공인인증기관 간 상호연동을 위한 사용자 인터페이스 기술규격

User Interface Specification for the Interoperability between Accredited Certification Authorities

v2.11

2015년 12월

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

공인인증기관 간 상호연동을 위한 사용자 인터페이스 기술규격

User Interface Specification for the Interoperability between Accredited Certification Authorities

1. 개요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계의 공인인증기관이 제공하는 공인인증서비스 간 상호연동과 공인인증기관이 발급한 공인인증서(이하 인증서)를 가입자가 쉽게 식별하고 편리하게 이용하도록 가입자 소프트웨어에 대한 인터페이스 관련 기술을 규정한다.

2. 규격의 구성 및 범위

본 규격은 공인인증기관 간 상호연동 시 사용자 데스크톱용 가입자 소프트웨어에 적용되는 사용자 인터페이스 기술에 대해 각 운영체제에서의 사용을 고려하여 명시하고 있으며 크게 두 부분으로 구성된다.

첫 번째로 사용자 측면에서 인증서비스와 관련된 기능으로 최상위인증기관 인증서 신뢰여부 확인기능, 공인인증서 저장에 대해 명시하고 있다.

두 번째로 부록에서는 최상위인증기관 인증서 신뢰여부 확인기능 구현의 예, 스마트카드 파일 구성도 및 메모리 맵, 스마트인증 인터페이스를 제시하고 있다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[RFC2119] IETF, RFC2119, *Key words for use in RFCs to Indicate Requirement Levels,* March 1997

[PKCS5] RSA, PKCS#5 v1.5 & v2.0, *Password-Based Cryptography Standard,* 1993

[PKCS8] RSA, PKCS#8 v1.2, *Private Key Information Syntax Standard,* 1993

[PKCS12] RSA, PKCS#12 v1.0, *Personal Information Exchange Syntax Standard,* 1999

3.2 국내 표준 및 규격

[KCAC.TS.CERTPROF] KISA, KCAC.TS.CERTPROF v1.70, *전자서명 인증서 프로파일 규격,* 2009

[KCAC.TS.DN] KISA, KCAC.TS.DN v1.21, *전자서명인증체계 DN규격,* 2009

[KCAC.TS.HSMU] KISA, KCAC.TS.HSMU v2.3, *보안토큰 기반 공인인증서 이용기술 규격,* 2014

[KCAC.TS.CT] KISA, KCAC.TS.CT v2.10, *무선단말기와 PC간 공인인증서 전송을 위한 기술규격,* 2012

3.3. 기타

해당사항 없음

4. 정의

본 규격에서 사용하는 용어의 정의는 제 4장에서 정한 것을 제외하고는 관련 법령 등이 정하는 바에 의한다.

4.1 전자서명법 용어 정의

본 규격에서 사용된 다음의 용어들은 전자서명법 및 동법 시행령, 공인인증기관의 시설 및 장비 등에 관한 규정(미래창조과학부 고시)에 정의되어 있다.

가) 인증서

나) 공인인증기관

다) 공개키

라) 가입자

4.2 용어의 정의

본 규격을 위하여 다음과 같은 용어들을 정의한다.

가) 인증기관 식별자 : 인증서 DN의 O(Organization) 값, [KCAC.TS.DN] 참고

나) 보안토큰 : 전자서명생성정보 등 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기

다) 스마트인증 : 데스크톱 환경 등에서 키 생성, 전자서명 생성 등을 무선단말기를 이용하여 구현한 서비스 또는 환경

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 따라야 할 구현 정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야 한다, 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 규격에서는 다음의 약어가 이용된다.

가) DN : Distinguished Name, 식별명칭

나) eSE : Embedded Secure Element

다) PKI : Public Key Infrastructure, 공개키 기반구조

라) microSD : Micro Secure Digital Card

마) PIN : Personal Identification Number, 개인식별번호

바) SKI : Subject Key Identifier, 소유자 키 식별자 확장필드, [KCAC.TS.CERTPROF] 참고

사) USB : Universal Serial Bus, 범용직렬버스

아) USIM : Universal Subscriber Identity Module, 범용사용자식별모듈

자) UTF8 : Universal Transformation Format, 8bit

6. 최상위인증기관 인증서 신뢰여부 확인 기능

사용자는 최상위인증기관 인증서 신뢰여부를 해쉬값 검증을 통해 확인할 수 있어야 한다.

