생체인식 정보관리 및 보안표준(X9.84)

이근*, 김재성*

*한국정보보호진흥원

Biometric Information Management and Security Standard(X9.84)

Keun Lee*, Jae-Sung Kim*

*Korea Information Security Agency

요 약

생체인식 정보관리 보안표준인 X9.84는 금융서비스에서 금융산업 서비스를 위하여 생체인식정보에 대한 안전한 운영관리를 목적으로 관리메커니즘 및 보안 고려사항 등을 정의하기 위하여 미국 ANSI에서 개발한 국가표준이다. 본 논문에서는 X.9.84에서 제시하는 적용범위, 준용표준, 관리 및 보안요구사항, Biometric 등록, 보안 고려사항 등을 분석하여 금융서비스, 전자상거래 등의 국내 사용자 인증서비스에 적용가능한 생체인식 보안표준으로 개발하기 위하여 준용사항과 암호학적 메커니즘 사용, 관리 및 보안요구사항, Biometric 등록, 보안고려사항, 감사기록 형식 등의 국내 고려사항을 적용하여 국내 생체인식 정보관리 및 보안표준(K-X9.84)으로 개발하고자 한다.

I. 서론

생체인식기술은 초기 출입통제분야에서 물리적인 접근수단을 제공하는 인증기술 및 범죄수사용 등으로 활용되어왔다. 최근에 생체인식기술은 현금자동지급기, PC 보안관리, 전자상거래용 인증시스템 등에 응용분야로 확대되어가고 있다[1]. 하지만, 생체인식기술의 보급은 각 응용분야에 사용됨에 있어 생체인식기술의 정확성 및 사용자 편의성, Biometric 데이터를 사용함에 있어서 개인정보 보호정책, 생체정보 관리문제가 있다. 생체인식제품은 다양한 분야에 사용될수있다. 금융이나 공공 서비스 등의 주요시설에 사용되는 경우도 있고, 개인용컴퓨터 보안을 위한 최소한의 인증수단으로 사용되는 경우도 있다. 각 분야에서 사용되는 Biometric 데이터는 등록, 검증, 저장, 전송 등의 과정에 있어 노출의 위험성이 존재한다.

미국 ANSI(American National Standards Institute)에서 개발된 X9.84 표준은 이러한 위험성으로부터 Biometric 데이터를 안전하게 사용할 수 있는 메커니즘을 제공하고 있다[2]. ANSI X9.84 표준에서는 Biometric 관리에 대한 정책은 각국의 현실에 맞게 사용하도록 권고하고 있다. 이에 따라 국내의 경우, X9.84 표준에 대한 국내 표준초안(K-X9.84)을 개발하여 국내 금융기관, 관련업체, 학계 전문가 의견을 수렴함으로서 국내 표준으로 정착될수 있도록 TTA/TC10 SG3을 통하여 표준화 작업을 진행중에 있다[3].

II. ANSI X9.84 표준 분석

1. 표준개요

미국의 경우 금융분야에서 사용자 인증에 사용되는 Biometric 데이터를 안전하게 관리 및 운영하기 위해서 ANSI는 X9.F4 워킹그룹을 통해서 Biometric 데이터를 안전하게 주고받을 수 있는 데이터구조와 생체인증 데이터에 대한 최소 보안요구사항을 표준으로 정의한 X9.84을 개발하였다. 또한 이 표준은 ISO/IEC SC27에 DIS- 21352 국제표준으로 검토단계에 있다.

2. 적용범위 및 준용표준

X9.84는 (그림 1)과 같은 구성요소를 가지는 시스템에서 Biometric 데이터의 효율적인 관리를 위해 아래와 같은 최소한의 보안 요구조건들을 명시하고 있다.

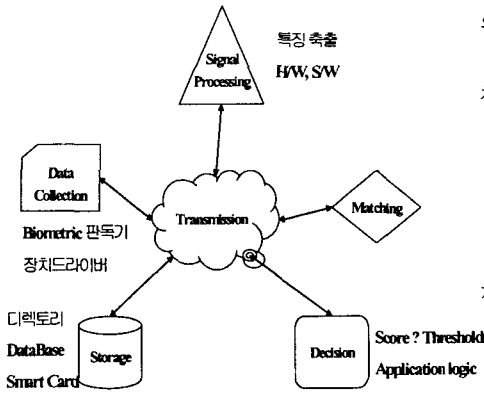

그림 1: 생체인식시스템 구성요소

또한 표준범위는 다음과 같다.

