                   Put Your Internet Draft Title Here
                     draft-ietf-lamps-pkix-shake-00

Abstract

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

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of [BCP 78](BCP 78) and [BCP 79](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 https://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 May 3, 2018.

Copyright Notice

Table of Contents

1. Change Log

   o draft-kampanakis-adding-shake-to-pkix-00:

      * Initial version

2. Introduction

   EDNOTE: More here.

3. Algorithm support

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

3.1. SHAKE One-Way Hash Functions

The SHA-3 family of one-way hash functions is specified in [SHA3].
In the SHA-3 family, two extendable-output functions, called SHAKE128
and SHAKE256 are defined. Four hash functions, SHA3-224, SHA3-256,
SHA3-384, and SHA3-512 are also defined but are out of scope for this

document. The output lengths, in bits, of the SHAKE hash functions
is defined by the parameter d. The corresponding collision and
preimage resistance security levels for SHAKE128 and SHAKE256 are
respectively min(d/2,128) and min(d,128) and min(d/2,256) and
min(d,256). The OIDs (Object Identifiers) for these two hash
functions are as follows:

```
id-shake128 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
                            country(16) us(840) organization(1) gov(101) cs
                            nistalgorithm(4) hashalgs(2) 11 }
```

```
id-shake256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
                        country(16) us(840) organization(1) gov(101) csor(3)
                        nistalgorithm(4) hashalgs(2) 12 }
```

The output length, d, is always 256 and 512 bits for SHAKE128 and
SHAKE256 respectively in this specification.

3.2. Signature Algorithms

3.2.1. RSA with SHAKE

EDNOTE: To be discussed by the WG about what RSA standard with SHAKE
is to be covered by this draft.

```
shake128WithRSAEncryption  OBJECT IDENTIFIER  ::=  { }
```

```
shake256withRSAEncryption OBJECT IDENTIFIER ::= { }
```

3.2.2. DSA with SHAKE

The DSA algorithm is defined in the Digital Signature Standard (DSS)
[FIPS186-4]. When SHAKE128 is used with DSA, the OID is:

```
  id-dsa-with-shake128 OBJECT IDENTIFIER  ::=  { joint-iso-ccitt(2)
                   country(16) us(840) organization(1) gov(101) csor(3)
                   algorithms(4) id-dsa-with-shake(3) x }
```

When SHAKE256 is used with DSA, the OID is:

```
id-dsa-with-shake256 OBJECT IDENTIFIER  ::=  { joint-iso-ccitt(2)
                   country(16) us(840) organization(1) gov(101) csor(3) algorith
                   id-dsa-with-shake(3) y }
```

EDNOTE: "x" and "y" will be specified by NIST later.

When the id-dsa-with-shake128 or id-dsa-with-shake256 algorithm
identifier appears in the algorithm field as an AlgorithmIdentifier,
the encoding SHALL omit the parameters field. That is, the
AlgorithmIdentifier SHALL be a SEQUENCE of one component, the OID id-
dsa-with-shake128 or id-dsa-with-shake256.

Encoding rules for DSA signature values are specified in [RFC3279].

Conforming CA implementations that generate DSA signatures for
certificates or CRLs MUST generate such DSA signatures in accordance
with all the requirements in Section 4 in [FIPS186-4]. The lengths
of p and q must be at least 2048 and 224 bits respectively.

3.2.3. ECDSA with SHAKE

The Elliptic Curve Digital Signature Algorithm (ECDSA) is defined in
"Public Key Cryptography for the Financial Services Industry: The
Elliptic Curve Digital Signature Standard (ECDSA)" [X9.62]. The
ASN.1 OIDs of ECDSA signature algorithms using SHAKE128 and SHAKE256,
are below:

```
id-ecdsa-with-shake128 OBJECT IDENTIFIER  ::=  { joint-iso-ccitt(2)
                       country(16) us(840) organization(1) gov(101) csor(3) al
                       id-ecdsa-with-shake(3) x }



id-ecdsa-with-shake256 OBJECT IDENTIFIER  ::=  { joint-iso-ccitt(2)
                       country(16) us(840) organization(1) gov(101) csor(3) al
                       id-ecdsa-with-shake(3) y }
```

   EDNOTE: "x" and "y" will be specified by NIST later.

