Algorithm Identifiers for the
HMAC-based Extract-and-Expand Key Derivation Function (HKDF)

Abstract

RFC 5869 specifies the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) algorithm. This document assigns algorithm identifiers to the HKDF algorithm when used with three common one-way hash functions.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8619.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

The HKDF algorithm [RFC5869] is a key derivation function based on the Hashed Message Authentication Code (HMAC). This document assigns algorithm identifiers to the HKDF algorithm when used with three common one-way hash functions. These algorithm identifiers are needed to make use of the HKDF in some security protocols, such as the Cryptographic Message Syntax (CMS) [RFC5652].

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. ASN.1

In this specification, values are generated using ASN.1 [X.680] using the Basic Encoding Rules (BER) and the Distinguished Encoding Rules (DER) [X.690].

2. HKDF Algorithm Identifiers

This section assigns three algorithm identifiers to HKDF [RFC5869] used with three common one-way hash functions that are specified in [SHS]: SHA-256, SHA-384, and SHA-512. When any of these three object identifiers appear within the ASN.1 type AlgorithmIdentifier, the parameters component of that type SHALL be absent.

The specification of AlgorithmIdentifier is available in [RFC5911], which evolved from the original definition in X.509 [X.509-88].
The assigned object identifiers are:

```
id-alg-hkdf-with-sha256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 28 }

id-alg-hkdf-with-sha384 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 29 }

id-alg-hkdf-with-sha512 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 30 }
```

3. ASN.1 Module

This section contains the ASN.1 module for the HKDF algorithm identifiers. This module imports types from other ASN.1 modules that are defined in [RFC5912].

```
HKDF-OID-2019
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
    smime(16) modules(0) id-mod-hkdf-oid-2019(68) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

-- EXPORTS All

IMPORTS

AlgorithmIdentifier(), KEY-DERIVATION
    FROM AlgorithmInformation-2009 -- [RFC5912]
        { iso(1) identified-organization(3) dod(6) internet(1)
            security(5) mechanisms(5) pkix(7) id-mod(0)
            id-mod-algorithmInformation-02(58) } ;

--

-- Object Identifiers

--

id-alg-hkdf-with-sha256 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 28 }

id-alg-hkdf-with-sha384 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 29 }

id-alg-hkdf-with-sha512 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 30 }
```
-- Key Derivation Algorithm Identifiers

KeyDevAlgs KEY-DERIVATION ::= {
    kda-hkdf-with-sha256 |
    kda-hkdf-with-sha384 |
    kda-hkdf-with-sha512,
    ... }

kda-hkdf-with-sha256 KEY-DERIVATION ::= {
    IDENTIFIER id-alg-hkdf-with-sha256
    PARAMS ARE absent
    SMIME-CAPS { IDENTIFIED BY id-alg-hkdf-with-sha256 } }

kda-hkdf-with-sha384 KEY-DERIVATION ::= {
    IDENTIFIER id-alg-hkdf-with-sha384
    PARAMS ARE absent
    SMIME-CAPS { IDENTIFIED BY id-alg-hkdf-with-sha384 } }

kda-hkdf-with-sha512 KEY-DERIVATION ::= {
    IDENTIFIER id-alg-hkdf-with-sha512
    PARAMS ARE absent
    SMIME-CAPS { IDENTIFIED BY id-alg-hkdf-with-sha512 } }

END

4. Security Considerations

Despite the simplicity of HKDF, there are many security considerations that have been taken into account in the design and analysis of this construction. An exposition of all of these aspects is well beyond the scope of this document. Please refer to [EPRINT] for detailed information, including rationale for the HKDF design.

5. IANA Considerations

One object identifier for the ASN.1 module in Section 3 was assigned in the "SMI Security for S/MIME Module Identifiers (1.2.840.113549.1.9.16.0)" registry [IANA-MOD]:

id-mod-hkdf-oid-2019 OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-9(9) smime(16) mod(0) 68 }
Three object identifiers for the HKDF algorithm identifiers were assigned in the "SMI Security for S/MIME Algorithms (1.2.840.113549.1.9.16.3)" registry [IANA-ALG]:

id-alg-hkdf-with-sha256 OBJECT IDENTIFIER ::= 
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 28 }

id-alg-hkdf-with-sha384 OBJECT IDENTIFIER ::= 
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 29 }

id-alg-hkdf-with-sha512 OBJECT IDENTIFIER ::= 
    { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) alg(3) 30 }

6. References

6.1. Normative References


6.2. Informative References


Author’s Address

Russell Housley
Vigil Security, LLC
515 Dranesville Road
Herndon, VA 20170
United States of America

Email: housley@vigilsec.com