보안토큰 기반의 공인인증서 사용자 인터페이스 가이드라인

Accredited Certificate User Interface Guideline for Hardware Security Module

v1.20

2007년 11월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

보안토큰 기반의 공인인증서 사용자 인터페이스 가이드라인
Accredited Certificate User Interface Guideline for Hardware Security Module

1. 개 요

본 가이드라인에서는 가입자가 보안토큰 기반의 공인인증서를 편리하게 이용할 수 있도록 가입자 소프트웨어 등이 갖추어야 할 사용자 인터페이스 관련 요구사항을 기술한다.

2. 구성 및 범위

본 가이드라인은 사용자 측면에서 보안토큰 기반의 공인인증서를 쉽게 이용할 수 있도록 보안토큰 연결 및 구동프로그램 설치, 보안토큰 접근비밀번호 설정, 보안토큰 기반의 공인인증서 발급·관리, 보안토큰 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.HSM] KISA, KCAC.TS.PKCS11 v1.50, *보안토큰 기반의 공인인증서 이용기술 규격*, 2007

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

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

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) PIN : Personal Identification Number, 개인식별번호

6. 보안토큰 기반의 공인인증서 사용자 인터페이스

6.1 보안토큰 용어 사용

보안토큰 기반의 공인인증서의 편의성을 제고하기 위해 '보안토큰 PIN' 라는 용어는 '보안토큰 비밀번호' 또는 '보안토큰 접근 비밀번호'로 대체하여 사용할 것을 권고한다.

6.2 보안토큰 초기 비밀번호 변경

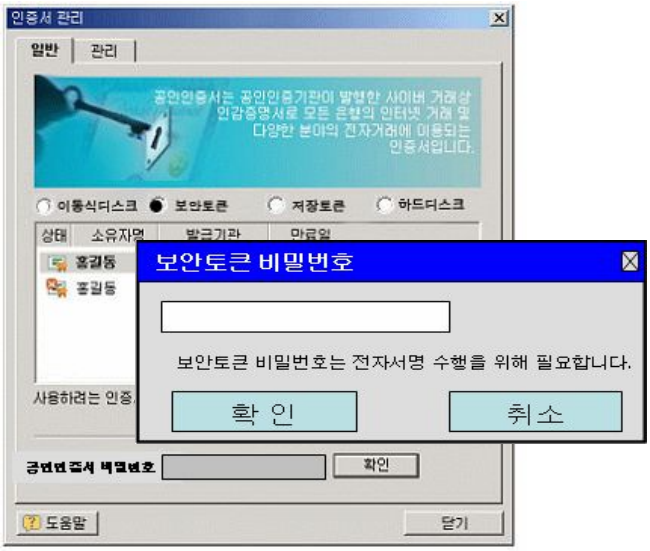
안전성을 고려하여 보안토큰 초기 비밀번호는 보안토큰 사용 전에 재설정할 것을 권고한다.

6.3 보안토큰 비밀번호 입력

가입자 소프트웨어는 사용자가 선택한 보안토큰에 대해서 보안토큰 비밀번호의 입력 요구없이 저장매체에 저장된 모든 공인인증서를 보여줄 것을 권고한다.

또한, 가입자 소프트웨어는 사용자에게 전자서명 수행시 마다 보안토큰 비밀번호의 입력을 요구하여야 하며, 사용 후 사용자의 보안토큰 비밀번호는 메모리에서 안전하게 삭제하여야 한다.

