스마트인증 인터페이스 가이드라인

User Interface Guideline for Mobile Hardware Security Module

v2.00

2013년 11월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

스마트인증 인터페이스 가이드라인
User Interface Guideline for Mobile Hardware Security

1. 개요

본 가이드라인에서는 가입자가 스마트폰 등 모바일 기기 내의 USIM, microSD 와 같은 하드웨어 보안토큰 기반으로 공인인증서를 편리하게 저장·이용할 수 있도록 가입자 소프트웨어 등이 갖추어야 할 사용자 인터페이스 관련 요구사항을 기술한다.

2. 구성 및 범위

본 가이드라인은 사용자 측면에서 스마트인증 기반의 공인인증서를 쉽게 이용할 수 있도록 스마트인증 연결 및 구동프로그램 설치, 접근 비밀번호 설정, 공인인증서 발급·관리, 오류사항 처리 등에 대해 명시하고 있다.

3. 관련 표준

3.1 국외 표준 및 규격

[PKCS11] RSA Laboratories PKCS#11, Cryptographic Token Interface Standard v2.11, 2001

3.2 국내 표준 및 규격

[KCAC.TS.HSMU] KISA, *보안토큰 기반의 공인인증서 이용기술 규격 v2.10*, 2012.11

[KCAC.TS.CM] KISA, *무선단말기에서의 공인인증서 저장 및 이용 기술규격 v1.30*, 2012.11

[KCAC.TG.DGH] KISA, *보안토큰 구동프로그램 배포 가이드라인 v1.0*, 2012

3.3 기타

[PC/SC] PC/SC Workgroup, *PC/SC Workgroup Specifications 2.01.3*, http://www.pcscworkgroup.com/specifications/overview.php

[USB 2.0] USB Implementers Forum, Inc., *Universal Serial Bus Revision 2.0 Specifications,* http://www.usb.org/developers/docs/

[ISO7816] ISO/IEC 7816, *Identification Cards – Integrated Circuit(s) cards with contacts Part 1 to 10*

4. 정의

4.1 전자서명법 용어 정의

본 가이드라인에서 사용된 다음의 용어들은 법률 제6585호 및 동법 시행령에 정의되어 있다.

가) 공인인증서

나) 가입자

다) 가입자 소프트웨어

4.2 용어의 정의

가) 스마트인증 : 스마트폰과 같은 모바일 기기의 USIM, eSE 등 보안모듈을 모바일 통신을 통해 PC와 같은 타 기기에 연결하여 전자서명생성키 등 비밀정보를 안전하게 저장·보관하고, 키생성 및 전자서명 생성 등을 처리하는 하드웨어와 소프트웨어의 총칭

나) 다중 USIM서비스 연계 : 가입자소프트웨어에서 구동프로그램을 호출 후 타 USIM서비스제공자의 가입자일 경우 해당 서비스제공자의 보안토큰 구동프로그램을 호출하는 방식을 총칭

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야한다, 필수이다, 강제한다 (기호 : M)
반드시 준수해야 한다.

나) 권고한다 (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.

다) 할 수 있다, 쓸 수 있다 (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.

라) 권고하지 않는다 (기호 : NR)

보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.

마) 금지한다, 허용하지 않는다 (기호 : X)
반드시 사용하지 않아야 한다.

바) 언급하지 않는다, 정의하지 않는다 (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어

본 가이드라인에서는 다음의 약어가 이용된다.

