HTTP Message Signatures

Justin Richer & Annabelle Backman
IETF 115
November 6, 2022

Since Last We Met

- Lots of editorial updates
- More examples
- Added "tag" parameter
- WGLC

Trailers?

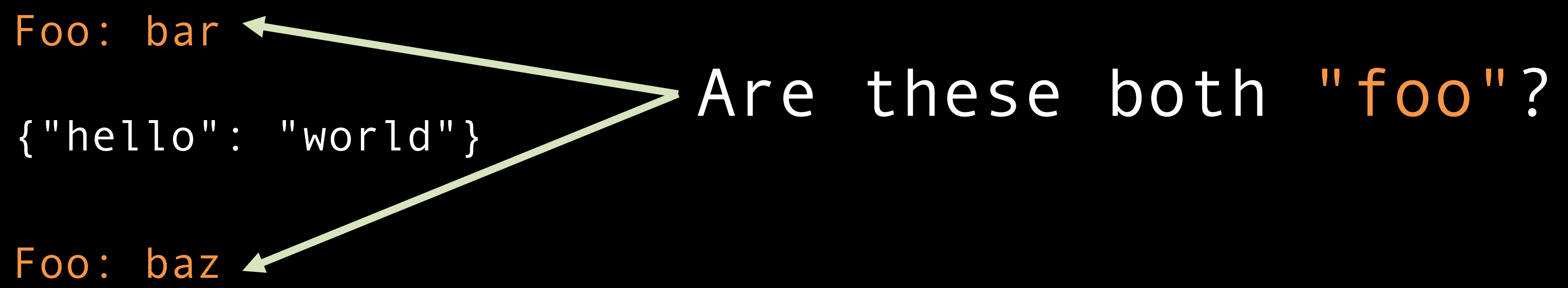
- Can these be trailers:
  - Signature / Signature-Input
  - Accept-Signature
- Can we sign trailers?
  - Do we mash them into the headers or should we treat them separately?
- *Are they even real?*

Example HTTP Message

```
POST /foo?param=value&pet=dog HTTP/1.1
Host: example.com
Date: Tue, 20 Apr 2021 02:07:55 GMT
Content-Type: application/json
Content-Length: 18
Foo: bar

{"hello": "world"}

Foo: baz
```



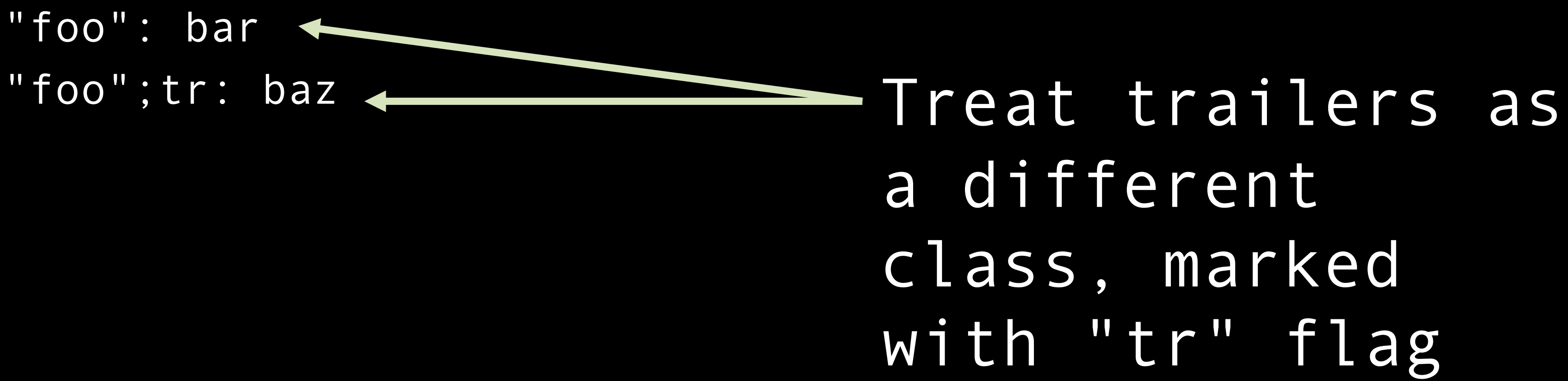
Are these both "foo"?

Signature Base

```
"foo": bar, baz
```

Combine them into a single value

Signature Base



```
"foo": bar
"foo";tr: baz
```

Treat trailers as a different class, marked with "tr" flag

Some Precedent

```
"foo": bar
"foo";req: baz
```

Fields from the request are flagged with "req"

Security Reviews & Implementations

- Presentation to SAAG this Friday
  - Calling for wide review from SEC folks
- Collecting implementations for page on httpsig.org