KS X 3185

KSKSKSKS
SKSKSKS
KSKSKS
SKSKS
KSKS
SKS
KS

KS

부가형 디지털 서명방식 표준

KS X 3185:1996

미 래 창 조 과 학 부 국 립 전 파 연 구 원

1996년 1월 6일 제정

서 문

1. 개요

본 표준은 개방형시스템의 상호접속을 지향하는 통신망 또는 정보처리시스템 상에서 이용할 수 있도록 임의의 길이를 갖는 메시지에 대한 부가형 디지털 서명 방식이 갖추어야 할 기본기능과 구조를 규정한다. 또한, 디지털 서명 방식의 기본 개념을 일반 모델화 시키고 이를 기초로한 서명방식의 표준화에 활용하도록 한다.

2. 다른 표준들과의 관계

본 표준은 국제표준 ISO/IEC JTC1/SC27 WG2에서 표준화로 진행중인 "Digital signature with appendix - Part 1 : General model"과 밀접한 관계를 가지고 있다.

3. 참고 표준 및 권고

3.1 국내표준 :

KSC 5869-92 : 개방형 시스템 상호접속 기본참조 모델-보안구조

3.2 ITU-T 권고 :

- ITU-T X.811(1994) : Information technology-Open systems interconnection-Security framework for open system : Authentication framework
- ITU-T X.509(1993) : Information technology-Open systems interconnection-The directory : Authentication framework

3.3 ISO 표준 :

- ISO 7498-2(1989) : Information processing systems-Open systems interconnection-Basic reference model, Part2 : Security architecture
- ISO/IEC 10181-2 (1994) : Information technology-Open systems interconnection-Security framework for open system : Authentication framework
- ISO/IEC 9594-8 (1993) : Information technology-Open systems interconnection-The directory : authentication framework
- ISO/IEC 9796 (1991) : Information technology-Security techniques-Digital signature mechanisms giving message recovery

3.4 CCITT 권고

CCITT X.800(1991) : Security architecture for open systems interconnection for CCITT application

4. 이력

판 수	발행일	제정 및 개정내역
제1판	1996. 1. 6.	제정

Preface

1. Summary

This standard specifies the basic functions and the structure of "digital signature scheme with appendix" for message having an arbitrary length, which can be used in open system or information processing system environment where the network interconnection is pursued. In addition, we define a general model for the fundamental concept of digital mechanisms on which the standardization and its applications are based.

2. The relation of other standard(International recommendation or standard, Domestic Standard, or etc.)

This standard is related to ISO/IEC JTC1/SC27 WG2 "Digital signature with appendix -Part 1 : General model".

3. Reference

3.1 Domestic Standard :

KSC 5869-92 : 개방형 시스템 상호접속 기본참조 모델-보안구조

3.2 ITU-T recommendation :

- ITU-T X.811(1994) : Information technology-Open systems interconnection-Security framework for open system : Authentication framework
- ITU-T X.509(1993) : Information technology-Open systems interconnection-The directory : Authentication framework

3.3 ISO Standard :

- ISO 7498-2(1989) : Information processing systems-Open systems interconnection-Basic reference model, Part 2 : security architecture
- ISO/IEC 10181-2(1994) : Information technology-Open systems interconnection-Security framework for open system : Authentication framework
- ISO/IEC 9594-8(1993) : Information technology-Open systems interconnection-The directory : Authentication framework
- ISO/IEC 9796(1991) : Information technology-Security techinques-Digital signature mechanisms giving message recovery

3.4 CCITT recommendation :

CCITT X.800(1991) : Security architecture for open systems interconnection for CCITT application

4. History Not applicable

Version	Issue Date	Contents
1	1996. 1. 6.	Established

목 차
CONTENTS

1. 표준의 개요

본 표준은 정보처리시스템 또는 정보통신망에서 이용할 수 있도록 임의의 길이를 갖는 메시지에 대한 부가형 디지털서명 방식이 갖추어야 할 기본기능과 구조를 규정한다. 또한, 부가형 디지털서명 방식의 기본개념을 일반 모델화시키고 이를 기초로 한 서명방식의 표준화에 활용하도록 한다.

