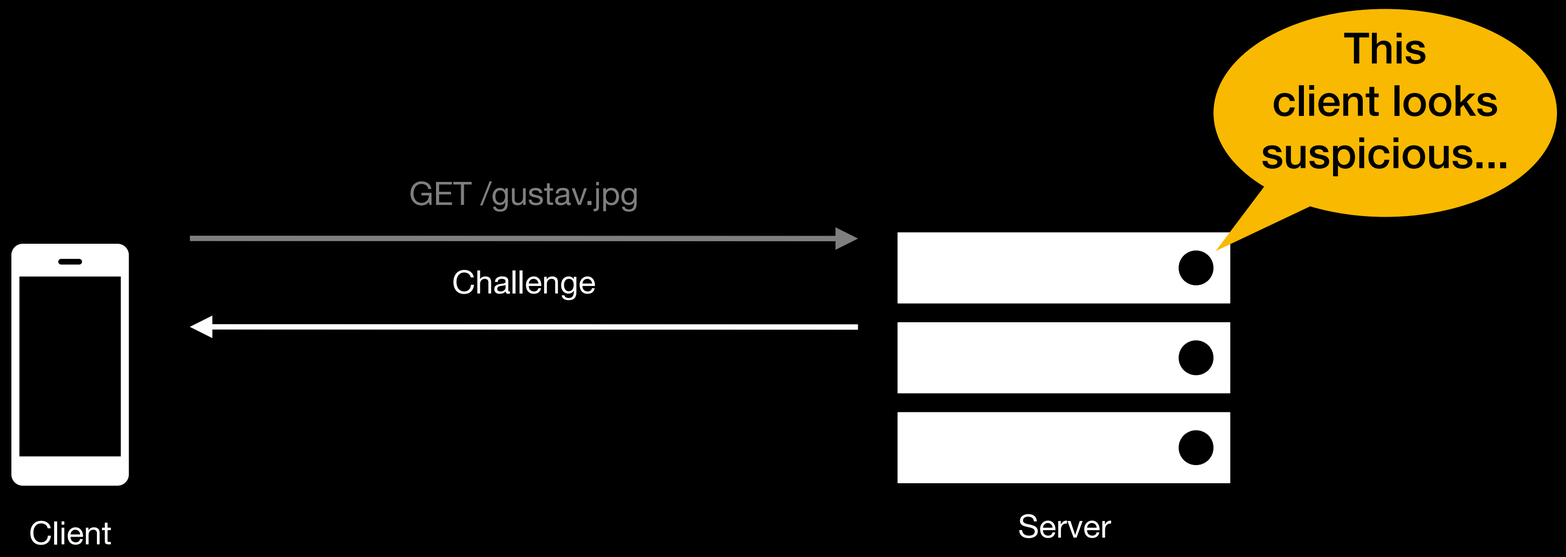
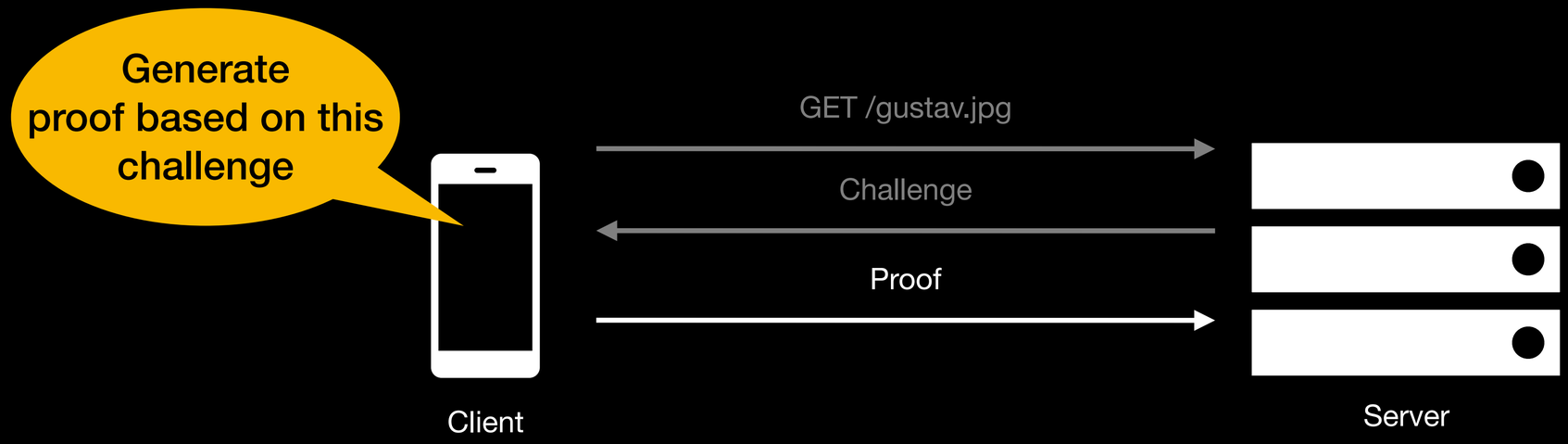
Privacy Pass Architecture and Attestation