가) eSE : Embedded Secure Element, 내장형 보안모듈

나) PIN : Personal Identification Number, 개인식별번호

다) microSD : Micro Secure Digital Card

라) USIM : Universal Subscriber Identity Module, 범용사용자식별모듈

6. 스마트인증 인터페이스

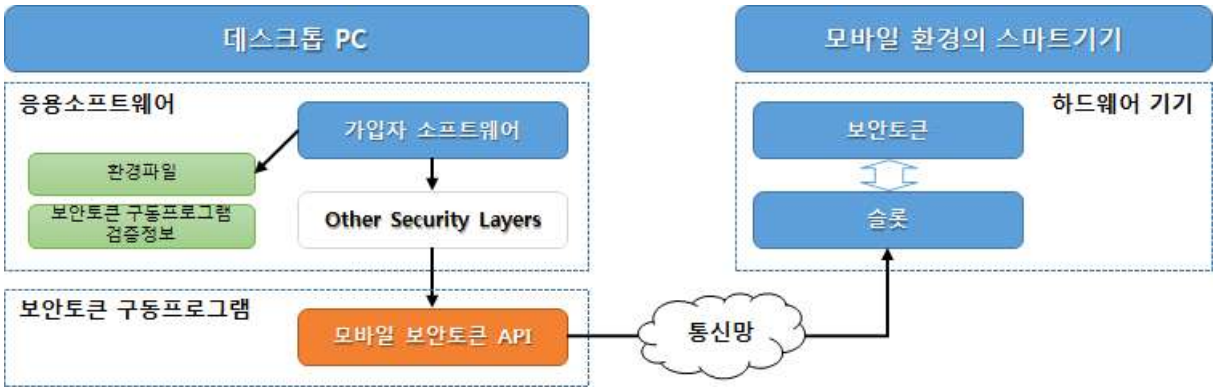
6.1 인터페이스 모델

보안토큰은 구현된 하드웨어 기기에 따라 다양한 형태를 가지며, 보안특성에 따라 전자서명생성키 등 비밀정보는 기기 외부로 노출 및 유출되지 않는다. 이러한 특성으로 인해 모바일 환경의 USIM, eSE, microSD카드 등에 구현된 보안토큰 내 저장된 인증서를 데스크톱PC 등 다른 기기에서 이용하고자 하는 경우 제약이 생긴다.

모바일 환경의 스마트폰 등 모바일 기기에서 보안토큰 이용 시, 보안토큰의 인증서 유·노출 방지라는 장점을 가진 채 데스크톱 환경에서도 이용할 수 있도록 보완한 것이 스마트인증 인터페이스이다.

모바일 환경의 보안토큰 하드웨어, 보안토큰을 이용하는 모바일 플랫폼 및 원격으로 연결하고자 하는 기기의 플랫폼, 가입자 소프트웨어 및 보안토큰 API(PKCS#11) 간의 일반적인 인터페이스 모델은 [그림 1]과 같다.

데스크톱과 무선단말기간의 연결 및 통신을 위해 중계서비스가 이용될 수 있으며, 중계서비스는 공인인증서의 발급, 공인인증서의 전송, 전자서명 요청 및 전송 등의 기능에 이용된다. 중계서비스는 안정적 서비스 제공을 위해 공인인증기관이 운영·



[그림 1] 스마트인증 인터페이스 모델

제공할 것을 권고한다.

스마트인증 인터페이스는 '보안토큰 기반 공인인증서 이용기술 규격'을 준용한다.

6.2 구동프로그램 설치

스마트인증 인터페이스 이용을 위해 구동프로그램이 필요한 경우, 공인인증서 가입자 소프트웨어에 스마트인증 구동프로그램을 함께 포함시키거나, 가입자에게 구동프로그램 설치와 관련한 공지 후 가입자가 직접 설치할 수 있도록 한다. 가입자 소프트웨어는 가입자에게 구동프로그램 설치를 공지하기 위해 홈페이지로 이동할 수 있도록 링크를 제공할 수 있다.

KISA는 가입자가 스마트인증 구동프로그램에 대한 정보를 제공하기 위해 평가인증 받은 모바일 기기용 보안토큰 제품사진, 구동프로그램 설치 URL 등을 홈페이지에 게시할 수 있다.

스마트인증 구동프로그램은 '보안토큰 기반 공인인증서 이용기술 규격' '부록 4. 환경파일을 이용한 보안토큰 구동프로그램 위치정보 관리'에 따라 환경파일을 구성·이용하여야 한다. 스마트인증의 경우 하위 섹션명은 '[USIM_****]' 하위에 위치정보를 구성하며 구동프로그램 정보(Info) 앞에 'MOBILE_'을 연접하여 사용한다. '****'은 일련번호로 USIM에 대한 구현적합성 평가인증 순서에 따라 부여한다.