사용자가 인증서 사용을 위해 가입자 소프트웨어를 다운로드받아 이를 설치하는 과정에서 최상위인증기관 인증서의 유효성 확인절차를 삽입하여 사용자가 최상위인증기관의 신뢰여부를 판단할 수 있는 방법을 제공해야 한다. 또한, 최상위인증기관 인증서가 갱신되는 경우 최상위인증기관 구 인증서가 이미 설치되어 있는 가입자는 업데이트 기능을 이용하여 최상위인증기관의 신 인증서를 배포 받아야 한다.

가입자 소프트웨어를 처음 설치하는 사용자의 경우에는 초기 설치 시 또는 소프트웨어 설치 후 업데이트 기능을 활용하여 구 인증서와 신 인증서를 모두 배포 받을 수 있어야 한다.

최상위인증기관은 최상위인증기관 인증서의 해쉬값을 인터넷 홈페이지에 공지해야 하며 공인인증기관은 동 해쉬값을 인증서 발급 확인서에 명기해야 한다. 사용자는 인증서 발급 확인서 또는 최상위인증기관 홈페이지를 통해 최상위인증기관 인증서 해쉬값을 획득할 수 있다. 사용자는 화면상에 표시되는 최상위인증기관 인증서 해쉬값과 자신이 알고 있는 최상위인증기관 인증서 해쉬값을 비교하여 일치할 경우에만 해당 인증서를 신뢰해야 한다.

최상위인증기관은 SHA-256 알고리즘을 이용하여 최상위인증기관 인증서의

해쉬값을 인터넷 홈페이지에 공지하여야 한다.

만약 사용자가 최상위인증기관 인증서를 신뢰하지 않는 경우 인증서 설치 도중에는 인증서 설치를 중단시키고, 인증서 사용 중에는 당해 최상위인증기관의 인증서를 삭제하고 최상위인증기관 홈페이지 등으로부터 인증서를 다시 다운로드 받아야 한다.

또한, 인증서 설치 이후에도 사용자가 최상위인증기관 인증서의 유효성을 확인하고자 할 경우 언제든지 확인할 수 있도록 최상위인증기관 신뢰여부 확인 기능을 가입자 소프트웨어에 구현해야 한다.

최상위인증기관 인증서 신뢰여부 확인기능 구현의 예는 [부록 1. 최상위인증기관 인증서 신뢰여부 확인기능 구현의 예]를 참고한다.

7. 공인인증서의 저장

공인인증서는 안전한 저장매체에 관리·보관되어야 한다.

공인인증서를 저장할 수 있는 저장매체로는 보안토큰, 보안모듈, 저장토큰 등이 있다. [표1]의 공인인증서 저장매체를 지원하는 경우 해당 규격 및 가이드라인을 준용하여야 한다.

<표 1> 공인인증서 저장매체

구분	설명	관련 규격 및 가이드라인	저장매체 종류 예
보안토큰	전자서명생성정보 등 비밀정보를 안전하게 저장·보관하기 위하여 키 생성·전자서명 생성 등이 기기 내부에서 처리되도록 구현된 하드웨어 기기	• KCAC.TS.HSMU • KCAC.TS.HSMS • 보안토큰 기반의 공인인증서 사용자 인터페이스 가이드라인 • 보안토큰 구동프로그램 배포 가이드라인	USB형 보안토큰, 카드형 보안토큰
	데스크톱 환경에서 무선단말기를 이용할 수 서비스 또는 환경	• 스마트인증 인터페이스 가이드라인	USIM, eSE 등
보안모듈	전자서명 생성이 기기내부에서 처리되도록 구현된 하드웨어 기기(해당 하드웨어 기기에서만 전자서명 생성 등 이용 가능)	• KCAC.TS.HSMU	하드웨어 저장방식 (CPU 등 정보처리기기 내장형 보안매체)
저장토큰	데이터 저장이 가능한 집적회로(IC)칩이 장착된 메모리형 전자식 카드 또는 독자적 파일구조를 지원하는 USB드라이브(하드웨어적 통제가 가능하며, 비밀번호 입력 오류 회수 제한 등 접근통제 등 구현)	• 부록 3. 스마트카드 파일 구성도 및 메모리 맵 • KCAC.TS.HSMU	하드웨어 저장방식 (메모리형 IC카드 등)

공인인증기관은 2019년 3월 1일 이후부터는 하드디스크, 이동식디스크 저장매체에 공인인증서 발급을 제한하고, 보안토큰 등 안전한 저장매체에 발급하여야 한다. 다만, 공인인증기관은 하드디스크, 이동식디스크 저장방식을 이용하는 가입자를 보호하기 위한 보안 솔루션을 자율적으로 개발하여 보급할 수 있다.

