Korea Communications Standard

방송통신표준
KCS.KO-12.0165 제정일: 2013 년 12 월 31 일

바이오 보안 토큰용 API

API for Biometric Hardware Security Module(BHSM)

미래창조과학부
국립전파연구원

방송통신표준
KCS.KO-12.0165 제정일: 2013 년 12 월 31 일

바이오 보안 토큰용 API

API for Biometric Hardware Security Module(BHSM)

미래창조과학부
국립전파연구원

서 문

1. 표준의 목적

본 표준은 바이오 인식과 공인 인증서를 결합하여 사용하기 위한 바이오 보안 토큰 규격, 응용 프로그램과 바이오 보안 토큰 간 인터페이스 모델 및 기본 요구 사항을 정의한다. 이를 통해 고도의 개인 확인이 필요한 응용에 바이오 보안 토큰이 사용될 수 있도록 상호 운용성이 보장되는 API 규격을 정의하는 것이 목적이다.

2. 주요 내용 요약

본 표준은 개인용 PC 및 모바일 환경에서 바이오 보안 토큰 기반 공인 인증서 이용을 위한 바이오 보안 토큰 규격, 응용 프로그램과 바이오 보안 토큰 간 인터페이스 모델 및 기본 요구 사항을 정의한다.

또한, 바이오 인식 기반의 바이오 보안 토큰 구현에 있어 바이오 정보의 저장 및 인증, 관리에 필요한 기기 내부에서 처리되는 기본 요구 사항과 바이오 보안 토큰을 이용함에 있어 필요한 기능적 요구 사항을 명시한다.

부속서에는 바이오 보안 토큰 API 및 바이오 보안 토큰 사용자 관리 API가 기술되어 있다.

3. 표준 적용 산업 분야 및 산업에 미치는 영향

본 표준은 개인 정보 도용 및 오용을 방지하기 위하여 보안 토큰이 내부적으로 갖추어야 할 API 및 이의 활용을 보여줌으로써 응용 시스템에서 개인 정보를 더 안전하게 활용할 수 있게 할 것이다. 또한 사용자 입장에서의 편리성 향상과 제품에 대한 신뢰성 증진 효과도 동시에 얻을 수 있게 될 것이다.

4. 참조 표준(권고)

4.1 국외 표준(권고)

해당 사항 없음.

4.2 국내 표준

- TTAK.KO-12.0165, '바이오 보안 토큰용 API', 2011.6.

5. 참조 표준(권고)과의 비교

5.1. 참조 표준(권고)과의 관련성

본 표준은 바이오인식 기술이 적용된 바이오 보안 토큰 API를 정의하기 위해서 'TTAK.KO-12.0165'를 일부 수정하여 작성하였다.

5.2. 참조한 표준(권고)과 본 표준의 비교표

KCS.KO-12.0165	TTAK.KO-12.0165	비고
1. 개요	1. 개요	동일
2. 표준의 구성 및 범위	2. 표준의 구성 및 범위	동일
3. 용어 정의 및 약어	3. 용어 정의	수정
4. 바이오 보안 토큰 요구 사항	4. 바이오 보안 토큰 요구 사항	동일
5. 바이오 보안 토큰 API	5. 바이오 보안 토큰 API	동일
부속서 A. 바이오 보안 토큰 API 요약	부록 I. 바이오 보안 토큰 API 정리	수정
부속서 B. 바이오 보안 토큰 사용자 관리 API	부록 II. 바이오 보안 토큰 사용자 관리 API 정리	수정
부록 I. 관련 문헌		추가

6. 지식 재산권 관련 사항

본 표준의 '지적 재산권 확약서' 제출 현황은 국립전파연구원 웹사이트에서 확인할 수 있다.

※본 표준을 이용하는 자는 이용함에 있어 지식 재산권이 포함되어 있을 수 있으므로, 확인 후 이용한다.

※본 표준과 관련하여 접수된 확약서 이외에도 지식 재산권이 존재할 수 있다.

7. 시험 인증 관련 사항

7.1. 시험 인증 대상 여부

해당 사항 없음.

7.2. 시험 표준 제정 여부

해당 사항 없음.

8. 표준의 이력 정보

8.1. 표준의 이력

판 수	제정·개정일	제정·개정 내역
제1판	2013.12.31.	제정 KCS.KO-12.0165

8.2. 주요 개정 사항

해당 사항 없음.

Preface

1. Purpose of Standard

By providing the BHSM specification, interface model between application program and BHSM, and fundamental requirements, this standard aims to support a BHSM based high level personal authentication and interoperability among the various systems by defining the BHSM API.

2. Summary of Contents

This standard defines the BHSM specification and interface model between application program and BHSM and fundamental requirements, which are used for biometrics based accredited certificate under personal PC and mobile environment.

This standard also clarifies fundamental requirements needed for saving, verifying and managing biometric information for application system based on BHSM, and functional requirements for using the BHSM in the system.

In the Annex, the BHSM API and BHSM user management API are described.

3. Applicable Fields of Industry and its Effect

This standard contributes to applications using personal private information in more secure ways, by showing the requirements for the BHSM in order to prevent identity theft and misuse of private information. This will lead to improve both reliability and trust to the system close to users.

4. Reference Standards(Recommendations)

4.1. International Standards(Recommendations)

None

4.2. Domestic Standards

- TTAK.KO-12.0165, 'API for Biometric Hardware Security Module', 2011.6.

5. Comparison between Reference Standards(Recommendations) and this Standard

5.1. Relevance of this Standard with Reference Standards(Recommendations)

This standard is based on the 'TTAK.KO-12.0165' to define API for biometric hardware security module and modified it.

5.2. A Comparative Table of Reference Standard(Recommendation) and this Standard

KCS.KO-12.0165	TTAK.KO-12.0165	Remarks
1. Introduction	1. Introduction	Same
2. Constitution and Scope	2. Constitution and Scope	Same
3. Terms Definition and Abbreviations	3. Terms and Definitions	Modified
4. Requirements of BHSM	4. Requirements of BHSM	Same
5. API for BHSM	5. API for BHSM	Same
Annex A. BHSM API	Appendix I. Abstract on BHSM API	Modified
Annex B. BHSM User Management API	Appendix II. Abstract on BHSM User Management API	Modified
Appendix I. Related Documents		Added

6. Statement of Intellectual Property Rights

"Written Confirmation of Intellectual Property Rights" for this standard can be referenced to the website of the National Radio Research Agency.

Those using this standard must confirm that whether intellectual property rights are included in this standard.

Other intellectual property rights may exist in relation to written confirmation received for this standard.

