보안토큰 구동프로그램 배포 가이드라인

Distribution Guideline for HSM Driver S/W

v1.00

2007년 10월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

보안토큰 구동프로그램 배포 가이드라인
Distribution Guideline for Security Token Device Driver

1. 개 요

보안토큰은 공인인증서 복사방지 기능을 갖는 하드웨어 보안 저장매체로써, 가입자 소프트웨어에서 보안토큰을 구동하기 위해서는 전용 구동프로그램이 설치되어야 한다. 본 가이드라인은 가입자가 해당 구동프로그램을 쉽게 배포 받을 수 있도록 가입자 소프트웨어 등이 갖춰어야 할 요구사항을 기술한다.

2. 구성 및 범위

보안토큰은 리더기와 보안토큰이 일체형으로 구현된 USB형 보안토큰과 리더기와 보안토큰이 구분되어 있는 스마트카드형 보안토큰으로 구분되기 때문에, 각각의 보안토큰 구동프로그램 배포방법은 다르게 구현된다.

본 가이드라인은 USB형 보안토큰과 스마트카드용 보안토큰으로 나누어 구동프로그램 배포방안을 제시하지만, 해당 배포방안은 PC 운영체제와 관계없이 적용될 수 있도록. USB 표준의 Enumeration 기능과 ISO/IEC 7816 표준의 ATR을 활용한다. 그리고 가입자 소프트웨어 배포시 함께 배포하는 방안을 제시한다. USB형 또는 스마트카드형 이외의 기타 인터페이스 방식에 대해서는 추가적으로 정의한다.

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 v1.20, *보안토큰 기반의 공인인증서 이용기술 규격,* 2007

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.

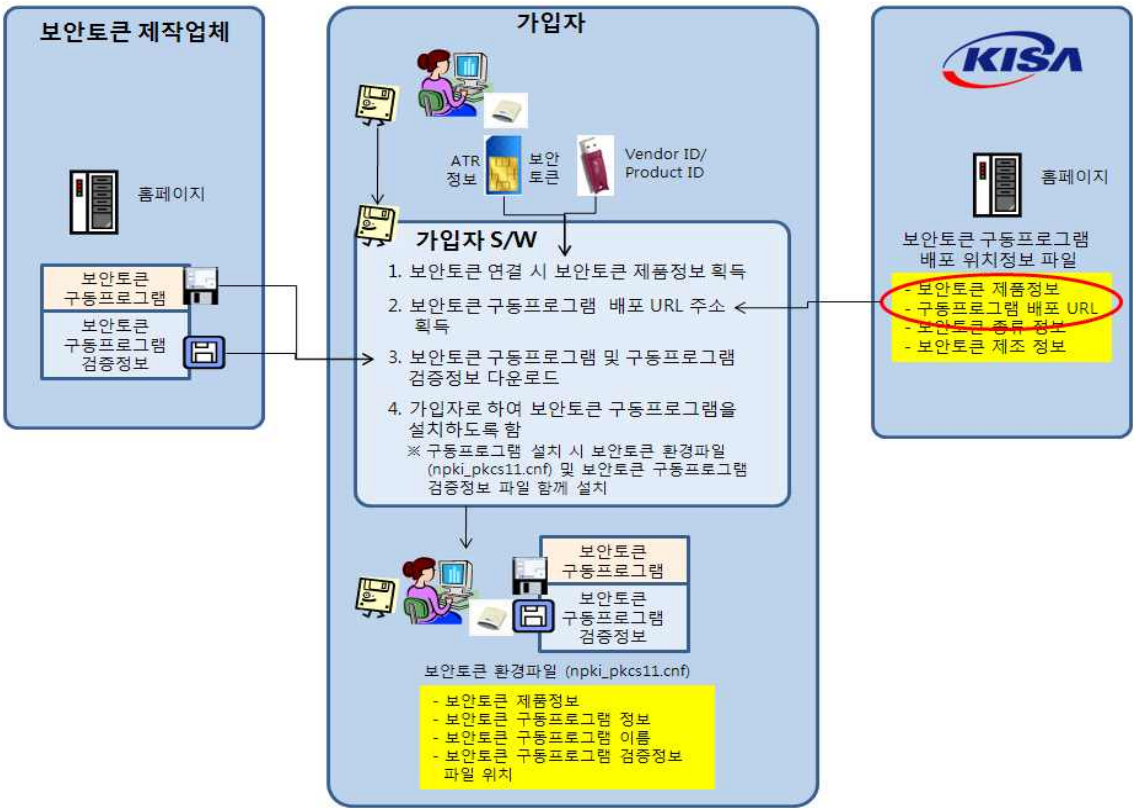
가) 해야한다, 필수이다, 강제한다 (기호 : M)
반드시 준수해야 한다.
나) 권고한다 (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.
다) 할 수 있다, 쓸 수 있다 (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.
라) 권고하지 않는다 (기호 : NR)
보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.
마) 금지한다, 허용하지 않는다 (기호 : X)
반드시 사용하지 않아야 한다.
바) 언급하지 않는다, 정의하지 않는다 (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어

