

PoP: AS <-> Client Key Distribution

draft-ietf-oauth-pop-key-distribution

John Bradley, Phil Hunt, Mike Jones, Hannes Tschofenig

Open Issues

- Security considerations for the use of PoP tokens with public clients.
- Guidance for use of asymmetric cryptography with resource servers in different origins.
- Allow client to tell server which key to associate with access token.
- We want to have an access token bound to a key. We want to allow a client to request a new PoP access token based on a refresh token (without a code). The need for a PoP refresh token may arrive later and may use token binding. Security consideration needs to say that the PoP tokens require confidential clients if requesting new PoP tokens² with different