draft-ietf-lamps-pkix-shake-02
draft-ietf-lamps-cms-shakes-01

P. Kampanakis, Cisco Systems

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

Changes to drafts for SHAKEs in PKIX and CMS

- New OIDs for RSASSA-PSS that hardcodes hash, salt and MFG, according the WG consensus in IETF-101.
- Updated Public Key sections to use the new RSASSA-PSS OIDs and clarify the algorithm identifier usage.
- Removed the no longer used SHAKE OIDs from section 3.1 in the PKIX draft.
- Consolidated subsection for message digest algorithms.
- Text fixes and document structure simplification.

OIDs

```
id-RSASSA-PSS-SHAKE128 OBJECT IDENTIFIER ::= { TBD }
id-RSASSA-PSS-SHAKE256 OBJECT IDENTIFIER ::= { TBD }
```

(Hardcoded hashes, MFG, salts and trailer.)

```
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) TBD }
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) TBD }
```

(Pre-defined hash output sizes to 32 and 64 bytes respectively.)

[EDNOTE: "TBD" will be specified later.]

OIDs (cont'd)

For CMS,

```
id-shake128-len OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
       us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 17 }
id-shake256-len OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
       us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 18 }
```

(Used in CMS DigestedData field and the Message Digest authenticated attribute. Pre-defined hash output sizes are 32 and 64 bytes respectively.)

```
id-KmacWithSHAKE128 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
       us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 TBD }
id-KmacWithSHAKE256 OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) country(16)
       us(840) organization(1) gov(101) csor(3) nistAlgorithm(4) 2 TBD }
```

(Used in the CMS AuthenticatedData macAlgorithm field. Pre-defined N, S, and L.)

[EDNOTE: "TBD" will be specified later.]

Questions/Comments ?