7. Statement of Testing and Certification

7.1. Object of Testing and Certification

None

7.2. Standards of Testing and Certification

None

8. History of Standard

8.1. Change History

Edition	Issued date	History
The 1st edition	2013.12.31.	Established KCS.KO-12.0165

8.2. Revision Related Details

None

목 차

Contents

바이오 보안 토큰용 API

(API for Biometric Hardware Security Module(BHSM))

1. 개요

본 표준은 전자 입찰 시스템에서 사용되고 있는 바이오 보안 토큰의 보안요구사항과 관련 규격을 정의하고, 제조사가 다르더라도 응용 프로그램에서도 바이오 보안 토큰이 원활하게 사용될 수 있도록 바이오 보안 토큰 간에 상호 운용성이 보장되는 API 규격을 정의한다. 국내에서 통용되는 '보안 토큰'이라는 용어를 영어권에서는 'HSM'이라고 불리우는 바, '바이오 보안 토큰' 용어를 본 표준에서 영어로 'BHSM'으로 표기한다.

2. 표준의 구성 및 범위

본 표준은 바이오 보안 토큰의 기능 중 반드시 필요하거나 구현이 권고되는 부분을 기술하여 바이오 보안 토큰이 탑재된 제품들 간에 상호 운용성이 보장될 수 있도록 API 규격을 정의한다. 따라서, 본 표준은 전자 입찰 시스템에 필요한 바이오 보안 토큰 내부에서 처리되는 기본 요구 사항과 바이오 보안 토큰을 이용함에 있어 필요한 바이오 보안 토큰의 기능적 요구 사항을 명시한다. 자세한 내용은 다음과 같다.

첫째, 개인용 PC 및 모바일 환경에서 바이오 보안 토큰 기반 공인 인증서 이용을 위한 바이오 보안 토큰 규격, 응용 프로그램과 바이오 보안 토큰 간 인터페이스 모델 및 기본 요구 사항을 정의한다.

둘째, 바이오 인식 기반의 바이오 보안 토큰 구현에 있어 바이오 정보의 저장 및 인증, 관리에 필요한 기기 내부에서 처리되는 기본 요구 사항과 바이오 보안 토큰을 이용함에 있어 필요한 기능적 요구 사항을 명시한다.

셋째, 부속서에는 바이오 보안 토큰 API 및 바이오 보안 토큰 사용자 관리 API를 기술한다.

3. 용어 정의 및 약어

3.1. 용어 정의

보안 토큰 (HSM, Hardware Security Module)	전자 서명 생성 키, 바이오 정보(지문, 홍채) 등 비밀 정보를 안전하게 저장, 보관하기 위하여 키 생성, 전자 서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기
바이오 보안 토큰 (BHSM, Biometric HSM)	바이오 센서와 마이크로 제어 장치, 보안 토큰으로 구성된 일체형 기기로 기기 내부에서 바이오 센서로 사용자의 바이오 정보를 인식하여, MCU에서 바이오 정보를 처리하여 보안 토큰에 안전하게 저장하며, 사용자 인증 시 바이오 센서에서 추출된 바이오 정보와 보안 토큰에 저장된 바이오 정보를 기기 내부 비교하여 사용자 인증을 처리하는 기기
PKCS#11 API	바이오 보안 토큰에 대한 응용 프로그램 인터페이스로 보안 토큰 API
바이오 보안 토큰 API	바이오 보안 토큰 적용을 위한 보안 토큰 API
바이오 보안 토큰 관리 API	바이오 보안 토큰 관리를 위한 인터페이스 함수 제공
사용자 식별 번호	주민등록번호 및 사업자 등록 번호를 말함
개인 식별 정보(PII)	본인과 타인을 구분하는 데 사용되는 모든 정보로서, 바이오 정보 및 사용자 식별 번호 등이 포함됨

3.2. 약어

API	Application Program Interface(응용 프로그램 인터페이스)
MCU	Micro Controller Unit(소형 제어기)
PKI	Pubulic Key Infrastructure(공개 키 기반 구조)
PKCS	Public Key Cryptography System(공개 키 암호화 시스템)

RSA Rivest Shamir Adelman

UART Universal Asynchronous Receiver/Transmitter(범용 비동기 송수신기)

UI User Interface(사용자 인터페이스)

4. 바이오 보안 토큰 요구 사항

바이오 보안 토큰은 전자 입찰 시스템과 같은 다양한 응용에 활용될 수 있는 사용자 인증을 위한 정보(개인 식별 정보, 바이오 인식 정보, 전자 서명 생성 키 등)를 저장할 수 있고, 바이오 센서와 MCU가 포함되어 있어, 토큰 내부에서 보안 토큰에 저장된 바이오 정보와 바이오 센서에서 얻은 바이오 정보를 비교하여 사용자 인증을 수행하는 등 다양한 응용 프로그램에서 활용이 가능한 기기이다.

바이오 보안 토큰 API는 바이오 보안 토큰을 이용하는 모든 애플리케이션에서 공통으로 구현해 사용해야 하는 기능들을 함수의 형태로 모아놓은 것이다. 바이오 보안 토큰 API는 다음과 같은 기본 개념을 근거로 정의한다.

기본적으로 바이오 보안 토큰에 의한 바이오 정보 유출을 방지하기 위하여, 바이오 템플릿의 추출과 바이오 정보의 인증은 보안 토큰 내에서 이루어져야 하며, 인증 결과만 외부로 제공해야 한다. 이 과정에서 바이오 정보는 바이오 보안 토큰 외부로 유출되지 않아야 하며, 사용자가 임의로 바이오 정보를 바이오 보안 토큰 외부로 유출할 수 없어야 한다.

4.1. 바이오 보안 토큰 API 요구 사항

바이오 보안 토큰API는 RSA 1024 비트 및 2048 비트의 공인 인증서를 지원하여야 하며, 개인 정보의 오남용 방지와 사용자의 편리성, 시스템의 안정성을 확보하기 위하여 필요한 추가적인 기능들이 포함된 함수들을 정의한다.

- 바이오 보안 토큰 이외의 저장 장치에서 공인 인증서가 이용되는 것을 방지하기 위한 바이오 보안 토큰 장치 인증 기능
- 바이오 보안 토큰 장애 시 개인 정보 악용 방지를 위한 기능
- 바이오 인증된 사용자의 법인 인증서와 개인 인증서를 개별로 읽어오도록 하여 사용자의 편리성을 증대시키고 처리 속도를 향상시키는 기능

4.2. 사용자 식별 정보와 공인 인증서의 정합

스마트카드에 공인 인증서를 저장할 때에는, 사용자별로 보안 토큰 내부에 정보 저장이 가능해야 한다. 바이오 보안 토큰 외부에서 생성된 전자 서명 생성 키를 바이오 보안 토큰에 저장 시 사용자의 바이오 정보와 전자 서명 생성 키 정보의 신원 확인을 통한 매핑을 위하여 스마트카드 내부나 외부에서 식별 정보의 검증을 통하여 정합 여부를 검사한 후 매핑 정보와 함께 저장한다.

부록 I의 [1]에 따라 바이오 보안 토큰에 저장된 공인 인증서를 사용 시 바이오 인증을 통하여 사용자의 신원을 확인하고, 해당 공인 인증서만을 사용할 수 있도록 하여야 하며, 바이오 보안 토큰에 저장된 사용자의 식별 정보를 사용하여 스마트카드 내부나 외부에서 식별 정보의 검증을 통하여 정합 여부를 검사한 후 사용하여야 한다.

