draft-dang-lamps-cms-shakes-hash-00 (should’ve been draft-lamps-cms-shakes-hash-00 instead)

Q. Dang, P. Kampanakis

National Institute of Standards and Technology (NIST) Cisco Systems

Adding SHAKE128/SHAKE256 to CMS

- Goal: Define the OIDs for digital signatures and MAC so that SHAKEs can be used in CMS:
    - RSASSA PKCS#1 v1.5 with SHAKEs
    - ECDSA with SHAKEs
    - KMAC
- Draft is still in early stage.

SHAKEs’ OIDs

- SHA3 defines SHAKE128 and SHAK256 with output size d.
  - collision and preimage resistance is min(d/2,128) and min(d,128) for SHAKE128 and min(d/2,256) and min(d,256) for SKAHE256.
- d = 256/512 bits for SHAKE128/256 in this specification.
- SHAKE OIDs
  - id-SHAKE128 OBJECT IDENTIFIER ::= {

    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) 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

    }

RSASSA PKCS#1 v1.5

- OIDs
  - id-rsassa-pkcs1-v1_5-with-SHAKE128 OBJECT IDENTIFIER ::= {
    joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 3 **x**
    }
  - id-rsassa-pkcs1-v1_5-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.
- When OIDs used as an AlgorithmIdentifier, the parameters field MUST contain NULL.

ECDSA [X9.62]

- OIDs
  - id-ecdsa-with-shake128 OBJECT IDENTIFIER ::= {

    joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) 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) algorithms(4) id-ecdsa-with-shake(3) y

    }

    x and y will be specified by NIST.
- When OIDs used as an AlgorithmIdentifier, the parameters field MUST be absent; not NULL but absent.

Message Authentication Codes with SHAKEs

- id-KmacWithSHAKE128 OBJECT IDENTIFIER ::= {

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

  }
- id-KmacWithSHAKE256 OBJECT IDENTIFIER ::= {

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

  }

x and y will be specified by NIST later.

- N and S are empty strings. L is 256 or 512 for KmacWithSHAKE128 or KmacWithSHAKE256 respectively.
- When the id-KmacWithSHAKE128 or id-KmacWithSHAKE256 algorithm identifier is used, the parameters field MUST be absent; not NULL but absent.

Next step and Comments ?

- Add DSA with SHAKEs in the next draft.
- Comments/questions ?