@justin _ _ richer

https://bspk.io/

HTTP Signing. Again.

Justin Richer

IETF101, London 2018

@justin_richer

https://bspk.io/

draft-ietf-oauth-signed-http-request

draft-ietf-oauth-signed-http-request

- Functional
- Implemented
- Flexible
- Expired
- Unloved

@justin _ _ richer

https://bspk.io/

draft-cavage-http-signatures

@justin _ _ richer

https://bspk.io/

JWT for everything

@justin _ _ richer

https://bspk.io/

draft-yasskin-http-origin-signed-responses

@justin_richer

https://bspk.io/

draft-yasskin-http-origin-signed-responses

- Adds a Signature header to HTTP
- Crypto flexibility (keys and certs)
- Multiple signatures / signers

draft-yasskin-http-origin-signed-responses

- Response only (not request)
- No body/payload protection (that's another draft)
- Tied to certificates and PKI (mostly)

@justin _ _ richer

https://bspk.io/

draft-thomson-http-mice

draft-thomson-http-mice

- Integrity protection of HTTP body
- Progressive integrity proofing (can be appended)
- Alternative to Digest

@justin _ _ richer

https://bspk.io/

None of this supports OAuth

So what now?

- Adapt signed responses to cover requests
- Use existing access token headers
- Use token confirmation key to sign request