공개 키 암호 표준인 PKCS#11 API를 이용한 공인 인증서 관리 기능을 지원하여야 하며, RSA 1024 비트 및 2048 비트의 공인 인증서의 관리를 지원하여야 한다. 토큰 내부에서 인증서 생성 시 바이오 보안 토큰에 사용자 식별 정보가 1 개 이상 등록되어 있는 경우 사용자 식별 정보를 검색하여 부록 I의 [2]에 의해 정합되는 정보가 존재할 경우 이를 매핑시켜 저장하며 존재하지 않을 경우 생성을 거부해야 한다.

4.3. USB 통신

USB 장치 해킹에 의한 데이터 유출을 방지하기 위하여 USB를 통한 데이터 송수신 시 중요 데이터에 한하여 암호화된 데이터로 송수신할 것을 권고한다.

4.4. 바이오 센서

바이오 센서는 사용자가 제공한 신원 확인 식별자를 식별한 후 이를 기반으로 사용자가 제공한 바이오 정보와 해당 사용자의 등록된 바이오 정보를 일대일 비교하여 정합 여부를 결정함으로써 사용자 신원을 인증하는 일대일 검증 방식을 적용한다.

바이오 센서는 실제 바이오 영상과 유사한 인공물(인공 지문, 또는 기타 인조물)을 이용한 사칭 시도나, 바이오 영상 획득 센서에 잔류하는 이전 사용자의 바이오 영상의 잔상을 이용한 재사용으로부터 보호되는 바이오 인식 방식을 적용하여야 한다.

4.5. 사용자 정보 관리

바이오 보안 토큰 사용자 정보는 바이오 정보와 사용자 식별 정보로 구성되며, 바이오 정보와 사용자 정보는 보안 토큰 내부의 저장소에 저장하며, 관리자에 의해서만 저장 및 삭제가 가능하도록 통제되어야 한다.

바이오 보안 토큰은 다수의 사용자에 대한 사용자 정보의 저장이 가능하여야 하며, 사용자 식별 번호는 '-' 등과 같은 구분자를 제거한 상태의 숫자 열로만 구성될 수 있다.

4.6. 바이오 보안 토큰의 성능 및 안정성 확보

바이오 보안 토큰에는 사용자 별로 바이오 인증이 가능한 2 개 이상의 바이오 정보의 저장이 가능하여야 하며, 바이오 인증 방법 1(예 : 오른쪽 눈 또는 엄지 지문 등)에 의한 바이오 인증이 실패하는 경우 바이오 인증 방법 2(예 : 왼쪽 눈 또는 검지 지문 등), 다수의 바이오 인증 방법에 의한 바이오 인증 방법을 제공하여야 한다.

4.7. 바이오 보안 토큰의 공유 사용

사용의 편리성 및 비용 부담을 최소화하기 위하여 보안 토큰에 다수 사용자들의 바이오 정보와 식별 정보의 저장이 가능하여야 한다.

바이오 보안 토큰에 등록된 사용자는 적합한 바이오 인증 후 사용되어야 하며, 하나의 바이오 보안 토큰으로 최소 복수의 사용자가 공유하여 사용할 수 있어야 한다.

5. 바이오 보안 토큰 API

보안 토큰 API는 PC 환경에서 보안 토큰과의 호환성을 제공할 수 있는 인터페이스로 RSA사의 PKCS#11API를 기반으로 한 보안 토큰API를 적용해야 하며, 일반적인 보안 토큰과 바이오 보안 토큰 간에 차이를 식별할 수 있는 장치 인증 값 생성 기능을 지원하여야 한다.

바이오 보안 토큰 API는 사용자의 편리성, 업무 특성으로 인하여 PKCS#11 API의 구현이 용이하지 않은 경우 바이오 보안 토큰을 시스템에 적용하기 위하여 응용 프로그램과 바이오 보안 토큰의 연동을 위한 처리 함수를 제공한다.

5.1. 바이오 보안 토큰 장치 모델

바이오 보안 토큰 장치는 바이오 정보의 처리를 위한 MCU, 바이오 정보 인식을 위한 바이오 센서, 개인 식별 정보 및 전자 서명 생성 키 등의 정보가 저장되는 스마트카드, 통신을 위한 USB 및 범용 비동기 송수신기(UART) 인터페이스 등의 장치로 구성된다. 바이오 보안 토큰의 외부 인터페이스는 PC 환경에서 연결할 수 있는 USB 장치로 구성되어야 한다.

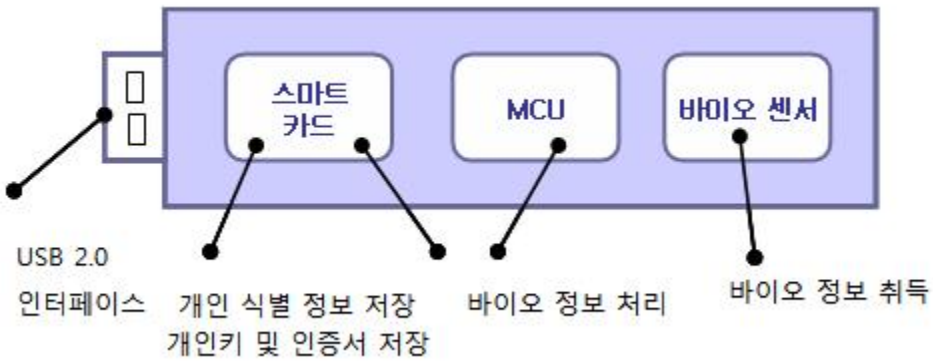


그림 5.1 바이오 보안 토큰 장치 모델의 한 예

5.2. 응용 프로그램과 바이오 보안 토큰 간 인터페이스 모델

다음 그림은 바이오 보안 토큰 API를 이용한 응용 프로그램과 바이오 보안 토큰 간 일반적 적용 모델을 도식화한 것이다.

