Validation Parameters (Proof of Primality) for PKCS#8

Benjamin Kaduk

16 July 2018

History[1]

- 20170807 — initial discussions on SAAG list
- 20170808 — revision -00 posted
- 20171211 — draft submitted to ISE for publication
- 20171221 — reviewed by Russ Housley (see shepherd write-up)
- 20180310 — reviewed by Stephen Farrell (see shepherd write-up)
- 20180319 — revision -01 posted
- 20180328 — ISE review
- 20180329 — revision -02 posted
- 20180329 — requested 5742 conflict review
- 20180618 — ISE asks secdispatch list for input
- 20180621 — IESG approves “do not publish” conflict review response
- 20180702 — on-list feedback from Benjamin Kaduk and Russ Housley
- 20180707 — Appeal of IESG Conflict Review response initiated
- 20180716 — This presentation in secdispatch session

[1] Made possible by Adrian Farrel, ISE

Premise of the document

- RSA and DSA key generation requires producing primes of a desired bit length
- There is history of composite “primes” being used for RSA[2]
- It is possible to generate a proof of primality along with the prime, e.g., the Shawe-Taylor algorithm in FIPS186-4
- If you have it, keep the proof alongside the private key in an attribute of the PKCS#8 container
- No restriction on use — private/internal bookkeeping, send to auditor, etc.

[2] e.g., `https://factorable.net/`

Is this the right scope?

- Can we give guidance on how to use this?
- Are there any other places we might want to have primality proofs?
- Should the IETF adopt this work?