- 생체측정 데이터의 수집, 분배, 처리과정에서 데이터 무결성 인증, 부인방지를 위한 보안

- 등록, 전송과 저장, 검증, 식별, 종료과정 동안 Biometric 데이터의 관리

- 인증과 식별을 위해 1:1 정합과 1:n 정합을 포함하는 생체인식기술의 사용법

- 내부사용자, 외부사용자, 논리적/물리적 접근 통제를 위한 생체인식기술의 적용

- Biometric 데이터의 캡슐화

- Biometric 데이터의 안전한 전송과 저장을 위한 메커니즘

- Biometric 데이터의 등록에서 종료과정동안 사용되는 물리적 하드웨어의 보호방법

- Biometric 데이터의 무결성과 비밀성 유지를 위한 기법

여기서 개인정보에 대한 프라이버시 문제와 Biometric 데이터의 소유권에 대해서는 표준범위에서 제외되었다.

X9.84에서 사용되는 무결성, 블록암호화 알고리즘, 키관리 메커니즘 등은 ISO 국제 표준이나 ANSI 미국 표준을 준용하여 사용하도록 권고하고 있다.

3. 관리 및 보안요구사항

각 적용분야에 필요한 Biometric 데이터의 관리와 보안을 위한 요구조건을 일반 요구사항과 주요 보안 요구사항으로 나누어 정의하고 있다.

1) 일반적인 고려사항

Biometric 데이터에 대한 일반적인 고려사항은 다음과 같다.

- Biometric 데이터를 사용하는 일반사용자들의 수용정도와 정책수립시 고려

- Biometric 데이터에 대한 제3자의 사기행위 차단

- 사용되는 Biometric 특성의 보편성, 고유성

- Biometric 시스템의 정확성 측정

- Biometric 특성의 안정성

- Template 저장시 요구사항(예, Template 크기)

- 시스템의 확인 능력

- 검증이나 식별을 시도하는 사용자의 샘플과 등록된 템플릿과의 비교 속도

- 사용되는 환경과 공유가능한 요소

2) 주요 보안요구사항

Biometric 데이터가 사용되는 모든 적용분야와 상황에 적용되는 주요 보안 요구사항을 다음과 같이 정의하고 있다.

① 메커니즘은 다음 방법들을 이용하여 두 구성요소간에 주고받는 Biometric 데이터와 검증결과의 무결성을 유지하기에 적절하여야 한다.

- 메시지 인증 코드(MAC)나 디지털 서명과 같은 암호학적 메커니즘

- 어떠한 전송도 일어나지 않고, 모든 구성요소들이 같은 Tamper resistant unit 내에 위치하는 물리적 보호

② 메커니즘은 다음 방법들을 이용하여 송수신자와 수신자 사이에서 Biometric 데이터와 검증결과의 송신지와 수신지를 상호 인증하기에 적절해야 한다.

- 메시지 인증 코드(MAC)나 디지털 서명과 같은 암호학적 메커니즘

- 어떠한 전송도 일어나지 않고, 모든 구성 요소들이 같은 Tamper resistant unit 내에 위치하는 물리적인 보호

③ 필요시 선택적으로 메커니즘은 다음 방법들을 이용하여 송수신자와 수신자 사이에서 Biometric 데이터와 검증결과의 송신지와 수신지를 상호 인증하기에 적절해야 한다.

- 암호화

- 어떠한 전송도 일어나지 않고, 모든 구성요소들이 같은 Tamper resistant unit 내에 위치하는 물리적인 보호

위와 같은 주요 보안 요구사항을 기반으로 생체인식시스템은 등록, 검증, 식별, 전송, 저장, 종

료, 보관 과정에서 다음과 같은 추가적인 사항들을 고려해야 한다.

