draft-ietf-lamps-pkix-shake-03
draft-ietf-lamps-cms-shakes-02

P. Kampanakis,
Cisco Systems

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

SHAKEs in PKIX and CMS drafts' Changes

- Addressed all of Jim S.' comments. Thank you Jim!
- Replaced ECDSA with Deterministic ECDSA
  - k generated with KMAC with SHAKE128 / 256 instead of HMAC. **Agreed?**
- Replaced MGF1 in RSASSA-PSS with SHAKE128/256
- Updated Security Considerations to point out that SHAKE will produce overlapping outputs when used with the same input and different output lengths.
- Updated IANA section.
- Text and nit fixes.

What is Next - Asks

Next

- We still need to add ASN.1 module.

Asks

- WGLC?
- We need more reviews.
- Questions – Comments?
- Jim asked about KMAC-tags shorter than 256 bits ?