Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 16, 2017

W. Conner
A. Langley
R. Sleevi
Google
A. Popov
Microsoft

June 14, 2017

BLAKE2 Algorithms and Identifiers for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

draft-wconner-blake2sigs-01

Abstract

This document describes the conventions for using the BLAKE2b-512 hash function with each of the following algorithms: RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP), RSA Probabilistic Signature Scheme (RSASSA-PSS), RSA Public-Key Cryptography Standards #1 version 1.5 (RSASSA PKCS#1 v1.5), Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), and Edwards-curve Digital Signature Algorithm (EdDSA). This specification applies to the Internet X.509 Public Key Infrastructure (PKI) when digital signatures are used to sign certificates and certificate revocation lists (CRLs). This document also specifies the object identifiers for the combinations of the BLAKE2b-512 hash function with the aforementioned algorithms.

Status of This Memo

This Internet-Draft will expire on December 16, 2017.

Copyright Notice

Table of Contents

1. Introduction

The SHA-2 family of hash functions is currently the only secure and widely supported option for digital signatures in the PKIX ecosystem [FIPS-180-4]. While there is no reason to be seriously concerned about the security of SHA-2, which is still acceptable according to NIST SP 800-131A rev. 1 [SP-800-131A], numerous previous hash functions have eventually suffered from collision attacks and needed to be replaced. Since it takes a very long time to establish support for new primitives in the PKIX ecosystem, it seems prudent to have an alternative prepared.

This document specifies object identifiers to identify the combination of the BLAKE2b-512 [BLAKE2] hash function with each of RSAES-OAEP, RSASSA-PSS, RSASSA PKCS#1 v1.5, DSA, ECDSA, and EdDSA.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Algorithm Support

This section describes the algorithms and corresponding object identifiers, which may be used in conjunction with the BLAKE2b-512 hash function.

2.1. BLAKE2b-512 One-Way Hash Function

[BLAKE2] specifies the BLAKE2 family of hash functions, including the BLAKE2b-512 hash function. The BLAKE2b-512 hash function is optimized for 64-bit platforms and produces 64-byte message digests. The object identifier for the BLAKE2b-512 hash algorithm is specified in [RFC7693] and included below for reference.

```
id-blake2b512 OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    private(4) enterprise(1) kudelski(1722) cryptography(12)
    hashAlgs(2) blake2b(1) 16
}
```

The object identifiers for the encryption and signature algorithms that use the BLAKE2b-512 hash function will appear under the following arcs derived from [RFC7693].

```
encAlgs OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    private(4) enterprise(1) kudelski(1722) cryptography(12) 4
}
```

```
sigAlgs OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    private(4) enterprise(1) kudelski(1722) cryptography(12) 5
}
```

2.2. BLAKE2b-512 Mask Generation Function

[RFC4055] specifies the object identifier for the mask generation function MGF1, which is included below for reference.

```
                id-mgf1 OBJECT IDENTIFIER ::= {
                    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
                    pkcs-1(1) 8
                }
```

The algorithm identifiers for the BLAKE2b-512 hash function and the mask generation function MGF1 that uses the BLAKE2b-512 hash function are the following.

```
                  blake2b512Identifier AlgorithmIdentifier ::= {
                      id-blake2b512, NULL
                  }
```

```
                  mgf1Blake2b512Identifier AlgorithmIdentifier ::= {
                      id-mgf1, blake2b512Identifier
                  }
```

2.3. RSAES-OAEP with BLAKE2b-512

[RFC4055] specifies the RSAES-OAEP algorithm and parameters. The sequence for the parameters is included below for reference.

```
                  RSAES-OAEP-params ::= SEQUENCE {
                      hashFunc    [0] AlgorithmIdentifier
                                      DEFAULT sha1Identifier,
                      maskGenFunc [1] AlgorithmIdentifier
                                      DEFAULT mgf1SHA1Identifier,
                      pSourceFunc [2] AlgorithmIdentifier
                                      DEFAULT pSpecifiedEmptyIdentifier
                  }
```

This section specifies a single object identifier to identify the combination of RSAES-OAEP with BLAKE2b-512.

```
               id-RSAEP-OAEP-with-blake2b512 OBJECT IDENTIFIER ::= { engAlgs
1 }
```

Using id-RSAEP-OAEP-with-blake2b512 requires the following RSAES-OAEP parameters.

```
                  RSAES-OAEP-blake2b512-params RSAES-OAEP-params ::=  {
                      hashFunc blake2b512Identifier,
                      maskGenFunc mgf1Blake2b512Identifier,
                      pSourceFunc pSpecifiedEmptyIdentifier
                  }
```

2.4. RSASSA-PSS with BLAKE2b-512

[RFC4055] specifies the RSASSA-PSS algorithm and parameters. The sequence for the parameters is included below for reference.

```
                  RSASSA-PSS-params ::= SEQUENCE {
                      hashAlgorithm    [0] HashAlgorithm
                                           DEFAULT sha1Identifier,
                      maskGenAlgorithm [1] MaskGenAlgorithm
                                           DEFAULT mgf1SHA1Identifier,
                      saltLength       [2] INTEGER DEFAULT 20,
                      trailerField     [3] INTEGER DEFAULT 1
                  }
```

This section specifies a single object identifier to identify the combination of RSASSA-PSS with BLAKE2b-512.

```
               id-RSASSA-PSS-with-blake2b512 OBJECT IDENTIFIER ::= { sigAlgs
1 }
```

