DKIM -base Open Issues

Eric Allman

IETF 65

March 22, 2006

(updated with results from 3/20 meeting)

carryover: draft-allman-dkim-base-01.txt - Should we have an r= tag in either the signature or key record

1183 lear@ofcourseimright.com OPEN

- no thread?
- There is a thread on making r= localpart only (from Mark D)
- ACTION: Doug Otis will argue for r= in the mail address, Phil [Paul?] Hoffman will argue against

carryover: Develop plan for transition of multiple crypto algs (a=)

1184 lear@ofcourseimright.com ACCEPT

- not much discussion of how to transition, though not much disagreement either
- 3/9: “Not much discussion; not much disagreement”
- http://mipassoc.org/pipermail/ietf/dkim/2006q1/002414.html
- ACTION: Mark Delany to provide text for a discussion of how to choose a signature

carryover: draft-allman-dkim-base-01.txt Transition sha-1 to sha-256

1185 lear@ofcourseimright.com ACCEPT

- not quite closed on the actual exact wording
- *[I think we had converged on MUST accept either, SHOULD generate sha-256]*
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002414.html
- ACTION: Eric to provide wording: above plus that a signer MUST use (be capable of using?) one or the other alg.

base spec: instead of signing the message, sign the hash

1193 lear@ofcourseimright.com ACCEPT

- no (recent) thread
- Summary: Hash the body, store that in header, hash and sign the header
- Hash could be in DKIM-Signature or another header field
- ACTION: Eric to insert appropriate wording; body hash value to be in DKIM-Signature header field; include l= considerations

base spec: whitespace in signature?

1194 not sure if this is the right thread DONE

- "Need to use appropriate folding rules for signature line (CFWS, et al)"
- Something to do with Structured vs. Unstructured header fields?
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002464.html
- About inserting explicit FWS/CFWS in spec ABNF — already done

draft-ietf-dkim-base-00 - 3.4.6 Example (Canonicalization)

1195 hsantos@santronics.com ACCEPT

- no discussion
- “1) Please note "relaxes" typo in 3.4.6 example:
  - "Assuming a "c=relaxes/relaxed" canonicalization algorithm, a message reading:” *[Fixed]*
- “2) Consider adding more examples to illustrate our possible algorithms and combinations.”
- http://mipassoc.org/pipermail/ietf/dkim/2006q1/002148.html
- ACTION: Eric to add examples (#1 is done)

Base: Upgrade indication and protection against downgrade attacks

1196 MarkD+dkim@yahoo-inc.com OPEN

- lots of discussion, no clear closure
- Summary: add tag in selector record indicating lowest algorithm that will ever be used for signing
- http://mipassoc.org/pipermail/ietf/dkim/2006q1/002163.html
- EKR: verifier choice what alg's to accept, regardless of signer preference. Russ: signer should state what gets used, verifier should choose. Status: remains open *(are they going to write up their positions?)*

MUST vs SHOULD in Verifier Actions section (-base)

1200 eric@sendmail.com ACCEPT

- “There are several places in the Verifier Actions section of draft-ietf-dkim-base-00 that say that a verifier MUST ignore bad or malformed signatures. This is really a local policy question, and we have been trying to stay out of that. Shall we change these to SHOULDs, or even just change these to read something like "Bad or malformed signatures MAY be ignored. This is a local policy decision and beyond the scope of this document."?”
- ACTION: Eric to provide updated text

change the syntax from SPF compat to human compat

1201 MarkD+dkim@yahoo-inc.com REDIRECT

- See 1217: SSP: should we drop the cryptic o=. syntax for something a little more readable?
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002219.html
- Really not appropriate for this session — SSP-specific
- Move to SSP discussion

extendable RR records?