또한, 공인인증기관은 웹 브라우저가 인식할 수 있도록 웹 표준을 준용하여 웹 브라우저 저장소에 발급할 수 있다. 그리고 [PKCS12]를 사용하는 경우, 구현은 [KCAC.TS.CT] 부록을 참고할 것을 권장한다.

가입자 소프트웨어는 사용자가 인증서 저장매체를 선택할 수 있도록 해당 기능을 제공하여야 하며 사용자가 선택한 저장매체에 저장된 모든 인증서 목록을 검색하여 표시하여야 한다. 이 경우, 해당 공인인증기관에서 발행한 인증서에 우선순위를 부여할 수 있다. 사용자가 선택한 인증서의 유효성을 검증하여 그 결과를 보여주도록 '인증서 검증' 기능을 제공해야 한다.

장애인이 비장애인과 동등하게 인증서를 이용할 수 있도록 보조기술을 활용하여 접근성을 제공하여야 한다.

부록 1. 최상위인증기관 인증서 신뢰여부 확인기능 구현의 예

1. 개요

공인인증기관의 등록대행기관은 사용자가 인증서 발급 신청 시 참조번호, 인가코드와 더불어 최상위인증기관의 인증서 해쉬값을 사용자에게 제공하여야 한다.

사용자가 공인인증기관으로부터 인증서를 발급 받았을 때 등록 시 배포된 최상위인증기관의 인증서 해쉬값을 이용하여 최상위인증기관의 인증서 유효성을 확인할 수 있는 메커니즘을 제공하여야 한다.

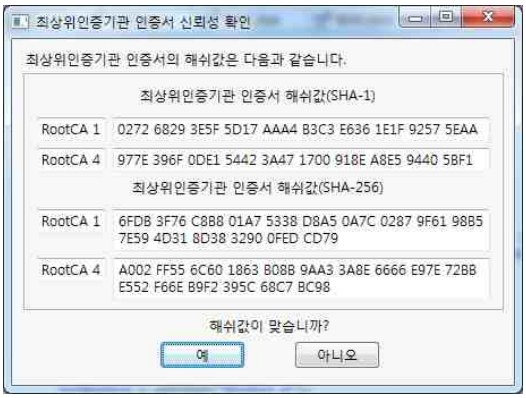
가입자 소프트웨어의 인증서 유효성 확인기능은 경우에 따라 '육안 확인'(최초 확인 시)과 '사용자 입력에 의한 확인'(사용자가 원할 시)이 있으며 경우에 따라 적절히 제공하여야 한다.

인증서 갱신되는 경우 또는 최상위인증기관 인증서가 여러 개 존재하는 경우에도 동일방법을 사용해야 한다.

2. 구현

2.1 육안 확인

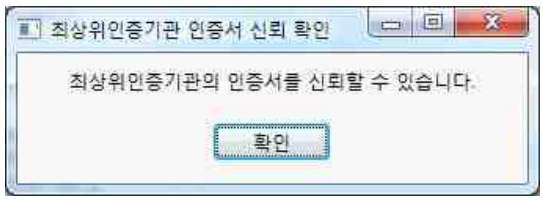
최상위인증기관 인증서의 해쉬값을 육안 확인 방법은 가입자 소프트웨어를 처음 설치할 경우 유용하며, 설치과정 중 자동으로 아래와 같은 화면을 보여주고 사용자로 하여금 최상위인증기관 인증서 해쉬값을 비교 확인하도록 한다. 해쉬값이 일치하지 않는 경우 가입자 소프트웨어 설치를 중단하여야 한다.