2. 적용범위

본 표준은 정보처리시스템 또는 정보통신망 환경하에서 인증, 무결성 및 부인봉쇄, 정보보호 서비스를 제공하기 위하여 공개키 암호시스템을 이용하는 부가형 디지탈서명 방식에 적용한다. 또한, 본 표준에서 규정하는 사항은 관련 후속 표준인 식별자를 이용한(identity-based) 서명과 확인서를 이용한(certificate-based) 서명 등의 표준에서 적용될 수 있다.

3. 준용표준

본 표준에서 별도로 규정하지 아니한 사항은 다음의 표준을 준용한다.

1) 국내표준

가. KSC 5869-92 : 개방형 시스템 상호접속 기본참조 모델-보안구조

2) 국제표준

가. CCITT X.800 (1991) : Security architecture for open systems interconnection for CCITT applications.

나. ISO 7498-2 (1989) : Information processing systems - Open systems interconnection - Basic reference model, Part 2 : Security architecture

다. ITU-T X.811 (1994) : Information technology - Open systems interconnection - Security framework for open system : Authentication framework

라. ISO/IEC 10181-2 (1994) : Information technology - Open systems interconnection - Security framework for open system : Authentication framework

마. ITU-T X.509 (1993) : Information technology - Open systems interconnection - The directory : Authentication framework

바. ISO/IEC 9594-8 (1993) : Information technology - Open systems interconnection - The directory : Authentication framework

사. ISO/IEC 9796 (1991) : Information technology - Security techniques - Digital signature scheme giving message recovery

4. 용어정의

1) 정보보호 관련기술에서 준용하는 용어

가. 디지털서명 : 메시지의 수신자로 하여금 그 메시지의 발신원과 무결성을 증명하고 위조를 방지하도록 하는 암호학적 변환 또는 원래의 메시지에 추가된 데이타를 말한다. (KSC 5869-92, ITU-T X.800, ISO 7498-2)

〈주〉 수기서명, 인감, 지문 등의 그래픽 이미지를 전자서류의 서명란에 표시하여 사용하는 경우가 있는데 이는 디지털서명이라 하지 않는다.

나. 신뢰할 수 있는 제3자(TTP ; trusted third party) : 안전성관련 행동에 관하여 다른 실체에 의해 신뢰받는 안전한 기관이나 대행기관. 본 표준에서 신뢰할 수 있는 제3자는 인증 목적을 위해 요구자나 검증자에 의해 신뢰를 받는다. (ITU-T X.811 또는 ISO/IEC 10181-2)

다. 암호시스템 : 평문을 암호문으로 또는 암호문을 평문으로 변환함수를 사용하는 시스템. 사용되는 특정 변환함수는 키에 의해서 선택된다. 이 변환함수는 일반적으로 수학적 함수에 의해 정의된다. (ITU-T X.509 또는 ISO/IEC 9594-8)

라. 해쉬 함수 :

① 대단히 많은 값들의 집합을 적은 값들의 집합으로 대응시키는 함수 (ITU-T X.811 또는 ISO/IEC 10181-2)

② 대단히 많은 값들의 집합을 적은 값들의 집합으로 대응시키는 함수로서 임의의 길이의 메시지를 일정한 길이로 압축시키는 것을 의미한다.

2) 본 표준 및 관련 후속표준에서 적용될 용어

가. 검증과정 : 서명된 메시지, 공개 검증키, 시스템 파라미터와 이와 관련 공개 데이터를 입력으로 취하고 그 서명 검증결과가 유효 또는 무효라는 것을 출력하는 과정

나. 공개 검증키 : 검증자가 알고 있거나 접근할 수 있는 서명자의 비공개 서명키에 관련되는 검증 과정에 사용되는 키.

다. 대칭 암호시스템 : 평문에서 암호문으로의 변환과 그 역변환에 동일하거나 유사한 키를 사용하는 암호시스템. 관용 암호시스템, 단일키 암호시스템, 비밀키 암호시스템등의 용어도 사용됨.

라. 메시지 : 임의의 길이로 구성된 비트열

마. 비대칭 암호시스템 : 평문에서 암호문으로의 변환과 그 역변환에 서로 다른 키를 사용하는 암호시스템. 암호의 난이도는 계산적 혹은 이론적 어려움에 근거함. 이중키 암호시스템, 공개키 암호시스템등의 용어도 사용됨.

바. 비공개 서명키 : 서명과정에 사용되는 서명자만이 알고 있는 키.

