

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

S. Turner
sn3rd
March 13, 2017

SHA-3 Related Algorithms and Identifiers for PKIX
draft-turner-lamps-adding-sha3-to-pkix-01

Abstract

This document describes the conventions for using the SHA-3 family of hash functions in the Internet X.509 PKI as one-way hash functions and with the ECDSA signature algorithm; the conventions for the associated ECDSA subject public keys are also described. Digital signatures are used to sign certificates and CRLs (Certificate Revocation Lists).

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 September 14, 2017.

Copyright Notice

Copyright (c) 2017 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 (<http://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.

Table of Contents

1.	Introduction	2
2.	Algorithm Support	2
2.1.	SHA-3 One-way Hash Functions	3
2.2.	ECDSA Signature Algorithm with SHA-3	3
2.3.	ECDSA Public Keys	4
3.	Security Considerations	4
4.	IANA Considerations	5
5.	References	5
5.1.	Normative References	5
5.2.	Informative References	6
Appendix A.	2015 ASN.1 Module	6
Appendix B.	1988 ASN.1 Module	9
	Author's Address	11

[1.](#) Introduction

[[RFC3279](#)], [[RFC4055](#)], [[RFC5480](#)], and [[I-D.ietf-curdle-pkix](#)] defines the contents of the signatureAlgorithm, signatureValue, signature, and subjectPublicKeyInfo fields within Internet X.509 certificates and CRLs (Certificate Revocation Lists) [[RFC5280](#)] for a number of algorithms. This document does the same for the SHA-3 family of one-way hash functions and their use with the ECDSA and RSA PKCS#1 v1.5 digital signature algorithms.

Familiarity with [[RFC5280](#)] is assumed.

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 [[RFC2119](#)].

[2.](#) Algorithm Support

This section describes cryptographic algorithms which may be used with the Internet X.509 Certificate and CRL profile [[RFC5280](#)]. This section describes one-way hash functions and digital signature algorithms which may be used to sign certificates and CRLs, and identifies OIDs (Object Identifiers) for public keys contained in a

certificate.

[2.1.](#) SHA-3 One-way Hash Functions

The SHA-3 family of one-way hash functions is specified in [[SHA3](#)]. In the SHA-3 family, four hash functions are defined: SHA3-224, SHA3-256, SHA3-384, and SHA3-512; two extendable-output functions, called SHAKE128 and SHAKE256, are also defined but are not addressed by this document. The respective output lengths, in bits, of the SHA-3 hash functions are 224, 256, 384, and 512 and as of this document's publication date correspond to 112, 128, 192, and 256 bits of security [[RFC3766](#)]. The OIDs (Object Identifiers) for these four hash functions are as follows:

```
id-sha3-224 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 7  
}
```

```
id-sha3-256 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 8  
}
```

```
id-sha3-384 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 9  
}
```

```
id-sha3-512 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 10  
}
```

When using the id-sha3-224, id-sha3-s256, id-sha3-384, or id-sha3-512 algorithm identifiers, the parameters field MUST be absent; not NULL but absent.

[2.2.](#) ECDSA Signature Algorithm with SHA-3

The ECDSA (Elliptic Curve Digital Signature Algorithm) is defined in [\[DSS\]](#). When ECDSA is used in conjunction with one of the SHA-3 one-way hash functions the OID is, respectively:

Turner

Expires September 14, 2017

[Page 3]

Internet-Draft

SHA-3 for PKIX

March 2017

```
id-ecdsa-with-sha3-224 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 9
}

id-ecdsa-with-sha3-256 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 10
}

id-ecdsa-with-sha3-384 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 11
}

id-ecdsa-with-sha3-512 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 12
}
```

When these algorithm identifiers appear as the algorithm field in an AlgorithmIdentifier, the encoding MUST omit the parameters field. That is, the AlgorithmIdentifier SHALL be a SEQUENCE of one component: the OBJECT IDENTIFIER id-ecdsa-with-sha3-224, id-ecdsa-with-sha3-256, id-ecdsa-with-sha3-384, or id-ecdsa-with-sha3-512.

The ECPParameters in the subjectPublicKeyInfo field of the issuer's certificate SHALL apply to the verification of the signature.