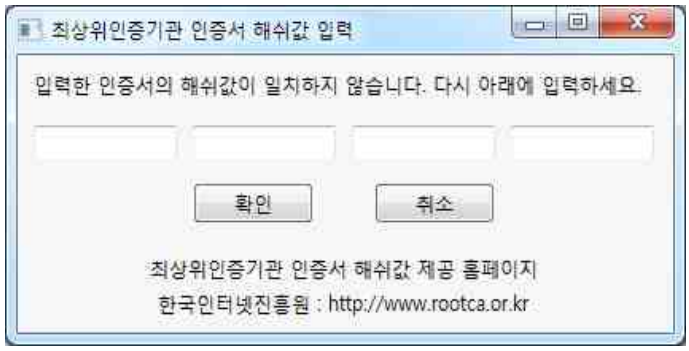
2.2 사용자 입력에 의한 확인

가입자 소프트웨어를 사용하는 도중 사용자가 원하는 경우 언제든지 확인 가능하도록 사용자가 해쉬값을 직접 입력하여 유효성을 확인하는 방법 등을 통해 최상위인증기관 인증서 신뢰방법을 제공하여야 한다.

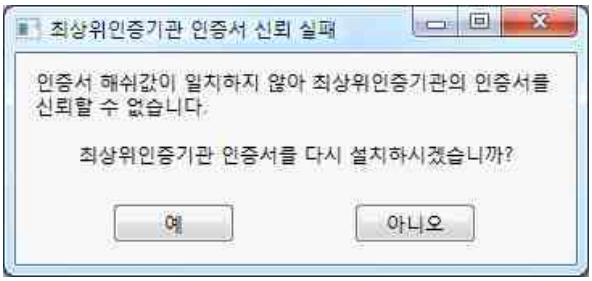
최상위인증기관의 인증서 해쉬값을 확인하여 최상위인증기관의 인증서가 확인되면 다음과 같은 확인 메시지를 보여주고 다음 절차를 진행한다.



입력한 인증서 해쉬값이 최상위인증기관 인증서의 공개키 해쉬값과 일치하지 않을 경우 다음과 같이 3번의 재시도 기회 제공한다.



3번의 재시도 후에도 최상위인증기관 인증서 해쉬값이 맞지 않을 경우에는 다음과 같이 에러메시지를 보여주고 최상위인증기관 인증서를 다운로드 할 수 있는 기능을 제공하여야 한다. 사용자가 '육안확인'으로 신뢰성 확인에 실패했을 경우에도 아래와 동일한 에러메시지를 보여주어야 한다.



최상위인증기관 인증서 설치 과정 중 자동으로 아래의 화면을 보여주고 사용자로 하여금 최상위인증기관 인증서 해쉬값을 비교 확인한 후 설치한다.

부록 2. 디스크 내 공인인증서의 저장

1. 저장방법

하드디스크, 이동식디스크 등 디스크 내에 공인인증서와 전자서명생성키를 저장하는 경우 암호화를 위해 [PKCS5]를 적용하여야 하며, 이 때 지원하는 버전은 기존 가입자 소프트웨어와의 호환을 위해 버전 1.5 및 버전 2.0을 모두 지원해야 한다. 암호화한 후에는 [PKCS8]의 전자서명생성키 저장형식을 준용하여 저장한다. 이 때, 전자서명생성키 암호화를 위한 비밀번호가 안전하게 선택될 수 있도록 비밀번호에 대한 안전성 검증도구를 제공할 것을 권고한다.

인증서는 생성되는 인증서 크기 및 범용성을 고려하여 DER형식으로 저장해야 한다. 사용자 인증서 및 전자서명생성키 저장 시 파일시스템 접근을 위해 관리자 권한 획득이 필요한 경우, 해당 운영체제가 지원하는 보안정책에 따라 사용자 동의 등을 통해 관리자 권한 획득 기능을 제공할 수 있다.

2. 저장위치 및 파일명명 규칙

인증서 저장위치는 운영체제별 환경에 따라 <표 5>와 같이 정의한다.

