무선단말기와 PC간 공인인증서 전송을 위한 기술규격

Certificate Transmission between PC to Mobile Device

v2.10

2012년 11월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

무선단말기와 PC간 공인인증서 전송을 위한 기술규격

Certificate Transmission between PC to Mobile Device

1. 개 요

본 규격은 유선인터넷을 통해 발급된 공인인증서를 휴대전화 등 무선단말기를 이용한 전자거래에 사용할 수 있도록 PC 등의 저장매체에 저장된 공인인증서 및 전자서명생성키를 무선단말기로 전송하거나, 무선단말기에 저장된 공인인증서 및 전자서명생성키를 PC 등으로 전송하기 위한 요구사항을 정의한다.

2. 규격의 구성 및 범위

본 규격은 인터넷망을 이용하여 공인인증서 및 전자서명생성키를 무선단말기에서 전송하거나 전송받는 경우에 대한 요구사항을 명시하며 다음과 같이 구성된다.

첫 번째로는 공인인증서 전송기능을 가지는 소프트웨어의 요구사항을 명시한다. 두 번째로는 PC와 무선단말기 간 전송채널의 요구사항을 명시하고 마지막으로 전송되는 공인인증서 및 전자서명생성키의 안전성 요구사항을 명시한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

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

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

3.2 국내 표준 및 규격

[KCAC.TS.UI] KISA, KCAC.TS.UI v1.83, *공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격*, 2012

[KCAC.TS.DSIG] KISA, KCAC.TS.DSIG, v1.30, *전자서명 알고리즘 규격*, 2009

[KCAC.TS.HASH] KISA, KCAC.TS.HASH, v1.20, *해쉬 알고리즘 규격*, 2009

[KCAC.TS.ENC] KISA, KCAC.TS.ENC, v1.21, *암호 알고리즘 규격*, 2009

3.3 기타

해당사항 없음

4. 정의

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) 가입자
나) 공인인증서
다) 전자서명생성키

4.2 용어의 정의

가) 인증서 전송서비스 제공기관 : PC등에 저장된 가입자의 공인인증서 및 전자서명생성키를 인터넷망을 이용하여 무선단말기로 전송하는 서비스를 제공하는 기관

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 무선단말기로 공인인증서 전송 서비스를 제공하는 공인인증서 관리 프로그램 및 전송시스템의 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) PC : Personal Computer, 가입자 개인 컴퓨터

나) VID : Virtual ID, 가상식별번호

6. 사용자 인증

PC 등에 저장된 공인인증서 및 전자서명생성키를 무선단말기로 전송하거나, 무선단말기에 저장된 공인인증서 및 전자서명생성키를 PC 등으로 전송하고자 하는 경우 해당 기능을 제공하는 소프트웨어는 공인인증서를 전송하고자 하는 사용자가 공인인증서의 소유자임을 확인하여야 한다. 이를 위해 전자서명생성키 암호화 비밀번호 확인 기능 등을 사용할 수 있다.

공인인증서 전송 요청은 사용자의 전자서명생성키로 전자서명하여 인증서 전송서비스 제공기관에 전송되어야 하며, 인증서 전송서비스 제공기관은 서명된 사용자의 공인인증서 전송 요청에 대한 검증 기능을 제공하여야 한다.

인증서 전송서비스 제공기관은 무선단말기와 사용자 사이에 안전한 사용자 인증 방안을 제공하여야 한다. 이를 위해 인증서 전송서비스 제공기관은 무선단말기 명의자와 사용자 일치 여부를 확인하거나, 무선단말기로 단문메시지를 전송하는 등의 방법을 사용할 수 있다.

무선단말기에 저장된 공인인증서 및 전자서명생성키를 PC등으로 전송하는 경우에는 무선단말기의 전화번호와 공인인증서를 전송받을 PC에서 입력한 무선단말기 전화번호의 일치여부를 확인하는 방법도 사용할 수 있다.

7. 전송채널의 암호화

공인인증서 및 전자서명생성키의 전송을 위해 사용되는 PC와 무선단말기 간 전송채널은 반드시 암호화되어야 한다. 전송채널은 RSA 1024비트 이상의 안전성에 준하여야 하며, 공인인증서 및 전자서명생성키의 전송 시마다 매번 새로운 암호화 키를 사용하여야 한다. 이때 알고리즘은 [KCAC.TS.DSIG], [KCAC.TS.HASH], [KCAC.TS.ENC]에 규정된 암호 알고리즘을 사용한다.

암호화된 전송채널은 안전한 난수생성함수를 이용하여 비밀정보를 유도·생성하여야 하며, 암호화를 위한 세션키 분배용도의 인증서 이용 등을 통해 안전하게 생성되어야 한다.

8. 인증서 전송

인터넷망을 통해 전송되어지는 공인인증서 및 전자서명생성의 형태는 [KCAC.TS.UI]에서 인증서 가져오기 및 내보내기 기능에 사용되는 [PKCS12] 등의 방법을 이용하여 전송메시지의 무결성을 보장해야 한다. [PKCS12]를 사용하는 경우 구현은 부록1을 참고할 것을 권고한다.

가입자가 전자서명용과 키분배용 공인인증서를 함께 소유한 경우에는 반드시 전자서명용과 키분배용 인증서를 함께 전송하여야 한다. 또한, 필요한 경우에는 공인인증기관 인증서를 함께 전송할 수 있다.

