

Digest Headers

(was: Resource Digests, was: RFC 3230)

HTTPWG Interim 2020-10

draft-ietf-httpbis-digest-headers

[\[see interim slides\]](#) [\[see IETF106 slides\]](#) [\[see the specifications\]](#)

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

- **03**: Allow Digest in trailers #1157. Deprecate SHA-1 and contentMD5
- **03**: Removed references to validators as they are implied by HTTP [#936/#937](#),
- **03**: Digest-algorithms are always case-insensitive but now the lower case is preferred
- **04**: Added Algorithm agility and improve considerations on encryption
- **04**: Obsolete parameters in Digest (eg. sha-256=fafafa;~~b=1.0~~) [#850/#1259](#)

Open Issues Needing Input

- [#970](#) - Is POST behavior extensible to all methods?
- [#1208](#) - Can Intermediaries alter Digest?
- [#1221](#) - forbid duplicate digest-algorithms, eg

Digest hash=256/babc..., hash=512/babc...

Open Issue [#970](#) - Digest semantics depends on method?

Following RFC3230, if a request contains a partial representation, Digest is computed on the complete representation-data: [this I-D doesn't change that.](#)

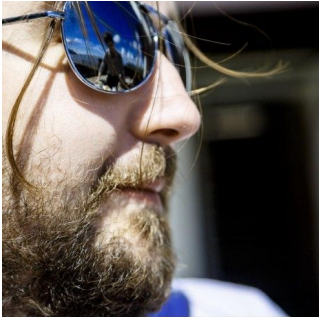
POST and PATCH do not carry partial representations but complete representations of actions/patch documents, so Digest is actually computed on the payload body.

Julian [suggests](#) to extend this behavior to all requests: "*even [...when a method can carries a partial representation...] Digest request [...] field would still reflect the contents of the payload, in this case the partial payload.*"

Thanks!

Roberto Polli - robipolli@gmail.com

Lucas Pardue - lucaspardue.24.7@gmail.com



© rjccartoons | Dreamstime.com



Backlog

id- prefix for digest-algorithms: should we strip id-sha-256? [#885](#)

obsolete all non crypto-algorithms but crc32c (eg. sum, cksum, unixcksum)

Hints for transitioning to Structured-Fields (eg. a new Digest-SF header,