Privacy Pass Metadata

https://github.com/ietf-wg-privacypass/base-drafts/issues/63

Metadata properties

Both client (C) and server (S) may have public and private metadata

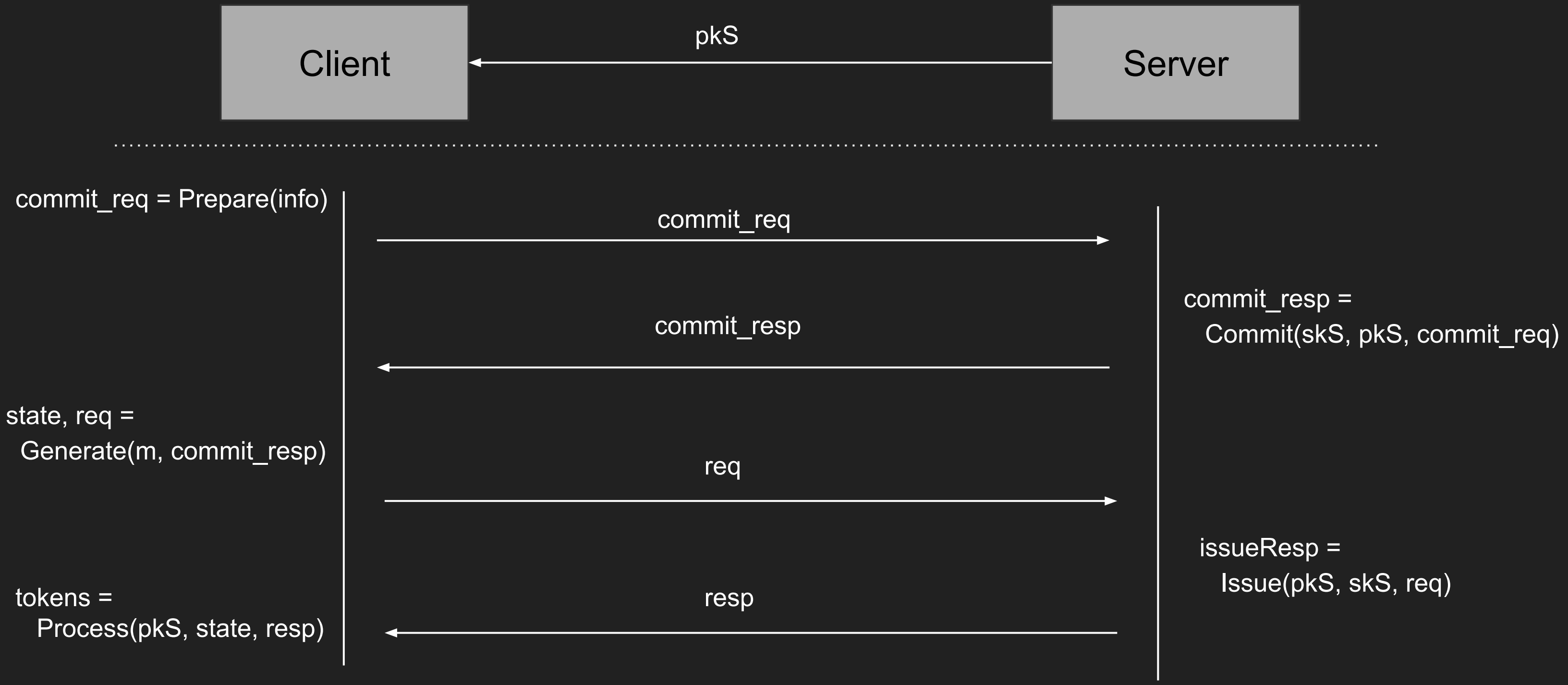
Underlying constructions exist with differing metadata support

- VOPRF protocol *does not* permit any public metadata
- PMBToken protocol permits a single server private metadata bit
- PrivateStats and AT with Public Metadata permit arbitrary public metadata

