draft-ietf-lamps-pkix-shake-01

P. Kampanakis, Q. Dang

Cisco Systems National Institute of Standards and Technology (NIST)
Adding SHAKEs in PKIX

• Draft defines the OIDs for PKIX so that SHAKEs can be used in X.509.
• Changes from -00
  • Removed DSA after WG discussions.
  • Updated shake OID names and parameters.
  • Added MGF1 section.
  • Updated RSASSA-PSS section.
  • Added Public key algorithm OIDs.
  • Updated Introduction and IANA sections.
  • Updated titles and section names.
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]

\[\text{id-mgf1} \quad \text{OBJECT IDENTIFIER} \quad ::= \quad \{ \text{pkcs-1 8} \}\]

To use SHAKE as MGF, the \text{id-mgf1} MUST have a hashAlgorithm value of \text{id-shake128-len} or \text{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 identifiers

• [RFC3279]
  rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }

• [RFC4055]
  id-RSASSA-PSS OBJECT IDENTIFIER ::= { pkcs-1 10 }

• [RFC5480]
  id-ecPublicKey OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

    ECPParameters ::= CHOICE {
      namedCurve OBJECT IDENTIFIER
      -- implicitCurve NULL
      -- specifiedCurve SpecifiedECDomain
    }
Security Considerations

• SHAKEs are deterministic functions.
• Protect signer’s private key.
• Sharing the KMAC key does not provide origin authentication.
• MAC keys must be chosen randomly or a (shared) secret pseudorandom key which meets the required security strength.
• Support crypto agility.
Questions/Comments ?