Digest Headers

(was: Resource Digests, was: RFC 3230)

HTTPWG Interim 2021-09

draft-ietf-httpbis-digest-headers

[last interim slides] [latest editor copy]
Since June 2021 Interim

Almost ready for Working Group Last Call.

Thanks for the reviews and feedback.

See

Two different fields ✅

Content-Digest: always computed on the message content in both requests and responses, like Content-MD5 see #1543

Digest: computed on the complete representation data retaining consistency with RFC3230; can support future methods standardizing partial representations in requests; it is useful.

Both fields have a Want-* twin.
Old algorithms (again) #1671

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>sha-256</td>
<td>standard</td>
</tr>
<tr>
<td>sha-512</td>
<td>standard</td>
</tr>
<tr>
<td>md5</td>
<td>deprecated🚫</td>
</tr>
<tr>
<td>sha</td>
<td>deprecated🚫</td>
</tr>
<tr>
<td>unixsum</td>
<td>deprecated🚫</td>
</tr>
<tr>
<td>unixcksum</td>
<td>deprecated🚫</td>
</tr>
<tr>
<td>crc32c</td>
<td>deprecated🚫</td>
</tr>
<tr>
<td>adler32</td>
<td>deprecated🚫</td>
</tr>
</tbody>
</table>

Q: don't forbid old algorithms to support weak consistency cases (eg. checksum-only, insecure, ... )

Waiting for Mark's proposal
id- algorithms: retain or strip?

Do we want to retain id-sha-* algorithms?

Do we want to strip them to another I-D #885 reserving the `id-` prefix?
Towards WGLC

The editors wish to WGLC soon after this interim meeting.

Any choice on those open issues should not block the last call.
Thanks!

Roberto Polli - robipolli@gmail.com

Lucas Pardue - lucaspardue.24.7@gmail.com