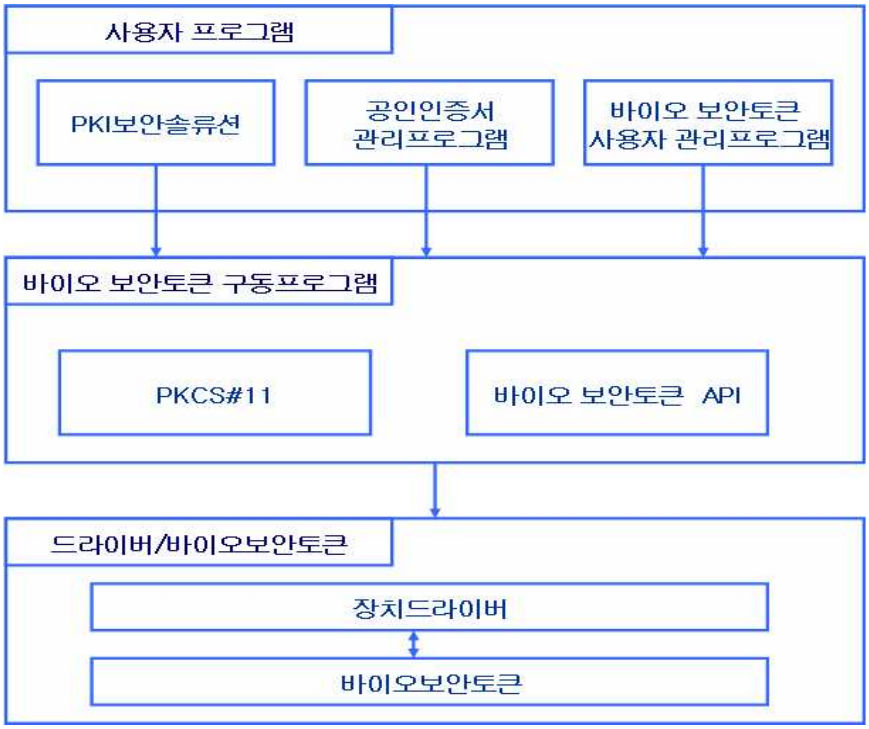


그림 5.2 응용 프로그램과 바이오 보안 토큰 간 인터페이스 모델

5.2.1. 보안 토큰 API

보안 토큰 API는 PC 환경에서 보안 토큰의 호환성을 제공할 수 있는 인터페이스로 RSA사의 PKSC#11 API을 기반으로 한 보안 토큰 API를 적용해야 한다.

5.2.2. 바이오 보안 토큰 API

일반적인 보안 토큰과의 구별을 위해 바이오 보안 토큰 여부를 식별할 수 있는 장치 인증 기능 지원 및 사용자 정보(주민등록번호, 사업자 번호)를 관리할 수 있어야 한다. 또한 보안 토큰 내부의 인증서와 사용자를 연결해 주기 위한 사용자 인증 기능을 제공하여야 하며, 인증된 사용자에 대하여 부록 I.[2]에 의해 식별된 인증서 정보를 제공하여야 한다. 이에는 보안 토큰 일련 번호, 바이오 정보 등록 유무 확인 등의 기능이 포함되어야 한다.

5.2.2.1. 바이오 보안 토큰 API 구조

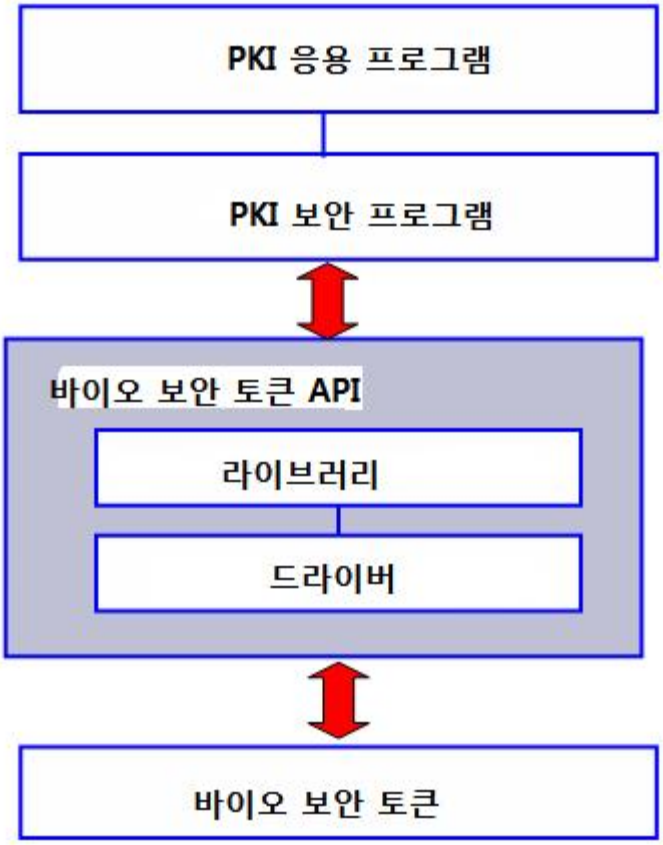


그림 5.3 바이오 보안 토큰 API 구조

바이오 보안 토큰 API는 공개 키 기반 구조(PKI) 보안 프로그램과 인터페이스를 담당하는 바이오 보안 토큰 API 라이브러리, 바이오 보안 토큰과 연동 및 하부 보안 기능을 제공하는 바이오 보안 토큰 드라이버로 구성된다.

바이오 보안 토큰 API는 바이오 보안 토큰 드라이브를 이용하여 사용자가 사용하는 보안 기능을 제공한다. 웹 접근성 지원을 위하여 바이오 보안 토큰 API는 Windows, Linux, Mac OS를 지원해야 한다. 또한 바이오 보안 토큰 드라이버는 바이오 정보를 관리하기 위한 바이오 보안 토큰 연결/해제, 전자 서명 생성, RSA 복호화 기능 등의 바이오 보안 토큰을 이용한 기본 기능을 제공한다.

5.2.2.2. 바이오 보안 토큰 API 사용법

1) bioOpenIn

- 바이오 보안 토큰과의 통신을 위한 채널을 Open 한다.
- int32 bioOpenIn(int32* ChID)

- Input

구분	타입	사이즈	비고
NA	NA	NA	NA

- Output

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

2) bioCloseOut

- 바이오 보안 토큰과의 통신을 위한 채널을 Close 한다.
- int32 bioCloseOut(int32 ChID)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

3) bioLoginBioAuth

- 바이오 보안 토큰의 등록되어 있는 BIO 정보 중 매칭되는 정보에 로그인 한다.
- int32 bioLoginBioAuth(int32 ChID)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

4) bioLoginSC

- 바이오 보안 토큰의 스마트카드에 로그인 한다.
- int32 bioLoginSC(int32 ChID, BYTE* PIN)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
PIN	BYTE*	8	로그인 사용자의 PIN

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

5) bioLogoutSC

- 바이오 보안 토큰의 스마트카드에서 로그아웃 한다.
- int32 bioLogoutSC(int32 ChID)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

6) bioGetTokenInfo

- 바이오 보안 토큰의 스마트카드에 저장된 인증서 정보를 구한다.
- 개인 인증서의 경우 인증된 사용자의 인증서만 사용 가능하도록 자동으로 설정한다.

- int32 bioGetTokenInfo(int32 ChID, int32 Division, BYTE* CertInfo)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2

- Output

구분	타입	사이즈	비고
CertInfo	BYTE*	6	스마트카드의 인증서 정보 주1)

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

주 1) 인증서 정보(6 bytes) = 현재 저장된 인증서 수(1 byte) + 인증서 유무 및 종류(4 bytes) + 예비용(RFU)(1 byte)

- 현재 저장된 인증서 수(1 byte)

※ 보안 토큰 내부에서는 전자 서명용, 키 분배용 인증서는 각각 다른 인증서로 취급된다.