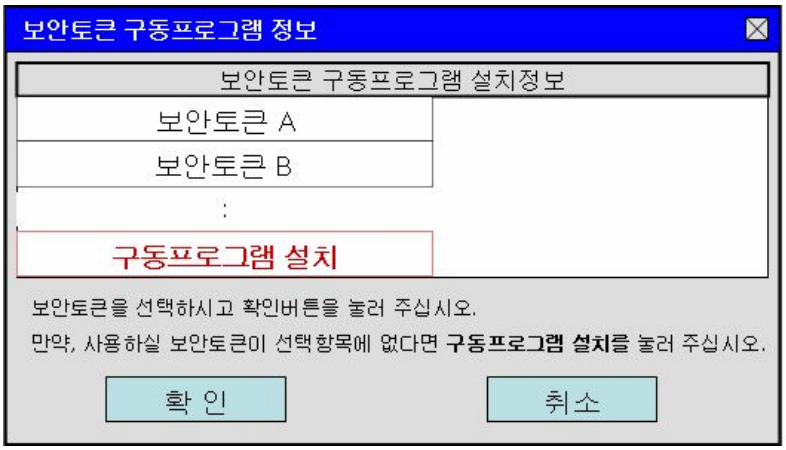
가입자 소프트웨어는 공인인증서 비밀번호(암호) 입력창을 통해 사용자의 보안토큰 비밀번호를 입력받을 수 있다. 또한, 별도의 인터페이스를 통해 보안토큰 입력받을 수 있는데, 이 경우 가입자 소프트웨어의 공인인증서 비밀번호(암호) 입력창은 비활성화 되어야 한다.



보안토큰 비밀번호 입력창에는 사용자가 전자서명을 수행한다는 사실을 인지할 수 있도록 확인메시지를 보여줄 것을 권고한다.

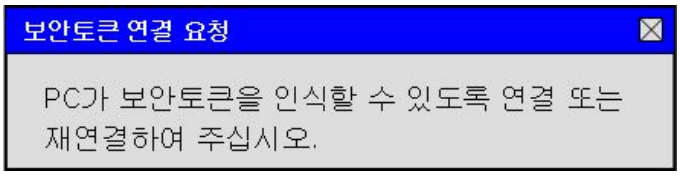
6.4 보안토큰 구동프로그램 설치

사용자가 가입자 소프트웨어를 통해 보안토큰 구동프로그램을 배포 받을 수 있도록 가입자 소프트웨어는 보안토큰 구동프로그램 설치 기능을 구현할 것을 권고한다. 보안토큰 구동프로그램 설치 기능은 이용자가 보안토큰 저장매체를 선택할 경우 나타나는 보안토큰 구동프로그램 설치정보 리스트 창에 구현할 수 있다.



사용자가 구동프로그램 설치를 클릭할 경우, 가입자 소프트웨어는 사용자에게 보안토큰을

연결하라는 메시지를 아래와 같이 보여줄 것을 권고한다.



사용자가 보안토큰을 PC에 연결하면, 운영체제는 신규로 연결되는 보안토큰에 대해서 WM_DEVICECHANGE 이벤트를 발생시킨다. 가입자 소프트웨어는 이러한 이벤트를 감지하여 아래의 **[새 하드웨어 검색 마법사창]** 및 위의 **[보안토큰 연결요청 창]**을 강제로 종료할 것을 권고한다.

또한, 가입자 소프트웨어는 SetupDiEnumDeviceInfo, SetupDiGetDeviceRegistryProperty 등 두 함수 호출을 통해 PC 시스템에 장착된 보안토큰 고유제품 정보를 획득할 수 있으며, [KCAC.TG.DGH]에 따라 획득한 KISA가 전자서명한 보안토큰 구동프로그램 배포 위치 정보를 확인하여 해당 구동프로그램을 자동 배포할 수 있다.

보안토큰 구동프로그램이 설치된 이후, 사용자가 가입자 소프트웨어에서 인증서 저장 매체 중 보안토큰을 다시 선택하도록 하되, 보안토큰이 인식되지 않을 경우 보안토큰 연결 또는 재연결을 요구할 수 있다.

또한, 가입자 소프트웨어는 사용자가 “구동프로그램 설치버튼” 클릭시, 사용자가 수동으로 보안토큰 구동프로그램을 직접 설치할 수 있도록 KISA 홈페이지 (http://www.rootca.or.kr/certs/hsm.html)로 안내할 수 있다.

