HTTP Signing
What are we solving?

- Message-level signature to HTTP requests
- Signature over headers, body, request elements
- Detached
Why are we solving it?

- Key possession proof
- Authentication
- Request message integrity
- Non-repudiation
- Audit
Why is it hard?

• Detached signatures required for HTTP transparency
  – Encapsulation breaks layers
• HTTP messages get transformed
• Common to parse and re-serialize
What about TLS?

• Proxies and reverse proxies
  – TLS protection stops at the terminator

• Mutual TLS doesn’t work for many use cases
  – Certificate deployment issues

• Relayed messages don’t work
What about S/HTTP?

- Wraps the entire request in a signed container
- Duplicates or hides HTTP functions
- Nobody’s heard of it
What about JOSE?

- Wraps whole request in JOSE object
- Duplicates or hides HTTP functions
- It’s SOAP with curly braces
  - Pls no
Options

- Cavage
- OAuth DPoP
- AWSv4
- OAuth PoP
- XYZ
Options

- **Cavage**

- **OAuth DPoP**

- **AWSv4**

- **OAuth PoP**

- **XYZ**
# "Standards"

<table>
<thead>
<tr>
<th></th>
<th>Cavage</th>
<th>OAuth DPoP</th>
<th>OAuth PoP</th>
<th>XYZ</th>
<th>AWSv4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method</strong></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td>Y (request)</td>
<td>Y (request)</td>
<td>Y (parsed)</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Headers</strong></td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Body</strong></td>
<td>Y (Digest header)</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Token</strong></td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y?</td>
<td>Y</td>
</tr>
<tr>
<td><strong>Keys</strong></td>
<td>Sym/Asym</td>
<td>Asym</td>
<td>Sym/Asym</td>
<td>Asym</td>
<td>Sym</td>
</tr>
<tr>
<td><strong>Draft</strong></td>
<td>ID (External Development)</td>
<td>ID (Pending WG)</td>
<td>WG Draft (Expired)</td>
<td>ID</td>
<td>Proprietary</td>
</tr>
</tbody>
</table>
Cavage Signature Drama

- draft-cavage-http-signatures published
- Used by editors in web payments draft specifications (W3C)

2013

- Used by a number of different separate efforts

2014+

- Adopted by EU financial API standards groups (Polish API, Berlin Group)

2018

- Editors of draft publish major updates in draft -11
- Everyone using it freaks out and pegs to draft -10

2019

- People realize that this isn't really a standard yet
- We figure out how to make this into a real standard?

2019+
What should we do?

- Combine drafts?
- Find a WG?
- Found a WG?