<표 2> 저장매체별 인증서 저장위치

저장매체	운영체제		인증서 저장위치
이동식 디스크	윈도우		(드라이브명):\NPKI\(인증기관식별자)
	UNIX/Linux		(마운트 디렉토리)/NPKI/(인증기관식별자)
	OS X		/Volumes/(디스크명)/NPKI/(인증기관식별자)
하드 디스크	윈도우	98, ME, XP	(하드디스크 레이블명[1]):\Program Files\NPKI\(인증기관식별자)
		비스타 이상[2]	%UserProfile%\AppData\LocalLow\NPKI\(인증기관식별자)
		8 Style UI	[KCAC.TS.CM] 참조
	UNIX/Linux		(사용자계정[3])/NPKI/(인증기관식별자)
	OS X		(사용자계정)/Library/Preferences/NPKI/(인증기관식별자)

최상위인증기관 및 공인인증기관 인증서는 <표 5>에 정의된 저장위치에 저장하며 파일명은 인증서 내 소유자 키식별자 확장필드와 인증서 일련번호를

1) MS社의 윈도우 운영체제가 설치된 하드디스크 볼륨 명칭
2) 윈도우 비스타 이상 운영체제라도 SHA-1 해쉬함수를 이용하여 발급된 공인인증서는 윈도우 98, ME, XP 운영체제 저장위치((하드디스크 레이블명):\Program Files\NPKI\(인증기관식별자))에 저장하여야 한다.
3) 사용자가 로그인한 계정

조합한 'SKI_일련번호.der' 형태로 생성해야 한다. SKI는 소유자 키 식별자 확장필드 값으로 40자리의 16진수로 나타내야 하며 일련번호는 10진수로 표현해야 한다.

사용자 인증서와 전자서명생성키를 파일로 저장하는 경우, <표 5>에 정의된 인증서 저장위치 하위의 'USER' 디렉토리 안에 사용자 식별명칭(DN)으로 디렉토리를 생성한 후 저장하여야 한다.

저장 시 파일명은 전자서명용과 암호키분배용을 구별하기 위해 용도별로 동일하게 명명하여야 하며, 인증서는 'der', 전자서명생성키는 'key' 확장자를 사용하여야 한다. 전자서명용은 signCert.der, signPri.key를, 암호키분배용은 kmCert.der, kmPri.key를 사용해야 한다.[4)]

3. 부가 기능

사용자가 인증서 저장매체로 하드디스크, 이동식디스크를 선택하는 경우 가입자 소프트웨어는 하드디스크가 보안토큰, 보안모듈, 저장토큰 등에 비해 인증서 유출 등의 가능성이 있으므로 안전하지 않은 저장매체임을 공지하는 메시지를 출력하여야 한다. 또한 공인인증서와 개인키의 보호를 위해 비밀번호 입력오류에 대해 입력횟수를 제한하는 기능을 제공할 수 있다.