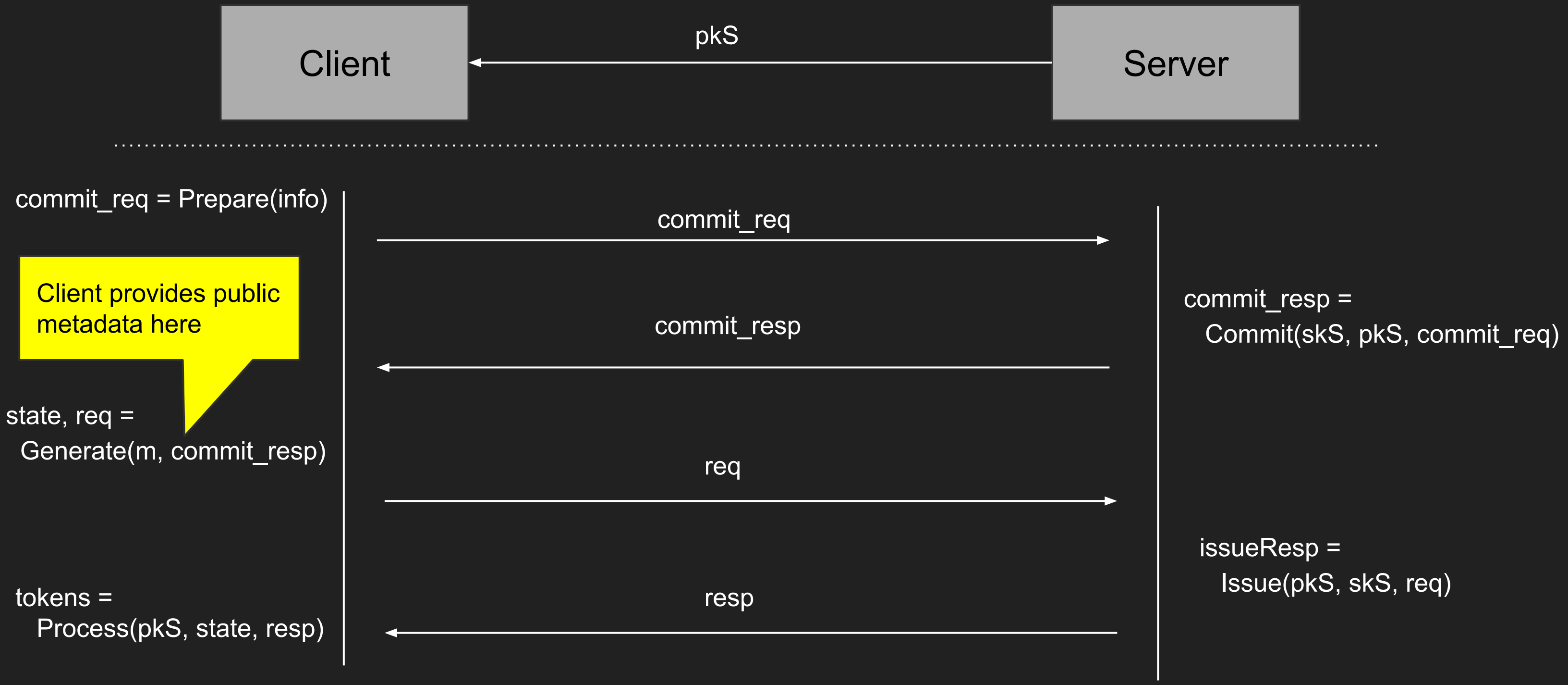
Ideally tokens are bound to different metadata:

$$\boxed{\text{tokens} = F(\text{C priv}, \text{C pub}, \text{S priv}, \text{S pub})}$$

Protocol


pkS
Client
Server
commit_req = Prepare(info)
commit_req
commit_resp
commit_resp =
Commit(skS, pkS, commit_req)
state, req =
Generate(m, commit_resp)
req
issueResp =
Issue(pkS, skS, req)
resp
tokens =
Process(pkS, state, resp)

Protocol



Client

pkS

Server

commit_req = Prepare(info)

commit_req

commit_resp =
  Commit(skS, pkS, commit_req)

commit_resp

Client provides public metadata here

state, req =
  Generate(m, commit_resp)