공인인증서 전송 서비스 제공을 위해 제3의 중계서버가 사용되는 경우 소프트웨어는 중계서버 인증서 등을 사용하여 중계서버의 신뢰성을 검증할 수 있는 방법을 제공하여야 한다. 또한 중계서버는 출입통제, 물리적 침입감시, 시스템 및 네트워크 보호 등의 사항에 대해 보호설비를 갖추어야 한다. 무선단말기로 공인인증서 및 전자서명생성키를 전달한 후 공인인증서는 중계서버의 기억장소(memory) 또는 임시파일에서 즉시 삭제되어야 한다.

9. 전자서명생성키 암호화 비밀번호의 안전성

무선단말기에 저장된 공인인증서 및 전자서명생성키를 PC등으로 전송하는 경우에 전자서명생성키 암호화 비밀번호가 안전성 기준을 만족하지 않으면 전자서명생성키 암호화 비밀번호를 안전성 기준에 만족하도록 재설정되어야 하며, 이를 이용하여 전자서명생성키를 암호화하여 PC등에 저장하여야 한다.

10. 기타 고려사항

무선단말기로 공인인증서 전송 기능 또는 무선단말기로부터 공인인증서 전송 기능은 사용자 편의성을 고려하여 공인인증서 관리 프로그램에 함께 구현될 수 있다.

무선단말기내 공인인증서 송·수신기능을 가지는 소프트웨어는 사전에 안전한 방법으로 무선단말기에 설치되어야 한다.

부록 1. PKCS#12 구현 시 고려사항

□ Integrity mode

AuthenticatedSafe에 대한 무결성 보장을 위하여 Password를 이용한 MAC을 생성하여야 한다.

MAC을 생성할 시에는 SHA-1함수를 이용하여야 하며 이 때 Salt값은 해쉬함수의 output 길이(20bytes)와 동일한 random값을 사용하고 iterationCount는 1024 이상으로 사용할 것을 권고한다.

PKCS#12 화일을 Import하는 경우에는 Integrity에 대한 검사를 수행하여 데이터가 변조된 경우에는 Import를 중단하여야 한다.

공개키 방식을 이용할 경우에는 이를 Import하는 Platform에 대한 적절한 고려가 선행되어야 한다.

□ Privacy mode

AuthenticatedSafe를 구성하는 SafeContents에 대한 기밀성이 요구되는 경우 Password 기반의 Privacy mode를 적용한다.

이 때 사용하는 알고리듬으로는 호환성을 고려하여 다음의 알고리듬만을 적용하며 그렇지 않을 경우에는 이를 Import하는 Platform에 대한 적절한 고려가 선행되어야 한다. 단, Microsoft와의 호환을 고려하여 추가적으로 pbeWithSHAAnd128bitRC2-CBC 알고리듬을 처리할 수 있어야 한다.

- pbeWithSHAAnd3-KeyTripleDES-CBC

Password를 이용하여 암호용 키를 생성할 때 사용되는 Salt와 iternationCount는 위의 Integrity mode의 경우에 준한다.

□ Password

Integrity와 Privacy를 위해서 두 개의 Password가 필요하게 될 경우 기본적으로 동일한 Password를 사용하며 서로 다른 Password를 사용하는 경우에는 이를 Import하는 Platform에 대한 적절한 고려가 선행되어야 한다.

□ AuthenticatedSafe의 구성

AuthenticateSafe는 기본적으로 두 개의 SafeContents를 가져야 한다. 하나는 PKCS-8ShroudedKeyBag으로 구성된 SafeContents이고 다른 하나는 CertBag들로 구성된 SafeContens이다. 모든 SafeContents는 순서에 무관하게 처리되어야 한다.

PKCS-8ShroudedKeyBag을 구성할 때 사용되는 암호알고리듬은 Privacy mode에서 언급한 알고리듬을 준용한다.

CertBag으로 구성된 SafeContents에는 사용자 인증서를 저장하여야 하며 Root CA까지의 인증서 체인을 저장할 수 있다. 인증서 체인을 저장하는 경우에는 순서에 무관하게 처리되어야 한다. 해당 SafeContents에는 Password 기반의 Privacy mode를 적용할 수 있다.

필요에 따라 CRLBag, SecretBag 등을 사용한 SafeContents를 추가할 수도 있으나 이 경우에는 Import하는 Platform에 대한 적절한 고려가 선행되어야 한다.

□ Bag Attribute의 사용

사용자의 개인키와 인증서간의 합치성을 표현하기 위하여 해당하는 PKCS-8ShroudedKeyBag과 CertBag에 localKeyId 속성을 사용할 것을 권고한다.

Microsoft 인증서 관리툴과의 연동을 고려하여 CertBag에는 해당 인증서를 식별할 수 있는 이름으로 friendlyName 속성을 사용할 것을 권고한다.

부록 2. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2007년 4월	o “무선단말기로 공인인증서 전송을 위한 기술 규격”으로 제정
v1.10	2008년 10월	o 관련 국내 표준 및 규격 갱신 내용 반영 o 법률 공포번호가 해당 법률 개정 시마다 변경되는 점을 고려하여 법령명으로 개정
v2.00	2010년 3월	o 휴대폰에서 PC등으로 공인인증서 전송이 가능하도록 관련 규정 추가
v2.10	2012년 7월	o 전송세션 암호화 보안요구사항 추가