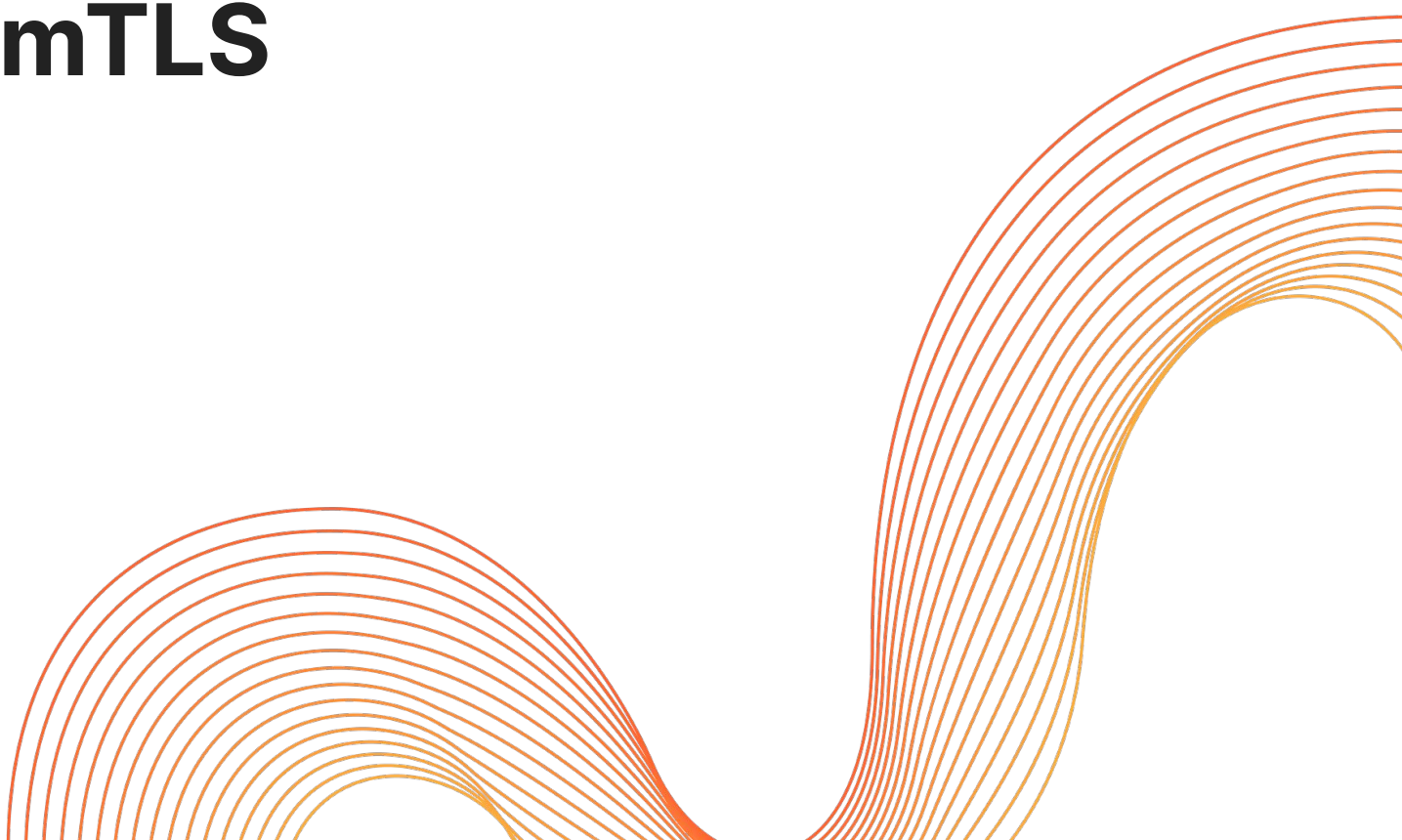
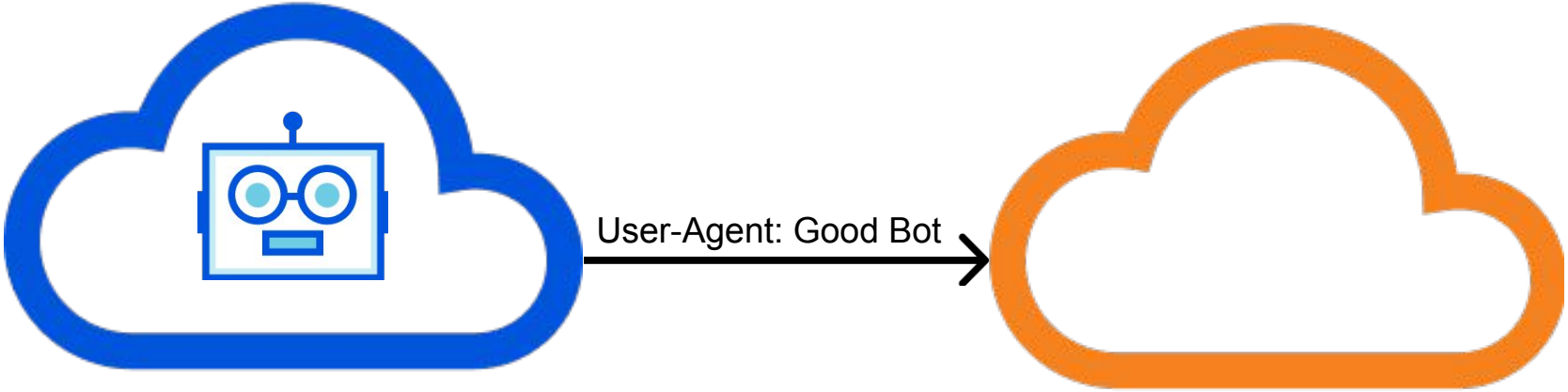
Request mTLS

