TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.xxxx 제정일: 2018년 12월 xx일

# 해시 함수 기반 메시지 인증 코드 (HMAC) - 제1부: 일반

# The Keyed-Hash Message Authentication Code (HMAC) - Part1: General

TTA 한국정보통신기술협회
Telecommunications Technology Association

**표준초안 검토 위원회** 정보보호기반 프로젝트그룹(PG501)

**표준안 심의 위원회** 정보보호 기술위원회(TC5)

| | 성명 | 소 속 | 직위 | 위원회 및 직위 | 표준번호 |
|---|---|---|---|---|---|
| **표준(과제) 제안** | 박제홍 | NSR | 책임연구원 | 정보보호기반 프로젝트그룹 위원 | TTAK.KO-12.xxxx |
| **표준 초안 작성자** | 박제홍 | NSR | 책임연구원 | 정보보호기반 프로젝트그룹 위원 | TTAK.KO-12.xxxx |
| | 김우환 | NSR | 책임연구원 | - | TTAK.KO-12.xxxx |
| **사무국 담당** | 박수정 | TTA | 책임 | - | |

본 문서에 대한 저작권은 TTA에 있으며, TTA와 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.12

# 서 문

## 1 표준의 목적

이 표준의 목적은 암호학적 해시 함수(cryptographic hash function)를 기반 함수로 사용하는 메시지 인증 코드 알고리즘인 HMAC을 규정하는 것이다.

## 2 주요 내용 요약

이 표준은 암호학적 해시 함수를 기반으로 정의된 메시지 인증 코드 알고리즘 HMAC의 상세 규격을 제시하고, 안전성과 효율성 고려사항을 정리한다.

## 3 인용 표준과의 비교

### 3.1 인용 표준과의 관련성

이 표준은 NIST FIPS 198-1에 정의된 HMAC 규격을 준용한다.

### 3.2 인용 표준과 본 표준의 비교표

| TTAK.KO-12.xxxx-Part1 | NIST FIPS 198-1 (2008) | 비고 |
|---|---|---|
| 1. 적용 범위 | - | 추가 |
| 2. 인용 표준 | - | 추가 |
| 3. 용어 정의 | 2.1. Glossary of Terms | 동일(일부 선택) |
| 4. 약어 | 2.2. Acronyms | 동일(일부 선택) |
| - | 3. Cryptographic Keys | 제외(※일부 내용은 해당사항이 없으며, 나머지는 5절에 포함) |
| 5. HMAC 규격 | 4. HMAC Specification | 수정(※수정사항 간략히 기재 |
| - | 5. Truncation | 제외(※5절에 포함) |
| 6. 안전성과 효율성 고려사항 | 6. Implementation Note | 확대(※효율성 고려사항으로 포함) |

# Preface

## 1 Purpose

The standard describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions.

## 2 Summary

The standard defines the detailed specification of the HMAC, a message authentication code algorithm based on a cryptographic hash function, and provides several considerations for security and efficiency.

## 3 Relationship to Reference Standards

The standard conforms to the specification of the HMAC in NIST FIPS 198-1.

# 목 차

# 해시 함수 기반 메시지 인증 코드 (HMAC)
# - 제1부: 일반
# (The Keyed-Hash Message Authentication Code (HMAC)
# - Part1: General)

## 1 적용 범위

메시지 인증 코드(MAC, message authentication code)는 메시지에 대한 무결성(integrity)과 근원 인증(source authentication)을 보장하기 위해 사용하는 암호 알고리즘이다. 메시지 인증 코드는 기능적으로 구분 가능한 두 개의 파라미터로 메시지 입력과 암호 키를 사용하며, 이때 암호 키는 메시지의 생성자와 의도된 수신자 이외에는 비밀로 관리되어야 한다.

메시지 인증 코드는 메시지 입력과 암호 키로부터 고정된 길이의 인증 태그(authentication tag)를 생성하는 용도로 사용된다. 메시지 생성자는 의도된 수신자와 공유한 암호 키를 사용하여 송신하는 메시지에 대한 인증 태그를 생성하고, 메시지와 인증 태그를 함께 수신자에게 전송한다. 수신자는 송신자와 공유한 암호 키와 수신된 메시지를 같은 메시지 인증 코드 알고리즘에 입력하여 인증 태그를 계산하고, 이 값을 수신된 인증 태그와 비교한다. 두 값이 같을 경우, 수신 과정에서 메시지의 위변조가 발생하지 않았음과 동시에 송신자가 같은 암호 키를 공유한 사용자임이 보장된다.

