Proof-of-Possession Key Semantics for JWTs

draft-ietf-oauth-proof-of-possession-03

Mike Jones

IETF 93
Prague
July 2015

Addressed WGLC Comments

- Separated the `jwk` and `jwe` confirmation members; the former represents a public key as a JWK and the latter represents a symmetric key as a JWE encrypted JWK.
- Changed the title to indicate that a proof-of-possession key is being communicated.
- Updated language that formerly assumed that the issuer was an OAuth 2.0 authorization server.
- Described ways that applications can choose to identify the presenter, including use of the `iss`, `sub`, and `azp` claims.
- Harmonized the registry language with that used in JWT [RFC 7519].
- Addressed other issues identified during working group last call.
- Referenced the JWT and JOSE RFCs.