- 인증서 유무 및 종류(4 bytes)
  - 0x00 : 없음
  - 0x01 : 서명용 범용
  - 0x02 : 서명용 용도 제한용(은행, 보험, 신용카드용)
  - 0x03 : 서명용 용도 제한용(조달청용)
  - 0x04 : 서명용 용도 제한용(증권, 보험용)
  - 0x05 : 키 분배용 범용
- 예비용(1 byte)
  - 0x06 ~ 0xFF
- 예) 0x04 0x03 0x03 0x03 0x03 0x00

  예) 범용 인증서(전자 서명용, 키 분배용이 모두 존재) 1 개가 저장되어 있는 경우

  -> 인증서에 전자 서명용과 키 분배용이 같이 존재함으로 보안 토큰에는 2 개의 인증이 서로 인식된다.

  -> 결과값 : 0x02 0x01 0x05 0x00 0x00 0x00

예) 금융 거래용 인증서(전자 서명용 존재), 범용 인증서(전자 서명용, 키 분배용이 모두 존재) 2 개가 저장되어 있는 경우

-> 금융 거래용 인증서에 전자 서명용만 존재함으로 보안 토큰에서 1 개의 인증서로 인식되고, 범용 인증서에 전자 서명용과 키 분배용이 존재함으로 보안 토큰에 2 개의 인증서로 인식됨으로 인증서 개수는 총 3 개가 되며, 그 종류는 순차적으로 표기된다.

-> 결과값 : 0x03 0x02 0x01 0x05 0x00 0x00

7) bioGetCertificate

- 바이오 보안 토큰의 스마트카드에 저장된 인증서를 읽어온다.
- int32 bioGetCertificate(int32 ChID, int32 Division, int32 CertIndex, BYTE* Certificate, int32* CertLength)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2
CertIndex	int32	1	사용할 인증서 Index (1 ~ 4)

- Output

구분	타입	사이즈	비고
Certificate	BYTE*	1600	스마트카드에 저장된 인증서
CertLength	int32*	1	인증서 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

8) bioGetRandom

- 바이오 보안 토큰의 스마트카드에 저장된 랜덤 값을 읽어온다.
- int32 bioGetRandom(int32 ChID, int32 Division, int32 CertIndex, BYTE* OutData, BYTE* CertPassword, int32 CertPasswordLength)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2
CertIndex	int32	1	사용할 인증서 Index (1 ~ 4)
CertPassword	BYTE*	1	인증서 비밀번호 문자열
CertPasswordLength	int32	1	인증서 비밀번호 문자열 길이

- Output

구분	타입	사이즈	비고
OutData	BYTE	20	개인 키 랜덤 값

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

9) bioGetSign

- 바이오 보안 토큰의 스마트카드에서 Sign 값을 구한다.
- int32 bioGetSign(int32 ChID, int32 Division, int32 CertIndex, BYTE* OutData BYTE* InData int32 InDataLength, BYTE* CertPassword, int32 CertPasswordLength)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2
CertIndex	int32	1	사용할 인증서 Index (1 ~ 4)
InData	BYTE*	1	서명할 데이터
InDataLength	int32	1	서명할 데이터 길이 (128 또는 256 bits)
CertPassword	BYTE*	1	인증서 비밀번호 문자열
CertPasswordLength	int32	1	인증서 비밀번호 문자열 길이

- Output

구분	타입	사이즈	비고
OutData	BYTE	20	Sign값

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

10) bioRSAPriDec

- 바이오 보안 토큰의 스마트카드에서 암호문을 RSA 복호화하여 값을 구한다.
- int32 bioRSAPriDec(int32 ChID, int32 Division, int32 CertIndex, BYTE* OutData, BYTE* InData int32 InDataLength, BYTE* CertPassword, int32 CertPasswordLength)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2
CertIndex	int32	1	사용할 인증서 Index (1~4)
InData	BYTE*	1	서명할 데이터
InDataLength	int32	1	서명할 데이터 길이 (128 또는 256 bits)
CertPassword	BYTE*	1	인증서 비밀번호 문자열
CertPasswordLength	int32	1	인증서 비밀번호 문자열 길이

- Output

구분	타입	사이즈	비고
OutData	BYTE	1	복호화된 데이터

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

11) bioGetIDN

- 스마트카드에서 사용자 식별 번호를 읽어온다
- int32 bioGetIDN(int32 ChID, int32 Division, BYTE* pIDN, int32* IDNLen);

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
Division	int32	1	법인 : 1, 개인 : 2

- Output

구분	타입	사이즈	비고
pIDN	BYTE*	20	사용자 식별 번호
IDNLen	int32	1	사용자 식별 번호 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

12) bioGetCSN

- 보안 토큰의 일련번호를 읽어온다
- int32 bioGetCSN(int32 ChID, BYTE* pSN, int32* SNLen);

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
pSN	BYTE*	20	보안 토큰 일련번호
SnLen	int32	1	보안 토큰 일련번호 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

13) bioGenDevAuth

- 장치 인증 값을 생성한다.
- int32 bioGenDevAuth(int32 ChID, BYTE KeyID, BYTE* pRandom, int32 Random Len, BYTE* pDevAuth, int32* DevAuthLen);

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID
KeyID	BYTE	1	장치 인증 키의 ID
pRandom	BYTE*	16	임의의 수
RandomLen	int32	1	임의의 수 길이

- Output

구분	타입	사이즈	비고
pDevAuth	BYTE*	1	장치 인증값
DevAuthLen	int32*	1	장치 인증값 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

14) bioGetManufacture

- 바이오 보안 토큰 제조사의 코드를 읽어온다.
- int32 bioGetManufacture(int32 ChID, BYTE* pCompCD, int32* CompCDLen);

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
pCompCD	BYTE*	3	제조사 코드 값
CompCDLen	int32*	1	제조사 코드 값 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

15) bioGetUserID

- 바이오 보안 토큰 API 모듈 객체 또는 이용 정보 객체의 사용자 ID를 반환한다.
- IE8이나 애플릿을 이용하는 환경에서 브라우저 창이 신규로 OPEN 되는 경우 기존의 창과 신규 창에서 사용되는 ActiveX나 애플릿에서 사용하는 정보가 유지되지 않는 부분을 해결하기 위해 사용한다.
- bioGetUserID() 함수에서 공유 정보 또는 필요한 정보를 가지고 있는 객체에 부여된 ID를 반환하고, bioSetUserID()에서는 입력받은 ID에 해당되는 객체에 공유 정보를 획득하여 bioOpenIn() 등과 같은 API 호출 없이 스마트카드 관련 기능을 사용 가능하도록 한다.
- int32 bioGetUserID(int32* userid);