1203 tony@att.com ACCEPT

- the title of this issue is misleading, its really about extra options to be specified in a DKIM TXT record
- “We allow extra options to be specified in a DKIM-Signature header, but do not allow extra options to be specified in a DKIM TXT record. (I don't recall this being discussed before, but just may not remember it.) Should we? If not, how would we do upwardly-compatible changes without requiring multiple DNS entries for both an old and new entry.”
- *[Described as part of tag-list syntax, §3.2: “*Unrecognized tags MUST be ignored.”*]*
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002260.html
- ACTION: Eric to try to clarify

issue with DKIM simple header algorithm and milter-based implementations

1204 tony@att.com CLOSED

- seemed like consensus but no clear change
- Q about milter handling of white space around colons in headers
- *[I have a sendmail patch to fix this] [oops, not yet]*
- http://mipassoc.org/pipermail/ietf/dkim/2006q1/002273.html
- STATUS: this is an MTA implementation issue, not a spec issue

clarifications on use of l= tag

1215 Eric Allman CLOSED

- no discussion
- http://mipassoc.org/pipermail/ietf/dkim/2006q1/002185.html (bad URL)
- (item was confirmation of language inserted into draft)
- No action required

signature h= and z= tags

1216 Hector Santos ACCEPT

- little discussion
- Can the lists differ? *[probably SHOULD NOT]*
- If they do, which one wins? *[h=]*
- Why so complex?
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002375.html
- ACTION: decouple the two. Eric to provide wording

ABNF: Sender = Originator / Operator

1222 dhc@crocker.net OPEN

- (also listed as 1221)
- some discussion
- Summary: never use the word “sender” ever again (use “originator” or “operator” instead) — except, presumably, for the Sender: header field
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002495.html
- Table for now; Dave has taken an action for -threats on this: discuss there

DKIM and mailing lists

1224 Stephen Farrell OPEN

- too much discussion
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002534.html
- http://www.sympa.org/wiki/doku.php?id=dkim_and_mailing_lists
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/001839.html
- Too long. Defer until Wednesday

512 too short?

1226 Stephen Farrell ACCEPT

- some discussion
- Summary: RSA key size should be 1024 minimum
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002620.html
- ACTION: Eric to incorporate Russ's text (already provided to list)

bunch of nits for base

1227 Stephen Farrell ACCEPT

- no discussion
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002615.html
- ACTION: Eric to incorporate

Why is s= REQUIRED?

1228 Stephen Farrell CLOSED

- a tiny bit of discussion
- Summary: shouldn't there be a default selector?
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002621.html
- No action; Stephen accepts explanation

z= field and EAI wg

1229 Stephen Farrell CLOSED (PENDING?)

- a tiny bit of discussion
- “Even if it doesn't hit anywhere else, presumably the EAI work will have to be taken into account for the z= field, with potential changes being required to the current ABNF?”
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002622.html
- ACTION: Paul Hoffman to act as liaison to EAI

selectors and key rollover

1230 Stephen Farrell CLOSED

- no discussion
- Summary: Version numbers on selector names
- Multiple keys per selector
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002619.html
- This is really a BCP issue, not a spec issue

some process-problematic references in base

1231 Stephen Farrell OPEN

- no discussion
- Summary: Search for DKK first creates problematic reference (skip this and revise doc later?)
- Authentication-Results *[should already be gone]*
- §6.6 (MUA Considerations) — necessary/useful?
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002616.html
- Discussion, but no resolution before closing

Clarify delegation to 3rd parties

N001 Stephen Farrell OPEN

- no discussion
- “I'd like there to be a very clear consensus as to what's included here, e.g. we are not going to mandate who generates keys, so we thus cannot say whether a private key is being used for >1 sending domain. As it is, the feature is mentioned a number of times, without ever really saying what's to be supported.
- “That may create potential holes. The problem is that there might be many of those. Is there any way that this feature could be separated out into some kind of extension spec? Anyway, perhaps a section specific to delegation should be added?”
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002618.html

base editorial

N002 Stephen Farrell OPEN

- no discussion
- Move “some of the text here” *[?]* to overview document
- Provide examples at the beginning of the document to make it easier to understand
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002617.html

Analyzing Failures: List of Possible Reasons

- N003 Hector Santos OPEN
- "I think section 6.5 is a good step but we need a section that is dedicated to all the possible reasons for failures as we KNOW it to possibly to occur. I think there should a special section:

  6.6 List of Possible Failures …"
- http://mipassoc.org/pipermail/ietf-dkim/2006q1/002694.html

X= and clock skew

- N004 Rescola OPEN
- Guidance about what happens in the case of clock skew

Editorial comments

- N005 Rescola OPEN
- A bunch of editorial comments