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

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

April 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-00

Abstract

This document describes the conventions for using the BLAKE2b-512 hash function with each of the following signature algorithms: RSA Public-Key Cryptography Standards #1 version 1.5 (RSA PKCS#1 v1.5), RSA Probabilistic Signature Scheme (RSASSA-PSS), RSA Encryption Scheme - Optimal Asymmetric Encryption Padding (RSAES-OAEP), 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 (OIDs) for the combinations of the BLAKE2b-512 hash function with the aforementioned signature algorithms.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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. 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 (OIDs) to identify the combination of BLAKE2b-512 [BLAKE2] with each of RSA PKCS#1 v1.5,

RSASSA-PSS, RSAES-OAEP, 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 signature algorithms and corresponding OIDs, which may be used in conjunction with the BLAKE2b-512 hash function. The OIDs will be assigned under the following OID arc, which is based on the OID tree from [RFC7693].

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

2.1. RSA PKCS#1 v1.5

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

```
id-rsaEncryption-with-blake2b512 OBJECT IDENTIFIER ::= TBD
```

2.2. RSASSA-PSS

[RFC4055] specifies the RSASSA-PSS signature algorithm. This section specifies a single OID to identify the combination of BLAKE2b-512 with RSASSA-PSS.

```
id-RSASSA-PSS-with-blake2b512 OBJECT IDENTIFIER ::= TBD
```

2.3. RSAES-OAEP

[RFC4055] specifies the RSAES-OAEP signature algorithm. This section specifies a single OID to identify the combination of BLAKE2b-512 with RSAES-OAEP.

```
id-RSAEP-OAEP-with-blake2b512 OBJECT IDENTIFIER ::= TBD
```


2.4. ECDSA

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

```
id-ecdsa-with-blake2b512 OBJECT IDENTIFIER ::= TBD
```

2.5. EdDSA

[RFC8032] specifies the EdDSA signature algorithm. This section specifies two OIDs to identify the combination of BLAKE2b-512 with the edwards25519 and edwards448 curves.

```
id-Ed25519-with-blake2b512 OBJECT IDENTIFIER ::= TBD

id-Ed448-with-blake2b512 OBJECT IDENTIFIER ::= TBD
```

3. IANA Considerations

None

4. 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.

5. Normative References

[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-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>.

[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