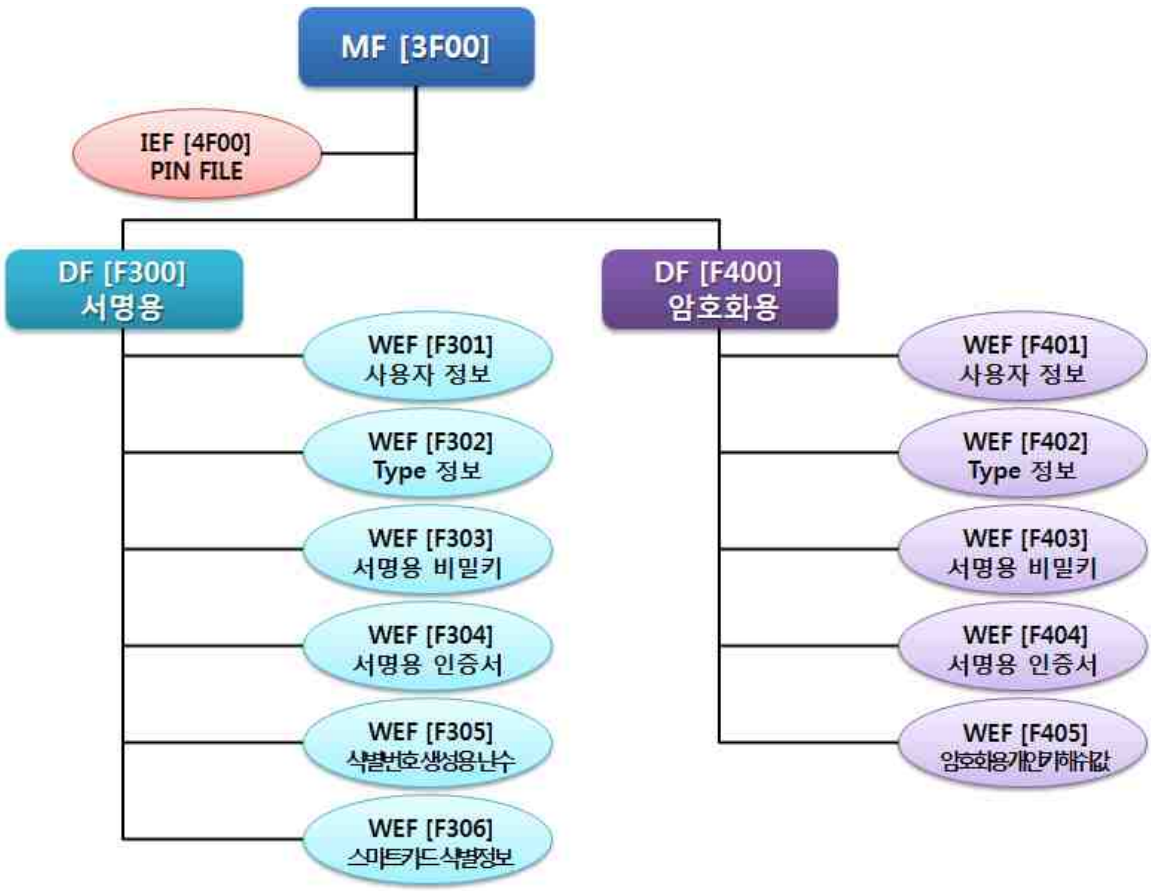
하드디스크, 이동식디스크의 경우 사용자가 전자서명생성키 및 인증서를 PKI 기반의 다른 응용 프로그램에서도 사용할 수 있도록 내보내기 및 가져오기 기능을 제공해야 하며 이를 위해 [PKCS12]를 준용해야 한다.

4) 가입자 소프트웨어는 공인인증서 및 전자서명생성키 파일명을 대소문자 구분 없이 이용할 수 있도록 구현하여야 한다.

부록 3. 스마트카드 파일 구성도 및 메모리 맵

1. 스마트카드 파일 구성도

메모리 타입의 스마트카드 파일 구성은 전자서명용과 암호화용을 따로 관리해야 한다. 기존에 발급된 스마트카드(암호화용 비밀키 및 인증서가 E맵에 저장된 카드)와의 연계성을 위하여 암호키분배용 가입자 소프트웨어에서 암호키분배용 비밀키와 인증서 획득을 위해 스마트카드 EEPROM의 E맵과 F맵을 모두 검색·처리토록 구현해야 한다.



※ 사용자정보 : 사용자 관련 정보를 기록하기 위해서 사용되는 영역
※ Type 정보 : 사용자카드의 구별자 정보
※ 서명용개인키 : 사용자의 서명용 개인키 정보를 기록하기 위해서 사용되는 영역
※ 서명용인증서 : 사용자의 서명용 인증서를 기록하기 위해서 사용되는 영역
※ 식별번호 생성용 난수 : 식별번호를 생성하는데 사용되는 160비트 이상의 안전한 임의의 난수를 저장하기 위해서 사용되는 영역

2. 스마트카드 메모리 맵

종류		FileID	Size
MF(3F00)	Password 파일	4F01	8 Byte
DF(F300)	사용자정보	F301	52 Byte
	TYPE 정보	F302	12 Byte
	서명용 개인키	F303	1560 Byte
	서명용 인증서	F304	2080 Byte
	식별번호 생성용 난수	F305	42 Byte
	스마트카드 식별정보	F306	6 Byte
DF(F400)	사용자정보	F401	52 Byte
	TYPE 정보	F402	12 Byte
	암호화용 개인키	F403	1560 Byte
	암호화용 인증서	F404	2080 Byte
	암호화용 개인키 해쉬	F405	42 Byte

