Privacy Pass Metadata

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

\[
\text{tokens} = F(C \text{ priv}, C \text{ pub}, S \text{ priv}, S \text{ pub})
\]
commit_req = Prepare(info)

state, req = Generate(m, commit_resp)

tokens = Process(pkS, state, resp)

commit_resp = Commit(skS, pkS, commit_req)

issueResp = Issue(pkS, skS, req)
Protocol

commit_req = Prepare(info)

commit_req = Commit(skS, pkS, commit_req)

state, req = Generate(m, commit_resp)

req = Issue(pkS, skS, req)

tokens = Process(pkS, state, resp)

resp = Issue(pkS, skS, req)

Client provides public metadata here
commit_req = Prepare(info)

state, req = Generate(m, commit_resp)

tokens = Process(pkS, state, resp)

Server provides public metadata as part of the key

Server provides public and private metadata here

commit_resp = Commit(skS, pkS, commit_req)

issueResp = Issue(pkS, skS, req)
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?