3) 등록

등록과정에서는 초기등록 및 재등록시 추가적인 보안고려사항이 고려되어야한다.

4) 검증

검증과정에서는 Biometric 데이터는 처리되기 전에 Biometric 데이터, 처리된 샘플 데이터, Biometric template을 포함하고 있고 이때, 오류율의 경우 FAR이 적어도 개인 식별 번호(PIN 번호) 기반 시스템에 의해 제공되는 정도 즉, FAR $\leq 10^{-4}$이고 X9.84 표준은 안전을 위해 FAR이 적어도 FAR $\leq 10^{-6}$가 되도록 적극 권장하고 있다. 따라서, 권장하는 FAR $\leq 10^{-6}$ 이고 의무적인 오류율은 $\leq 10^{-4}$ = PIN 기반 FAR 이다. 또한 FRR에 대해서는 고객에 대한 심각한 서비스 문제가 발생하지 않도록 고려되이야 한다.

5) 식별

식별과정에서는 보안요구조건들은 검증에서와 같고 식별을 위한 부가적인 고려사항으로는 대용량 DB를 사용하는 경우 높은 시스템 정확도를 보증하기 위해서는 고품질 이미지 획득을 위한 고수준의 센서 및 높은 임계지 설정이 요구된다.

6) 전송

전송과정에 있어서는 등록과정이 일어나는 장소와 Biometric 템플릿이 생성되는 장소, 템플릿이 생성되는 장소, 저장되는 장소가 다를 경우 전송이 필요하다. 이때 전송 요구조건은 주요 보안요구사항에 따르도록 권장한다.

7) 저장

저장과정에 있어서는 Biometric 데이터가 중앙 DB에 저장되고 검증과 식별은 온라인으로 수해오디는 경우와 Biometric 템플릿이 스마트카드와 같은 휴대용 장치에 저장될 경우가 있다. 중앙 DB, 스마트카드의 경우 각각 저장되는 경우 비인가된 접근을 방지하기에 적절한 대처방법이나 정책을 적용되는 분야의 정책을 설정하고 암호학적 메커니즘을 적용할수있게 시스템이 실계되어야 한다.

8) 종료

종료과정은 사용자의 Biometric 데이터를 삭제하거나, 데이터를 폐기하는 과정을 의미한다. Biometric 종료는 사용자의 고용이 끝났을때, 등록기간이 만료되었을때, Biometric 시스템 업그레이드, 다른 Biometric 기술로 대처할때, Biometric 데이터가 이전 Biometric 데이터를 대신할만큼 충분히 변했을때, 다른 방식의 식별, 검증 방법이 개발되었을때, Biometric 데이터가 손상되었을때, 법적으로 또는 정책적으로 조처를 취할 필요가 있을 경우 들에 대해서 발생되는 모든 사항에 대해서 감사기록을 기록을 권고하고있다.

9) 보관

보관은 사전에 정해진 기간동안 또는 불확정한 시간동안 Biometric 데이터를 저장해 두는 과정을 의미한다. 이때 만료일은 등록과정에서 정해지며, Biometric 헤더에 기록되어있다. 저장하는 과정에 있어 접근제어 메커니즘이 필요하며 이때, 비인가된 접근을 방지하기에 적절해야한다.

III. 국내 표준초안(K-X9.84) 개발

1. 표준개요

국내의 경우, Biometric 데이터를 사용함에 있어 체계적인 생체정보의 사용과 관리정책이 부재한 상태이며, 시스템에 대한 안전한 보안메커니즘 지원 등 보안성을 고려하여 국내 생체인식제품 개발을 추진하여야 함이 바람직하다 할 것이다 .

미국 ANSI 표준인 X9.84를 기반으로 국내에서의 안전한 생체정보 유통을 위한 표준초안(K-X9.84)을 개발하여, TTA/TC10 SG3에 금년 8월에 상정되었다. 또한 표준초안을 대상으로 국내 전문가의 의견수렴을 거쳐 다음과 같은 고려사항을 적용한 국내 생체인식 정보관리 및 보안표준으로 개발하고자 한다.

