*

Using RSA Algorithms with COSE Messages

draft-jones-cose-rsa

Mike Jones

IETF 96, Berlin

July 2016

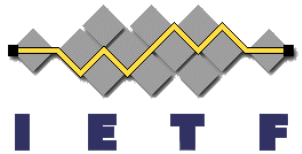
Spec Overview

- Defines how to use standard RSA algorithms with COSE
- Need identified in COSE Issue #21:
  - “Restore RSA-PSS and the ‘RSA’ key type”
  - https://github.com/cose-wg/cose-issues/issues/21
- This draft was written to fill this need
- Specifically, enables use of:
  - RSA key type
  - RSASSA-PSS algorithm
  - RSAES-OAEP algorithm
- Uses text from draft-ietf-cose-msg-05 – the last COSE message draft before the RSA algorithms were removed

Why do both my draft and Jim's algs draft exist?

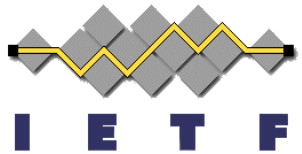
- Quirk of timing
- In Issue #21, I volunteered to write this on Dec 5, 2015
- On Mar 21, 2016, Jim wrote his draft. I was offline on vacation and didn't notice.
- On Apr 4, 2016, I wrote my draft
- At the opening reception on Sunday, Kepeng told me both existed ☺

Differences between my draft and Jim's draft



- Mine enables RSA. Jim's enables RSA and also enables OKP key type and EdDSA algorithm.
- Mine kept numeric identifier assignments, such as -26 for PS265 and 3 for RSA key type. Jim's uses TBD#.
- Plus a few editorial differences…

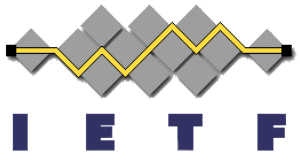
Standards Status of Additional Algorithms



- The RSA algorithms are done
  - A draft referencing only mature algorithms could be approved quickly – possibly at the same time as COSE Messages
  - Consecutive RFC numbers, anyone? ☺
- EdDSA is not yet done
  - Finishing an algorithms RFC using EdDSA will block on completion of draft-irtf-cfrg-eddsa RFC

- *Comments above only on timing implications, not on the desirability of enabling the use of all of these algorithms*

Resolving the Duplication



- We should clearly resolve the duplication
- I can see two credible options:
  1. Adopt Jim's draft
     - Means RFC would block on EdDSA RFC
  2. Adopt my draft and Jim's draft, removing RSA from Jim's
     - Means RSA RFC could happen quickly and EdDSA RFC when ready
     - I would be happy to add Jim as a co-editor on my draft

- I prefer second option because we want to use RSA soon
- Others may have other views or options

- Discussion…