본 가이드라인에서는 다음의 약어가 이용된다.

가) ATR : Answer to Reset, 보안토큰 초기화 정보

6. 보안토큰의 구동프로그램 배포



가입자 소프트웨어는 제6.1절에서 기술하는 보안토큰 제품정보)를 획득하고 제6.2절 '보안토큰 구동프로그램 배포 위치정보 파일'의 보안토큰 구동프로그램 배포 URL를 참조하여 해당 고유 제품정보(ID)에 해당하는 보안토큰 구동프로그램을 다운로드 할 수 있다. 본 가이드라인은 리더기와 보안토큰이 일체된 USB형 보안토큰과 리더기와 보안토큰이 분리된 스마트카드형으로 구분하여 구동프로그램 배포방안을 기술한다.

6.1 보안토큰의 고유 제품정보

6.1.1 USB형 보안토큰의 고유 제품정보

USB형 보안토큰의 고유 제품정보는 USB Enumeration 기능에 따라 하드웨어 기기가 사용자 시스템에 제공하는 보안토큰 제작사 ID(Vid)와 보안토큰 제품 ID(Pid)의 연접정보이다. Vid와 Pid는 각각 4자리 Hexa 문자열로, 연접정보는 Vid 값과 Pid 값을 "&"로

연접한다. 이때 Vid 값은 “Vid_” 구분자를 포함하고, Pid 값은 “Pid_”를 구분자로 포함하여야 한다(보안토큰 고유 제품정보 예시 : Vid_0529&Pid_0514. 신규로 연결되는 보안토큰 고유 제품정보를 확인할 수 있는 PC의 운영체제 별 저장위치는 다음과 같다.