6.3 비밀번호 관리

스마트인증 인터페이스를 활용한 공인인증서비스 편의성을 제고하기 위해 '스마트인증 PIN' 용어는 '스마트인증 비밀번호'로 대체하여 사용한다.

스마트인증 이용의 안전성을 고려하여 스마트인증 초기 비밀번호를 사용 전에 재

설정할 수 있도록 가입자에게 공지하여야 한다.

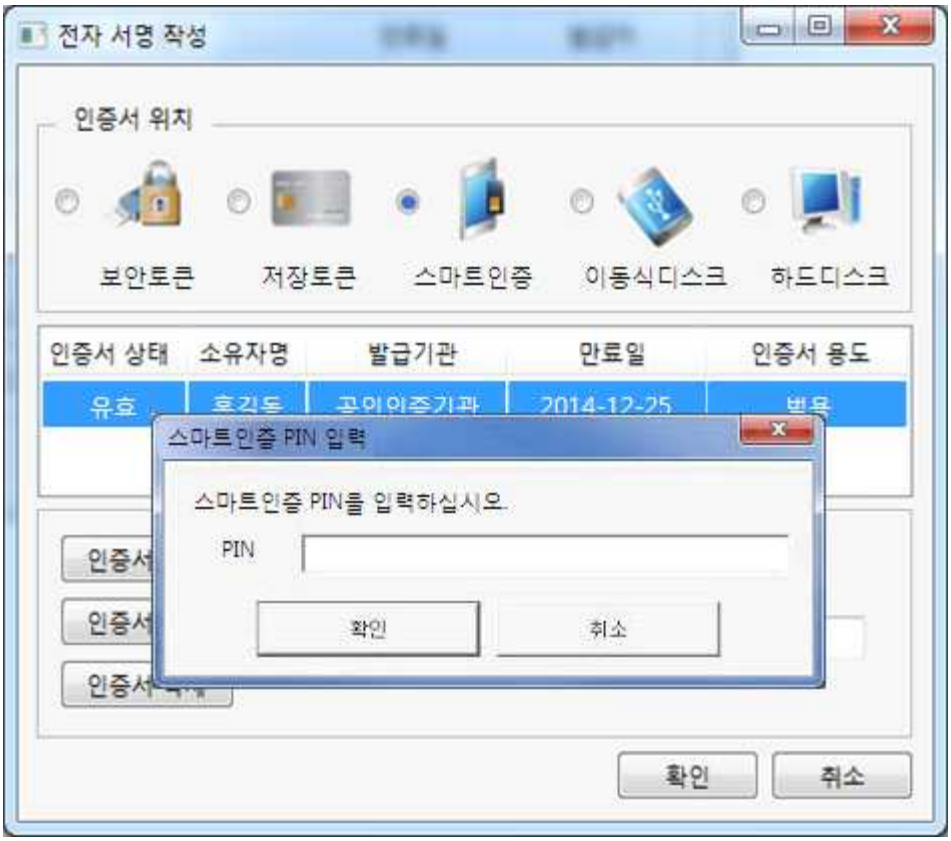
6.4 스마트인증 이용

스마트인증 인터페이스 이용을 위해 데스크톱PC와 모바일환경의 모바일 기기 간의 연결이 필요하며, 연결을 위한 추가적인 정보를 요구할 수 있다. 연결이 완료된 후 모바일 기기내의 보안토큰에 저장된 모든 공인인증서 목록을 PC화면 또는 스마트 기기 화면에 표시한다.

가입자는 모바일 기기에서 전자서명 수행 시마다 스마트인증의 비밀번호를 입력하여야 한다. 스마트인증 비밀번호는 PC 또는 스마트 기기에서 입력할 수 있으며, 사용 후 메모리에서 안전하게 삭제하여야 한다.

가입자 소프트웨어는 공인인증서 비밀번호(암호) 입력창을 통해 가입자의 스마트인증 비밀번호를 입력받을 수 있다. 또한, 별도의 인터페이스 또는 스마트인증 구동프로그램을 통해 비밀번호를 입력받을 수 있는데, 이 경우 가입자 소프트웨어의 공인인증서 비밀번호(암호) 입력창은 비활성화 되어야 한다.