이러한 일반적인 용도와 함께, 메시지 인증 코드는 의사 난수 함수(PRF, pseudo random function)의 역할로 키 유도(key derivation)나 난수 생성(random number generation), 키 싸기(key wrap) 등의 다양한 암호 알고리즘의 기반 함수로도 사용된다.

메시지 인증 코드는 블록 암호나 해시 함수를 기반으로 설계할 수 있으며, 이 표준에서는 암호학적 해시 함수를 기반으로 동작하는 메시지 인증 코드 알고리즘인 HMAC의 규격을 제시한다. 주요 표준 해시 함수를 HMAC의 기반 함수로 사용하여 생성한 참조 구현 값은 별도의 연계 표준으로 제시한다.

## 2 인용 표준

NIST FIPS PUB 198-1 (2008), The Keyed-Hash Message Authentication Code (HMAC)

# 3 용어 정의

## 3.1 메시지 인증 코드(MAC, Message Authentication Code)

임의 길이의 입력 메시지와 암호 키로부터 고정 길이의 인증 태그(authentication tag)를 생성하는 암호 알고리즘으로, 암호 키의 비밀성에 의존하여 메시지의 위변조 여부를 판단하는 데 사용

## 3.2 암호 키(cryptographic key)

암호 알고리즘과 함께 사용되는 파라미터로 해당 알고리즘의 특정 연산을 결정함. 이 표준에서 암호 키는 HMAC에서 입력 메시지에 대한 인증 태그를 생성하는 데 사용

## 3.3 해시 함수(hash function)

임의 길이의 메시지를 입력으로 받아 일정 길이의 출력값으로 압축하며, 다음 두 가지 성질을 가지는 암호 알고리즘

- 주어진 출력값에 대응하는 입력 메시지를 찾는 것이 어려움
- 주어진 입력 메시지에 대해, 같은 출력값을 가지는 다른 메시지를 찾는 것이 어려움

## 3.4 의사 난수 함수(PRF, pseudo random function)

주어진 정의역(domain)과 치역(range)에 대해 정의되는 모든 함수(function)의 집합에서 균등한 확률(uniform probability)에 따라 무작위로 선택된 함수(random function)와 구별이 어려우면서, 효율적으로 계산 가능한 함수

**[출처(3.1~3.3)]** NIST FIPS PUB 198-1

# 4 약어

| | |
|---|---|
| FIPS | Federal Information Processing Standard |
| FIPS PUB | FIPS Publication |
| HMAC | Keyed-Hash Message Authentication Code |
| NIST | National Institute of Standards and Technology |

# 5 HMAC 규격

## 5.1 주요 파라미터

HMAC의 절차를 설명하기에 앞서, 사용되는 주요 함수와 파라미터를 기술한다.

| | |
|---|---|
| B | 해시 함수의 입력 블록 길이(단위: 바이트) |
| H | 해시 함수 |
| ipad | Inner pad, 바이트 0x36을 B개 연접하여 구성 |
| K | 메시지 생성자와 수신자 사이에 공유한 암호 키 |
| L | 해시 함수의 출력 블록 길이(단위: 바이트) |
| len(x) | 입력 데이터 x의 바이트 길이를 반환하는 함수 |
| opad | Outer pad, 바이트 0x5c를 B번 연접하여 구성 |
| text | HMAC 연산이 적용되는 n 비트($n \in [0, 2^B - 8B)$) 크기의 데이터 |
| $(0x00)^s$ | 바이트 0x00을 s개 연접하여 구성한 바이트열 |

## 5.2 상세 규격

HMAC 알고리즘을 사용하여 입력 메시지 'text'에 대한 인증 태그를 계산하기 위해서는 다음의 연산을 수행한다.

$$HMAC(K, text) = H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text)).$$

여기에서 $K_0$는 암호 키 K의 바이트 크기에 따라 사전 계산을 통해 B 바이트가 되도록 유도된 값이다.

암호 키 K로부터 $K_0$를 유도하는 절차를 포함하여, 해시 함수 H를 기반 함수로 사용하여 동작하는 HMAC의 구체적인 동작 절차는 알고리즘 1과 같다.