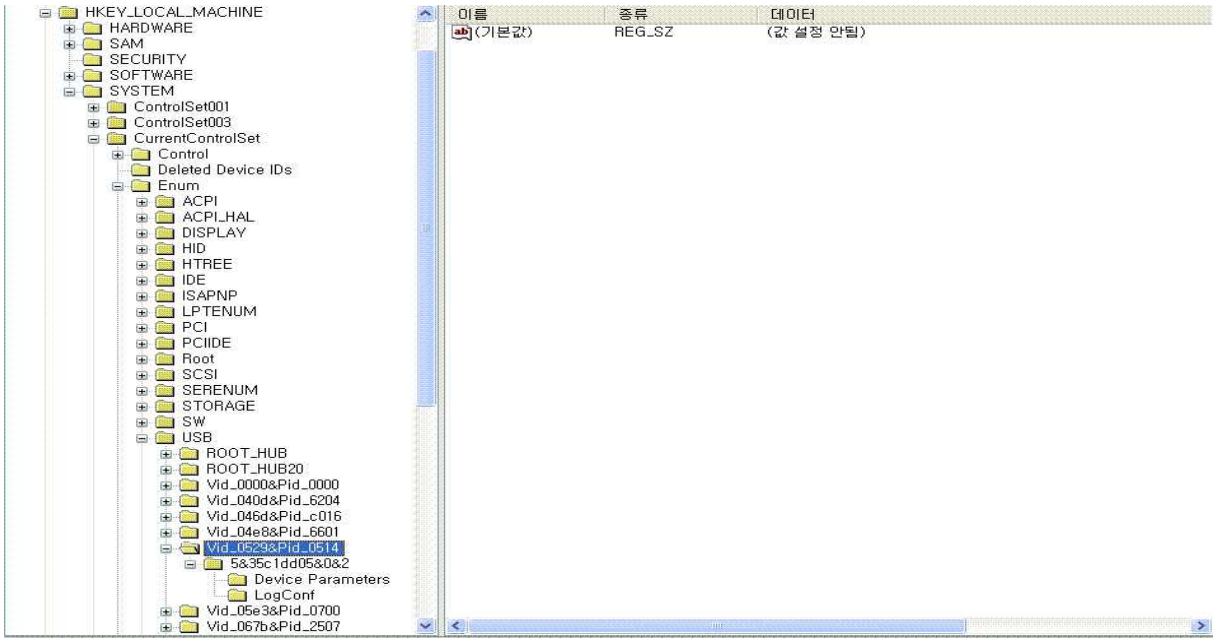
o MS 윈도우 : ‘HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB’(레지스트리)

- MS 윈도우에 보안토큰이 연결될 경우 WM_DEVICECHANGE 이벤트가 발생하며, SetupDiEnumDeviceInfo, SetupDiGetDeviceRegistryProperty 등 두 함수 호출을 통해 PC 시스템에 장착된 보안토큰 고유제품 정보를 획득할 수 있다.

o 리눅스 : /proc/bus/usb/devices

o 매킨토시 : GetDescriptor 함수 또는 ioreg -p IOUSB -l 명령을 통해 보안토큰 제품정보를 가져올 수 있다.

<MS 윈도우 레지스트리의 보안토큰 고유 제품정보 예제>



6.1.2 스마트카드형 보안토큰 고유 제품정보

스마트카드형 보안토큰의 경우 리더기와 보안토큰 등으로 기기가 분리되어 있기 때문에 개별 기기에 대한 전용 구동프로그램이 각각 설치되어야 한다. 보안토큰의 고유 식별자(ID)는 리더기에 보안토큰 삽입시 발생하는 보안토큰 초기화 정보인 전체 ATR(Answer To Reset) 값을 활용한다.

가입자 소프트는 ATR 값은 별도의 명령어에 의해서도 획득할 수 있다.

<스마트카드 ATR 구성>

ATR 바이트	필수여부	값 (Hex)
TS	Mandatory	Direct 혹은 inverse convention flag
T0	Mandatory	xF - 'x'는 유효한 interface character들의 값이고 F는 15개의 historical 바이트의 존재를 표시
TA_i - TD_i	Optional	지원되는 프로토콜과 parameter를 기술하는 최대 14개까지의 인터페이스 character들
T1	Optional	80 - compact TLV data object들의 따라옴을 표시
T2	Optional	25 - 5바이트의 issuer ID number가 따라옴을 표시하는 태그
T3	Optional	RID_1 (Registered Application Identifier)
T4	Optional	RID_2
T5	Optional	RID_3
T6	Optional	RID_4
T7	Optional	RID_5
T8	Optional	56 - 6바이트의 ICC issuer data가 따라옴을 표시하는 태그
T9	Optional	$Model_1$
T10	Optional	$Model_2$
T11	Optional	$Model_3$
T12	Optional	$Model_4$
T13	Optional	$Model_5$
T14	Optional	Major
T15	Optional	Minor
TCK	Conditional	Checksum byte

6.2 보안토큰 구동프로그램 배포 위치정보 요구사항

보안토큰 구동프로그램 배포 위치정보(이하, 위치정보)는 가입자 소프트웨어가 제6.1절의 보안토큰 고유 제품정보에 해당하는 전용 구동프로그램을 배포하기 위해 참조하는 정보를 말한다.

