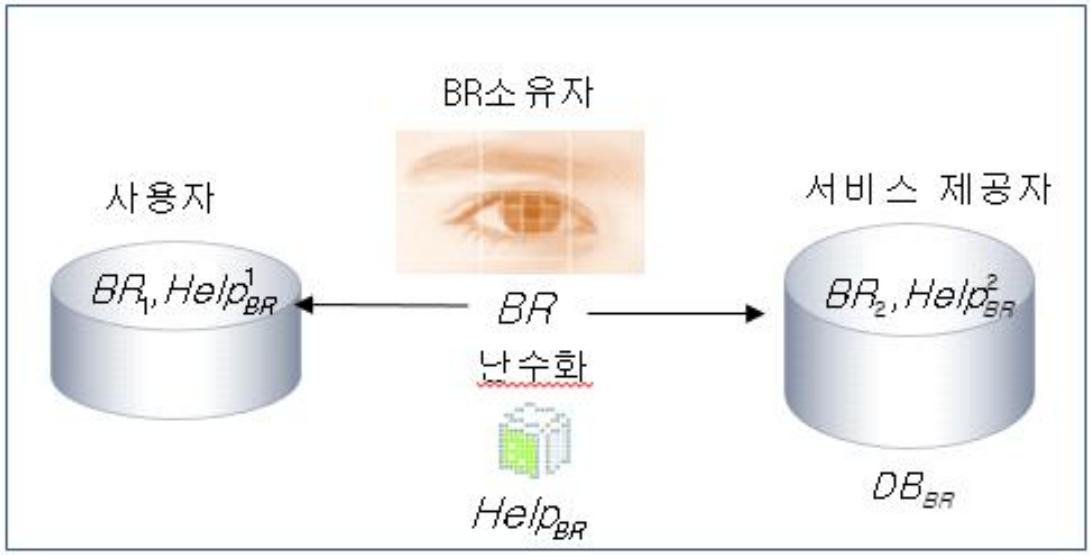
위에서, 두 개의 랜덤 데이터로 나누는데 사용된 정보는 $Help_{BR}$에 저장되는데, 이것 역시 $Help_{BR}^1$와 $Help_{BR}^2$의 두 개의 정보로 랜덤 분리된 후 각각 저장함으로서, 두 개의 정보가 동시에 주어져야만, 원래의 바이오인식 정보 BR을 복구 할 수 있다. 이와 같이 랜덤한 방식에 의해 바이오인식 정보분할을 수행하는 경우, 충분한 무작위성을 보장하여 각각의 정보 조각에서 원래의 정보 BR을 복구하거나 알아낼 수 없어야 한다.

6.1.3 랜덤 분할된 정보의 등록

사용자의 IR과 BR을 (1)~(4)의 방식으로 랜덤하게 분할하여 서비스 제공자의 DB와 사용자의 저장소(보안토큰 등)에 분할하여 그림 6-1, 그림 6-2와 같이 저장하여 놓는다. 이때, 서비스 제공자는 사용자를 유일하게 특정 지을 수 있는, 로그인 이름의 역할을 하는 공통식별자(Common identifier)를 사용자에게 요구한다. 이렇게 함으로서 서비스 제공자의 데이터베이스에서는 $\{CI, IR_2, Help_{IR}^2, BR_2, Help_{BR}^2\}$ 형태의 데이터레코드가 저장되게 된다. 등록과정에서 사용자와 서비스 제공자 간에는 안전한 채널이 확보 되어야 한다.



(그림 6-1) 분할된 개인식별 정보의 등록



(그림 6-2) 분할된 바이오인식 정보의 등록

6.1.4 랜덤 분할된 개인식별 정보의 인증

사용자는 자신의 CI와 함께 서비스 제공자가 요구하는 $\widetilde{IR}$을 제시한다. 이때, $\{IR_1, Help^1_{IR}, BR_1, Help^1_{BR}\}$이 함께 전송된다. 서비스 제공자는 제시된 CI를 이용하여, 저장되어 있는 $\{IR_2, Help^2_{IR}, BR_2, Help^2_{BR}\}$를 이용하여 (1)(2)식을 이용하여 저장되어 있는 IR을 추출한다. 이렇게 추출된 IR을 사용자에 의해 제시된 $\widetilde{IR}$와 비교를 수행한다. 이때, IR과 $\widetilde{IR}$가 일치한다면 본인임을 인증한다. 이때, 사용자의 개인 정보 보호를 위해서 서비스 제공자는 $\{IR_1, Help^1_{IR}, BR_1, Help^1_{BR}\}$, IR을 사용직후 저장하지 않고 즉시 폐기하여야 한다.