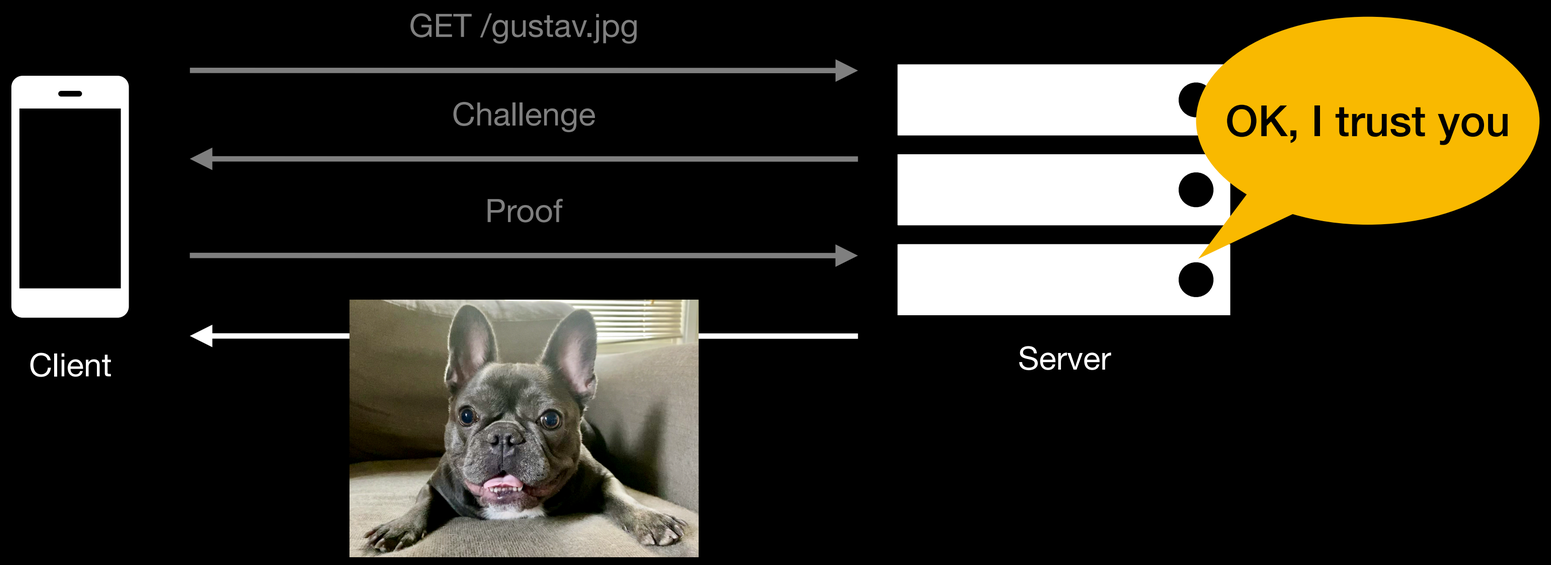
Christopher A. Wood

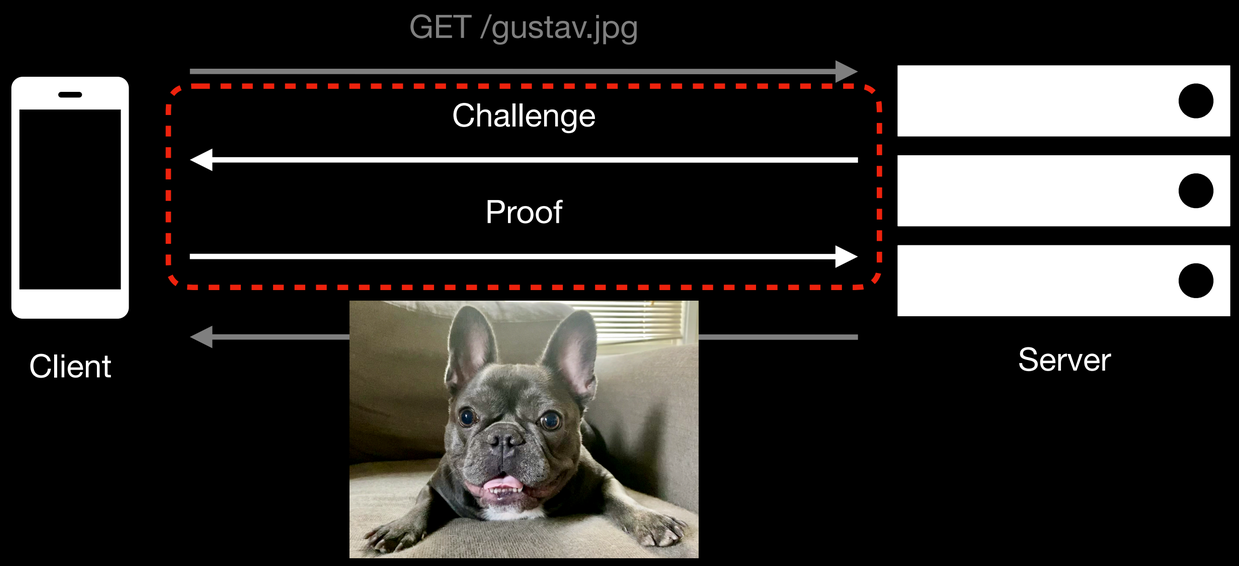
W3C Anti-Fraud CG Meeting - July 8, 2022