스마트인증 구동프로그램은 확인메시지 표시 등을 통해 가입자가 스마트인증을 통해 전자서명이 수행되고 있음을 인지할 수 있도록 하여야 한다.



[그림 2] 스마트인증의 PIN 입력의 예

6.5 공인인증서 발급

스마트인증 인터페이스를 통해 공인인증서 발급·관리 시 지연될 수 있는 시간(1분 이상)에 대해 가입자에게 고지할 수 있다.

스마트인증 인터페이스를 통한 공인인증서 발급·관리 시 오류가 발생할 경우 예외처리를 통해 스마트인증 내 메모리를 원상태로 되돌릴 수 있도록 한다.

6.6 메모리 관리

가입자 소프트웨어는 모바일 기기의 보안토큰 메모리가 부족하여 공인인증서 신규 발급, 재발급, 갱신, 가져오기 등이 수행되는 도중 오류가 발생할 수 있음을 가입자에게 고지할 수 있다. 가입자 소프트웨어는 C_GetTokenInfo 함수를 통해 스마트인증 내에 가용한 공개영역 메모리를 확인할 수 있는데, 해당 공개영역 메모리 여유분이 인증서 개당 최소 필요 메모리보다 적을 경우 가입자에게 메모리 부족 메시지를 보여줄 것을 권고한다.

또한, 가입자 소프트웨어는 가입자가 모바일 기기의 보안토큰 내 불필요한 인증서를 삭제하고 메모리를 확보할 수 있도록 삭제 기능 및 자동으로 불필요한 키쌍 등을 삭제할 수 있는 모바일 기기의 보안토큰 메모리 정리기능을 제공할 수 있다.

6.7 오류사항 처리

[KCAC.TS.HSMU] 중 “부록 6. 보안토큰 API(PKCS#11) 반환값 프로파일”에 따라 스마트인증 가입자에게 오류사항을 고지할 수 있다.

7. 스마트인증(USIM)

스마트폰 USIM을 활용한 스마트인증 서비스(이하 USIM 스마트인증) 제공에 대한 기본 요구사항, USIM과의 연결을 통한 공인인증서의 발급·저장 및 이용절차 등의 사항을 기술한다.

7.1 기본 요구사항

USIM 스마트인증 이용을 위해서는 스마트폰용 앱 설치와 데스크톱용 구동프로그램 설치 등이 필요하다. 스마트폰용 앱은 해당 스마트폰 앱스토어를 통해 설치하며 데스크톱용 구동프로그램은 스마트폰용 앱과 함께 제공되는 서비스 안내페이지

또는 스마트폰용 앱을 통해 다운받아 설치할 수 있다. 데스크톱용 구동프로그램이 가입자 소프트웨어에 포함되어 배포되는 경우 별도의 설치과정을 생략할 수 있다.

