IETF DMARC WG Interim DMARCbis Discussion

27 May 2021

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

IETF

Agenda

1. 9:00-9:10 PT Chairs opening
2. 9:10-10:10 PT Base spec
3. 10:10-10:30 PT Aggregate reporting
4. 10:30-10:40 PT Failure reporting
5. 10:40-10:50 PT Wrap up and next steps

Do we have a note taker for Etherpad?

https://codimd.ietf.org/notes-ietf-interim-2021-dmarc-01-dmarc

Chairs opening

- GOAL: **Standards Track DMARC document at the IETF**
- Current Statuses:
  - RFC 7489 (DMARC) is **INFORMATIONAL** and was not a product of the IETF
  - RFC 8617 (ARC) is **EXPERIMENTAL**
  - RFC 7208 (SPF) is **PROPOSED STANDARD**
  - RFC 6376 (DKIM) is **INTERNET STANDARD**
  - DMARC extensions for PSD is **EXPERIMENTAL**; in RFC editor queue
  - DMARCbis targeting **PROPOSED STANDARD**

Working group model for DMARCbis

- We’d like to start having REGULAR Interim meetings to accelerate to rough consensus and burn through all open tickets
- The output of these meetings should be PROPOSED TEXT for the documents (either as part of the Interim, or immediately following)
- The Chairs will ensure that the conversation stays within the tickets and proposed text. As a reminder:
  - The Chairs are not looking to rewrite DMARC from scratch
  - Chairs are not planning to expand scope of DMARC protocol, i.e. to address things it was not designed to do

Charter guidelines for DMARC bis work:

- Updates based on operational experience
  - and/or data aggregated from multiple sources
  - or to close security loopholes
- Preserve interoperability with the installed base of DMARC systems, and provide detailed justification for any non-interoperability.

DMARCbis - base spec

Ticket 4 - Definition of “fo” Tag

- Tag allows domain owner to request various types of failure reports:
  - ‘0’ - If all authentication methods fail
  - ‘1’ - If any authentication method fails
  - ‘d’ - If DKIM validation fails
  - ‘s’ - If SPF validation fails
- Definition in RFC 7489 allows for any combination of options, separated by colons:

  “The value of this tag is a colon-separated list of characters that indicate failure reporting options as follows:”

- This language allows nonsensical combinations such as “0:1:d:s”
  - Low occurrence of such values in the wild, but they’re still there.

- Proposed text in dmarcbis-01 tries to clarify this:

  “Failure reporting options are shown below. The value of this tag is either ‘0’, ‘1’, or a colon-separated list of the options represented by alphabetic characters.”

Ticket 47 - Remove “pct” Tag

- Tag allows domain owner to request message handling (p=) for just a percentage of unauthenticated mail, rather than all.
- Ticket reporter claims that pct tag is poorly implemented, poorly understood, and implementations are not statistically sound.
- One data set in ticket of tens of thousands of DMARC records in March 2021:
  - 5,548 had a pct tag
  - 5,066 of those with pct tag were pct=100
  - 482 of those with pct tag have pct= other than 0 or 100
  - 53 of those with pct tag were pct=0
- Other data from Comcast in ticket

Not well understood, not widely used. Should we remove it or continue to support it?

Ticket 50 - Remove “ri” Tag

- Tag allows domain owner to request aggregate reports at defined intervals (measured in seconds)
- Not widely used, no evidence that it’s honored
- One data set in ticket of tens of thousands of DMARC records in March 2021:
  - Most had no ri=tag, so defaults to 86400
  - 1,383 had ri=86400
  - 1,102 had ri=3600
  - 107 had ri=84600
  - Remainder had other values
- Other similar data from Ale Vesely in ticket

Should we remove the tag, keep it but list it as deprecated (not unlike ‘ptr’ tag in RFC 7208), or keep it as is?

Ticket 52 - Remove Strict Alignment (adkim and aspf tags)

- Strict alignment mean that the domain specified in the SPF or DKIM validation check must match exactly the RFC5322.From domain in the message.
- Reporter claims it’s not widely used and doesn’t provide additional security, especially when cloud services are used for sending.
- Datasets from various sources reported in ticket show usage of ‘s’ value for these tags ranging from 2% to 5% across the dataset.

Keep the tags or remove them?

Ticket 53 - Remove Reporting Message Size Chunking

- Original spec allows domain owner to request that reports be “chunked” by adding ! and requested chunk size to end of either the rua or ruf tag (e.g., rua=dmarcreports@foo.com!15m for 15MB chunks)
- Reporter claims no one uses it and that reporting systems haven’t implemented it.
- Datasets reported in ticket show minimal usage, between 0% and 2.3% depending on dataset.

Should this be kept or deleted?

Ticket 54 - Recipients Per Report

- Ticket request is to remove or expand the limit on recipients per report. Claim is that no reporter has enforced any limits.
- RFC 7489 (section 6.2 - “DMARC URIs”) includes the sentence:
  - “Receivers MAY impose a limit on the number of URIs to which they will send reports but MUST support the ability to send to at least two.”
- Proposal for this ticket is to remove that sentence from dmarcbis-01 and subsequent versions, and rearrange other sentences in paragraph to read:
  - “The place such URIs are specified...allows a list of these to be provided. The list of URIs is separated by commas (ASCII 0x2c). A report is normally sent to each listed URI in the order provided by the Domain Owner.”

Ticket 82 - Deprecate rf= Tag

- rf tag allows domain owner to specify requested format for failure reports.
- There is only one valid value (afrf) and it’s likely there will never be another valid value.
- Proposed text is to deprecate the tag, with added note describing reason for deprecation (ever-broadening privacy laws leading to severely redacted reports leading to likelihood that there will never be a format other than ‘afrf’).

Keep, deprecate, or drop entirely?

DMARCbis - aggregate reporting

How badly do we want to break the Aggregate format?

- We have several tickets that relate to:
  - Poor documentation about elements in RFC7489 (resulting in missing information)
  - Additions/subtractions for DMARCbis compared to RFC7489
- Do we just say “Reports have been varied formats for years”?
- Can/Should we note in the TXT record which version is preferred? Irrelevant?

Reporting Extensions

- We have a few tickets (unresolved) that sort of seem like they may be better resolved as extensions
- Should we suggest reporters begin working toward extensions?

DMARCbis - failure reporting

Failure reporting

- The design team editors believe all tickets have been addressed in the document
  - Ticket #55 - privacy considerations language, believe Ale addressed a couple months ago but will confirm.
  - Ticket #28 - Reporting mail loop issue. Murray kicked off a thread in January that reopened the ticket. Need to review thread.

- Are there any issues this group wishes to raise?

WRAP UP and NEXT STEPS