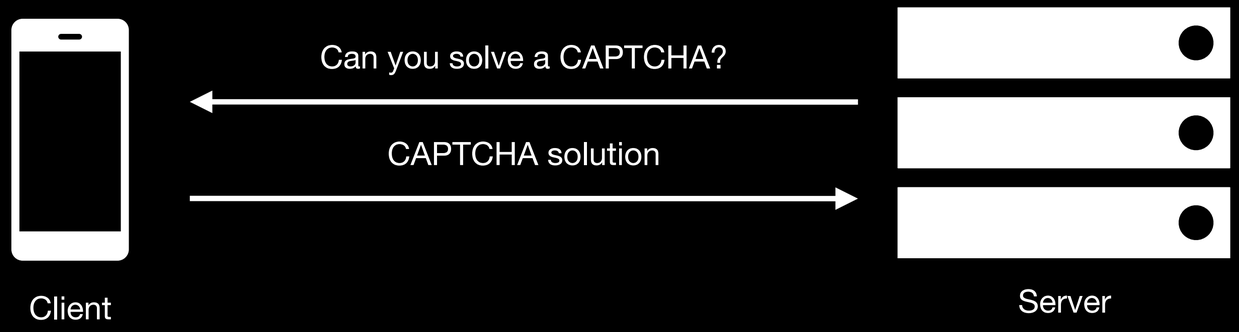

GET /gustav.jpg
Client
Server

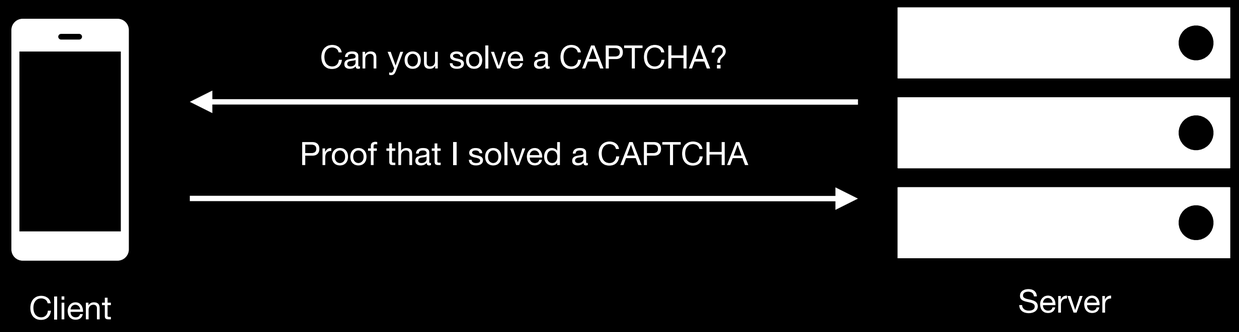

This client looks suspicious...
GET /gustav.jpg
Challenge
Client
Server

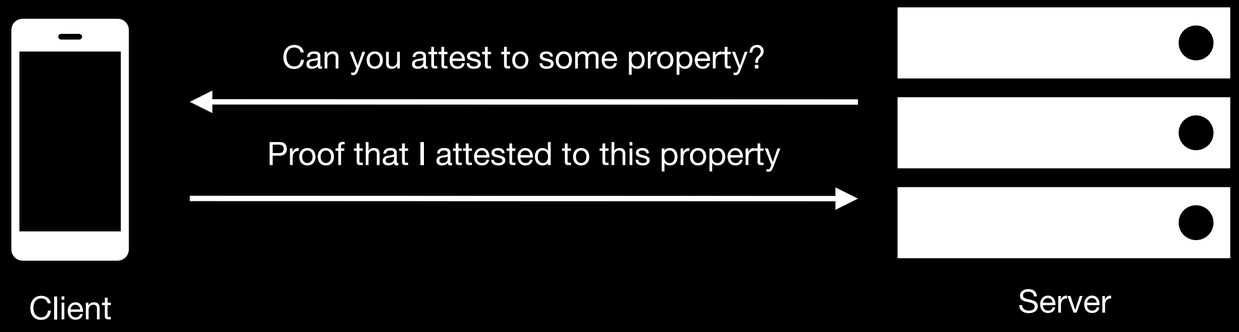

Generate
proof based on this
challenge
GET /gustav.jpg
Challenge
Proof
Client
Server