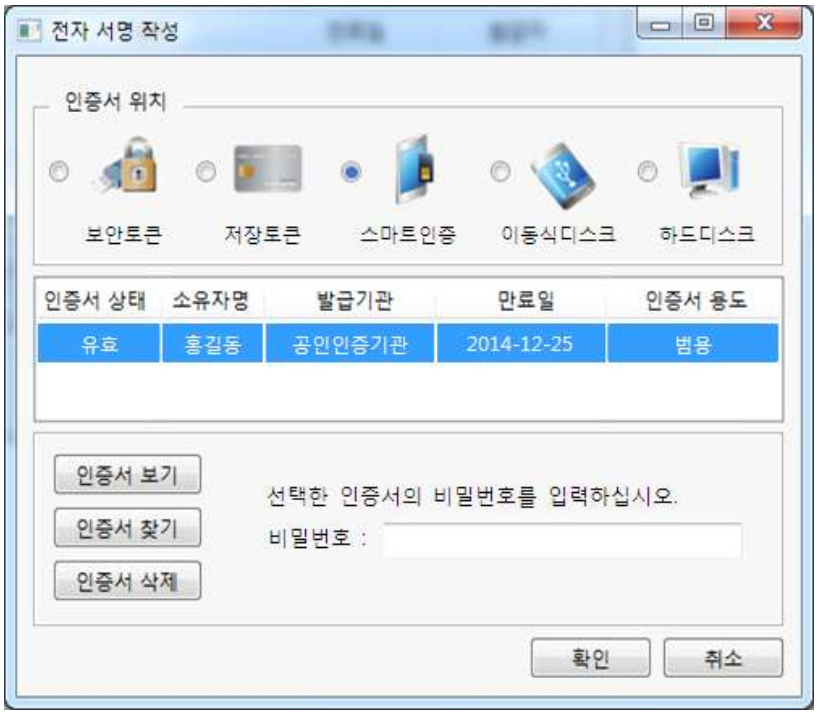
7.2 USIM 구동프로그램 호출

가입자 소프트웨어는 USIM 스마트인증 선택 시 데스크톱용 구동프로그램을 호출하며, 다수의 데스크톱용 구동프로그램이 설치되어 있는 경우 사용자가 원하는 스마트인증 서비스를 원활히 이용할 수 있도록 데스크톱 구동프로그램 간에 연계할 것을 권고한다.

데스크톱 구동프로그램 간 연계는 부록 1. 다중 USIM 서비스 연계 보안토큰 프로파일을 준용한다. USIM 스마트인증 초기화 과정에서 사용자가 가입된 USIM 스마트인증을 이용할 수 있도록 이동통신사 및 USIM 서비스 가입정보를 연계하여 적합한 데스크톱 구동프로그램을 실행하도록 한다. 이 경우 이동통신사, 스마트폰 번호 등의 정보를 구동프로그램에 전달하여 이동통신사, 스마트폰 번호 입력을 생략할 수 있다.

7.3 USIM과의 연결

스마트폰 USIM과의 연결을 위해서는 이동통신사의 선택, 스마트폰 번호의 입력 등 USIM과의 연결을 위한 추가적인 정보를 요구할 수 있다. 데스크톱과 USIM과의 연결이 완료된 후 USIM에 저장된 모든 공인인증서 목록을 데스크톱 화면 또는 스마트폰 화면에 표시한다.



7.4. 인증서 발급 및 저장

인증서를 USIM 스마트인증에 저장하는 방법은 인증서 신규발급 또는 기존 발급 받은 인증서를 USIM 스마트인증으로 전송하여 저장하는 방법이 있다.

1) 인증서 신규발급 방법

① 사용자는 인증서 발급을 원하는 사이트에서 인증서 저장매체를 '스마트인증(또는 USIM)'으로 선택한다.

② 스마트인증 서비스를 제공하는 통신사 선택 및 휴대폰 번호를 입력한다.

③ 스마트폰 앱 실행 후 전자서명 확인 및 PC에서 서비스 비밀번호를 입력한다.

④ 인증서 발급이 완료되고 스마트폰 앱에서 발급된 인증서를 확인한다.

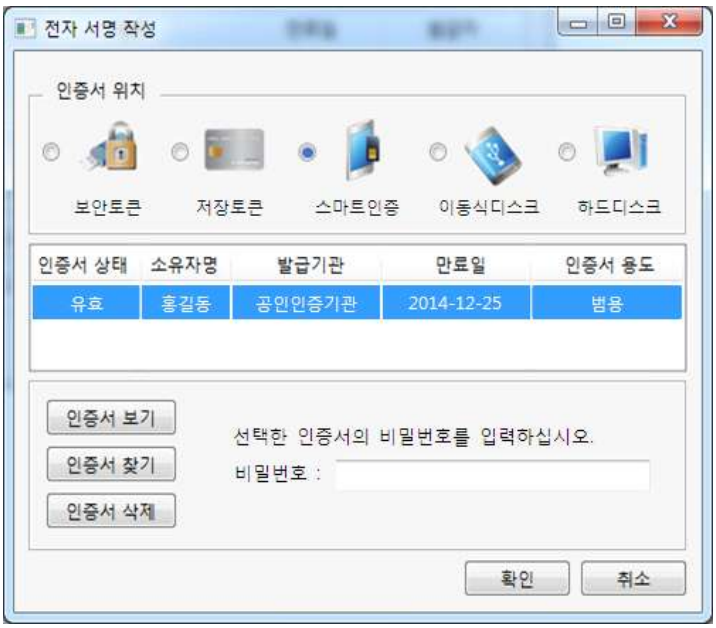
2) 인증서 가져오기 방법

인증서를 데스크톱에서 스마트폰으로 가져오기 방법은 '무선단말기와 PC간 공인인증서 전송을 위한 기술규격'을 준용한다.

