무선 전자서명 알고리즘 구현 가이드라인

Implementation Guideline for the Wireless Electronic Signature Algorithm

v1.00

2003년 8월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

무선 전자서명 알고리즘 구현 가이드라인(안)

Implementation Guideline for the Wireless Electronic Signature Algorithm(Draft)

1. 개요

본 가이드라인에서는 전자서명인증체계 무선환경에서 사용되는 전자서명 알고리즘의 구현 방법을 정의하여 무선 공인인증서비스의 상호연동성을 확보하고자 한다.

2. 가이드라인의 구성 및 범위

본 가이드라인은 무선 PKI 공인인증서비스에서 사용되는 전자서명 알고리즘의 구현을 위한 가이드로서 다음과 같이 두 부분으로 나누어진다.

첫 번째로 ECDSA 구현시 사용되는 서명대상, 서명생성, 서명값 구조에 대해 정의한다.

두 번째로 RSA 구현시 사용되는 서명대상, 서명생성, 서명값 구조에 대해 정의한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[X9.62] ANSI, X9.62-1999, *Public Key Cryptography for the Financial Services Industry : The Elliptic Curve Digital Signature Algorithm(ECDSA),* 1999

[SHA-1] NIST, FIPS PUB 180-1, *National Institute of Standards and Technology,* 1994

[WAPScript] OMA, WAP-161-WMLScriptCrypto-20010620-a, *WMLScript Crypto Library*, Version 20-Jun-2001

[WAPWTLS] OMA, WAP-261-WTLS-20010406-a, *Wireless Transport*

Layer Security, Version 06-Apr-2001

[PKCS1] RSA, PKCS#1 v2.0, *RSA Cryptography Standard*, October 1, 1998

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

[RFC3279] IETF, RFC3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* April 2002

3.2 국내 표준 및 규격

[KCAC.WALSP] KISA, KCAC.WALSP, "*무선 응용계층 보안프로토콜 규격*", 2003년 4월, http://www.rootca.or.kr

[KCAC.TCI] KISA, KCAC.TCI, "*무선 환경을 위한 최상위 인증기관 인증서 신뢰 규격*", 2003년 6월, http://www.rootca.or.kr

[KCAC.WTLSCert] KISA, KCAC.WTLSCert, "*무선 WLTS 인증서 프로파일 규격*", 2001년 9월, http://www.rootca.or.kr

3.3. 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어 정의

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

가) 인증서
나) 전자서명인증체계
다) 가입자
라) 가입자 소프트웨어

4.2 용어의 정의

해당사항 없음

4.3 용어의 효력

본 가이드라인에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 전자서명 알고리즘을 생성하거나 처리하는데 따라야 할 구현 정도를 의미하는 것으로 [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) TCI : Trusted Certificate Authority Information, 최상위인증기관 신뢰 정보
나) ASN.1 : Abstract Syntax Notation One

6. ECDSA 구현 방법

6.1 서명 대상

서명하고자 하는 메시지에 [SHA-1]을 사용하여 160bit로 해쉬한 후 이 값을 서명대상으로 해야 한다.

6.2. 서명 생성

6.1에서 계산된 서명 대상에 [X9.62]를 준수한 서명 절차를 수행하여 r과 s를 생성해야 한다.

6.3 서명값 구조

6.2에서 계산된 서명값(r과 s)은 다음과 같은 2가지 방법으로 구성된다.

6.3.1 연접구조

[WAPWTLS]에 명시된 방법으로 r과 s를 연접(concatenation)하여 사용하는 방법이다.

서명값인 정수 r과 s를 [X9.62]에서 정의된 Integer-to-Octet-String 변환 규칙에 의해 문자열(옥텟스트링) R과 S로 변환한 후 이를 연접하여 서명값 구조를 생성한다. 이때 생성된 서명값 구조(Sig)를 기호로 표시하면 다음과 같다.

Sig : R | S

위의 구조는 [KCAC.WTLSCert]에서 정의한 WTLS 인증서의 signature 필드, [KCAC.WALSP]에서 정의한 SignedContents의 signature 필드 및 [KCAC.TCI]의 TCI 구조체에 포함되는 signature 필드에 사용해야 한다.

SignedContents가 유선 환경과의 호환성을 가지기 위해서는 컨텐츠제공자(CP)에서 서명값 연접구조를 ASN.1 구조로 변환하여 사용해야 한다.

