DKIM Base Issue Review
IETF 66 — Montréal

Eric Allman

2006-07-11

1287: Signature Removal

- https://rt.psg.com/Ticket/Display.html?id=1287
- http://mipassoc.org/pipermail/ietf-dkim/2006q2/003764.html
- Remove sentence “Signers SHOULD NOT remove any DKIM-Signature header fields from messages they are signing, even if they know that the signatures cannot be verified.”
- “John Levine to propose text” *(on further consideration, believes it should remain)*

1288: Signing Address

- https://rt.psg.com/Ticket/Display.html?id=1288
- http://mipassoc.org/pipermail/ietf-dkim/2006q2/003768.html
- Define “signing address” in intro (§1.2)
- *Changed “associated with” to “defined in” (for -04)*

1289: Signature Process Clarification Requested

- https://rt.psg.com/Ticket/Display.html?id=1289
- http://mipassoc.org/pipermail/ietf-dkim/2006q2/003817.html
- Does b= tag in signed DKIM-Signature header fields get deleted before signing? (§3.5)
- *Language changed in -03*

1293: worst-case scenario/duration of exploit/use of deprecated

- https://rt.psg.com/Ticket/Display.html?id=1293
- http://mipassoc.org/pipermail/ietf-dkim/2006q2/003831.html
- Tag DKIM-Signature and key record with “deprecated” flag

1294: i= parameter conflict

- https://rt.psg.com/Ticket/Display.html?id=1294
- http://mipassoc.org/pipermail/ietf-dkim/2006q2/003763.html
- §1.2 seems to conflict with §5.1
- From jabber: “CLOSE with no change... pending confirmation on mailing list.”
- *(No confirmation as yet)*

1308: Security Considerations for _domainkey subdomain

- https://rt.psg.com/Ticket/Display.html?id=1308
- “Doug repeated a request that he's made before: "There should be some consideration give the Security Consideration section regarding the affects of the _domainkey subdomain use."

1316: multiple minor issues (1/8)

- Many editorial that have been incorporated
- https://rt.psg.com/Ticket/Display.html?id=1316
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004019.html
- #1: §2.6: Multibyte characters
- #2: §3.1: Dots in selectors *(see issue 1323)*
- #3: §3.2: Max length for tags? *(none)*
- #4: §3.2: Unicode in tag values

1316: multiple minor issues (2/8)

- #5: §3.2: final ';' always required? *(no)*
- #6: §3.3.4: what does "long lived key" mean?
  - Just demand 1024 bit key?
- #7: §3.4: "Empirical evidence demonstrates"? Reference?
- #8: §3.4 ¶5: incorrect wording *(fixed)*; hashing inside of signing algorithm *(resolved, I think)*

1316: multiple minor issues (3/8)

- #9: §3.4 ¶last: I18N issues
- #10: §3.4.1: quoted spaces remain quoted? *(yes)*
- #11: §3.4.2: relaxed form of "□=20□" single space or unchanged? *(Unchanged — '=' is not a special character in this context)*
- #12: §3.4.4: replace relaxed body C14N with the one from S/MIME or PGP? *(See also issue New01)*

1316: multiple minor issues (4/8)

- #13: §3.4.5, 3.5, 3.7: outlaw l=0 and use omission of bh= instead? *(no)*
- #14: §3.5: complex relationship between d= and i= *(fixed in -04 — thanks Jim)*
- #15: §3.5: special punycode support? *(no)*
- #16: §3.5: i= also needs to be punycode *(done)*

1316: multiple minor issues (5/8)

- #17: §3.5: key consistency between key servers
  - If multiple key servers are listed in DKIM-Signature q= tag, what are their requirements?
  - Current: “If there are multiple query mechanisms listed, the choice of query mechanism MUST NOT change the interpretation of the signature.”
  - Stephen: may be different CRLs, timeouts, etc.
  - Proposal: “All query mechanisms listed must produce keys that result in substantially the same verification result during normal circumstances.”

1316: multiple minor issues (6/8)

- #18: §3.6.1: wildcarding in g= tag *(see issue 1325)*
- #19: §3.6.1: sha-256 requirement *(fixed)*
- #20: §3.6.1: k= exponent fixed at 65537? *(see issue 1322)*
- #21: §3.6.2.1: remove i= arg to key lookup *(done)*
- #22: §5.4: h= specify non-existent headers — remove?

1316: multiple minor issues (7/8)

- #23: §5.5: removing existing results header fields *(removed)*
- #24: §6 ¶2: verifiers MAY add an authentication status header — remove?
  - *New wording: "A border or intermediate MTA MAY verify the message signature(s). An MTA who has performed verification MAY communicate the result of that verification by adding a verification header field to incoming messages."*

1316: multiple minor issues (8/8)

- #25: §6.1: OK to only try to verify a single signature? *(yes, but discouraged)*
- #26: §6.1.1: signer MUST sign From header field. Verifier should check. *(done)*
- #27: §6.1.2, #4: could attacker force looping DNS queries? *(no)*
- #28: §6.1.1 list: can verifier reject a key if too short?