   When the id-ecdsa-with-SHAKE128 or id-ecdsa-with-SHAKE256, algorithm
   identifier appears in the algorithm field as an AlgorithmIdentifier,
   the encoding MUST omit the parameters field. That is, the
   AlgorithmIdentifier SHALL be a SEQUENCE of one component, the OID
   ecdsa-with-SHAKE128 or ecdsa-with-SHAKE256.

   Conforming CA implementations MUST specify the hash algorithm
   explicitly using the OIDs specified above when encoding ECDSA/SHAKE
   signatures in certificates and CRLs.

   Conforming client implementations that process ECDSA signatures with
   any of the SHAKE hash algorithms when processing certificates and
   CRLs MUST recognize the corresponding OIDs specified above.

   Encoding rules for ECDSA signature values are specified in [RFC3279],
   Section 2.2.3, and [RFC5480].

   Conforming CA implementations that generate ECDSA signatures in
   certificates or CRLs MUST generate such ECDSA signatures in
   accordance with all the requirements specified in Sections 7.2 and
   7.3 of [X9.62] or with all the requirements specified in
   Section 4.1.3 of [SEC1]. They MAY also generate such ECDSA
   signatures in accordance with all the recommendations in [X9.62] or
   [SEC1] if they have a stated policy that requires conformance to
   these standards. These standards above may have not specified
   SHAKE128 and SHAKE256 as hash algorithm options. However, SHAKE128
   and SHAKE256 with output length being 256 and 512 bits respectively
   are subtitions for 256 and 512-bit output hash algorithms such as

SHA256 and SHA512 used in the standards.

EDNOTE: Depending on the updates to the Charter, the group may want
to consider an EdDSA with SHAKE section here.

3.3. Public Keys

The conventions for RSA, DSA and ECDSA public keys are as specified
in [RFC3279] and [RFC5480].

We include them here for convenience:

EDNOTE: Add the public key OIDs here.

... OBJECT IDENTIFIER ::= { }

... OBJECT IDENTIFIER ::= { }

4. Acknowledgements

   We would like to thank Sean Turner for his valuable contributions to
   this document.

5. 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. The description is as follows:

   o EDNOTE: More here

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

6. Security Considerations

    EDNOTE: More here.

7. References

7.1. Normative References

    [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, <https://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,
               <https://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,
               <https://www.rfc-editor.org/info/rfc5480>.

    [SHA3]   National Institute of Standards and Technology, "SHA-3
               Standard - Permutation-Based Hash and Extendable-Output
               Functions FIPS PUB 202", August 2015,
               <https://www.nist.gov/publications/sha-3-standard-
               permutation-based-hash-and-extendable-output-functions>.

7.2. Informative References

    [FIPS186-4]
               National Institute of Standards and Technology, "Digital
               Signature Standard (DSS) FIPS PUB 186-4", July 2013,
               <http://nvlpubs.nist.gov/nistpubs/FIPS/
               NIST.FIPS.186-4.pdf>.

   [SEC1]   Standards for Efficient Cryptography Group, "SEC 1:
               Elliptic Curve Cryptography", May 2009,
               <http://www.secg.org/sec1-v2.pdf>.

   [X9.62]   American National Standard for Financial Services (ANSI),
               "X9.62-2005 Public Key Cryptography for the Financial
               Services Industry: The Elliptic Curve Digital Signature
               Standard (ECDSA)", November 2005.

Appendix A. ASN.1 module

   EDNOTE: More here.

Authors' Addresses

   Panos Kampanakis
   Cisco Systems

   Email: pkampana@cisco.com

   Quynh Dang
   NIST
   100 Bureau Drive, Stop 8930
   Gaithersburg, MD 20899-8930
   USA

   Email: quynh.dang@nist.gov