KISA는 사용자가 보안토큰 구동프로그램을 수동으로 설치할 수 있도록 홈페이지에 평가인증된 보안토큰에 대한 제품사진, 구동프로그램 설치 URL 등을 게재하여야 한다.

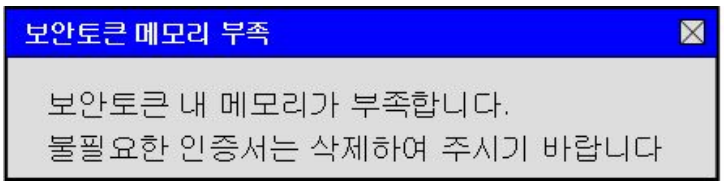
6.5 보안토큰 기반의 공인인증서 발급·관리

보안토큰 기반의 공인인증서 발급·관리시 지연될 수 있는 시간(1분 이상)에 대해 사용자에게 고지할 수 있다.

보안토큰 기반의 공인인증서 발급·관리시 오류가 발생할 경우 예외처리를 통해 보안토큰내 메모리를 원상태로 되돌릴 수 있도록 한다.

6.6 보안토큰 메모리 관리

가입자 소프트웨어는 보안토큰 내 메모리가 부족하여 공인인증서 신규발급, 재발급, 갱신, 가져오기 등이 수행되는 도중 오류가 발생할 수 있음을 사용자에게 알려줄 것을 권고한다. 가입자 소프트웨어는 C_GetTokenInfo 함수를 통해 보안토큰 내에 가용한 공개영역 메모리를 확인할 수 있는데, 해당 공개영역 메모리 여유분이 인증서 개당 최소 필요 메모리인 3,500 바이트 보다 적을 경우 사용자에게 아래와 같이 메시지를 보여줄 것을 권고한다.



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

6.7 보안토큰 오류사항 처리

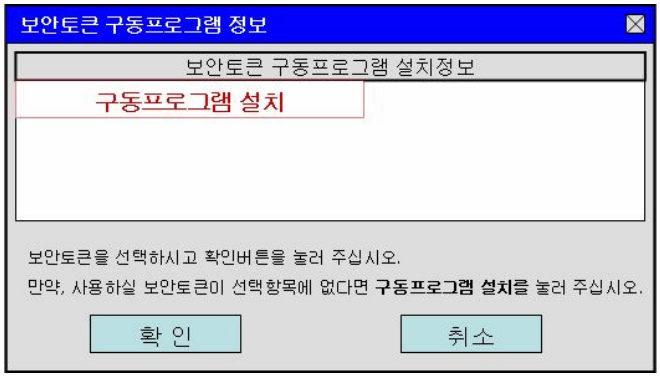
“보안토큰 기반의 공인인증서 이용기술 규격” 중 부록 6. 보안토큰 API(PKCS#11) 반환값 프로파일에 따라 처리중 보안토큰 사용자에게 오류사항을 고지할 수 있다.

부록 1. 보안토큰 사용자 인터페이스 구현의 예

① 사용자가 보안토큰 저장매체 선택

o 기존 PC에 보안토큰 구동프로그램이 설치되어 있지 않은 경우

②-1 기존 PC에 설치되어 있는 보안토큰 구동프로그램이 없는 경우 사용자로 하여금 아래와 같이 [구동프로그램 설치]를 수동으로 선택하도록 구현할 수 있으며, 또는 자동으로 '③ 이후의 구동프로그램 설치 과정'이 처리되도록 구현할 수도 있다.



