Digest Headers

(was: Resource Digests, was: RFC 3230)

HTTPWG Interim

draft-ietf-httpbis-digest-headers

[see IETF106 slides] [see the specifications]

Who is using Digest?

- MICE content-coding (draft-thomson-http-mice)
- Signature specs: http-signatures, signed-exchanges (draft-yasskin-http-origin-signed-responses)
- Banking APIs via http-signatures

Changes in 02

- Editorial sweep

1. Emphasis on Representation Digest
2. Digest of error responses
3. Use http-core terminology

We need some help to move on!

Open Issues Needing Input

Low hanging fruit

- #936/#937 - relationship with validators/cache
- #850 - digest-algorithm “parameter” spec gap

Not straightforward

- #970 - Is POST behavior extensible to all payload bodies?

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

#850 - digest-algorithm “parameter” spec gap

RFC3230 states the following and we import it verbatim:

```
For some algorithms, one or more parameters may be supplied.

      digest-algorithm = token

The BNF for "parameter" is as is used in RFC 2616 [4].  All
digest-algorithm values are case-insensitive.
```

Problems:

- No example of parameter, anywhere.
- Reference to BNF needs updating

#936/#937 - Cache, Digest and cache-validators

RFC 3230 states the following:

> The instance is specified by the Request-URI and **any cache-validator** contained in the message.

we translated it in to RFC 723x terms:

> The resource is specified by the effective request URI and **any validator field** contained in the message.

But how **do** validators specify a resource? Is "specify" the correct term?

Open Issue #970 - Is POST behavior extensible to all payload bodies?

Julian - "*I just don't think that it would be a good idea to vary the semantics based on the request method.*"

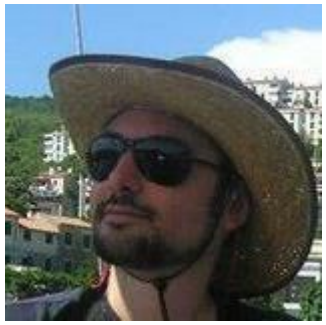
We can address this with some rewording but should we? E.g

Does a present or future method convey a partial representation, and if so the digest should always be computed on the complete representation.

Thanks!

Roberto Polli - robipolli@gmail.com

Lucas Pardue - lucaspardue.24.7@gmail.com



Digest HTTP Field summary

```
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

encoded digest output