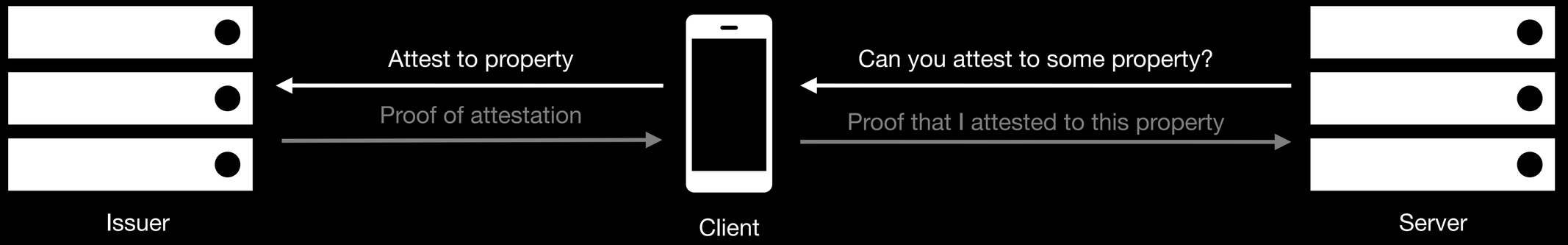

GET /gustav.jpg
Challenge
Proof
OK, I trust you
Client
Server

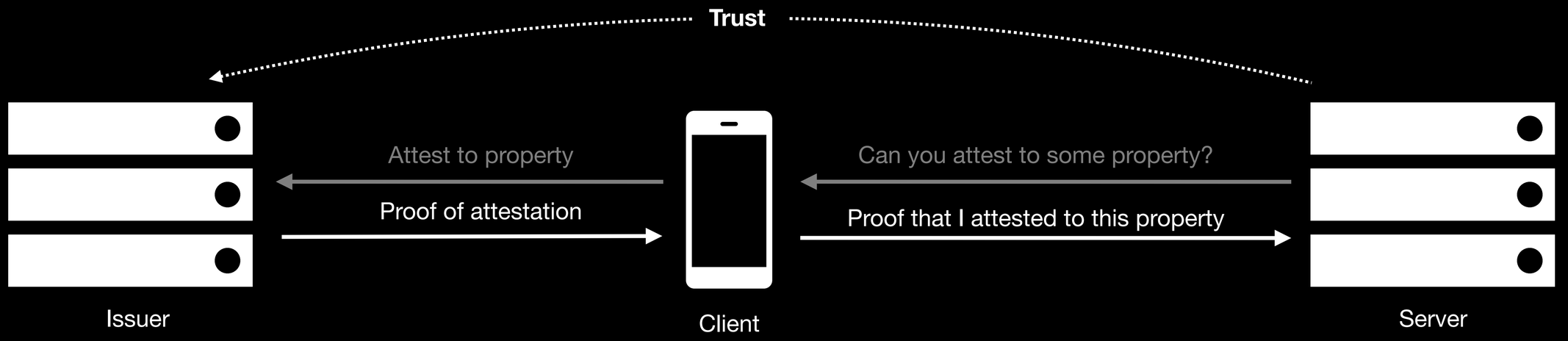

GET /gustav.jpg
Challenge
Proof
Client
Server

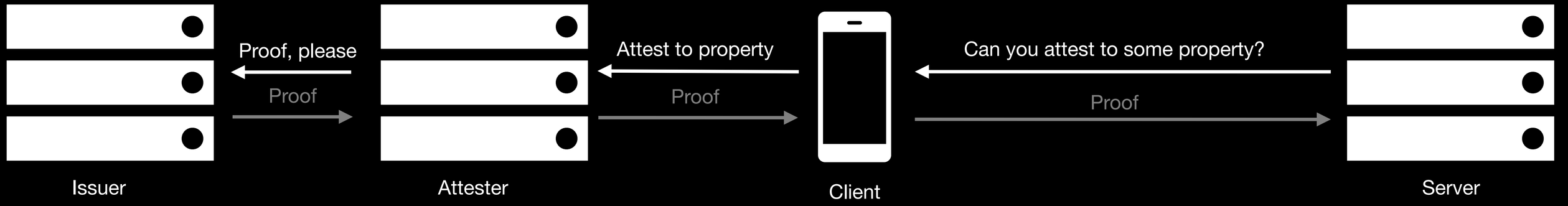