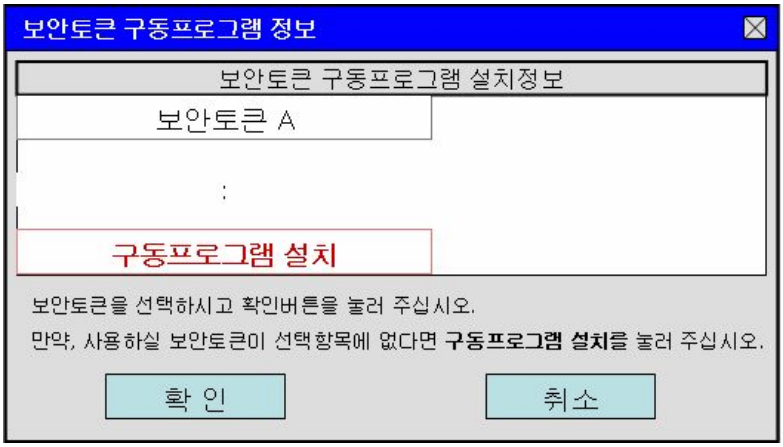
o 기존 PC에 한개의 보안토큰 구동프로그램만 설치되어 있는 경우,

②-2 기존 PC에 설치되어 있는 보안토큰 구동프로그램 한 개만 설치되어 있는 경우,

- 기본적으로, 가입자 소프트웨어는 사용자 개입없이 기존 보안토큰을 자동으로 구동할 것을 권고한다. 보안토큰이 정상적으로 구동될 경우 사용자가 보안토큰 비밀번호를 입력할 수 있도록 한다. 다만, 해당 구동프로그램으로 보안토큰이 구동이

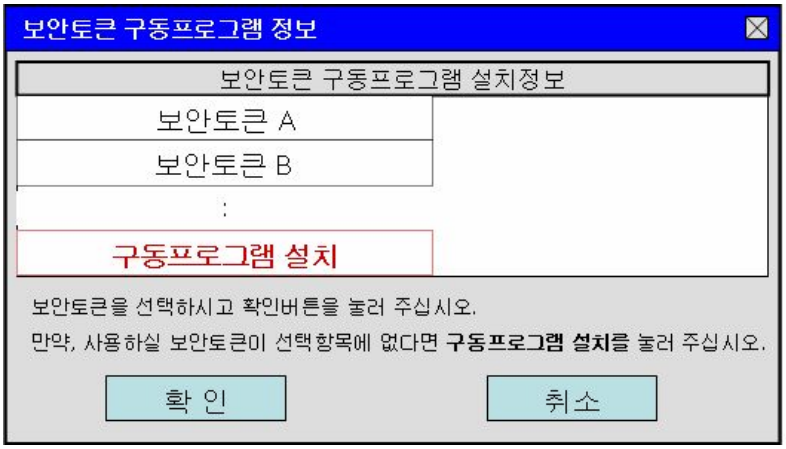
되지 않을 경우 '③ 이후의 구동프로그램 설치 과정'이 처리되도록 구현할 것을 권고한다.

- 또는, 선택적으로 '보안토큰 구동프로그램 설치정보창'을 보여주고 사용자가 해당 구동프로그램을 수동으로 선택하도록 구현할 수 있다.



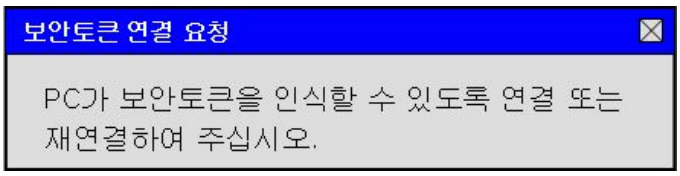
o 기존 PC에 한개 이상의 보안토큰 구동프로그램이 설치되어 있는 경우,

②-3 기존 PC에 설치되어 있는 보안토큰 구동프로그램 한 개 이상이 설치되어 있는 경우, 가입자 소프트웨어는 사용자가 적절한 보안토큰을 선택할 수 있도록 '보안토큰 구동프로그램 설치정보창'을 보여줄 것을 권고한다. 사용자가 선택한 보안토큰이 정상적으로 구동될 경우 사용자가 보안토큰 비밀번호를 입력할 수 있도록 한다.