2. 고려사항

1) 기본요구사항

X9.84의 최소요구사항에 대해서 각 부분별로 다음과 같은 부분에 대해서 고려하여 수용해야한다.

- 캡처 디바이스로부터 생체인증 데이터를 안정하게 캡처

- 캡처된 데이터는 정해진 절차를 이용하여 인가된 인터페이스를 통해서 수용

- 생체인증 데이터의 조작을 막기 위한 안전한 메커니즘의 구현

- 생체인증 데이터의 손실 혹은 노출 방지를 위한 메커니즘 구현

2) 암호학적 메커니즘

국내의 경우 암호학적 메커니즘은 기본적으로 ISO 등의 국제표준을 준용하고 기타 알고리즘에 대해서는 국내 표준을 사용하는 것을 원칙으로 한다. 아래와 같은 표준은 적용될 수 있는 국내 표준이 없으므로 예외적으로 ANSI 표준 사용을 고려해야한다.

- ANSI X9.52-1999 Triple Date Encryption *Algorithm Modes of Operation*

- ANSI X9.66(draft) Security Requirements for Cryptographic Modules

다음과 같은 안전한 보안 알고리즘을 국내에 권고하고자 한다.

- 전자서명 알고리즘 : KCDSA, EC-KCDSA (국내표준), RSA, DSA, ECDSA(미국표준)

- MAC 알고리즘 : HMAC(미국표준)

- 암호화 알고리즘 : SEED(국내표준), TripleDES, AES(미국표준)

- 해쉬 알고리즘 : HAS-160(국내표준), SHA (미국표준)

3) Biometric 데이터 등록

Biometric 등록과정에 있어서 개인에 대한 신원확인, 영상품질 등이 고려되어야한다. 첫째, 신원확인에 필요한 정보의 수집메커니즘은 정보보호서비스에 포함된 가치 또는 위험성에 기초를 두고 각 적용분야에서 정책적으로 선택할 수 있는 방법이 제시되어야한다. 둘째, 품질검사는 등록단계에서 채취되는 생체정보의 영상품질 여부를 일정한 값으로 정의하여 분류하여 저장하여야 한다.

4) 보안고려사항

X9.84에서와 같이 주요 보안 요구사항을 기반으로 Biometric 시스템들은 등록, 검증, 식별, 전송, 저장, 종료, 보관 과정에서 추가적인 사항들을 고려해야한다. 핵심보안요구사항에서는 국내 적용가능한 표준을 준용하여 사용해야하고, 각 운영과정에서 발생하는 사항에 대해서는 적용되는 분야별로 정책 및 성능 수치의 기준을 제시해야한다. 이부분에 대해서는 TTA/TC10 SG3에 소속된 금융, IT, Biometric제품 공급자, 보안제품 공급자들과 지속적인 협의가 요구되는 부분이다.

IV. 결론

안전한 Biometric 정보를 사용을 지원하기위한 Biometric 정보 관리 및 보안 표준으로 X9.84를 분석하였다. 본 표준은 국내 환경에 적용가능하게 만들기 위해서 2001년 11월 표준초안이 개발되었으며, 2002년 8월 국내 표준화 추진을 위해서 TTA/TC10 SG3에 K-X9.84 표준초안을 상정하였다. 국내 금융서비스, 전자상거래 등에 적용가능한 보안표준으로 개발하기 위해서는 암호학적 메커니즘 사용, 관리 및 보안요구사항, Biometric 등록, 보안고려사항, 감사기록 형식 등의 고려사항을 국내 전문가에게 의견을 수렴하여 국내 생체인식 정보관리 및 보안표준으로 개발할 예정이다.

참고문헌

[1] 김재성, "국내 생체인식기술 표준화 및 평가현황", NETSEC-KR 2002, 2002년 5월.

[2] ANSI, "X9.84-2001 : Biometric Information Management and Security", ANSI, March, 2001.

[3] TTA, "K-X9.84 2002-563 : 생체인식 정보관리 및 보안표준", TTA, Aug. 2002.

[4] 김재성, 방지호, 이현정, "국내외 생체인식기술 표준화 및 평가현황", 정보보호학회지, 2002년 4월