draft-lamps-cms-shakes-hash-00
(was draft-dang-lamps-cms-shakes-hash-00)

Q. Dang, National Institute of Standards and Technology (NIST)

P. Kampanakis Cisco Systems

Adding SHAKE128/SHAKE256 to CMS

- Defines the OIDs for digital signatures and MAC (KMAC) so that SHAKEs can be used in CMS.
- Changes from draft-dang-lamps-cms-shakes-hash-00
  - Various updates to title and section names.
  - Replaced RSASSA PKCS#1 v1.5 with RSASSA-PSS
  - Content changes, filling in text and references.

SHAKEs' OIDs

```
id-shake128-len OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
                    country(16) us(840) organization(1) gov(101) csor(3)
                    nistalgorithm(4) hashalgs(2) 17 }

id-shake256-len OBJECT IDENTIFIER ::= { joint-iso-itu-t(2)
                    country(16) us(840) organization(1) gov(101) csor(3)
                    nistalgorithm(4) hashalgs(2) 18 }

ShakeOutputLen ::= INTEGER -- Output length in octets
```

ShakeOutputLen MUST be present and >= 32 for `id-shake128-len` or >= 64 for `id-shake128-len`

Mask Generation Function (MGF)

- [RFC8017]

```
id-mgf1  OBJECT IDENTIFIER  ::=  { pkcs-1 8 }
```

- To use SHAKE as MGF, the `id-mgf1` MUST have a hashAlgorithm value of `id-shake128-len` or `id-shake256-len`

RSASSA-PSS [RFC4055]

- OIDs

```
id-RSASSA-PSS  OBJECT IDENTIFIER  ::=  { pkcs-1 10 }

RSASSA-PSS-params  ::=  SEQUENCE  {
            hashAlgorithm      HashAlgorithm,
            maskGenAlgorithm   MaskGenAlgorithm,
            saltLength         INTEGER,
            trailerField       INTEGER }
```

- When the SHAKE128 or SHAKE256 OIDs is used as the `hashAlgorithm`, it MUST also be used as the `maskGenAlgorithm`.
- When used as `hashAlgorithm` the ShakeOutputLen parameter MUST be present and equal to 32 or 64.
- When used as `maskGenAlgorithm` the ShakeOutputLen parameter must be (n - 264)/8 or (n - 520)/8 respectively, where n is the RSA modulus in bits.
- saltLength MUST be 32 or 64 bytes respectively
- Public Key `rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}` [RFC3279] or `id-RSASSA-PSS` [RFC4055]

ECDSA

- OIDs

```
id-ecdsa-with-SHAKE128 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
            us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 3  x }

          id-ecdsa-with-SHAKE256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
            us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 3  y }

x and y will be specified by NIST.
```

The ShakeOutputLen parameter of SHAKE128 or SHAKE256 MUST be 32 or 64 bytes respectively when it is used in ECDSA

- Public key [RFC5480]

```
id-ecPublicKey OBJECT IDENTIFIER ::= {
            iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

ECParameters ::= CHOICE {
        namedCurve         OBJECT IDENTIFIER
        -- implicitCurve   NULL
        -- specifiedCurve  SpecifiedECDomain }
```

Message Authentication Codes with SHAKEs

- OIDs

```
id-KmacWithSHAKE128 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
      us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 z }
id-KmacWithSHAKE256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
      us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 w }
 z and w will be specified by NIST.
```

- When the `id-KmacWithSHAKE128` or `id-KmacWithSHAKE256` algorithm identifier is used, the parameters field MUST be absent; not NULL but absent.
- When calculating the KMAC output, the variable N is 0xD2B282C2, S is an empty string, and L, the integer representing the requested output length in bits, is 256 or 512 for KmacWithSHAKE128 or KmacWithSHAKE256 respectively in this specification.

Comments/questions ?