6.1.5 랜덤 분할된 바이오인식 정보의 인증

사용자는 자신의 CI와 함께 $\widetilde{BR}$을 제시한다. 이때, $\{IR_1, Help^1_{IR}, BR_1, Help^1_{BR}\}$이 함께 전송된다. 바이오인식 시스템은 제시된 CI를 이용하여, 저장되어 있는 $\{IR_2, Help^2_{IR}, BR_2, Help^2_{BR}\}$를 이용하여 (3)(4)식을 이용하여 저장되어 있는 BR을 추출한다. 이렇게 추출된 BR을 $\widetilde{BR}$와 비교하여 바이오인증을 수행한다. 이때, 바이오인식 시스템에는 사전에 정해져 있는 문턱값과 비교하여 BR과 $\widetilde{BR}$의 유사도가 크다면 본인임을 인증한다. 이때 사용자의 개인 정보 보호를 위해서 서비스 제공자는 $\{IR_1, Help^1_{IR}, BR_1, Help^1_{BR}\}$, $\widetilde{BR}$, BR을 사용직후 저장하지 않고 즉시 폐기하여야 한다.

6.2 암호학적 기법에 의한 바이오인식 정보의 분할과 응용

6.2.1 암호학적 기법에 의한 개인식별 정보의 분할

개인식별정보 IR은 (5)와 공개키 암호를 적용하여, 개인키 K_i^s로 암호화 한 후, E_{IR_1}과 E_{IR_2}의 2개의 조각으로 사전에 정해진 방식대로 분할한다.

$$E_{IR} = E_{K_i^s}(IR) \tag{5}$$

$$E_{IR} = E_{IR_1} \| E_{IR_2} \tag{6}$$

위에서, 암호에 사용된 개인키 K_i^s의 키 쌍인 공개키 K_i^p는 인증기관에 보관하거나 서비스 제공자에게 별도로 전송 될 수 있다. 이와 같이 암호화 방식에 의해 개인식별 정보분할을 수행하는 경우, 안전한 암호와 충분한 키의 길이를 보장하여 각각의 정보 조각에서 원래의 정보 IR을 복구하거나 알아낼 수 없어야 한다.

6.2.2 암호학적 기법에 의한 바이오인식 정보의 분할

바이오인식 정보 BR은 (7)과 같이 공개키 암호를 적용하여, 개인키 K_b^s로 암호화 한 후 E_{BR_1}과 E_{BR_2}의 2개의 조각으로 사전에 정해진 방식대로 분할한다.