- Input

구분	타입	사이즈	비고
NA	NA	NA	NA

- Output

구분	타입	사이즈	비고
userid	int32	1	객체의 사용자 ID

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

16) bioSetUserID

- bioGetUserID에서 얻은 객체 사용자 ID를 바이오 보안 토큰 API 모듈에 설정한다.
- IE8이나 애플릿을 이용하는 환경에서 브라우저 창이 신규로 OPEN 되는 경우 기존의 창과 신규 창에서 사용되는 ActiveX나 애플릿에서 사용하는 정보가 유지되지 않는 부분을 해결하기 위해 사용한다.
- bioGetUserID() 함수에서 공유 정보 또는 필요한 정보를 가지고 있는 객체에 부여된 ID를 반환하고, bioSetUserID()에서는 입력 받은 ID에 해당되는 객체에 공유 정보를 획득하여 bioOpenIn() 등과 같은 API 호출 없이 스마트카드 관련 기능을 사용 가능하도록 한다.
- 정보 보호를 위하여 기존 정보가 없는 신규 프로세스에서 이 함수를 호출 시 PIN 인증과 같은 보안 조치를 취하여야 한다.
- int32 bioSetUserID(int32 userid)

- Input

구분	타입	사이즈	비고
userid	int32	1	객체의 사용자 ID

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

17) bioLogoutBioAuth

- 바이오 정보에서 로그아웃한다
- int32 bioLogoutBioAuth(int32 ChID)

- Input

구분	타입	사이즈	비고
ChID	Int32	1	채널 ID

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

18) bioUsbDataEnc

- USB로 전송할 데이터를 암호화한다
- int32 bioUsbDataEnc(BYTE *inData,int32 inLength,BYTE *outData,int32 outLength)

- Input

구분	타입	사이즈	비고
inData	BYTE	1	암호화할 데이터
inLength	Int32	1	암호화할 데이터 길이

- Output

구분	타입	사이즈	비고
outData	BYTE	1	암호화된 데이터
outLength	Int32	1	암호화된 데이터 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

19) bioUsbDataDec

- USB에서 전송된 데이터를 복호화한다
- int32 bioUsbDataDec(BYTE *inData,int32 inLength,BYTE *outData,int32 outLength)

- Input

구분	타입	사이즈	비고
inData	BYTE	1	복호화할 데이터
inLength	Int32	1	복호화할 데이터 길이

- Output

구분	타입	사이즈	비고
outData	BYTE	1	복호화된 데이터
outLength	Int32	1	복호화된 데이터 길이

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

20) bioGetFunctionList

- 지원하는 함수의 리스트를 제공한다
- Int32 bioGetFunctionList(char *FunList,int32 *FunNamesize, int32 *FunNum)

- Input

구분	타입	사이즈	비고
NA	NA	NA	NA

- Output

구분	타입	사이즈	비고
FunList	char	1	지원 함수 리스트 배열
FunNameSize	Int32	1	지원 함수명 길이 배열
FunNum	Int32	1	지원 함수의 수

- Return

구분	타입	사이즈	비고
Return Value	int32	1	0(성공) 또는 에러 코드

21) 에러 코드

구분	코드	내 용
장치	100	보안 토큰이 연결되어 있지 않는 경우
	101	최대 연결 오류(PC에 연결 가능한 보안 토큰 수 초과 오류)
	102	보안 토큰이 PC에 인식되지 않아 연결 에러 발생
	103	USB 통신 오류
	104	카드 명령어 수행 에러
	105	바이오 인증 없이 카드 사용
바이오 정보	131	바이오 정보 템플릿 없음 바이오 정보가 등록되어 있지 않아 오류 발생
	132	바이오센서 타임 아웃(20 초)
	133	바이오 인증 실패
	134	바이오 인증 ID 없음
	135	바이오 센서 H/W 에러
	136	바이오 알고리즘 비정상 종료
카드	141	스마트카드 연결 안 됨
	142	스마트카드 응용 프로토콜 데이터 단위(APDU, Application Protocol Data Unit) 인증 에러
PIN	27012	PIN Lock 상태(0x6984)
	25540 ~ 25536	PIN 인증 오류 - 25540 : PIN 인증 4 회 남음 - 25539 : PIN 인증 3 회 남음 - 25538 : PIN 인증 2 회 남음 - 25537 : PIN 인증 1 회 남음 - 25536 : PIN 인증 0 회 남음 (0x63Cx : x : PIN 인증 남은 횟수)

구분	코드	내 용
파라미터	4000	파라미터 값이 유효하지 않음

5.2.3. 바이오 보안 토큰을 위한 사용자 정보 관리 API

바이오 보안 토큰을 위한 사용자 정보 관리 API는 다음 그림에서와 같이 네 가지 기능 영역으로 구분될 수 있다.

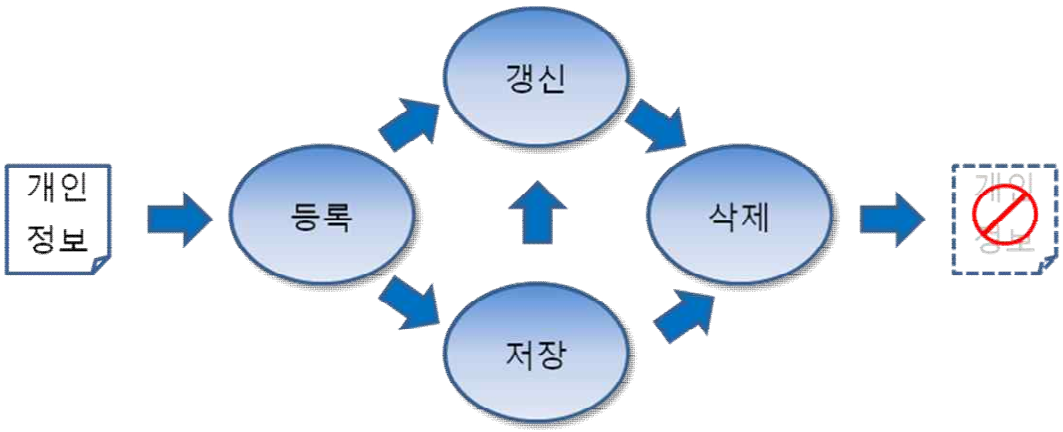


그림 5.4 바이오 보안 토큰에서의 사용자 개인 정보 관리를 위한 API 구조

5.2.3.1. 바이오 보안 토큰을 위한 사용자 정보 등록 API

바이오 보안 토큰을 위한 사용자 정보 등록 API란 지문 센서나 기타 바이오 센서를 통해 수집한 바이오 정보와 사용자 개인의 사적 정보들과 같이 바이오 보안 토큰을 사용하는 응용 시스템에서 개인 식별에 사용되는 정보들을 시스템에 등록하기 위해 필요한 API들을 말한다. 등록되는 정보로는 센서를 통해 수집한 바이오 정보 또는 바이오 정보에서 추출된 특징 정보가 있고, 이밖에 사용자의 사적 정보들이 포함된다. 바이오 보안 토큰을 사용하는 응용 시스템의 요구 조건에 따라 이와 같은 사용자 정보는 암호화되어 등록되는 것이 가능하다.

