“OpenID: an actually distributed identity system”

http://www.openid.net/

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

x, y Private keys of Consumer and Server

X, Y Public keys of Consumer and Server

h Session handle generated by Server

t_v Validity time chosen by Server

k Session MAC key shared by Consumer and Server

K Encrypted session MAC key

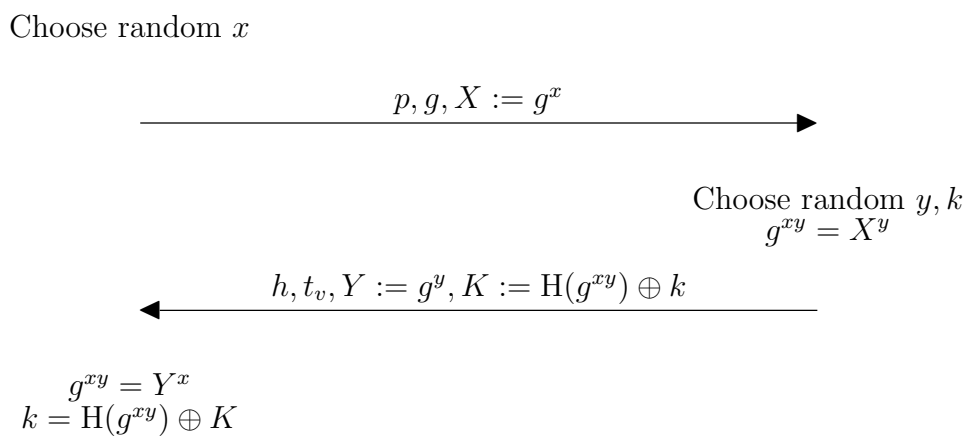
I, C, S Names of Identity, Consumer and Server

t, n Timestamp, Nonce

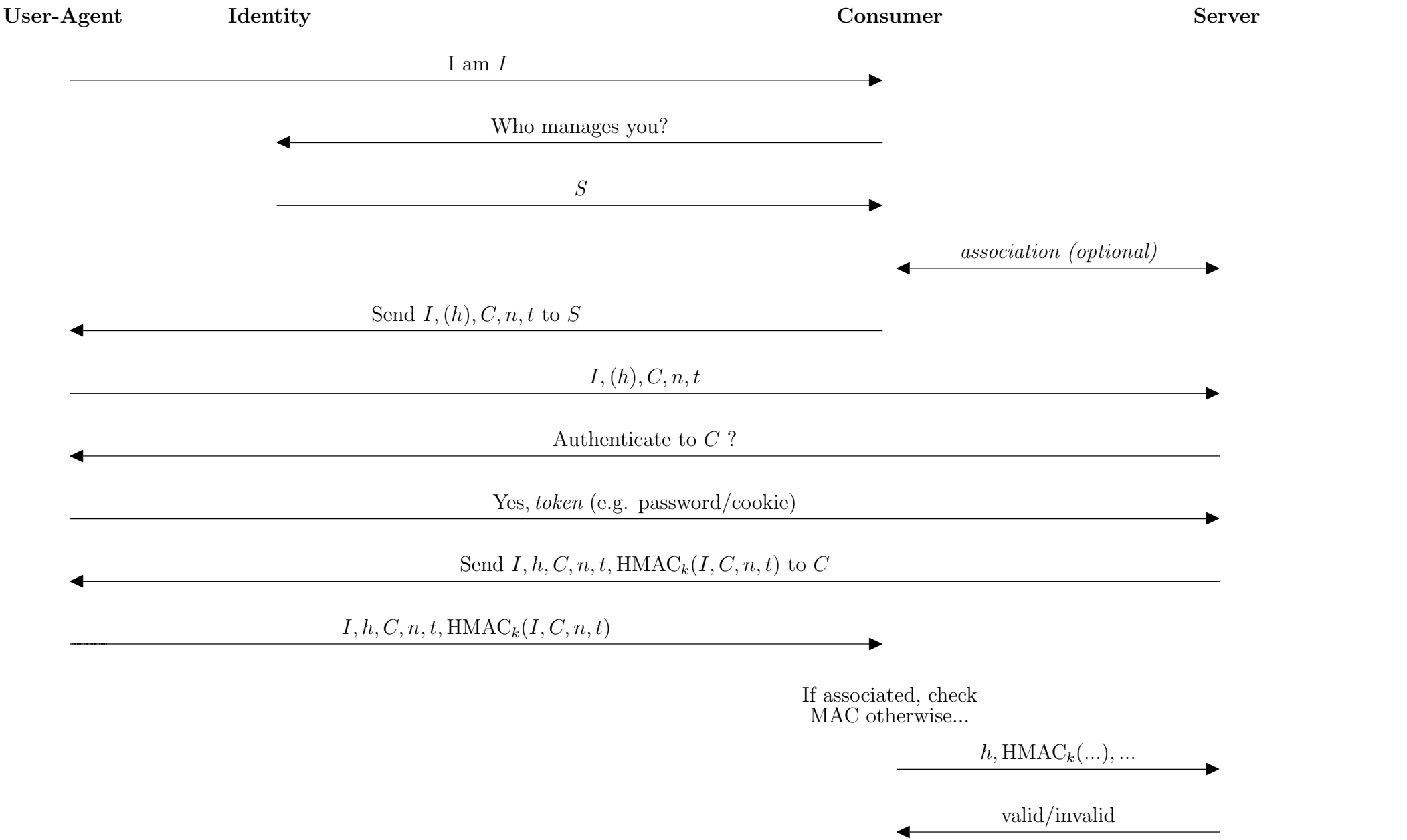
token Authentication token of User-Agent for Server

Association

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



Check Identity



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`