

# HTTP Problem Types for Digest Fields

Marius Kleidl, Lucas Pardue  
IETF 120, 25 July 2024

# 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
```

```
/1F5HF9bvEF8FabDg==:
```

```
{"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/1F5
HF9bvEF8FabDg==:

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

## Response:

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

{
  "type":
    "https://[...]#mismatching-digest-value",
  "title":
    "mismatching digest value",
  "algorithm":
    "sha-256",
  "provided-digest":
    " :RK/0qy18MlBSVnWgjw[...]EF8FabDg=",
  "calculated-digest":
    " :d435Qo+nKZ+gLcUHn7t[...]AgPiTGpK="
}
```

# HTTP Problem Types for Digest Fields

- Small number of high level problem types:
  - Mismatching digest values
  - Unsupported hashing algorithm
  - Invalid digest value
- Building blocks for other work (inside and outside of IETF)
- Potentially useful for HTTP Message Signatures (RFC 9421)
- Is there interest in this?