Can you solve a CAPTCHA?
CAPTCHA solution
Client
Server

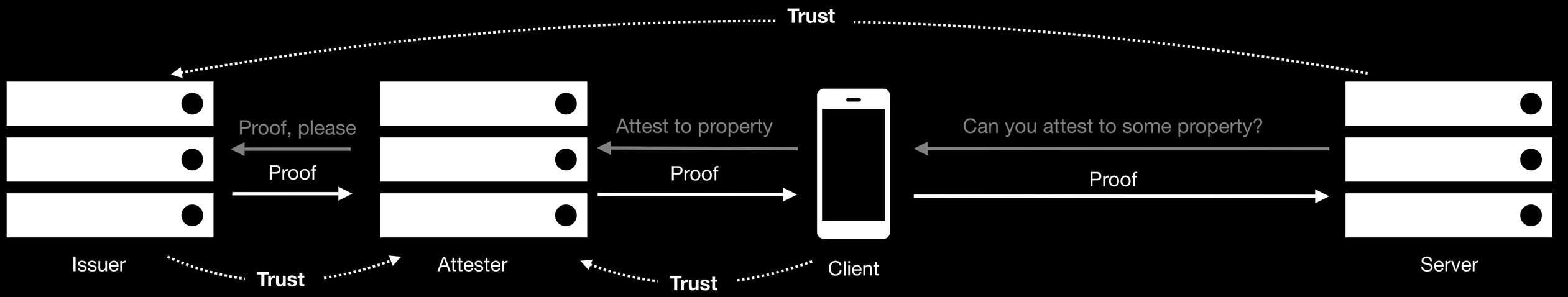

Can you solve a CAPTCHA?
Proof that I solved a CAPTCHA
Client
Server


Can you attest to some property?
Proof that I attested to this property
Client
Server