1317: Editorial and nits (1/8)

- #1: abstract: “proof” and “non-repudiation” — say “evidence” instead *(need consensus)*
- #2: §1.1, 1st set of bullets: difference between DKIM and S/MIME or PGP is expectation of failure
- #3: §1.1, 2nd set of bullets: is DNS a TTP? *(changed to add “additional”)*
- #4: §1.1 ¶last: too early to introduce selectors? *(done)*

1317: Editorial and nits (2/8)

- #4′: §3.3 ¶1: wording about signature algs *(done)*
- #5: §3.3.1, 3.3.2: phrasing about signing *(see issue 1322)*
- #6: §3.3.3: “do not understand” → “cannot verify” *(done)*
- #7: §3.3.4: wording about modulus and key size *(resolved?)*

1317: Editorial and nits (3/8)

- #8: §3.3.4: say “Verifier security policies may use the length” *(done)*
- #9: §3.4: change “authentication failure” to “signature verification failure” *(done)*
- #10: §3.4.5: minor wording *(done)*
- #11: §3.4.5, 2nd note: can verifier ignore “l=“ tag? *(yes, that is what was intended)*

1317: Editorial and nits (4/8)

- #12: §3.4.5 ¶3: minor wording *(done)*
- #13: §3.4.5, 2nd note: delete *(merged into 1st note)*
- #14: §3.4.5, 3rd note: delete *(done)*
- #15: §3.5: wording inconstency *(fixed)*
- #16: §3.5: example needs bh= *(done)*

1317: Editorial and nits (5/8)

- #17: §3.6.1: wording *(done)*
- #18: §3.6.2.1: formating *(fixed)*
- #19: §3.7: wording about hash functions — part of the signing API? *(added informative note)*
- #20: §3.7 ¶6, “When calculating the hash…”: MUA guidance? *(no, referring to 8→7 bit MTA downgrading)*

1317: Editorial and nits (6/8)

- #21: §3.7: “sans”? *(yes, it’s an English word)*
- #22: §5.2 ¶last: “remove key” vs “revoke key”
- #23: §5.5 ¶last 2: I= discussion duplicative *(informative note removed, other left)*
- #24: §6: “expire” → “revoke” *(done)*
- #25: §6.1, note 1: “other clues” opaque

1317: Editorial and nits (7/8)

- #26: §6.1: wording "; this is local policy" confusing (?)
- #27: §6.1.3: "create a canonicalized copy" misleading *(changed to "canonicalized version")*
- #28: §6.2: remove ref to ID-AUTH-RES *(done)*
- #29: §8.1.1: missing example *(done)*

1317: Editorial and nits (8/8)

- #30: §8.2: mention hardware signing *(done)*
- #31: §A.2: examples need bh= *(done)*
- #32: §A.3: don't use Authentication-Results *(changed to X-Authentication-Results)*
- #33: §B: (use cases) need to talk about 3rd party MTAs (e.g., IETF)?
- #34: §C: (creating a public key) drop? *(keep it but reword)*

1318: is s= really needed?

- https://rt.psg.com/Ticket/Display.html?id=1318
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004021.html
- Is “s=” (key record, service type) needed? *(yes)*

1319: “Rewrite” Section 5?

- https://rt.psg.com/Ticket/Display.html?id=1319
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004022.html
- Quite a bit of normative language in section 5 (Signer Actions) that perhaps should not be normative
- *Proposal: Stephen and Eric do an editing session before Wednesday meeting*

1320: IANA Considerations

- https://rt.psg.com/Ticket/Display.html?id=1320
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004023.html
- “This section needs to be expanded to be specific” — Paul Hoffman
- *Suggest we unanimously volunteer Paul (Tony?)*

1321: key-*-tag minor issues

- https://rt.psg.com/Ticket/Display.html?id=1321
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004029.html
- #1: §3.6.1: g= tag includes CFWS *(fixed)*
- #2: §3.6.1: p= tag needs to allow zero length value *(fixed)*
- #3: §3.6.1: h= tag (acceptable hash algs) should allow wildcarding

1322: more details of key record format in base

- https://rt.psg.com/Ticket/Display.html?id=1322
- http://mipassoc.org/pipermail/ietf-dkim/2006q3/004060.html
- Get rid of hard-coded 65537 exponent?
  - Current draft says “That hash is then signed by the signer using the RSA algorithm … with an exponent of 65537”
  - Exponent included as part of the public key — needed here?
- *Reword along the lines of EKR’s mail*
- *Need a volunteer….*

1323: dots in selectors (1/2)

- https://rt.psg.com/Ticket/Display.html?id=1323
- Are dots permitted in selectors?
- How do they interact with DNS labels?
- *(Believe this to be resolved)*

1323: CNAMEs? (2/2)

- Allow DNS key records to use CNAMEs?
- *Consensus seems to be "yes" — any wording changes needed?*

1325: g= wildcarding in key records

- https://rt.psg.com/Ticket/Display.html?id=1325
- Current spec allows arbitrary wildcarding with “*”; this may be hard to implement
- Limit to a single wildcard?
- Limit to the start and end of the pattern, just the end, or allow anywhere?
- *Propose limiting to a single wildcard anywhere in string*

New01: Drop relaxed body canonicalization?

- Should we drop “relaxed” body canonicalization?
- No known cases where it is required
- See also issue 1316 #12
- *Proposal: drop it, but keep the concept of multiple body canonicalizations so that it (or something else) can be added back later*

New02: Wildcarding in h= tag

- Proposal to allow wildcarding in h= tag to prevent addition of any new headers
- Example: X-Message-Flag in Outlook (contents displayed in yellow at top of message view)
- (Presumably an exemption for trace headers)

Other Issues?