Resource Digest for HTTP

Refreshing RFC 3230

IETF 105 Montréal

draft-ietf-httpbis-digest-headers

Digest HTTP Header Field

- defined in 2002 by RFC3230 (Mogul)
- algorithms updated in 2010 via rfc5843
- based on "entity" and "instance" terminology, now inconsistent with RFC723x and http-core
- a hash of representation-data ~ payload body

An example

```
Request:
  GET /items/123

Response:
  HTTP/1.1 200 Ok
  Content-Type: application/json
  Content-Encoding: identity
  Digest: sha-256=X48E9qOokqqrvdts8nOJRJN3OWDUoyWxBf7kbu9DBPE=

  {"hello": "world"}
```

Digest Algorithm
ADLER32
CRC32c
MD5
SHA
SHA-256
UNIXsum
UNIXcksum

https://www.iana.org/assignments/http-dig-alg/http-dig-alg.xhtml

The "new" digest

- Minimal changes to improve clarity
- Same semantic, RFC723x terminology

```
"entity" -> "representation"
```

```
"instance" -> "(selected) representation data"
```

- Examples to clarify usage with Range-Requests and different Content-Encodings

- Security Considerations for Signatures and PATCH

Algorithms

Weak algorithms

SHA1, MD5 now NOT RECOMMENDED

New content-coding-independent algorithms

id-sha-256 and id-sha-512

Open Issues Needing Input

- #851 - consider describing use with HTTP signatures
- #853 - digest & PATCH
- #850 - digest-algorithm parameters spec gap
- #849 - digest of an empty representation
- #855 - use Structured Headers (sparingly)
- #828 - deprecate ADLER32?
- #832 - citing SHA-
- #852 - add a threat model?
-

divisiveness

https://github.com/httpwg/http-extensions/issues?q=is%3Aissue+is%3Aopen+label%3Adigest-headers

Thanks from the yak-shavers

Roberto Polli - robipolli@gmail.com

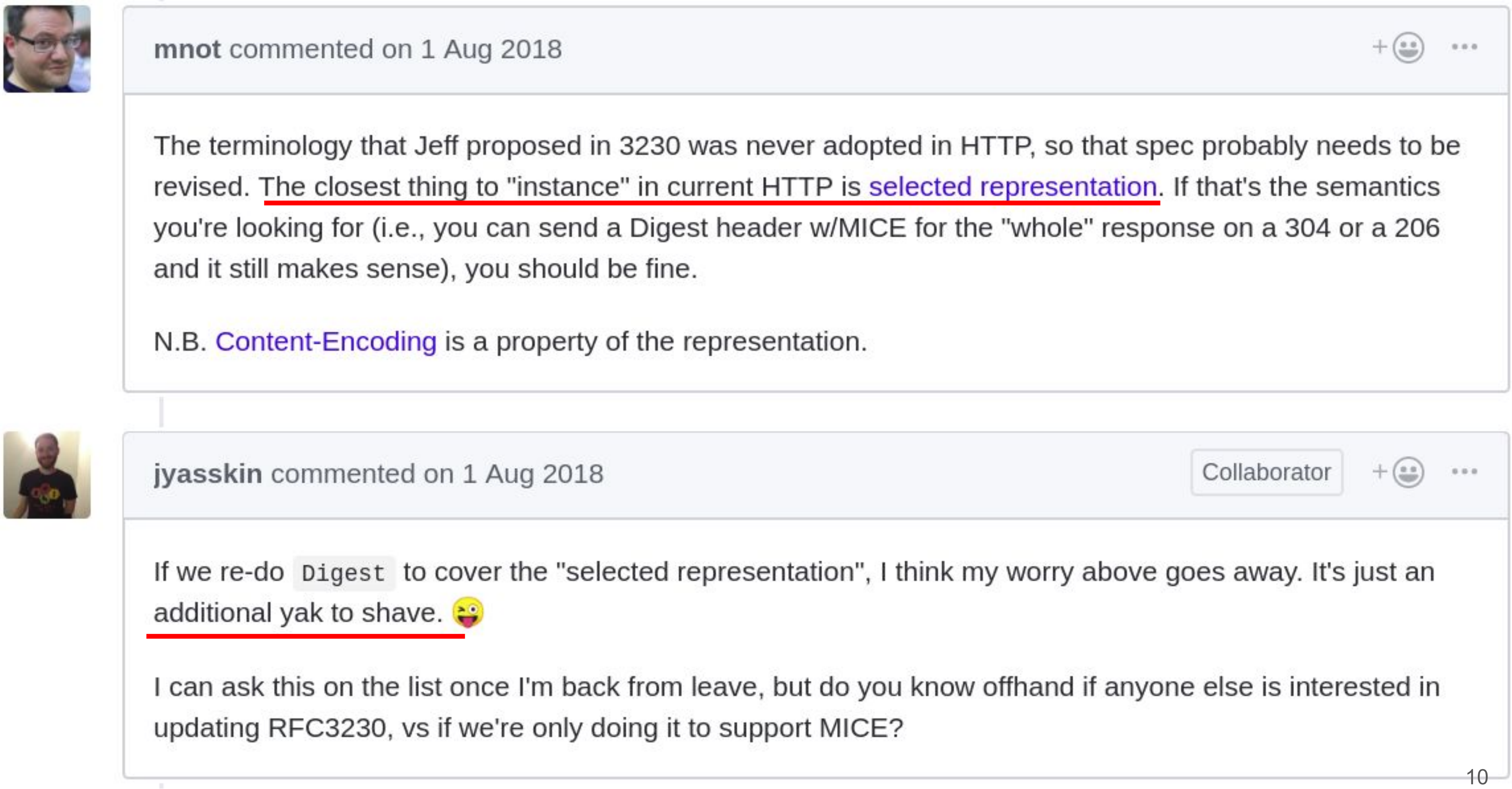
Lucas Pardue - lucaspardue.24.7@gmail.com

© rjccartoons | Dreamstime.com

Backup slides

Who is using Digest?

- Signature specs: http-signatures, signed-exchanges
- MICE content-coding
- Banking APIs via http-signatures



mnot commented on 1 Aug 2018

The terminology that Jeff proposed in 3230 was never adopted in HTTP, so that spec probably needs to be revised. The closest thing to "instance" in current HTTP is selected representation. If that's the semantics you're looking for (i.e., you can send a Digest header w/MICE for the "whole" response on a 304 or a 206 and it still makes sense), you should be fine.

N.B. Content-Encoding is a property of the representation.

jyasskin commented on 1 Aug 2018

If we re-do `Digest` to cover the "selected representation", I think my worry above goes away. It's just an additional yak to shave. 😜

I can ask this on the list once I'm back from leave, but do you know offhand if anyone else is interested in updating RFC3230, vs if we're only doing it to support MICE?