※ 암호화용 FID는 'FXXX' 로 확정
※ 암호화용 WEF들의 크기는 서명용과 동일하게 확정
※ 기존 E맵을 사용하는 공인인증기관을 위해 현재 사용중인 관리 프로그램을 F 맵과 E맵 모두를 사용할 수 있는 관리 프로그램으로 변경 필요
※ F306을 지원하지 않는 구형 스마트카드의 경우, F303에는 PKCS#5 v1.5를 적용한 서명용 개인키를 저장하고, F305에는 [TTA.120029]를 참조하여 식별번호 생성용 난수를 저장
※ F306을 지원하는 스마트카드의 경우, F306에는 식별정보로써 4바이트의 데이터(00 00 00 01)를 저장하고, F303에는 PKCS#5 v2.0을 적용한 서명용 개인키와 식별번호 생성용 난수정보를 저장

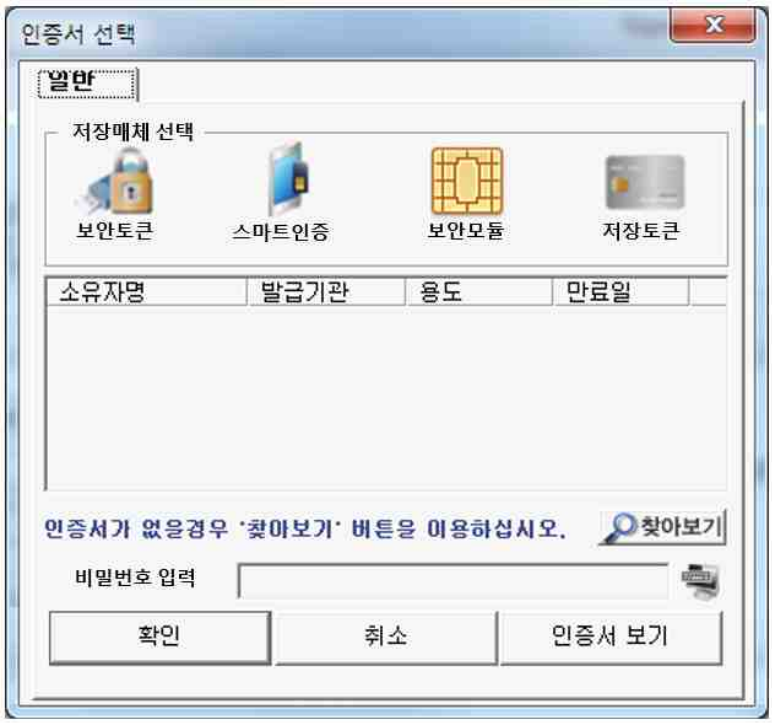
3. 부가기능

사용자가 전자서명생성키 및 인증서를 PKI 기반의 다른 응용 프로그램에서도 사용할 수 있도록 내보내기 및 가져오기 기능을 제공해야 하며 이를 위해 [PKCS12]를 준용해야 한다.

부록 4. 사용자 인터페이스 화면 구성의 예

1. 사용자 인터페이스 화면 구성

인증서 저장매체로 보안토큰, 보안모듈, 스마트인증, 저장토큰 등을 선택할 수 있도록 인터페이스를 지원하고, 선택한 저장매체 내의 모든 공인인증서를 표시하여야 한다.



2. 인증서 저장매체 선택 시 인증서 목록보기

공인인증서 저장매체 내의 공인인증서를 화면에 표시할 때 인증서의 상태, 소유자명, 발급기관, 만료일 등을 표시할 수 있다.

구분	내용
인증서 상태	o 인증서 검증 결과(유효, 폐지 등) 표시
소유자명	o 사용자의 인증서 CN(인증서 정보 이용) o 기관인 경우 기관의 실명(또는 인증기관 식별자)으로 표시
발급기관	o 공인인증기관의 실명(인증서 정보 이용)으로 표시
만료일	o 인증서 만료일(또는 유효기간) 표시
인증서 용도	o 공인인증서의 용도(범용, 용도제한용)