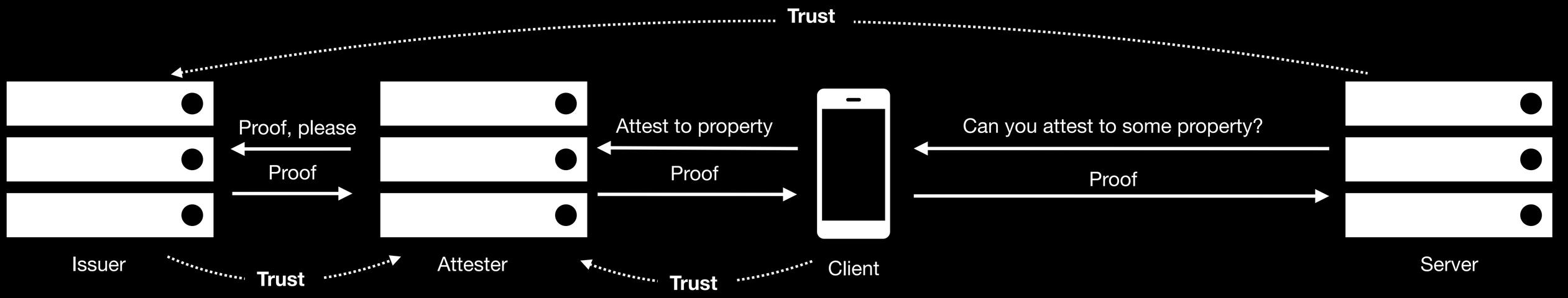

Attest to property
Proof of attestation
Can you attest to some property?
Proof that I attested to this property
Issuer
Client
Server


Trust
Attest to property
Proof of attestation
Can you attest to some property?
Proof that I attested to this property
Issuer
Client
Server

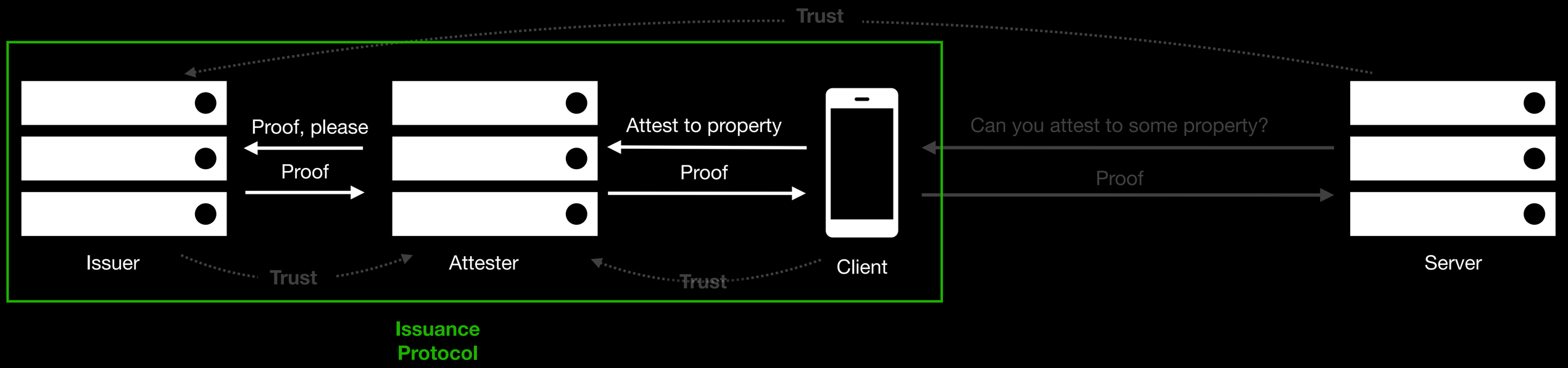

Proof, please
Proof
Attest to property
Proof
Can you attest to some property?
Proof
Issuer
Attester
Client
Server


Trust
Proof, please
Proof
Attest to property
Proof
Can you attest to some property?
Proof
Issuer
Trust
Attester
Trust
Client
Server

