SHA-3 For PKIX?

•••

draft-turner-lamps-adding-sha3-to-pkix

Sean Turner ~ IETF 98 ~ LAMPS

What do I want?

Message Digest Algorithms - From FIPS 202

Included

Message Digest/Hash Functions:

- SHA3-256
- SHA3-384
- SHA3-512

Not Included

Message Digest/Hash Function:

- SHA3-224

Extendable-Output Functions:

- SHAKE128
- SHAKE256

Signature Algorithms

Included

ECDSA with SHA3-256

ECDSA with SHA3-384

ECDSA with SHA3-512

Not Needed

ECDSA with SHA3-224

DSA with SHA3-*

Not Included Yet

RSASSA-PKCS1-v1.5 with SHA3-256/384/512

RSASSA-PSS with SHA3-256/384/512

ASN.1 MODULES

NIST defined OIDS (kind of) here but there's no ASN.1 module ...

This draft includes two: one for '88 and one for '15.

Both use the OIDs defined by NIST.

GH repo

https://seanturner.github.io/draft-turner-lamps-adding-sha3-to-pkix/

PRs welcome.

Next Steps

Let die gracefully?

Adopt in WG after recharter?