

IETF DKIM Interim Slides

June 17, 2026

Bron Gondwana

Hashing X-Headers

A new header field:

```
Message-Extra-Headers: hn=x-foo:x-bar;  
                        h=sha256:abcd1234...
```

Rules for recipes:

1. If you add a header to M-E-H; you **MUST** include a recipe for it
2. If a previous M-I header has a recipe for an x-header, you **MUST** add a recipe if you change that header
3. Obviously Message-Extra-Headers itself is a regular header and changes to it also get handled by recipes.

Changed behaviour:

- Recipe covered header tracking.

Hashing Body Lines

A new body recipe item:

`['c', start, end]` - existing

`['z', nlines]` - generate 'n' lines of 'x' (not empty)

A new ranged hash:

Ranged-Hashes: 3:20:sha256:a1b2c3..., 23:501:sha256:d4e5f6...

Changed behaviour:

- Hash each mime part on first hop (or any hop, but trust only goes back to the first hasher of course)
- Can tell THOSE LINES are unchanged even if other parts redacted

Hashed Body Properties

- Only “trust” if it’s a complete MIME part of course...
- Can download only start of the message and verify a MIME part (e.g. BODYSTRUCTURE says these lines are the text/html, just verify that)
- Can tell an attachment is un-tampered even after going through security device, so long as the attachment lines can be recreated after

ALTERNATIVE:

- Hash based on IMAP MIME parts instead, but needs all software to understand them.
 - We already work in lines everywhere
- Not too hard to start a separate hasher immediately after each MIME separator until the next one.
 - Just keep leaves; they are what clients care about.