When signing, the ECDSA algorithm generates two values. These values are commonly referred to as *r* and *s*. To easily transfer these two values as one signature, they MUST be ASN.1 encoded using the ECDSA-Sig-Value defined in [[RFC3279](#)] but repeated here for convenience:

```
ECDSA-Sig-Value ::= SEQUENCE {  
    r  INTEGER,  
    s  INTEGER }
```

[2.3.](#) ECDSA Public Keys

The conventions for ECDSA public keys is as specified in [[RFC5480](#)].

[3.](#) Security Considerations

TBD

Turner

Expires September 14, 2017

[Page 4]

Internet-Draft

SHA-3 for PKIX

March 2017

[4.](#) IANA Considerations

IANA is kindly requested to register two OIDs in the SMI Security for PKIX Module Identifier registry for the ASN.1 modules found in [Appendix A.1](#) and A.2. The description is as follows:

- o id-mod-pkix1-sha3-2015

- o id-mod-pkix1-sha3-1988

where the four digits at the end represent the ASN.1's publication date.

[5.](#) References

[5.1.](#) Normative References

[DSS] National Institute of Standards and Technology, U.S. Department of Commerce, "Digital Signature Standard, version 4", NIST FIPS PUB 186-4, 2013.

[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>>.

- [RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", [RFC 3279](#), DOI 10.17487/RFC3279, April 2002, <<http://www.rfc-editor.org/info/rfc3279>>.
- [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>>.
- [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", [RFC 5480](#), DOI 10.17487/RFC5480, March 2009, <<http://www.rfc-editor.org/info/rfc5480>>.
- [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, <<http://www.rfc-editor.org/info/rfc5912>>.

Turner

Expires September 14, 2017

[Page 5]

Internet-Draft

SHA-3 for PKIX

March 2017

- [SHA3] National Institute of Standards and Technology, U.S. Department of Commerce, "SHA-3 Standard - Permutation-Based Hash and Extendable-Output Functions", NIST FIPS PUB 202, August 2015.

[5.2.](#) Informative References

- [I-D.ietf-curdle-pkix]
Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed25519ph, Ed448, Ed448ph, X25519 and X448 for use in the Internet X.509 Public Key Infrastructure", [draft-ietf-curdle-pkix-03](#) (work in progress), November 2016.
- [RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For

Public Keys Used For Exchanging Symmetric Keys", [BCP 86](#),
[RFC 3766](#), DOI 10.17487/RFC3766, April 2004,
<<http://www.rfc-editor.org/info/rfc3766>>.

[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>>.

[Appendix A](#). 2015 ASN.1 Module

```
PKIXAlgsForSHA3-2015 { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkix1-sha3-2015(TBD) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL;

IMPORTS

PUBLIC-KEY, SIGNATURE-ALGORITHM, DIGEST-ALGORITHM, SMIME-CAPS
FROM AlgorithmInformation-2009 -- in [RFC5912]
{ iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0)
    id-mod-algorithmInformation-02(58) }

pk-ec, id-ecPublicKey, ECPublicKey, ECDSA-Sig-Value
FROM PKIXAlgs-2009 -- in [RFC5912]
```

```
{ iso(1) identified-organization(3) dod(6) internet(1) security(5)
    mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkix1-algorithms2008-02(56) }

;

--
-- Message Digest Algorithms (mda-)
```

--

```
HashAlgs DIGEST-ALGORITHM ::= {  
    ...,  
    -- This expands HashAlgs from [RFC5912]  
    mda-sha3-256 |  
    mda-sha3-384 |  
    mda-sha3-512  
}  
  
-- SHA3-256  
  
mda-sha3-256 DIGEST-ALGORITHM ::= {  
    IDENTIFIER id-sha3-256  
    PARAMS ARE absent  
}  
  
id-sha3-256 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 8  
}  
  
-- SHA3-384  
  
mda-sha3-384 DIGEST-ALGORITHM ::= {  
    IDENTIFIER id-sha3-384  
    PARAMS ARE absent  
}  
  
id-sha3-384 OBJECT IDENTIFIER ::= {  
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)  
    csor(3) nistAlgorithm(4) hashAlgs(2) 9  
}  
  
-- SHA3-512  
  
mda-sha3-512 DIGEST-ALGORITHM ::= {  
    IDENTIFIER id-sha3-512  
    PARAMS ARE absent  
}
```

```
id-sha3-512 OBJECT IDENTIFIER ::= {
```



```

    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) hashAlgs(2) 10
}

--
-- Public Key (pk-) Algorithms
--

-- See [RFC5912].

--
-- Signature Algorithms (sa-)
--

SignatureAlgs SIGNATURE-ALGORITHM ::= {
    ...,
    -- This expands SignatureAlgorithms from [RFC5912]
    sa-ecdsaWithSHA3-256 |
    sa-ecdsaWithSHA3-384 |
    sa-ecdsaWithSHA3-512
}

-- ECDSA with SHA3-256

sa-ecdsaWithSHA3-256 SIGNATURE-ALGORITHM ::= {
    IDENTIFIER id-ecdsa-with-SHA3-256
    VALUE ECDSA-Sig-Value
    PARAMS TYPE NULL ARE absent
    HASHES { mda-sha3-256 }
    PUBLIC-KEYS { pk-ec }
    SMIME-CAPS { IDENTIFIED BY id-ecdsa-with-SHA3-256 }
}

id-ecdsa-with-sha3-256 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 10
}

-- ECDSA with SHA3-384

sa-ecdsaWithSHA3-384 SIGNATURE-ALGORITHM ::= {
    IDENTIFIER id-ecdsa-with-SHA3-384
    VALUE ECDSA-Sig-Value
    PARAMS TYPE NULL ARE absent
    HASHES { mda-sha3-384 }
    PUBLIC-KEYS { pk-ec }
    SMIME-CAPS { IDENTIFIED BY id-ecdsa-with-SHA3-384 }
}

