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

<table>
<thead>
<tr>
<th>Included</th>
<th>Not Included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message Digest/Hash Functions:</strong></td>
<td><strong>Message Digest/Hash Function:</strong></td>
</tr>
<tr>
<td>SHA3-256</td>
<td>SHA3-224</td>
</tr>
<tr>
<td>SHA3-384</td>
<td><strong>Extendable-Output Functions:</strong></td>
</tr>
<tr>
<td>SHA3-512</td>
<td>SHAKE128</td>
</tr>
<tr>
<td></td>
<td>SHAKE256</td>
</tr>
</tbody>
</table>
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?