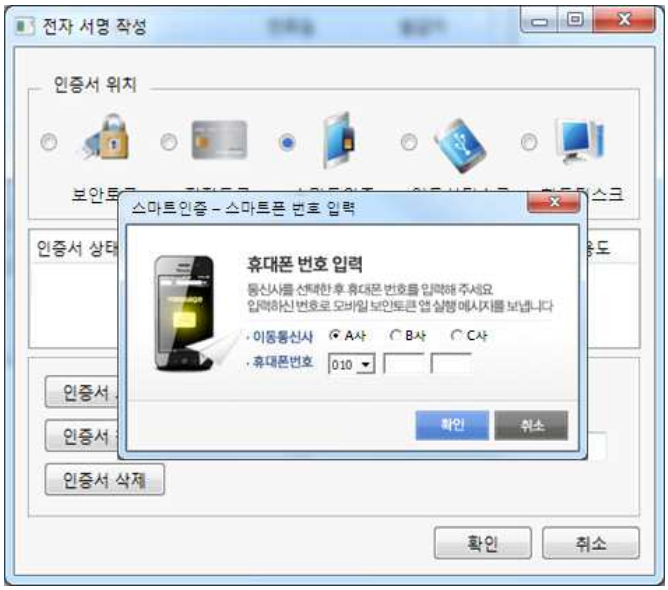
7.5. 전자서명

본 서비스를 이용하여 전자서명하기 위해서는 가입자의 통신사 선택 및 스마트폰 번호 입력 등을 통하여 서비스 가입여부 확인 후 전자서명을 할 수 있다.

① 사용자는 PC에서 인증서의 저장매체로 "스마트인증'을 선택한다.



② 스마트인증 서비스를 제공하는 이동통신사 선택 및 스마트폰 번호를 입력한다.



③ 스마트인증에 저장된 인증서 목록을 PC 화면에 보여주고, 목록에서 서명할 공인인증서를 선택 후 스마트인증 비밀번호를 입력하여 전자서명 생성을 완료한다.

부록 1. 다중 USIM 서비스 연계 보안토큰 프로파일

1. PKCS#11 연계

서비스 정보처리를 위한 MOBILETOKEN_ARGS 구조체는 PKCS#11 API의 초기화 함수인 C_Initialize 함수를 이용하여 사용한다.

USIM 스마트인증 구동프로그램에 서비스정보를 전달하기 위한 C_Initialize 파라미터인 CK_C_INITIALIZE_ARGS 구조체는 다음과 같다.

```
typedef struct CK_C_INITIALIZE_ARGS {
    CK_CREATEMUTEX      CreateMutex;
    CK_DESTROYMUTEX     DestroyMutex;
    CK_LOCKMUTEX        LockMutex;
    CK_UNLOCKMUTEX      UnlockMutex;
    CK_FLAGS            flags;
    CK_VOID_PTR         pReserved;
} CK_C_INITIALIZE_ARGS;
```

일반적으로 보안토큰 사용 시 C_Initialize의 입력파라미터로 NULL을 사용하나 스마트인증의 경우 서비스 정보처리를 위하여 C_Initialize 함수의 옵션 파라미터인 CK_C_INITIALIZE_ARGS의 pReserved에 MOBILETOKEN_ARGS 구조체 포인터를 연결하여 서비스 정보를 처리한다.

CK_C_INITIALIZE_ARGS의 pReserved이외의 항목에 대해서 본 가이드에서는 참조하지 않는다.

Prototype

```
CK_DEFINE_FUNCTION(CK_RV, C_Initialize) (
    CK_VOID_PTR pInitArgs
);
```

Parameter

pInitArgs : NULL 이거나 CK_C_INITIALIZE_ARGS 구조체 포인터

Return Value

성공경우 0, 에러일 경우 에러코드를 리턴.

