Internet Engineering Task Force (IETF)
Request for Comments: 8619
Category: Standards Track
ISSN: 2070-1721

R. Housley
Vigil Security

June 2019

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

Copyright Notice

Table of Contents

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

[SHS] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/info/rfc5652>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[X.680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2015, August 2015.

[X.690] ITU-T, "Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1:2015, August 2015.

6.2. Informative References

[EPRINT] Krawczyk, H., "Cryptographic Extraction and Key Derivation: The HKDF Scheme", Proceedings of CRYPTO 2010, August 2010, <https://eprint.iacr.org/2010/264.pdf>.

[IANA-ALG] IANA, "SMI Security for S/MIME Algorithms (1.2.840.113549.1.9.16.3)", <https://www.iana.org/assignments/smi-numbers/>.

[IANA-MOD] IANA, "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)", <https://www.iana.org/assignments/smi-numbers/>.

[RFC5911] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, DOI 10.17487/RFC5911, June 2010, <https://www.rfc-editor.org/info/rfc5911>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/info/rfc5912>.

[X.509-88] CCITT, "Recommendation X.509: The Directory - Authentication Framework", 1988.

Author’s Address

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

Email: housley@vigilsec.com