5.2.3.2. 바이오 보안 토큰을 위한 사용자 정보 저장 API

사용자 정보는 일차적으로 등록 과정을 거쳐 시스템에 최종 저장된다. 등록이 맨 처음 인증에 참여할 개인의 식별 정보를 입력하는 과정이라고 하면 여기서의 저장은 등록 이후에도 추가될 수 있는 개인 정보들을 별도로 관리하기 위한 기능 구분이라고 할 수 있다.

5.2.3.3. 바이오 보안 토큰을 위한 사용자 정보 갱신 API

일부 개인 정보에 있어서 등록 또는 저장 후 수정이 필요한 경우가 발생할 수 있다. 이 경우, 바이오 보안 토큰을 위한 사용자 정보 갱신 API를 이용하여 시스템으로 하여금 정보 갱신을 수행토록 유도할 수 있다. 이 경우 갱신 전후의 정보에 대한 무결성, 내용의 정확성 등이 보장될 수 있도록 표준 API를 통한 갱신 절차를 규격화할 필요가 있다.

5.2.3.4. 바이오 보안 토큰을 위한 사용자 정보 삭제 API

더 이상 사용하지 않는 개인 식별 정보 등은 적법한 절차를 거쳐 삭제가 가능해야 한다. 보안 토큰 내의 모든 정보는 표준 API를 이용한 삭제 진행이 이루어져야 안전한 폐기가 가능해진다.

5.2.3.5. 기타 API

위 네가지 기능 분류에 속하지는 않지만 사용자 정보, 즉, 개인 식별 정보와 바이오 정보, 사용자 개인 정보 등을 다루는 데 있어 필요한 기능들을 API화하여 정리한다.

부 속 서 A

바이오 보안 토큰 API 요약

구분	함수명	기능
바이오 보안 토큰	bioOpenIn	바이오 보안 토큰과의 통신을 위한 채널을 Open한다.
	bioCloseOut	바이오 보안 토큰과의 통신을 위한 채널을 Close한다.
스마트카드	bioLoginSC	스마트카드에 로그인한다.
	bioLogoutSC	스마트카드에 로그아웃한다.
	bioGetTokenInfo	스마트카드에 저장된 인증서 정보를 구한다.
	bioGetCertificate	스마트카드에 저장된 인증서를 읽어온다.
	bioGetRandom	스마트카드에 저장된 개인 키의 랜덤값을 읽어온다.
	bioGetSign	스마트카드에서 Sign값을 구한다
	bioRSAPriDec	스마트카드에서 암호문을 RSA 복호화하여 값을 구한다.
	bioGetIDN	스마트카드에서 사용자 식별 번호를 읽어온다
	bioGetCSN	보안 토큰의 일련번호를 읽어온다
	bioGenDevAuth	장치 인증 값을 생성한다.
	bioGetManufacture	보안 토큰 제조사 코드를 읽어온다
바이오인증	bioLoginBioAuth	바이오 보안 토큰의 등록되어 있는 바이오 템플릿 중 매칭되는 바이오 정보에 로그인 하되 지문 인증이 성공할 때까지 결과를 반환하지 않는다
	bioLogoutBioAuth	바이오 정보에서 로그아웃한다
기타	bioGetUserID	사용자 ID를 반환한다.
	bioSetUserID	사용자 ID를 설정한다.
	bioUsbDataEnc	USB로 전송할 데이터를 암호화한다
	bioUsbDataDec	USB에서 송신한 데이터를 복호화 한다.
	bioGetFunctionList	제공하는 함수 리스트 제공

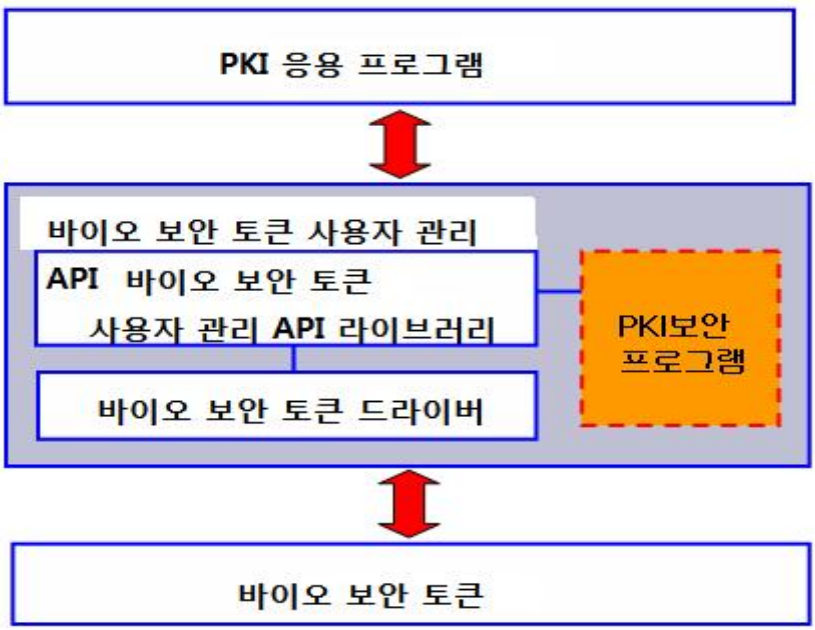
부 속 서 B

바이오 보안 토큰 사용자 관리 API

B.1. 바이오 보안 토큰을 위한 사용자 관리 API

구분	함수명	기능
관리자 API 기능	DataEncrypt	입력된 데이터를 암호화 및 전자 서명한다.
	DataDecrypt	입력된 데이터를 복호화 및 전자 서명 검사한다.
	GetUserCert	사용자의 인증서를 읽어온다.
	BHManageReq	바이오 보안 토큰 관리 요청 메시지를 생성한다.
	BHManageReg	바이오 보안 토큰에 바이오 정보를 등록, 추가, 삭제, 보기, 초기화 등 관리한다.
	BHGetCSN	바이오 보안 토큰에서 제품 일련번호를 읽는다.
	BHGetManufacture	바이오 보안 토큰에서 제조사 정보를 읽는다.
	BHCheckKey	장치 인증 키가 저장되었는지 확인한다.
	BHWriteDeviceKey	장치 인증 키를 저장한다.
	BHRestPIN	핀 번호 초기화 수행

B.2. 바이오 보안 토큰 관리자 API 구조



바이오 보안 토큰 관리자 API는 보안 토큰 관리 프로그램과 인터페이스를 담당하는 바이오 보안 토큰 관리 ActiveX, 사용자의 바이오 정보를 등록 및 관리하는 기능을 제공하는 바이오 보안 토큰 드라이브, 관리 API 외부로 데이터 전달 시 정보보호를 위한 PKI 보안 프로그램으로 구성된다.