Jonathan Hoyland

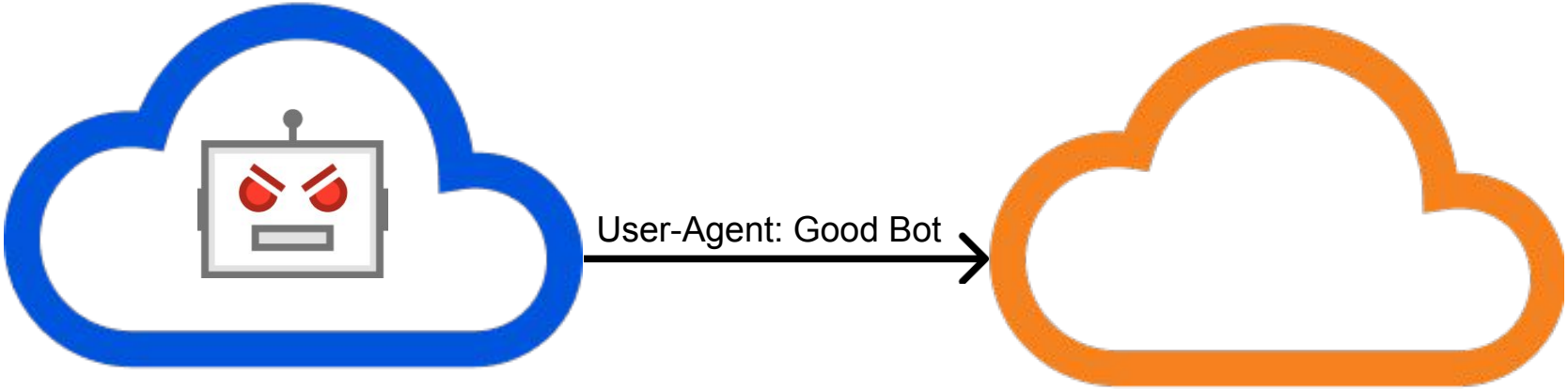


Distinguishing Bots is Hard



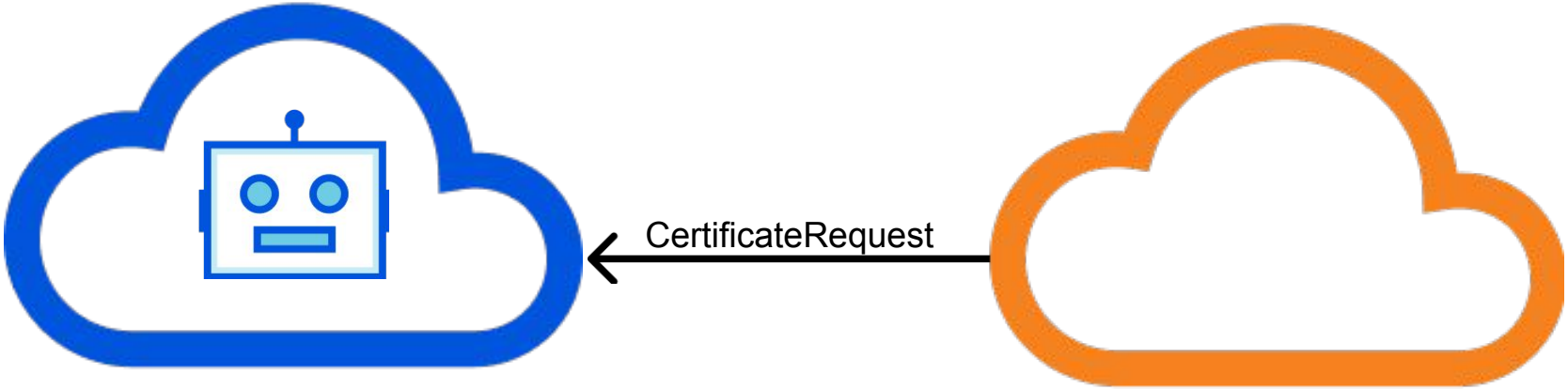
- Many bots come from public clouds
- Bots distinguish themselves by setting a special user agent

