HTTP Problem Types for Digest Fields

Marius Kleidl, Lucas Pardue, Roberto Polli
IETF 122, 19 March 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/lF5
HF9bvEF8FabDg==:

{"hello": "wo"XYZ"}
```

Response:

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

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

Don’t expose calculated digest (#3)

- Exposing the calculated digest opens the door for information leakage and oracle attacks
- Attacker can learn about the input to the hashing algorithm

- Let’s remove it from the problem type

Response:

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

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

Problem Types for Message Signatures (RFC 9421)? (#2)

- At IETF 121 Justin Richer presented HTTP Message Signatures (RFC 9421) (recording)
- Technical overlap between message signatures and digest fields
- Should this draft also include problem types for message signatures?
- Issues with that:
    - Signatures are much more complex than digest fields
    - More attack vendors possible through problem types for signatures
    - HTTP messages can include digest fields and signatures, necessitating a way to distinguish what caused a problem
- Let’s keep the draft focused on digest fields?