Example

```
CK_C_INITIALIZE_ARGS initArgs;
CK_RV rv;
MOBILETOKEN_ARGS mobileTokenArgs;
memset((CK_VOID_PTR)initArgs, 0x00, sizeof(CK_C_INITIALIZE_ARGS));
memset((CK_VOID_PTR)mobileTokenArgs, 0x00, sizeof(MOBILETOKEN_ARGS));

// mobileTokenArgs 구조체 설정
mobileTokenArgs.pWndHandle = (CK_VOID_PTR)hWindow;
initArgs.pReserved = &mobileTokenArgs;

rv = C_Initialize(&initArgs);
if(rv != CKR_OK) {
    // 스마트인증 초기화 실패 또는 서비스 사용불가
    // 프로그램 종료
}

C_Finalize();
```

C_Initialize 함수를 이용하여 서비스 가입자 정보를 획득한 후, 사용자가 가입한 서비스에서 제공하는 스마트인증 구동프로그램을 로드하여 서비스에 이용한다.

2. 서비스 정보 처리

스마트인증 서비스의 서비스 정보처리를 위하여 MOBILETOKEN_ARGS 구조체를 정의한다.

```
typedef struct MOBILETOKEN_ARGS {
    CK_VOID_PTR     pWndHandle;
    CK_CHAR         szSiteDomainURL[64];
    CK_ULONG        nSelectTelco;
    CK_CHAR         szPhoneNo[16];
    CK_CHAR         szDriverName[256];
    CK_CHAR         szDriverDownloadURL[1024];
    CK_CHAR         szServiceServerIP[64];
    CK_ULONG        nServiceServerPort;
    CK_VOID_PTR     pReserved;
} MOBILETOKEN_ARGS;
```

구조체의 각 구성요소는 다음과 같이 처리한다.

CK_VOID_PTR pWndHandle

[입력] 구동프로그램을 호출하는 가입자S/W의 윈도 핸들값

CK_CHAR szSiteDomainURL[64]

[입력] 구동프로그램 호출사이트 명

CK_ULONG nSelectTelco

[입/출력] 가입자 통신자 정보로서 정보가 없는 경우 C_Initialize의 가입자 정보 입력창에서 입력한 정보를 획득하여 이동통신사 정보를 설정한다. 가입자 통신사 정보가 이미 설정된 경우 설정된 통신사 정보를 활용한다.

이동통신사	구분코드
SKT	1
KT	2
LG U+	3

CK_CHAR szPhoneNo[16]

[입/출력] 가입자 전화번호 정보로서 정보가 없는 경우 C_Initialize의 가입자 정보 입력창에서 입력한 정보를 획득하여 전화번호 정보를 구분기호를 제외한 숫자만으로 설정한다. 가입자 전화번호 정보가 이미 설정된 경우 설정된 가입자 정보를 활용한다.

CK_CHAR szDriverName[256]

[출력] 보안토큰 환경설정파일(npki_pkcs11.cnf)에 설정되는 드라이버 명칭(PKCS#11.Driver섹션의 Driver)으로 가입자 정보를 처리하기 위한 구동프로그램과 다른 종류의 구동프로그램을 사용하게 될 경우 보안토큰 구동프로그램을 로드하기 위하여 설정한다.

CK_CHAR szDriverDownloadURL[1024]

[출력] 서비스를 위한 구동프로그램이 설치되지 않은 경우 설치프로그램 다운로드가 가능한 URL
(예) http://rootca.kisa.or.kr/kor/hsm/hsm.jsp

CK_CHAR szServiceServerIP[64]

[입력] 서비스서버 접속 Domain 또는 IP. 서비스 서버 설정이 필요없는 경우 길이가 0인 스트링(“”)으로 설정한다.

CK_ULONG nServiceServerPort

[입력] 서비스서버 접속Port. 서비스 서버 설정이 필요없는 경우 0으로 설정한다.

CK_VOID_PTR pReserved

[입력] 향후 처리를 위한 파라미터로 현재는 NULL 을 입력한다.

부록 2. 가이드라인 연혁

버전	제·개정일	제·개정내역
v1.00	2013년 11월	o “모바일토큰 인터페이스 가이드라인”으로 제정
v1.00	2014년 4월	o “모바일토큰”을 “스마트인증”을 변경