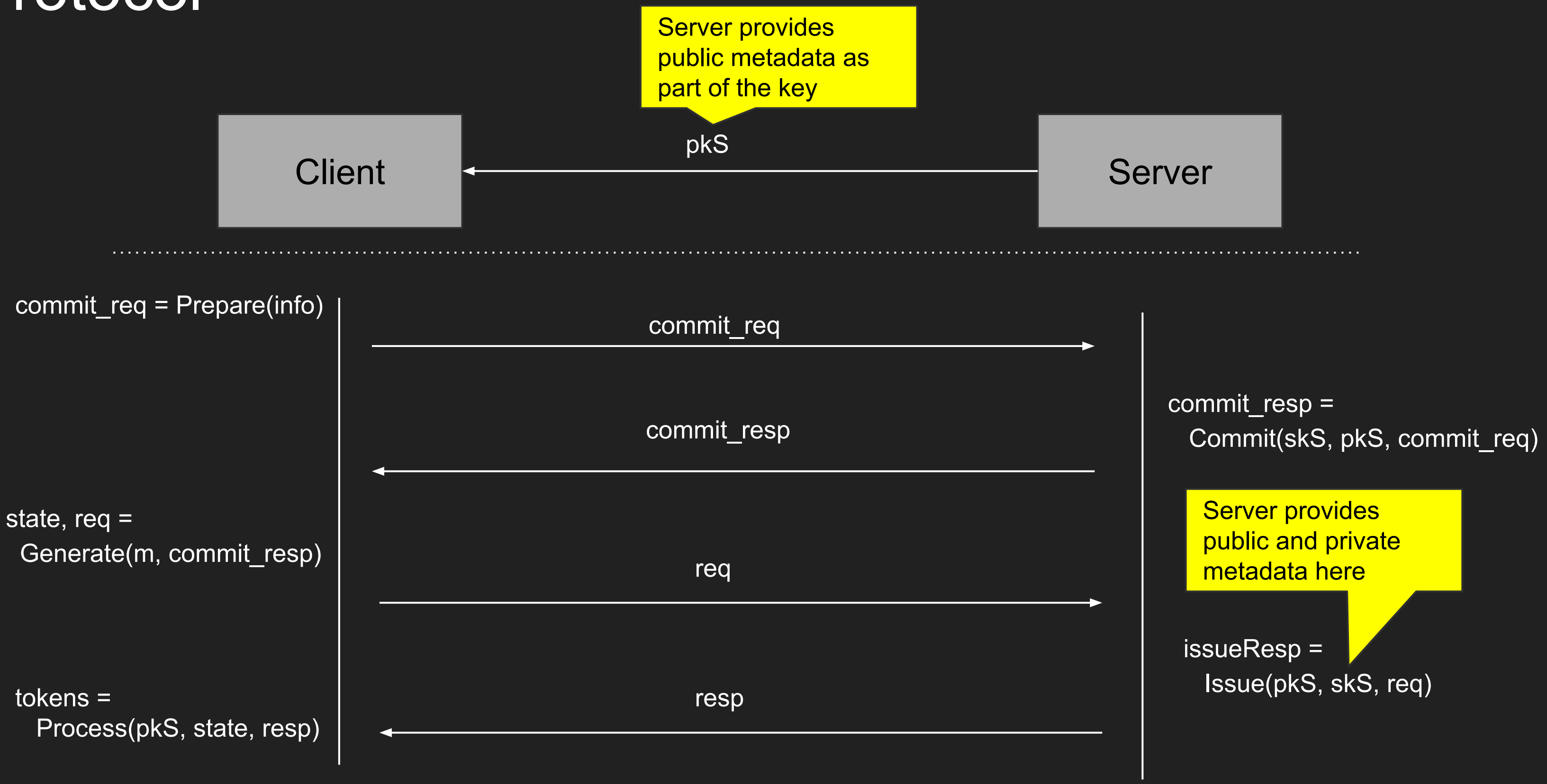
req

issueResp =
  Issue(pkS, skS, req)

resp

tokens =
  Process(pkS, state, resp)

Protocol



Server provides public metadata as part of the key

pkS

Client

Server

commit_req = Prepare(info)

commit_req

commit_resp

commit_resp =
  Commit(skS, pkS, commit_req)

Server provides public and private metadata here

state, req =
  Generate(m, commit_resp)

req

issueResp =
  Issue(pkS, skS, req)

tokens =
  Process(pkS, state, resp)

resp

Questions

Should the API support arbitrary client and server metadata, and if so, how?

Should metadata limits be imposed by protocol, underlying cryptographic construction, or both?

- PMBTokens permit only a single private bit
- PrivateStats and AT permit arbitrary many public bits

What sort of guidance should the protocol or architecture give about the metadata limits?