사. 서명과정 : 메시지, 비공개 서명키, 시스템 파라미터, 공개 또는 비공개 데이터를 함수의 입력으로 취하고 이함수의 출력으로 서명을 생성하는 과정

아. 서명된 메시지 : 메시지와 디지털 서명 정보가 연속적으로 붙은 형태의 비트열

자. 시스템 파라미터 : 시스템내의 모든 실체들이 알고 있거나 혹은 접근할 수 있는 값의 집합

차. 해쉬코드 : 해쉬함수의 출력 비트열

5. 기호와 표기

본 표준 및 관련 후속 표준에서 적용될 기호와 표기는 다음과 같다.

H : 해쉬코드(해쉬결과)
H′ : 구조화된 해쉬코드
I : 식별자
I′ : 구조화된 식별자
K : 난수 값
M : 메시지
M′ : 구조화된 메시지
Red : 용장 생성 함수
X : 비공개 서명키
Y : 공개 검증키
Z : 공개 시스템 파라미터
Σ : 서명
h : 해쉬함수
p, q : 소수
g : 원시원소 혹은 위수가 큰 원소

6. 일반사항

1) 디지털서명 과정

모든 공개키 암호시스템을 이용한 디지털서명 기법은 다음의 세가지 기본적인 과정으로 구성된다.

가. 키 생성과정 : 비공개 서명키와 해당 공개 검증키를 생성하는 과정.

나. 서명 생성과정 : 비공개 서명키와 이와 관련 공개 정보등을 이용하여 서명을 생성하는 과정.

다. 서명 검증과정 : 공개 검증키와 이와 관련 공개 정보 등을 이용하여 서명을 검증하는 과정.

2) 디지털서명의 종류

디지털서명은 공개키 암호시스템을 사용하여 직접서명을 생성하고 검증하는 직접서명 방식과 신뢰할 수 있는 중재자를 통해 서명을 생성하고 검증하는 형태의 중재자를 통한 서명방식등 두가지로 나눌수 있다. 직접서명은 복원형 디지털서명과 부가형 디지털서명으로 구분되며, 본 표준에서는 중재자를 통한 서명방식에 관하여는 규정하지 않는다. (그림 1 참조)

가. 복원형 디지털서명

서명의 검증과정에서 원래의 메시지가 복원되는 형태의 서명을 말한다. 용장 생성함수(redundancy generating function)를 이용하여 서명할 제한된 길이의 메시지를 일정한 규칙에 따라 변환시켜 서명을 생성하고, 복원된 메시지가 용장 생성함수의 규칙에 따라 생성된 것인지를 확인함으로써 서명을 검증한다. 이러한 형태의 서명은 ISO/IEC 9796에서 규정하고 있으므로 본 표준에서는 규정하지 않는다.

나. 부가형 디지털서명

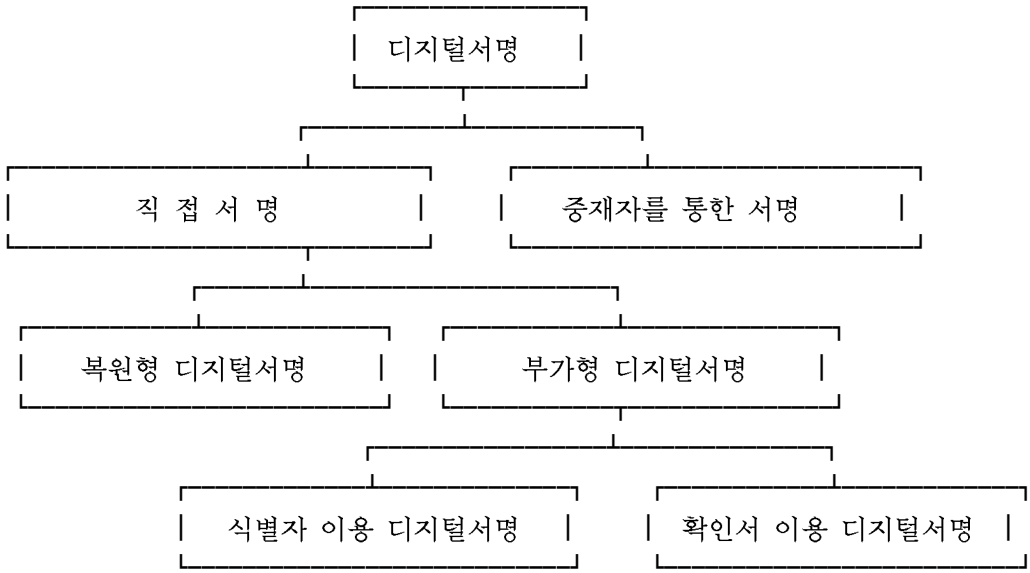
임의의 길이의 메시지에 서명부분을 부가하는 방식으로서 서명생성 및 검증 과정에서 메시지가 입력의 일부분이 되는 것을 부가형 디지털서명이라 하며, 이들 과정에서 동일한 해쉬함수를 사용한다. 부가형 디지털서명은 공개 검증키의 관리방법에 따라 식별자를 이용한 서명과 공개키 확인서를 이용한 서명으로 나눌 수 있으며, 이들은 7항과 8항에서 상세히 규정한다.