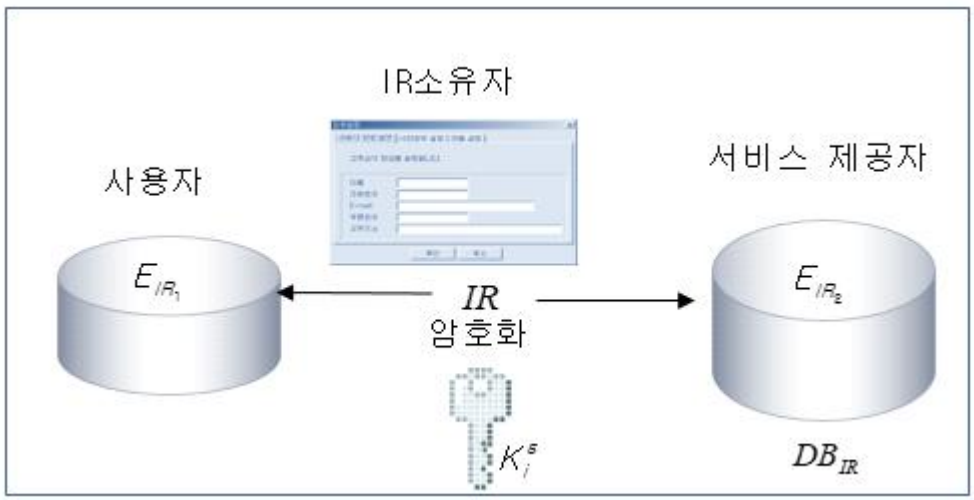
$$E_{BR} = E_{K_b^s}(BR) \tag{7}$$

$$E_{BR} = E_{BR_1} \| E_{BR_2} \tag{8}$$

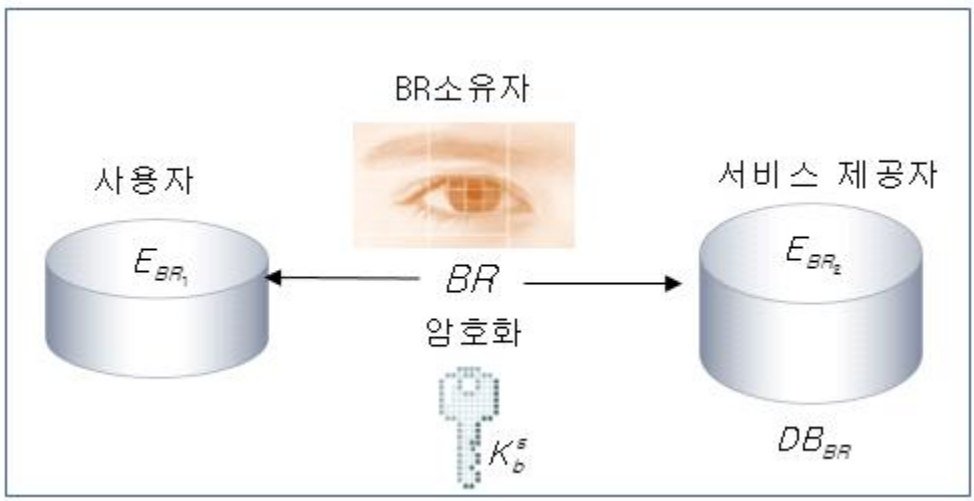
위에서, 암호에 사용된 개인키 K_b^s의 키 쌍인 공개키 K_b^p는 인증기관에 보관하거나 서비스 제공자에게 별도로 전송 될 수 있다. 이와 같이 암호화 방식에 의해 바이오인식 정보분할을 수행하는 경우, 안전한 암호와 충분한 키의 길이를 보장하여 각각의 정보 조각에서 원래의 정보 BR을 복구하거나 알아낼 수 없어야 한다.

6.2.3 암호학적 기법에 의한 분할된 정보의 등록

사용자의 IR과 BR을 (5)~(8)의 방식으로 암호화 한 후 분할하여 서비스 제공자의 데이터베이스와 사용자의 저장소(보안토큰 등)에 분할하여 그림 6-3, 그림 6-4와 같이 저장하여 놓는다. 이때, 서비스 제공자는 사용자를 유일하게 특정 지을 수 있는, 로그인 이름의 역할을 하는 공통식별자(Common identifier; CI)를 사용자에게 요구한다. 이렇게 함으로서 서비스 제공자의 데이터베이스에서는 $\{CI, E_{IR_2}, E_{BR_2}\}$ 형태의 데이터 레코드가 저장되게 된다. 등록과정에서 사용자와 서비스 제공자 간에는 안전한 채널이 확보 되어야 한다.



(그림 6-3) 분할된 개인식별 정보의 등록



(그림 6-4) 분할된 바이오인식 정보의 등록

6.2.4 암호학적 기법에 의한 분할된 개인식별 정보의 인증

사용자는 자신의 CI와 함께 서비스 제공자가 요구하는 $\widetilde{IR}$을 제시한다. 이때, $\{CI, E_{IR_1}, K_i^p, E_{BR_1}, K_b^p\}$ 이 함께 전송된다. 서비스 제공자는 제시된 CI를 이용하여, 저장되어 있는 $\{CI, E_{IR_2}, E_{BR_2}\}$과 함께 (5)(6)식을 이용하여 복호화 하여 IR을 추출한다. 이렇게 추출된 IR을 사용자에 의해 제시된 $\widetilde{IR}$와 비교한다. 이때, IR과 $\widetilde{IR}$가 일치한다면 본인임을 인증한다. 이때, 사용자의 개인정보 보호를 위해서 서비스 제공자는 $\{CI, E_{IR_1}, K_i^p, E_{BR_1}, K_b^p\}$, IR을 사용한 후 저장하지 않고 즉시 폐기하여야 한다.

6.2.5 암호학적 기법에 의한 분할된 개인식별 정보의 인증

사용자는 자신의 CI와 함께 $\widetilde{BR}$을 제시한다. 이때, $\left\{CI, E_{IR_1}, K_i^p, E_{BR_1}, K_b^p\right\}$이 함께 전송된다. 바이오인식 시스템은 제시된 CI를 이용하여, 저장되어 있는 $\left\{CI, E_{IR_2}, E_{BR_2}\right\}$를 이용하여 (7)(8)식을 이용하여 복호화 하여 BR을 추출한다. 이렇게 추출된 BR을 $\widetilde{BR}$와 비교하여 바이오인증을 수행한다. 이때, 바이오인식 시스템에는 사전에 정해져 있는 문턱값과 비교하여 BR과 $\widetilde{BR}$의 유사도가 크다면 본인임을 인증한다. 이때, 사용자의 개인정보 보호를 위해서 서비스 제공자는 $\left\{CI, E_{IR_1}, K_i^p, E_{BR_1}, K_b^p\right\}$, $\widetilde{BR}$, BR을 사용한 후 저장하지 않고 즉시 폐기하여야 한다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

- 해당 사항 없음

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

- 해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

- 해당 사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ISO/IEC 24745, "Information technology - Security techniques - Biometric information protection“, 2011

[2] 이대종, 조래성, 전명근, “분할된 정보 기법에 의한 안전한 바이오인식 응용”, 한국지능시스템학회 춘계학술대회, 2019.

※ 상기 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따름

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

- 해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2019.12.11	제정 TTAx.xx-xx.xxxx	정보분할에 의한 바이오인식 정보 보호	바이오인식 프로젝트그룹 (PG505)