Terminology

**User-Agent** (UA) Web browser accessing Consumer (C). Cannot do any crypto and can only perform requests of the form “Send a, b, c to D”

**Identity** (I) Web server acting as the identity of UA. No crypto and can only return a static webpage

**Consumer** (C) Web server which wants assurance that UA has control over I. Can produce dynamic content and may or may not be able to do crypto

**Server** (S) Web server trusted by I to authenticate user-agents. Should not have to store dynamic state

- $p$ Diffie Hellman prime
- $g$ Diffie Hellman generator

**Association**

**User-Agent**  **Identity**  **Consumer**  **Server**

Choose random $x$

$$p, g, X := g^x$$

Choose random $y, k$

$$g^{xy} = X^y$$

$h, t_v, Y := g^y, K := H(g^{xy}) \oplus k$

$$g^{xy} = Y^x$$

$k = H(g^{xy}) \oplus K$
Check Identity

User-Agent    | Identity    | Consumer | Server

I am I

Who manages you?

S

association (optional)

Send $I, (h), C, n, t$ to $S$

$$I, (h), C, n, t$$

Authenticate to $C$?

Yes, token (e.g. password/cookie)

Send $I, h, C, n, t, HMAC_k(I, C, n, t)$ to $C$

$$I, h, C, n, t, HMAC_k(I, C, n, t)$$

If associated, check MAC otherwise...

$h, HMAC_k(...), ...$

valid/invalid

Unofficial diagram by Steven J. Murdoch [http://www.cl.cam.ac.uk/users/sjm217/]
openid-protocol.tex 2112 2006-05-17 17:49:10Z sjm217