3) 디지털서명의 응용

디지털서명은 정보처리시스템 또는 정보통신망 환경하에서의 정보보호 서비스 구현에 필수적인 기술로 대부분의 암호 프로토콜 설계시 기본적인 도구가 되며, 대표적인 응용의 예는 다음과 같다.

가. 전송되는 정보의 불법변경 여부 판별을 위한 무결성 서비스, 사용자 인증 서비스 및 정보의 송수신을 부인할 수 없게 하는 부인봉쇄 서비스등.

나. 전자자금이체, 전자현금, 전자결재, 바이러스 검사 및 전자선거 시스템등의 응용 프로토콜.



(그림 1) 디지털서명의 분류방법

7. 요구사항

디지탈서명의 표준화 과정과 알고리즘은 공개적인 검토를 거쳐 안전성이 확보되어야 하며, 국제 표준과 연동성을 유지하여야 한다. 이를 위하여 다음 사항을 고려하여야 한다.

1) 기술적인 요구사항

디지털서명의 안전성을 확보하기 위하여 검증에 사용되는 공개키로부터 서명에 사용된 비공개키가 계산되는 것이 실행불가능해야 하며, 서명은 메시지 내용, 서명자 비공개키와 사용자 정보에 의존되어야 한다. 또한, 디지털서명 방식은 중요도에 따른 안전도와 안전한 키분배 방식이 별도로 제공되어야 한다.

디지털서명에 사용되는 비밀키와 공개키의 생성이 간단해야 하며, 서명과정과 검증과정에 필요한 계산이 효율적이어야 한다. 그리고 디지털서명이 유효하기 위해서는 다음의 요구조건들을 만족해야 한다.

가. 공개 검증키로 부터 비공개 서명키를 유도하는 것이 계산상 불가능하여야 하는 등의 안전성이 보장 되어야 한다. (안전성)

나. 공개정보나 이미 서명된 서명자의 다른 서명들로 부터 어떤 새로운 메시지에 대해서도 유효한 서명을 생성하는 것은 계산상 불가능해야 한다. (서명의 위조불가성)

다. 서명자 조차도 같은 서명에 대해 서로 다른 두 메시지를 찾아내는 것은 계산상 불가능해야 한다. (서명자의 부인불가성)

라. 누구나 공개정보로부터 해당서명이 그 서명자의 서명임을 검증할 수 있어야 한다. (분쟁해결 가능성)

2) 기타 고려사항

디지털서명이 증거능력을 보유할 수 있도록 법적 효력이 확보되어야 하며 키관리 제도가 확립되어야 한다. 또한, 디지털서명에 사용되는 표준화된 해쉬함수가 제공되어야 하며, 연산 속도 향상을 위한 안전 파라미터의 크기에 대한 권고가 있어야 한다.

그리고 해쉬함수는 임의의 길이의 메시지(비트열)를 일정한 길이로 압축시키는 함수로서 부가형 서명방식에서는 필수적으로 요구된다. 이러한 해쉬함수는 다음의 조건들을 만족시켜야 한다.

가. 어떤 해쉬결과가 주어졌을 때, 이 해쉬결과를 주는 해쉬함수의 입력 메시지를 찾는 것은 계산상 불가능해야 한다. (일방향성)

나. 주어진 입력 메시지에 대해 같은 해쉬결과를 주는 다른 입력 메시지를 찾는 것은 계산상 불가능해야 한다. (약한 충돌 회피성)

다. 같은 해쉬결과를 주는 임의의 서로 다른 두 입력 메시지를 찾는 것은 계산상 불가능해야 한다. (강한 충돌 회피성)