Distinguishing Bots is Hard



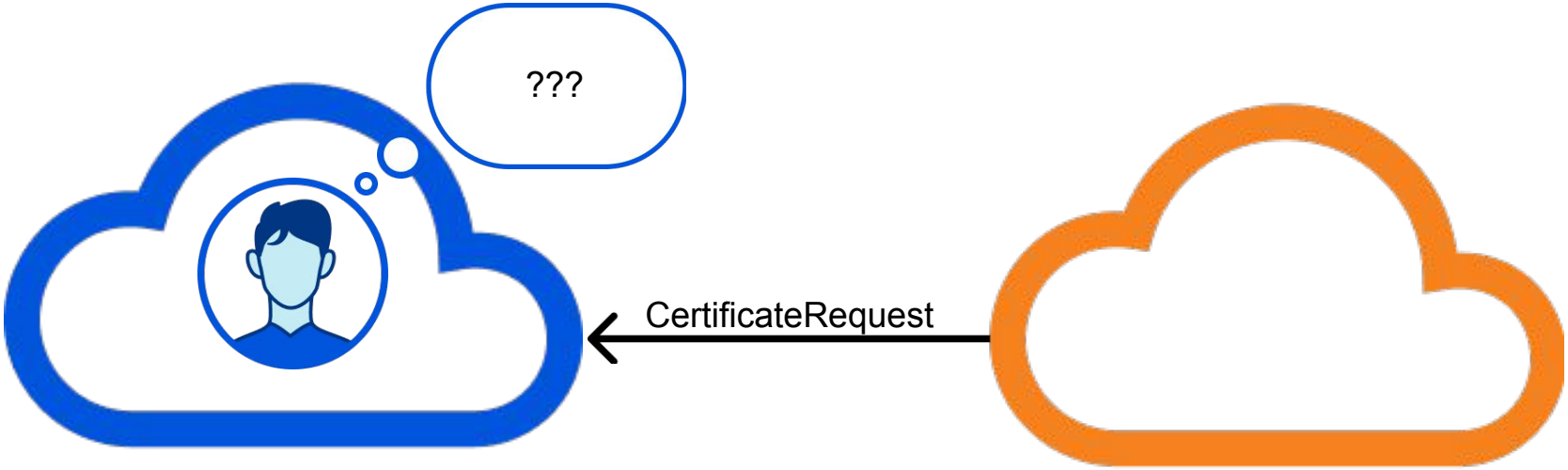
- Both these signals are easy to forge

CertificateRequest lets us Identify Bots



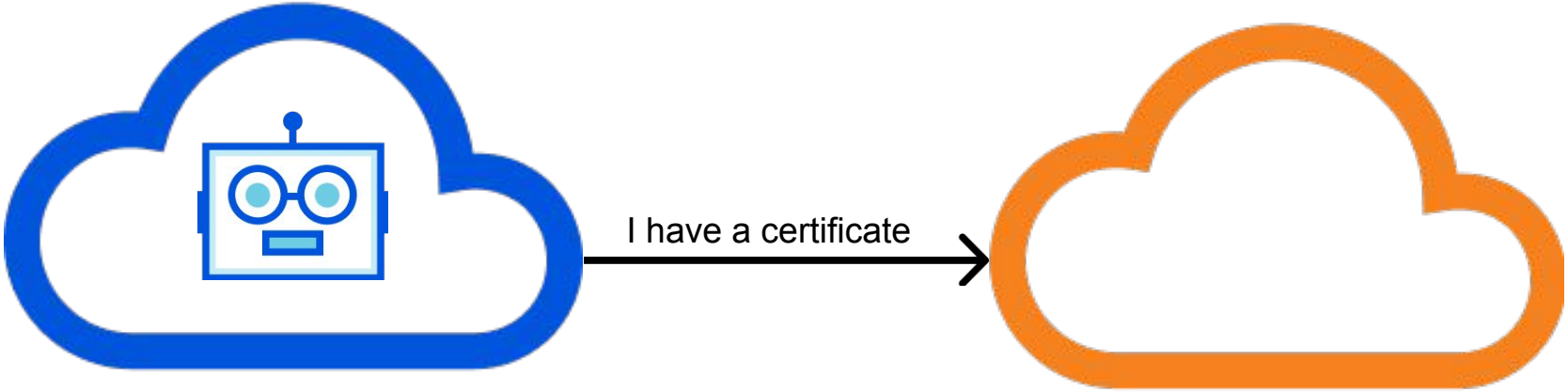
- Mutual TLS needs to be initiated by the server
- Post-handshake auth and Exported Authenticators add an extra RTT

But Humans might be confused



- If we incorrectly send a CertificateRequest to a human they probably won’t know what to do

Request mTLS Flags



- Configure the client to send a hint when a client certificate is available
- TLS Flags is perfect for this

CLOUDFLARE

Questions?

- I have two working interoperable implementations (C and Go)
- Working on open sourcing them
- Demo server running at https://tls-flags.research.cloudflare.com/
- If you send the TLS Flags extension with flag 80 (0×50) set it will ask you for a certificate
- Adoption call?