# draft-ietf-lamps-pkix-shake-00

P. Kampanakis, Q. Dang

Cisco Systems National Institute of Standards and Technology (NIST)

# Adding SHAKE in PKIX

- Goal: Define the OIDs for PKIX so that SHAKEs can be used in X.509.
- For now we will focus
  - DSA
  - ECDSA
  - RSA
- 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.
- SHAKEs’ 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

    }

# DSA [FIPS186-4]

- OIDs
  - 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

    }
  - id-dsa-with-shake256 OBJECT IDENTIFIER ::= {

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

    }

  "x" and "y" will be specified by NIST later.
- When OIDs used as an AlgorithmIdentifier, the encoding MUST omit the parameters field.

# 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 later.
- When OIDs used as an AlgorithmIdentifier, the encoding MUST omit the parameters field.

# Public Key identifiers

- Formats defined
  - [RFC3279] and
  - [RFC5480]

# Questions/Comments ?

- What RSA standard(s) should we specify in the next version ?
- Comments/questions ?