가입자 소프트웨어는 한국정보보호진흥원 또는 공인인증기관 홈페이지에 게재된 위치정보 파일을 참조할 수 있다.

- o 한국정보보호진흥원 : "http://www.rootca.or.kr/certs/hsm.der"
- o 한국정보인증 : "http://xxx.xxx.xxx/hsm.der"
- o 코스콤 : "http://xxx.xxx.xxx/hsm.der"
- o 금융결제원 : "http://xxx.xxx.xxx/hsm.der"
- o 한국정보사회진흥원 : "http://xxx.xxx.xxx/hsm.der"
- o 한국전자인증 : "http://xxx.xxx.xxx/hsm.der"
- o 한국무역정보통신 : "http://xxx.xxx.xxx/hsm.der"

가입자 소프트웨어는 구동프로그램의 안전한 배포를 위해 한국정보보호진흥원이 전자서명한 위치정보 전자서명값(SignatureValue)를 검증하여 위치정보의 무결성을 확인하여야 한다.

o 위치정보 ASN.1

```
DEFINITIONS ::= BEGIN

IMPORTS
AlgorithmIdentifier, Certificate, CertificateList, CertificateSerialNumber, Name FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6) internet(1) security(5)
mechanisms(5) pkix(7) mod(0) pkix1-explicit(18) }

Type ::= INTEGER {usb(0), smartcard(1)}

TokenDistributionURL ::= SEQUENCE {
        tokenID                 IA5String,
          -- 보안토큰 고유 제품정보로써, USB형 보안토큰은 Vendor ID와 Product
          -- ID 연접정보를 말하여, 스마트카드형 보안토큰은 ATR정보를 말함
       driverInfo               SEQUENCE OF DriverInfo
}

DriverInfo ::= SEQUENCE {
        supportedOSVersion  PrintableString,
        -- 지원되는 PC 운영체제 종류를 ','로 구분하여 나열(예 : Microsoft Windows
        -- XP, Microsoft Windows 98)
        version             PrintableString,
          -- 보안토큰 구동프로그램 버전정보
        name                GeneralName,
          -- 보안토큰 구동프로그램 배포위치를 나타내며, IP 주소를 사용할 것을 권고
        type                Type,
          -- USB형 보안토큰의 경우 0, 스마트카드형 보안토큰의 경우 1로 표시
        cp                  GeneralName
          -- 보안토큰 제작업체에 대한 정보(URL, 전화번호 등)
        info                PrintableString OPTIONAL
          -- 보안토큰 모델명 등 보안토큰 제품 정보
 }
SignatureValue ::= SEQUENCE {
```

```
toBeSigned              SEQUENCE OF TokenDistributionURL,
    -- 보안토큰 구동프로그램 DLL이 여러 DLL로 구성되어 있을 경우
    -- 각 DLL에 대한 무결성을 보증하기 위해 SEQUENCE OF로 구성
signatureAlgorithm      AlgorithmIdentifier,
    -- 전자서명 알고리즘의 OID
signerAndSerialNumber SignerAndSerialNumber,
    -- 전자서명 생성자의 (KISA 3280 루트인증서)
signature               BIT STRING }        -- toBeSigned에 대한 전자서명값
END
```

가입자 소프트웨어는 지원되는 PC 운영체제 종류 'supportedOSVersion'를 확인하여 가입자 PC 운영체제에 적합한 구동프로그램을 설치하여야 한다.

또한, 가입자 소프트웨어는 버전정보 'version'와 [KCAC.TS.HSM] 부록 4. 환경파일을 이용한 보안토큰 구동프로그램 위치정보의 Info키에 명시된 보안토큰 구동프로그램의 버전정보를 상호 비교하여 구동프로그램을 업데이트할 수 있다.