```

```
    }

id-ecdsa-with-sha3-384 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 11
}

-- ECDSA with SHA3-512

sa-ecdsaWithSHA3-512 SIGNATURE-ALGORITHM ::= {
    IDENTIFIER id-ecdsa-with-SHA3-512
    VALUE ECDSA-Sig-Value
    PARAMS TYPE NULL ARE absent
    HASHES { mda-sha3-512 }
    PUBLIC-KEYS { pk-ec }
    SMIME-CAPS { IDENTIFIED BY id-ecdsa-with-SHA3-512 }
}

id-ecdsa-with-sha3-512 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) sigAlgs(3) 12
}

--
-- SMIME Capabilities (sa-)
--

SMimeCaps SMIME-CAPS ::= {
    ...,
    -- The expands SMimeCaps from \[RFC5912\]
    sa-ecdsaWithSHA3-256.&smimeCaps |
    sa-ecdsaWithSHA3-384.&smimeCaps |
    sa-ecdsaWithSHA3-512.&smimeCaps
}

END
```

[Appendix B.](#) 1988 ASN.1 Module

```
PKIXAlgsForSHA3-1988 { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkix1-sha3-1988(TBD) }

DEFINITIONS EXPLICIT TAGS ::=
```

BEGIN

Turner

Expires September 14, 2017

[Page 9]

Internet-Draft

SHA-3 for PKIX

March 2017

```
-- EXPORTS ALL;

-- IMPORTS NONE;

--
-- Message Digest Algorithms
--

-- SHA3-256
-- Parameters are absent

id-sha3-256 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) hashAlgs(2) 8
}

-- SHA3-384
-- Parameters are absent

id-sha3-384 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) hashAlgs(2) 9
}

-- SHA3-512
-- Parameters are absent

id-sha3-512 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
    csor(3) nistAlgorithm(4) hashAlgs(2) 10
}

--
-- ECDSA Keys, Signatures, and Curves
--

-- OID for ECDSA signatures with SHA3-256

id-ecdsa-with-sha3-256 OBJECT IDENTIFIER ::= {
```

```
joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
csor(3) nistAlgorithm(4) sigAlgs(3) 10
}
```

-- OID for ECDSA signatures with SHA3-384

```
id-ecdsa-with-sha3-384 OBJECT IDENTIFIER ::= {
  joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
  csor(3) nistAlgorithm(4) sigAlgs(3) 11
}
```

Turner

Expires September 14, 2017

[Page 10]

Internet-Draft

SHA-3 for PKIX

March 2017

```
}
```

-- OID for ECDSA signatures with SHA3-512

```
id-ecdsa-with-sha3-512 OBJECT IDENTIFIER ::= {
  joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
  csor(3) nistAlgorithm(4) sigAlgs(3) 12
}
```

-- See [[RFC5480](#)] for ECDSA-Sig-Value, which is the format for
-- the value of an ECDSA signature value.

-- See [[RFC5480](#)] for ECDSA Keys and Curves.

END

Author's Address

Sean Turner
sn3rd

Email: sean@sn3rd.com

Turner

Expires September 14, 2017

[Page 11]