6.3.2 ASN.1 구조

[X9.62]에 명시된 방법으로 정수 r과 s를 ASN.1 구조체인 ECDSA-Sig-Value 형태로 변환하여 사용하는 방법이다.

ECDSA-Sig-Value 구조체의 ASN.1 형태는 다음과 같다.

```
ECDSA-Sig-Value ::= SEQUENCE
{
        r  INTEGER,
        s  INTEGER    }
```

이 구조체는 X.509 인증서의 signature 필드에 사용해야 한다.

7. RSA 구현 방법

7.1 서명 대상

7.1.1 메시지 해쉬값

[WTLS]에 명시된 방법으로, 서명하고자 하는 메시지를 [SHA-1]으로 해쉬한 160bit 결과값을 서명 대상으로 한다.

[KACA.WTLSCert]에서 정의한 WTLS 인증서의 signature 필드, [KCAC.TCI]의 TCI 구조체 signature 필드를 생성하는 경우에는 서명대상으로 메시지 해쉬값을 사용해야 한다.

7.1.2 DigestInfo 구조체

서명하고자 하는 메시지를 [SHA-1]으로 해쉬한 후 해쉬값을 [PKCS1]에서 정의된 DigestInfo 형태로 변환하여 서명하는 방식이다. DigestInfo의 ASN.1 형태는 다음과 같다.

```
DigestInfo ::= SEQUENCE
{
        digestAlgorithm  Algorithmidentifier,
```

Digest OCTET STRING }

이 구조체에서 Digest는 6.1.1에서의 160bit 해쉬값과 동일하다.

[KCAC.WALSP]에서 정의한 SignedContents의 signature 필드 및 X.509인증서의 signature 필드를 생성하는 경우에는 서명 대상으로 위의 DigestInfo 구조체를 사용해야 한다.

7.2 서명 생성

7.1에서 생성된 서명대상에 [PKCS1]를 준용하여 서명한다.

7.3 서명값 구조

7.2에서 계산된 옥텟 스트링(octet string)이 서명값 구조이다.

8. 요약

무선 환경에서 사용되는 ECDSA와 RSA의 서명값 구조 및 서명대상을 전자서명을 사용하는 응용 대상별로 정리하면 다음과 같다.

알고리즘 / 대상	ECDSA		RSA	
	서명 대상	서명값 구조	서명 대상	서명값 구조
WTLS 인증서	메시지해쉬값	연접구조	메시지 해쉬값	옥텟스트링
SignedContents	메시지해쉬값	연접구조	DigestInfo 구조체	옥텟스트링
TCI	메시지해쉬값	연접구조	메시지 해쉬값	옥텟스트링
X509 인증서	메시지해쉬값	ECDSA-Sig-Value 구조체	DigestInfo 구조체	옥텟스트링

부록 1. 가이드라인의 연혁

버전	제・개정일	제・개정내역
v1.00	2003년 8월	“무선 전자서명 알고리즘 구현 가이드라인”으로 제정

가이드라인 작성 공헌자

본 가이드라인의 제·개정 및 발간을 위해 아래와 같이 여러분들이 공헌을 하였습니다.

구분	성명	소속사
가이드라인 제안	암호인증기술팀	한국정보보호진흥원
가이드라인 초안 제출	암호인증기술팀	한국정보보호진흥원
가이드라인 검토	임선간	한국정보보호진흥원
	이석래	한국정보보호진흥원
	박종욱	한국정보보호진흥원
	전인경	한국정보보호진흥원
	박상환	한국정보보호진흥원
	박배효	한국정보보호진흥원
	최태규	한국정보보호진흥원
	심희원	한국정보인증
	장재환	한국정보인증
	이성진	한국증권전산
	이상철	한국증권전산
	김준태	한국증권전산
	이만호	금융결제원
	이한욱	금융결제원
	오중효	금융결제원
	이성철	한국무역정보통신
	국상진	한국무역정보통신
	박종헌	드림시큐리티
	장형도	드림시큐리티
	심재성	드림시큐리티
	오명선	드림시큐리티
	임진수	케이사인
	최민호	케이사인
	박현주	시큐어소프트
	조민규	시큐어소프트
	전경호	시큐어소프트
	김민형	SK텔레콤
	최지희	LG텔레콤
가이드라인안 편집	전인경	한국정보보호진흥원