# HTTP Problem Types for Digest Fields

Marius Kleidl, Lucas Pardue, Roberto Polli
IETF 123, 23 July 2025

draft-ietf-httpapi-digest-fields-problem-types

# RFC 9530: Digest Fields

- Request can include integrity fields with one or multiple digests
- `Repr-Digest` for representation data
- `Content-Digest` for message content

- No standard method for signaling integrity-related errors back to client

```
PUT /items/123 HTTP/1.1
Host: foo.example
Content-Type: application/json
Repr-Digest:
sha-256=:RK/0qy18MlBSVnWgjwz6lZEWjP
/lF5HF9bvEF8FabDg==:

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

# RFC 9457: Problem Details for HTTP APIs

- Machine-readable description of problem
- Encodable in JSON or XML
- Problem is identified by a specific type

  (maybe from the problem details registry)
- Problem may include additional details

```
HTTP/1.1 403 Forbidden
Content-Type: application/problem+json
Content-Language: en

{
 "type": "https://[..]/prob/out-of-credit",
 "title": "You do not have enough credit.",
 "detail": "Your current balance is 30, but
that costs 50.",
 "instance": "/account/12345/msgs/abc",
 "balance": 30,
 "accounts": ["/account/12345",
              "/account/67890"]
}
```

# Example: Mismatching digest values

Request:

```
PUT /items/123 HTTP/1.1
Host: foo.example
Content-Type: application/json
Repr-Digest: sha-256=:RK/0qy18MlBSVnWgjwz6lZEWjP/lF5HF9bvEF8FabDg==:
Content-Digest: sha-256=:RK/0qy18MlBSVnWgjwz6lZEWjP/lF5HF9bvEF8FabDg==:

{"hello": "woXYZ"}
```

# Example: Mismatching digest values

Response:

```
HTTP/1.1 400 Bad Request
Content-Type: application/problem+json

{
  "type": "https://iana.org/assignments/http-problem-types#digest-mismatching-values",
  "title": "Mismatching digest values",
  "mismatching-digests": [
    {
      "algorithm": "sha-256",
      "provided-digest": ":RK/0qy18MlBSVnWgjwz6lZEWjP/lF5HF9bvEF8FabDg=:",
      "header": "Repr-Digest"
    },
    {
      "algorithm": "sha-256",
      "provided-digest": ":RK/0qy18MlBSVnWgjwz6lZEWjP/lF5HF9bvEF8FabDg=:",
      "header": "Content-Digest"
    }
  ]
}
```

# Allow reporting problems on multiple digests (#5)

- Requests can include multiple integrity fields (`Content-Digest, Repr-Digest, Want-Content-Digest, Want-Repr-Digest`)
- Each field can contain multiple digests/algorithms
  - ➢ Multiple problems of same type in one request are possible
  - ➢ Response can now carry information about multiple instances of the same problem

# New digest: `Unencoded-Digest`

- Digest of unencoded representation (i.e. without Content-Encoding)
- draft-pardue-httpbis-identity-digest adopted by httpbis WG

➢ Do we have to update this draft (or wait)?

# New digest: `Unencoded-Digest`

- Digest of unencoded representation (i.e. without Content-Encoding)
- draft-pardue-httpbis-identity-digest adopted by httpbis WG

➢ Do we have to update this draft (or wait)?

- I don’t think so.
- RFC 9530 defines *integrity (preference) fields*
- draft-ietf-httpapi-digest-fields-problem-types used these definitions
- draft-pardue-httpbis-identity-digest would update these definitions

➢ We are good to go for the future

# Next steps

- WGLC