Using id-RSASSA-PSS-with-blake2b512 requires the following RSASSA-PSS parameters.

```
                  RSASSA-PSS-blake2b512-params RSASSA-PSS-params ::=  {
                      hashAlgorithm blake2b512Identifier,
                      maskGenAlgorithm mgf1Blake2b512Identifier,
                      saltLength 20,
                      trailerField 1
                  }
```

2.5. RSASSA PKCS#1 v1.5 with BLAKE2b-512

[RFC2313] specifies the RSASSA PKCS #1 v1.5 signature algorithm. This section specifies a single object identifier to identify the combination of RSASSA PKCS#1 v1.5 with BLAKE2b-512.

```
                  id-rsassa-pkcs1-v1_5-with-blake2b512 OBJECT IDENTIFIER
                                                     ::= { sigAlgs 2 }
```

2.6. DSA with BLAKE2b-512

NIST FIPS PUB 186-4 [FIPS-186-4] specifies the DSA signature algorithm. This section specifies a single object identifier to identify the combination of DSA with BLAKE2b-512.

```
               id-dsa-with-blake2b512 OBJECT IDENTIFIER ::= { sigAlgs 3 }
```

2.7. ECDSA with BLAKE2b-512

NIST FIPS PUB 186-4 [FIPS-186-4] specifies the ECDSA signature algorithm. [RFC5758] specifies identifiers for using the SHA-2 family of hash functions with ECDSA. This section specifies a single object identifier to identify the combination of ECDSA with BLAKE2b-512.

```
               id-ecdsa-with-blake2b512 OBJECT IDENTIFIER ::= { sigAlgs 4 }
```

2.8. EdDSA with BLAKE2b-512

[RFC8032] specifies the EdDSA algorithm. This section specifies a single object identifier to identify the combination of EdDSA with the edwards448 curve and BLAKE2b-512 hash function.

```
               id-Ed448-with-blake2b512 OBJECT IDENTIFIER ::= { sigAlgs 5 }
```

3. Security Considerations

For BLAKE2-specific security considerations, Section 4 of [BLAKE2] includes a brief security analysis of the BLAKE2 hash algorithm. The BLAKE hash algorithm, which was the predecessor of BLAKE2, was analyzed as part of the SHA-3 competition [BLAKE]. The BLAKE2 hash algorithm builds on BLAKE with some tweaks.

For general PKIX Certificate and CRL Profile security considerations, Section 8 of [RFC5280] provides a good overview.

4. IANA Considerations

Although the algorithm identifiers are currently specified under the object identifier arc specified in [RFC7693], the authors would not oppose the assignment of these algorithms to object identifiers in a more suitable location under the IANA object identifier space in future drafts.

5. Acknowledgements

The authors would like to thank the [BLAKE2] designers for answering our questions about BLAKE2 and allowing us to use their object identifier space. In particular, our email exchanges with Jean-Philippe Aumasson were very helpful.

The authors would also like to thank the participants of the LAMPS working group who provided valuable feedback.

6. Normative References

[BLAKE] Aumasson, J., Henzen, L., Meier, W., and R. Phan, "SHA-3 proposal BLAKE", December 2010, <https://131002.net/blake/blake.pdf>.

[BLAKE2] Aumasson, J., Neves, S., Wilcox-O'Hearn, Z., and C. Winnerlein, "BLAKE2: simpler, smaller, fast as MD5", January 2013, <https://blake2.net/blake2_20130129.pdf>.

[FIPS-180-4]
National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, August 2015, <https://dx.doi.org/10.6028/NIST.FIPS.180-4.pdf>.

[FIPS-186-4]
National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-4, July 2013, <https://dx.doi.org/10.6028/NIST.FIPS.186-4>.

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

[RFC2313] Kaliski, B., "PKCS #1: RSA Encryption Version 1.5", RFC 2313, DOI 10.17487/RFC2313, March 1998, <http://www.rfc-editor.org/info/rfc2313>.

[RFC4055] Schaad, J., Kaliski, B., and R. Housley, "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 4055, DOI 10.17487/RFC4055, June 2005, <http://www.rfc-editor.org/info/rfc4055>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC5758] Dang, Q., Santesson, S., Moriarty, K., Brown, D., and T. Polk, "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA", RFC 5758, DOI 10.17487/RFC5758, January 2010, <http://www.rfc-editor.org/info/rfc5758>.

[RFC7693] Saarinen, M-J., Ed. and J-P. Aumasson, "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)", RFC 7693, DOI 10.17487/RFC7693, November 2015, <http://www.rfc-editor.org/info/rfc7693>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <http://www.rfc-editor.org/info/rfc8032>.

[SP-800-131A] Barker, E. and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A Rev. 1, November 2015, <http://dx.doi.org/10.6028/NIST.SP.800-131Ar1>.

Authors' Addresses

William Conner
Google
320 N Morgan St #600
Chicago, IL 60607
USA

Email: wconner@google.com

Adam Langley
Google
340 Main St
Venice, CA 90291
USA

Email: agl@google.com

Ryan Sleevi
Google
200 W Franklin St #300
Chapel Hill, NC 27516
USA

Email: sleevi@google.com

Andrei Popov
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

Email: Andrei.Popov@microsoft.com