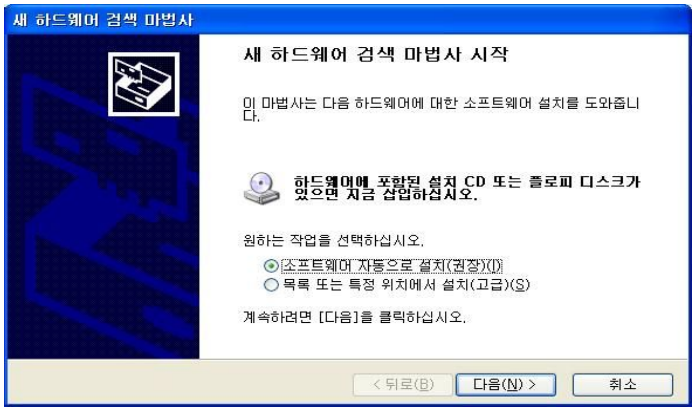


<보안토큰 구동프로그램 설치 과정>

③ 사용자가 '② 보안토큰 구동프로그램 설치정보'에서 구동프로그램을 클릭할 경우, 가입자 소프트웨어는 보안토큰 구동프로그램의 배포를 위한 정보를 얻기 위해 사용자에게 보안토큰 연결 또는 재연결을 요구



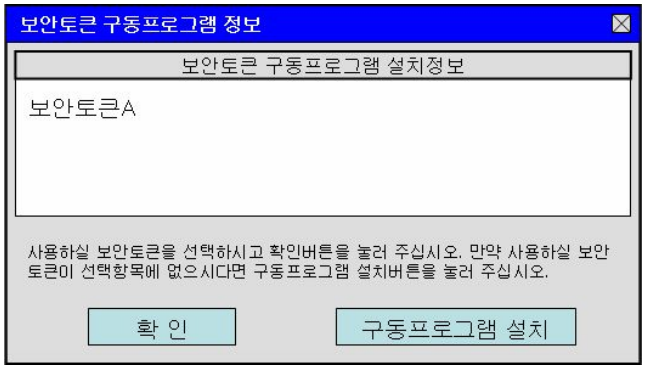
사용자가 보안토큰을 PC에 연결하면, 운영체제는 신규로 연결되는 보안토큰에 대해서 WM_DEVICECHANGE 이벤트를 발생시킨다. 가입자 소프트웨어는 이러한 이벤트를 감지하여 아래의 **[새 하드웨어 검색 마법사창]** 및 위의 **[보안토큰 연결요청 창]**을 강제로 종료할 것을 권고한다.



이후, 가입자 소프트웨어는 SetupDiEnumDeviceInfo, SetupDiGetDeviceRegistryProperty 등 두 함수 호출을 통해 PC 시스템에 장착된 보안토큰 고유제품 정보를 획득할 수 있으며, [KCAC.TG.DGH]에 따라 획득한 KISA가 전자서명한 보안토큰 구동프로그램 배포 위치 정보를 확인하여 해당 구동프로그램을 자동 배포할 수 있다.

④ 사용자는 다시 보안토큰 저장매체 선택

⑤ 사용자는 보안토큰 구동프로그램을 선택하고 확인버튼을 클릭



⑥ 보안토큰이 인식된 경우 보안토큰내 인증서를 자동으로 검색하여 보여주고, 보안토큰 기반의 전자서명 생성시 인증서 선택후 보안토큰 비밀번호를 입력하도록 한다.

부록 2. 가이드라인 연혁

버전	제·개정일	제·개정내역
v1.00	2007년 10월	· "보안토큰 기반의 공인인증서 이용을 위한 사용자 인터페이스 가이드라인"으로 제정
v1.10	2007년 10월	· “보안토큰 메모리 관리 분야” 신설
v1.20	2007년 11월	· 공인인증서 발급·관리시 보안토큰 메모리 관련오류 처리를 6.5 보안토큰 기반의 공인인증서 발급·관리에 포함 · 키쌍 등에 대한 메모리 정리기능을 6.6 보안토큰 메모리 관리에 포함