해쉬 알고리즘 기술규격

Hash Algorithm Specification

v1.20

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

해쉬 알고리즘 기술규격

Hash Algorithm Specification

1. 개 요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계 유·무선 공인인증서비스에서 사용되는 해쉬 알고리즘 규격을 정의한다.

2. 규격의 구성 및 범위

본 규격은 공인전자서명인증체계 유·무선 공인인증서비스에서 사용되는 해쉬 알고리즘을 나열하고 각각의 구현에 따른 요구사항을 정의한다.

첫 번째로 제6장에서는 해쉬 알고리즘(SHA-1)에 대한 구현 요구사항을 규정한다.

두 번째로 제7장에서는 해쉬 알고리즘(HAS-160)에 대한 구현 요구사항을 규정한다.

세 번째로 제8장에서는 해쉬 알고리즘(SHA-256)에 대한 구현 요구사항을 규정한다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

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

[SHA-2] NIST, FIPS PUB 180-3, National Institute of Standards and Technology, 2008

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

3.2 국내 표준 및 규격

[TTA-120011/R1] TTA, TTAS.KO-12.0011/R1, *해쉬함수표준-제2부 : 해쉬함수 알고리즘 표준(HAS-160),* 2000

3.3 기타

해당사항 없음

4. 정의

본 규격에서 사용하는 용어의 정의는 제4장에서 정한 것을 제외하고는 관련 법령 등이 정하는 바에 의한다.

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) 공인인증서
나) 공인인증기관
다) 가입자

4.2 용어의 정의

가) 유선 공인인증서비스 : 인터넷 기반의 전자거래를 위해 공인인증서를 이용하는 서비스
나) 무선 공인인증서비스 : 무선 단말기 기반의 전자거래를 위해 공인인증서를 이용하는 서비스

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 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

해당사항 없음

6. SHA-1 알고리즘

SHA-1은 임의의 길이의 메시지를 160비트의 축약된 메시지로 만들어내는 해쉬 알고리즘으로, 공인인증시스템 및 가입자설비는 [SHA-1]을 준용한 해쉬값 생성기능을 제공하여야 한다.

7. HAS-160 알고리즘

HAS-160은 임의의 길이의 메시지를 160비트의 축약된 메시지로 만들어내는 국내 해쉬 알고리즘이다. 유선 공인인증서비스를 제공하는 공인인증시스템은 [TTA-120011/R1]을 준용한 해쉬값 생성기능을 제공할 것을 권고한다. 유선 공인인증서비스를 제공하는 가입자설비는 [TTA-120011/R1]을 준용한 해쉬값 생성기능을 제공하여야 한다.

8. SHA-256 알고리즘

SHA-256은 임의의 길이의 메시지를 256비트의 축약된 메시지로 만들어내는 해쉬 알고리즘으로, 공인인증시스템 및 가입자설비는 [SHA-2]을 준용한 해쉬값 생성기능을 제공하여야 한다.

9. 해쉬 알고리즘의 안전성 확보

가입자 공인인증서는 공인인증체계의 전자서명키를 상향 조정하는 시점부터 해쉬 알고리즘은 256비트 (또는 224비트) 이상의 출력값을 가지는 해쉬 알고리즘을 사용하여야 한다. 단, HMAC, 난수생성, 세션키 등의 키를 유도하거나 전자서명법령, 고시 및 공인전자서명인증체계의 타 기술규격에서 명시한 경우에는 160비트 해쉬알고리즘을 이용할 수 있다.

공인인증체계의 전자서명키를 상향 조정하는 시점은 미래창조과학부가 별도로 고시하여 정한날로 한다.

부록 1. 규격 연혁

버전	제・개정일	제・개정내역
v1.00	2007년 4월	・“해쉬 알고리즘 기술규격”으로 제정
v1.10	2008년 10월	・관련 국내 표준 및 규격 갱신 내용 반영 ・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.20	2009년 9월	・공인인증서 암호체계 고도화에 따른 알고리즘 변경 사항 반영