부록 5. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2001년 10월	o "공인인증기관 상호연동을 위한 사용자 인터페이스 기술규격"으로 제정
v1.10	2003년 12월	o 전체 문서 형식 및 구성을 전자서명인증체계 규격 문서 양식에 맞게 개정 o 인증서 저장매체 다양성과 비 MS 윈도우즈 사용자의 편의성을 고려하여 기술규격을 개정 o 인증서 저장매체의 재분류에 의한 인증서 저장위치 변경 및 추가 o MS 윈도우즈 운영체제에서 하드디스크에 인증서 저장위치 변경 o 인증서 저장방법은 DER 형식을 필수로 함 o 비 MS 윈도우즈 환경을 고려한 인증서 파일명과 저장위치를 정의함 o 최상위인증기관 및 공인인증기관 인증서 파일명명 규칙 변경 및 각 공인인증기관별 기존 인증서 저장위치 삭제 o PKI관련 스마트카드 기술규격 v1.00을 부록 2.스마트카드 파일 구성도 및 메모리 맵으로 통합 o 부록 1. 최상위인증기관 인증서의 신뢰여부 확인 기능 구현의 예를 다수의 인증서가 존재하는 경우에도 적용 가능하도록 명시 o 부록 2. 사용자 인터페이스 초기화면에서 만료일 표시방법 추가
v1.11	2004년 11월	o '인증서 검증' 기능을 9. 부가기능에 포함 o 인증서 저장매체 종류<표1>에서 "불러오기" 삭제 o 부록 1. 최상위인증기관 인증서 신뢰여부 확인 실패시의 에러 메시지 추가 o 부록 2. 사용자 인터페이스 초기화면의 예 변경 o 부록 2-2. 스마트카드 메모리 맵에서 F305 용도 변경
v1.20	2006년 10월	o 8.3 저장위치 및 파일명명규칙에서 매킨토시에 대한 공인인증서 저장 위치 변경

버전	제·개정일	제·개정내역
v1.30	2007년 1월	o 8.2 저장방법에서 운영체제의 보안정책 변경에 따른 추가 기능 제공 문구 삽입
v1.50	2007년 3월	o 사용자 인터페이스에서 공인인증서 저장매체를 보여주는 순서 권고사항 변경에 따라, – 7. 초기화면상의 인증서 표시방법 삭제 및 8. 절을 7. 절로 변경 – 사용자 인터페이스 화면에서 공인인증서 저장매체 표시 방법을 7.1 저장매체에 기술하고 관련내용을 부록 1.에 반영 o 7.2 저장위치의 <표 1>에서 인증서 저장매체 구분체계 및 저장매체명 변경 o 7.3 저장위치 및 파일명명규칙의 <표 2>에서 인증서 저장매체 구분체계 및 저장매체명 변경
v1.60	2007년 4월	o 무선환경을 위한 최상위인증기관 인증서 신뢰규격 v1.00 흡수 통합
v1.70	2008년 10월	o 2,048비트 길이의 전자서명키를 저장할 수 있도록 스마트카드 메모리 맵 크기를 변경
v1.80	2009년 9월	o 공인인증서 암호체계 고도화에 따른 알고리즘 변경 사항 반영
v1.81	2010년 3월	o 공인인증서 가입자에게 자신이 사용하는 공인인증서 비밀번호의 안전도 수준을 알릴 수 있도록 비밀번호 안전성 검증툴을 제공 ※ 현 기술규격 내용으로 안전하지 않은 비밀번호를 사용하지 못하도록 하겠다는 취지는 아니며, 향후 안전하지 않은 비밀번호 이용 제한을 위해서는 비밀번호 안전성 기준 등의 마련이 필요 o 윈도우 비스타 OS 등에서 자바 기반 공인인증서 가입자 S/W의 상호연동성 확보를 위해 공인인증서 저장위치 변경
v1.82	2010년 10월	o 공인인증서 암호체계 고도화 추진에 따른 공인인증서 이용 시 혼란 방지 및 상호연동성 확보를 위해 윈도우 비스타 운영체제라도 SHA-1 해쉬함수를 이용해 발급된 공인인증서는 윈도우 XP 운영체제의 저장위치에 저장토록 기술규격 개정
v1.83	2012년 11월	o 하드디스크 내에 공인인증서 저장 및 이용을 위한 요구사항 반영 o 장애인에 대한 접근성 제공사항 반영

버전	제·개정일	제·개정내역
v1.90	2013년 3월	o '모바일토큰' 정의 추가
v2.00	2014년 4월	o '모바일토큰'을 '스마트인증'으로 변경
v2.10	2015년 4월	o 공인인증서 저장과 관련한 안전성 강화를 위해 공인인증서를 안전한 저장매체에 저장하도록 기술
v2.11	2015년 12월	o 웹 표준화에 따른 공인인증서 발급과 관련한 저장형태 및 저장방식 변경사항 반영