Signing HTTP Requests and Responses

Dave Tonge, OAuth Security Workshop 2019

Use case:

Non-repudiation for backend JSON API calls

Example 1: A payment request sent as a JSON payload to an API endpoint

Example 2: A JSON API response from a bank containing the financial information.

1. Just use a JWT (maybe with content-negotiation)
2. Detached JWT (RFC7515 appendix-F)
3. Detached JWT unencoded payload (RFC7797)
4. Unencoded JWS JSON Serialization (RFC7797)
5. Draft-Cavage-HTTP-Signing combined with RFC7235 (Auth header) and RFC3230 (Digests)
6. JSON Canonicalisation + SHREQ

Scheme	Self-Contrained	Human Readable	Deals with accidental body corruption	Deals with accidental header corruption	Uses JOSE
JWT	■		■	■	■
Detached JWT		■		■	■
Detached Unencoded		■		■	■
Unencoded JSON Serialisation	■	■		■	■
Draft Cavage		■			
JCS + SHREQ	■	■	■	■	■