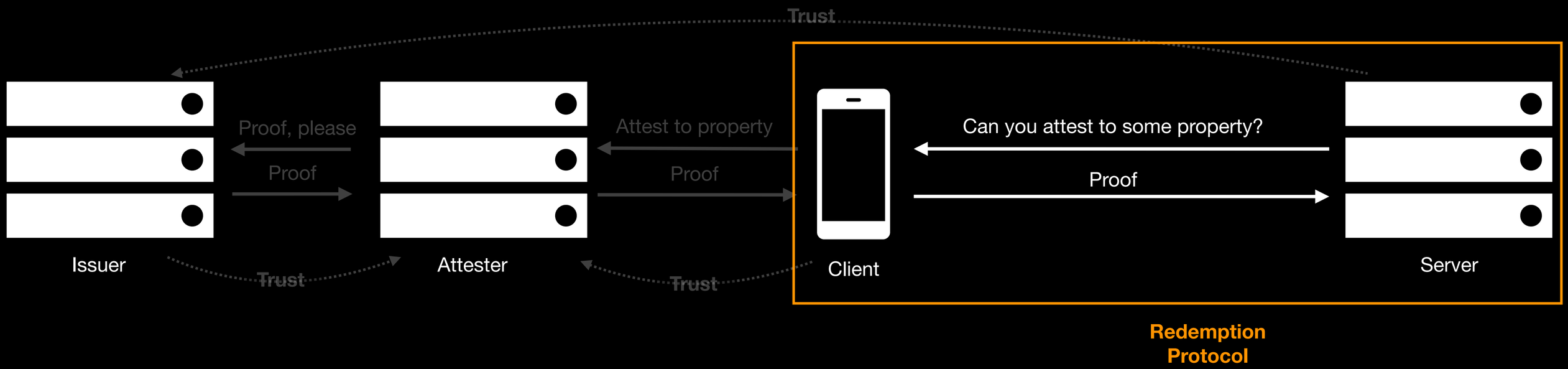
Privacy Pass Architecture



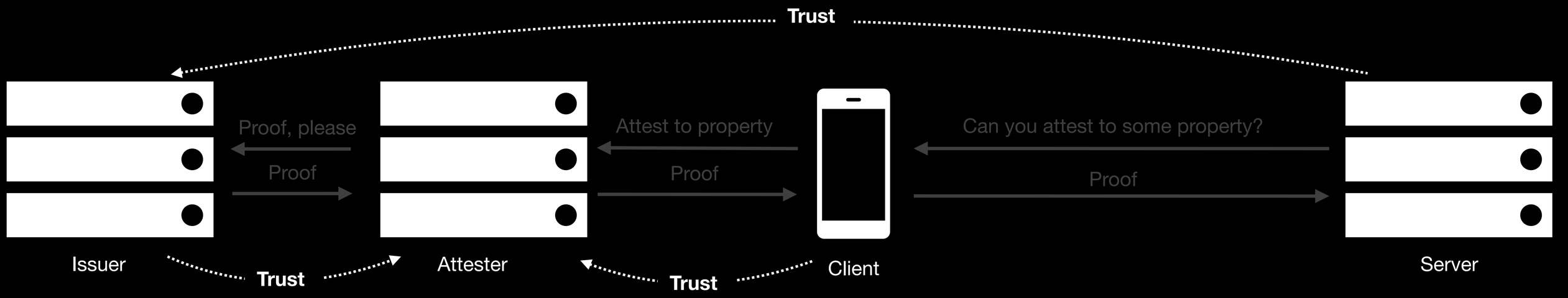
Privacy Pass Protocols



Privacy Pass Protocols

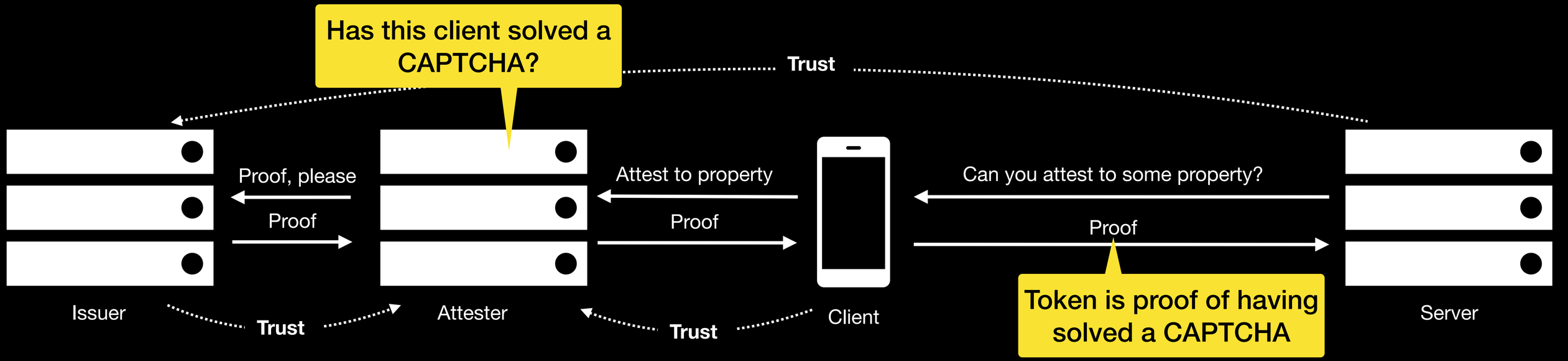


Privacy Pass Trust Model

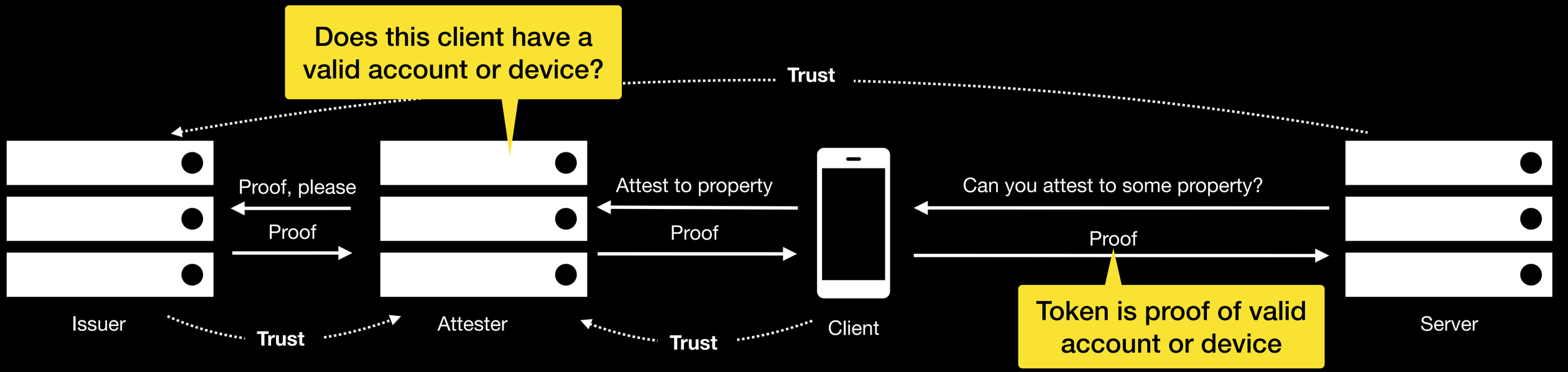


The *value* of the proof depends on the type of attestation performed during the issuance protocol

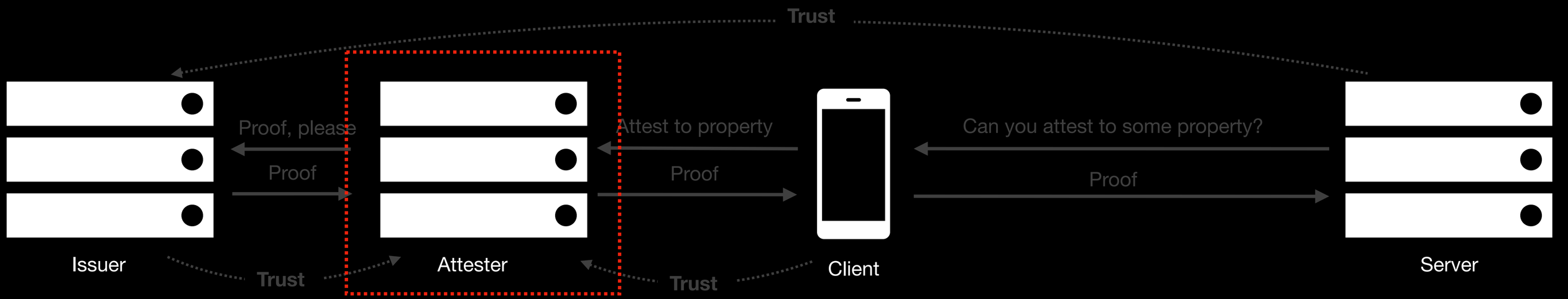
Privacy Pass Trust Model



Privacy Pass Trust Model



Privacy Pass Attestation



Attestation is the most important piece of Privacy Pass

Attestation
Considerations

How hard is the attestation? What happens if attestation is not possible?

How specific is the attestation? How does it contribute to client fingerprint?

How reliable or trustworthy is the attestation?

How does attestation help or harm centralization?

Attestation

Principles

1. Root attestation in trustworthy sources.
2. Attest to minimal viable signals with maximal impact.
3. Make attestation user-friendly with reasonable fallbacks for non-compliant clients.

Attestation

Proposal

1. Converge around device attestation with CAPTCHA as a fallback

   Apple Private Access Tokens and DeviceCheck

   Android SafetyNet

   Windows Health Attestation

2. Build anti-fraud systems *on top* of this attestation (attestation should not deprecate and replace existing mechanisms)

Questions?

Privacy Pass Attestation

Christopher A. Wood