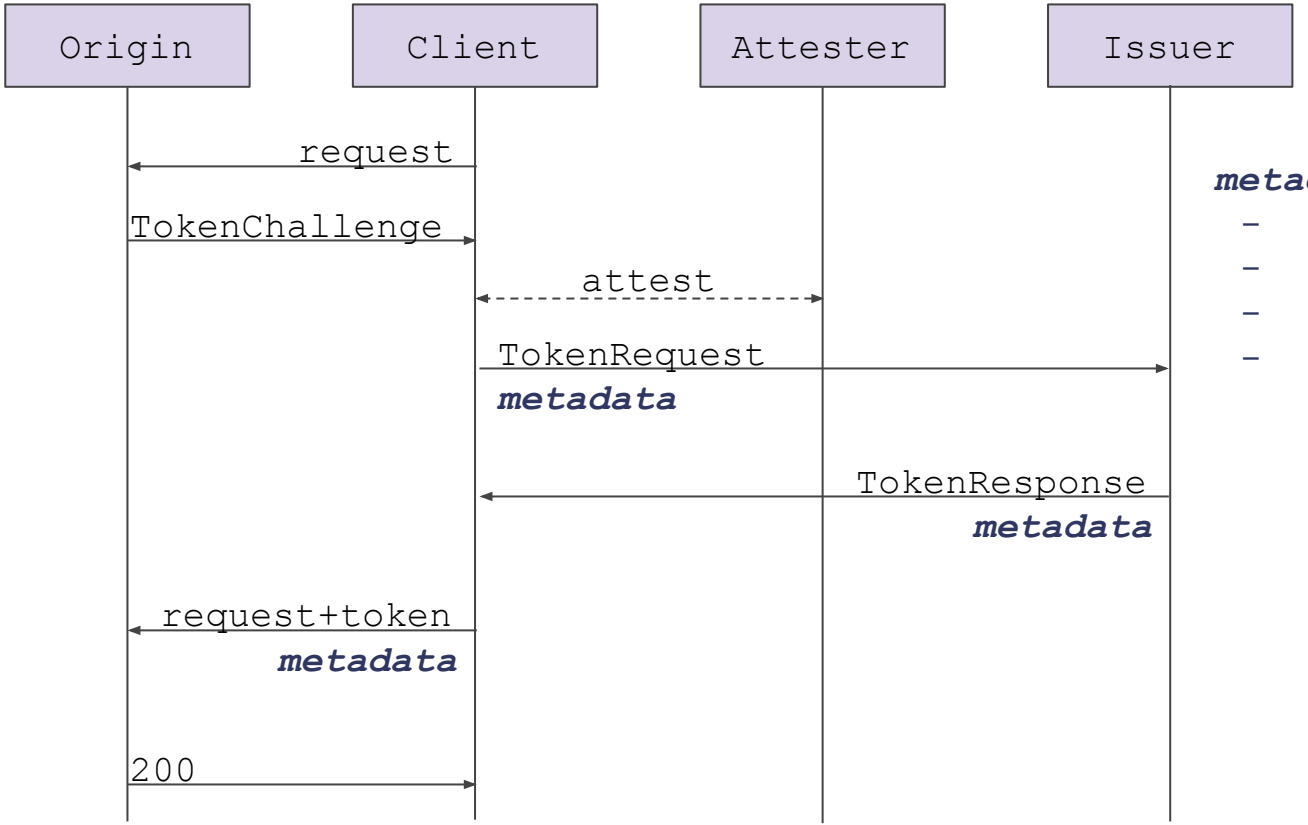
Public Metadata Tokens

based on draft-amjad-cfrg-partially-blind-rsa

Scott Hendrickson with help from Ghous Amjad, Christopher Wood, Kevin Yeo

IETF 116 - Privacy Pass



metadata

- visible to all parties
- encodes arbitrary bits
- any party may reject
- deployment specific

Motivation

- Token Type Blind RSA (0x02) enables public verification
  - Differentiating groups of clients with 0x02 requires issuer per group
  - Token expiry bound by speed of key rotation
  - Public key must propagate completely to origins

- Similar deployments can share issuers
- Deployments can avoid quick key rotation
  - Particularly with cached redemption context

Implementation

- draft-amjad-cfrg-partially-blind-rsa proposes an RSA based protocol that is:
  - Publicly verifiably
  - Allows for public metadata
- Propose a new token type (0xDA7A) that employs draft-amjad-cfrg-partially-blind-rsa

- 00 in datatracker: draft-hendrickson-privacypass-public-metadata
- https://github.com/smhendrickson/draft-hendrickson-privacypass-public-metadata-issuance