

PKClient Starts challenge generation protocol

Auth Starts DAGA server's protocol

CreateContext Starts context generation protocol

RPC: protocol buffers over websockets

Entity/Client

runs daga client's protocol:

- 1) build initial tag
- 2) interactive proof of knowledge (call PKClient to obtain (honest) challenge in exchange of commitments)
- 3) create auth. request
- 4) call Auth
- 5) receive final tag

3rd-party service's admin

- 1) collect public keys of clients/subscribers (- administrative partnership with conode admins)
- 2) call CreateContext
- 3) receive auth. context