OAuth PoP Signing

Justin Richer

IETF97
Parallels with Bearer tokens

• Getting a token (6749)
  – Now getting a token + key

• Using a token (6750)
  – Now present token + signature

• Validating a token (7662, 7519, etc)
  – Now validating token + signature (from key)
Current presentation spec

- Signing
- Presentation
- HTTP Request Protection
Signing a Request

• Create a JSON Object
  – Add access token
  – Add timestamp (or nonce)
• Wrap in JWS
• Sign with token’s key
Presenting a Request

• Place JWS into:
  – Header \texttt{Authorization: PoP [JWS]}
  – Form-body \texttt{pop\_token=[JWS]}
  – Query parameter \texttt{pop\_token=[JWS]}
HTTP Request Protection

• Detached signature mechanism
• Optional coverage for all elements
  – Method, Authority, Path, Query, Headers, Body
• Robust against request manipulation
• Not comprehensive (by design)
• Sign what makes sense for your API
Proposal going forward

• Split into two documents
  – Base signing & presentation
  – HTTP detached signature

• Move both forward separately
Alternate Presentation Mechanisms

• Could use methods other than JWS
  – None defined yet?
  – Don’t wait for theoretical other options