6.3 보안토큰 제작업체 요구사항

보안토큰 제작업체는 [KCAC.TS.HSM] 부록 4. 환경일을 이용한 보안토큰 구동프로그램 위치정보의 Info키에도 보안토큰 구동프로그램 버전정보를 포함할 것을 권장하며, 이때 구분자는 ':' 문자를 사용하여야 한다.

보안토큰 제작업체는 보안토큰 고유 제품정보, 지원하는 OS버전, 구동프로그램 버전으로 구동프로그램을 식별할 수 있도록 해당 배포 URL 정보를 한국정보보호진흥원에 제공하여야 한다. 또한, 보안토큰 구동프로그램의 안전한 배포를 위해 코드서명 하여야 한다.

6.4 가입자 소프트웨어 요구사항

하나 이상의 보안토큰 구동프로그램이 사용자 시스템에 기 설치되어 있는 경우, 가입자 소프트웨어는 신규로 삽입되는 보안토큰 구동프로그램 배포·설치 필요여부를 확인하기 위해, '보안토큰 기반의 공인인증서 이용기술 규격'의 부록 4. 환경파일을 이용한 보안토큰 구동프로그램 위치정보 관리 파일'의 하위 섹션명(보안토큰 고유식별자)를 참조할 수 있다.

7. 가입자 소프트웨어와 함께 배포하는 방안

가입자 소프트웨어는 지원할 수 있는 보안토큰 구동프로그램을 자신의 자동설치 파일에 내장하여 배포할 수 있다.

부록 7. 가이드라인 연혁

버전	제・개정일	제・개정내역
v1.00	2007년 9월	"보안토큰 구동프로그램 배포 가이드라인"으로 제정

가이드라인 작성 공헌자

본 가이드라인의 제정을 위해 아래와 같이 많은 분들이 공헌을 하였습니다.

구분	성명	소속사
가이드라인 제안	전자인증팀	한국정보보호진흥원
가이드라인 초안 제출	전자인증팀	한국정보보호진흥원
가이드라인 검토	이석래	한국정보보호진흥원
	박상환	한국정보보호진흥원
	이원철	한국정보보호진흥원
	김영준	한국정보보호진흥원
	장재환	한국정보인증
	김근옥	한국정보인증
	임지영	코스콤
	이성국	코스콤
	이성진	코스콤
	이만호	금융결제원
	오중효	금융결제원
	이한욱	금융결제원
	정성아	금융결제원
	박명수	한국정보사회진흥원
	박성익	한국정보사회진흥원
	김재홍	한국정보사회진흥원
	최현호	한국정보사회진흥원
	이성철	한국무역정보통신
	국상진	한국무역정보통신
	강광석	KEBT
	김국진	KEBT
	박민수	KEBT
	이용호	Nets
	김월용	NLS시스템
	조윤호	NLS시스템
	이종서	NLS시스템
	박경봉	SCT
	권유미	드림시큐리티
	강명호	비티웍스
	김종협	비티웍스
	정재웅	비티웍스
	김기영	소프트포럼
	강효관	소프트포럼
	박길동	시큐리티테크놀로지
	박찬석	위노블
	최규태	위노블
	황남진	위노블
	신동규	유넷시스템
	박준석	유비닉스
	김덕엽	이니텍

구분	성명	소속사
	이준형	이니텍
	전병권	이니텍
	김남희	이니텍
	한성기	인터넷시큐리티
	남경원	인터넷시큐리티
	김세준	장미디어
	황한웅	케이사인
	정성균	펜타시큐리티
	임정훈	하이스마텍
	주충호	한울로보틱스
	김홍석	한국마이크로소프트
	정 용	재익정보통신
	김중선	LG히다찌
규격안 편집	박상환	한국정보보호진흥원