바이오 보안 토큰 관리 라이브러리는 보안 토큰 드라이버와 PKI 보안 프로그램을 이용하여 관리자가 사용자의 바이오 정보를 관리하는 기능과 관리 UI(User Interface)와 보안 기능을 제공한다.

바이오 보안 토큰 드라이버는 바이오 보안 토큰의 바이오 정보를 관리하기 위한 사용자 등록/변경/삭제, 바이오 정보 등록/수정/삭제의 기본 기능을 제공한다.

PKI 보안 프로그램은 API 외부로 정보를 전달 시 토큰 내부의 정보를 보호하기 위하여 사용된다. PKI 보안 프로그램은 자체 개발 또는 상용 제품을 사용하거나 특정 목적으로 사용하는 PKI 보안 프로그램을 이용하여도 된다.

관리자 보안 토큰은 바이오 보안 토큰 관리자API를 지정된 관리자 이외의 임의 사용자가 사용을 하지 못하도록 하기 위하여 별도 보안 토큰으로 만들어 제공하여야 한다. 바이오 보안 토큰 관리자 API 동작 시 반드시 관리자 보안 토큰이 존재하는지 확인하여 존재하지 않는 경우 동작을 하지 않도록 한다.

B.3. 바이오 보안 토큰 관리자 API 설명

B.3.1. DataEncrypt

- 입력된 값에 대하여 전자 서명을 첨부한 후 PKCS#7 메시지를 생성한다.
- BSTR *DataEncrypt(BSTR inData, BSTR inCert)
- (In JavaScript) var DataEncrypt(var inData, var inCert)

- Input

구분	타입	사이즈	비고
inData	BSTR	1	입력 데이터
inCert	BSTR	1	서버 암호화 인증서

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	PKCS#7 메시지

B.3.2. DataDecrypt

- 서버로부터 전송되어온 값에 대하여 PKCS#7 복호화 및 전자 서명 검사를 수행.
- BSTR *DataDecrypt(BSTR inData)
- (In JavaScript) var DataDecryp(var inData)

- Input

구분	타입	사이즈	비고
inData	BSTR	1	PKCS#7 데이터

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	int32	1	PKCS#7 메시지

B.3.3. GetUserCert

- 관리자가 보안 처리를 위하여 선택한 인증서를 반환한다.
- BSTR *GetUserCert(BSTR inType)
- (In JavaScript) var GetUserCert(var inType)

- Input

구분	타입	사이즈	비고
inType	BSTR	1	인증서 타입 S: 전자 서명 인증서 E: 암호화 인증서

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	1	PEM 타입 인증서

B.3.4. BHManageReq

- 입력된 값을 이용하여 서버로 전송할 바이오 보안 토큰 관리 요청 메시지를 생성.
- BSTR *BHManageReq(BSTR inManageCode, BSTR inBizNo, BSTR inNationalID, BSTR inCert)
- (In JavaScript) var BHManageReq(var inManageCode, var inBizNo, var inNationalID, var inCert)

- Input

구분	타입	사이즈	비고
inManageCode,	BSTR	2	관리코드 “RE” : 요청 정보 확인 “RG” : 사용자 등록 “FU” : 바이오 정보 추가등록 “DU” : 사용자 삭제 “IQ” : 정보 조회 “PI” : PIN 초기화 “TI” : 토큰 초기화
inBizNo	BSTR	10	사업자 번호
inNationalID	BSTR	13	주민등록번호
inCert	BSTR	1	서버 암호화 인증서

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	1	PEM 타입 인증서

B.3.5. BHManageReg

- 관리자가 보안 처리를 위하여 선택한 인증서를 반환한다.
- BSTR BHManageReg(BSTR inManageCode, BSTR inData, BSTR inCert)
- (In JavaScript) var BHManageReg(var inManageCode, var inData, var inCert)

- Input

구분	타입	사이즈	비고
inManageCode,	BSTR	2	관리 코드 “RE” : 요청 정보 확인 “RG” : 사용자 등록 “FU” : 바이오 정보 추가 등록 “DU” : 사용자 삭제 “IQ” : 정보 조회 “PI” : PIN 초기화 “TI” : 토큰 초기화
inData	BSTR	1	관리 요청 정보 PKCS#7 메시지 (전자 서명 및 암호화 형식)
inCert	BSTR	1	서버 암호화 인증서

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	1	PKCS#7 메시지

B.3.6. BHGetCSN

- 바이오 보안 토큰에서 제품 일련번호를 얻어온다.
- BSTR*BHGetCSN()
- (In JavaScript) var BHGetCSN()

- Input

구분	타입	사이즈	비고
NA	NA	NA	NA

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	20	제조사 제품 일련번호

B.3.7. BHGetManufacture

- 바이오 보안 토큰에서 제조사 코드를 얻어온다.
- BSTR *BHGetManufacture()
- (In JavaScript) var BHGetManufacture()

- Input

구분	타입	사이즈	비고
NA	NA	NA	NA

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	3	제조사 코드

B.3.8. BHCheckKey

- 바이오 보안 토큰에서 장치 인증 키가 등록되어 있는지 확인한다.
- BSTR*BHCheckKey(BSTR KeyID)
- (In JavaScript) var BHCheckKey(var KeyID)

- Input

구분	타입	사이즈	비고
KeyID	BSTR	2	‘01’을 사용

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	1	등록 여부 1: 등록, 0: 미등록

B.3.9. BHWriteDeviceKey

- 바이오 보안 토큰에서 장치 인증 키를 저장한다.
- BSTR*BHWriteDeviceKey(BSTR KeyID, BSTR DeviceKey)
- (In JavaScript) var BHWriteDeviceKey(var KeyID, var DeviceKey)

- Input

구분	타입	사이즈	비고
KeyID	BSTR	2	'01'을 사용
DeviceKey	BSTR	32	장치 인증 키 Hexa 스트링

- Output

구분	타입	사이즈	비고
NA	NA	NA	NA

- Return

구분	타입	사이즈	비고
Return Value	BSTR	1	1: 성공, 0: 실패

부 록 I

관련 문헌

다음 문서들은 본 표준의 이해를 돕기 위한 문서로서 특정 문서(발행일 및 판 번호 또는 개정 번호를 명시한 것)와 일반 문서로 구별된다.

- 특정 문서인 경우 해당 판본 이후의 개정판은 적용되지 않는다.
- 일반 문서인 경우 최신 판본이 적용된다.

[1] KISA, KCAC.TS.HSM, '보안 토큰 기반의 공인 인증서 이용 기술 규격', 2007.

[2] KISA, KCAC.TS.SIVID, '식별 번호를 이용한 본인 확인 기술 규격', 2009.

방송통신표준

바이오 보안 토큰용 API
(API for Biometric Hardware Security Module(BHSM))

발행인 : 미래창조과학부 장관
발행처 : 미래창조과학부 국립전파연구원
140-848, 서울 용산구 원효로41길 29
발행일 : 2013.12.
국립전파연구원 고시 제 2013-20호