## 5.3 절삭(truncation)

HMAC은 운용 환경의 안전성과 효율성을 고려하여 출력 T의 일부만 인증 태그로 사용하는 것을 허용한다. 이런 경우, HMAC의 출력 T에서 LSB를 기준으로 운용 환경에서 정의한 길이만큼 절삭한 결과를 사용해야 한다.

| 알고리즘 1 HMAC 함수: $T \leftarrow HMAC(K, text)$ | |
|---|---|
| 입력: 암호 키 K, 메시지 text<br>출력: L 바이트 인증값 T | |
| 1: **if** len(K) = B **then** | |
| 2: $K_0 \leftarrow K$; | |
| 3: **else if** len(K) > B **then** | |
| 4: $K_0 \leftarrow H(K) \| (0x00)^{B-L}$; | // $len(K_0) = B$ |
| 5: **else** | |
| 6: $K_0 \leftarrow K \| (0x00)^{B-len(K)}$; | // $len(K_0) = B$ |
| 7: **end if** | |
| 8: $K_1 \leftarrow K_0 \oplus ipad$; | |
| 9: $data_1 \leftarrow K_1 \| text$; | |
| 10: $h \leftarrow H(data_1)$; | // $H((K_0 \oplus ipad) \| text)$ |
| 11: $K_2 \leftarrow K_0 \oplus opad$; | |
| 12: $data_2 \leftarrow K_2 \| h$; | // $(K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text)$ |
| 13: $T \leftarrow H(data_2)$; | // $H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text))$ |

## 6 안전성과 효율성 고려사항

### 6.1 안전성 고려사항

메시지 인증 코드를 통해 메시지와 인증 태그를 수신한 사용자는 인증 태그를 생성한 사용자에 대한 인증이 가능하다. 그러나 메시지와 인증 태그를 제시하는 개체가 인증 태그를 생성한 개체와 다를 수 있다. 따라서 메시지 인증 코드는 유효한 메시지/인증 태그 쌍을 공격자가 가로채어 재전송하는 공격(replaying attack)에 대한 안전성은 보장하지 않는다.

### 6.2 효율성 고려사항

HMAC 계산 과정에서 $K_1$ ($=K_0 \oplus ipad$)과 $K_2$ ($=K_0 \oplus opad$)의 크기는 기반 해시 함수의 압축 함수 입력 단위와 같다. 따라서 HMAC에 암호 키 K가 입력으로 사용되는 시점에서 $K_1$과 $K_2$의 압축 함수를 계산하여 그 결과를 저장한 후, 암호 키를 변경하기 전까지 계속 사용하는 것이 가능하다. 이러한 방법은 HMAC 계산에 있어 두 개의 블록에 대한 기반 해시 함수의 압축 함수 계산을 줄일 수 있어, 짧은 메시지 단위로 빠르게 인증 태그를 생성하는 경우에 유용하다. 이러한 최적화 구현 시, $K_1$과 $K_2$의 압축 함수 계산 결과 저장 및 사용에 있어 암호 키 K와 같은 수준으로 보호되어야 한다.

# 부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 지식재산권 확약서 정보

해당 사항 없음

※ 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

# 부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 시험인증 관련 사항

## Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

## Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

# 부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 본 표준의 연계(family) 표준

## Ⅰ-3.1 TTAK.KO-12.0xxx-Part2

이 표준에서 제시하는 HMAC의 기반 해시 함수로 SHA-2[2]를 사용하는 경우의 참조 구현값을 제시함

## Ⅰ-3.2 TTAK.KO-12.0xxx-Part3

이 표준에서 제시하는 HMAC의 기반 해시 함수로 LSH[1]를 사용하는 경우의 참조 구현값을 제시함

# 부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 참고 문헌

[1] TTA TTAK.KO-12.0276, “해시 함수 LSH”.

[2] NIST FIPS PUB 180-4, “Secure Hash Standard (SHS)”, 2015. 8.

# 부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 영문표준 해설서

해당 사항 없음

# 부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 표준의 이력

| 판수 | 채택일 | 표준번호 | 내용 | 담당 위원회 |
|---|---|---|---|---|
| 제1판 | 2018.12.xx | 제정<br>TTAK.KO-12.xxxx-Part1 | - | 정보보호기반 PG<br>(PG501) |