Delegated credentials

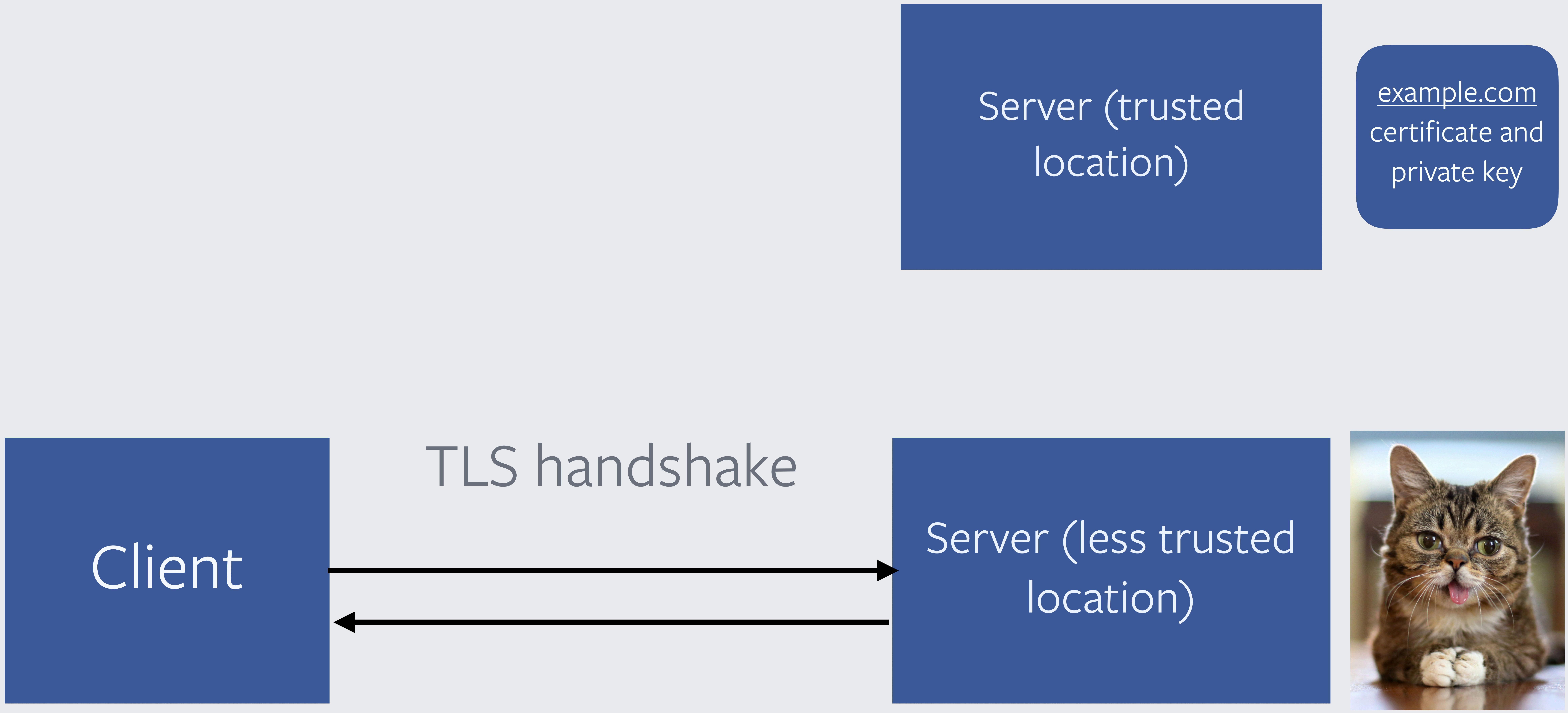
Subodh Iyengar

Facebook

Outline

- Brief overview / recap
- Draft changes
- Hackathon results
- Open discussion

Brief overview



Server (trusted location)

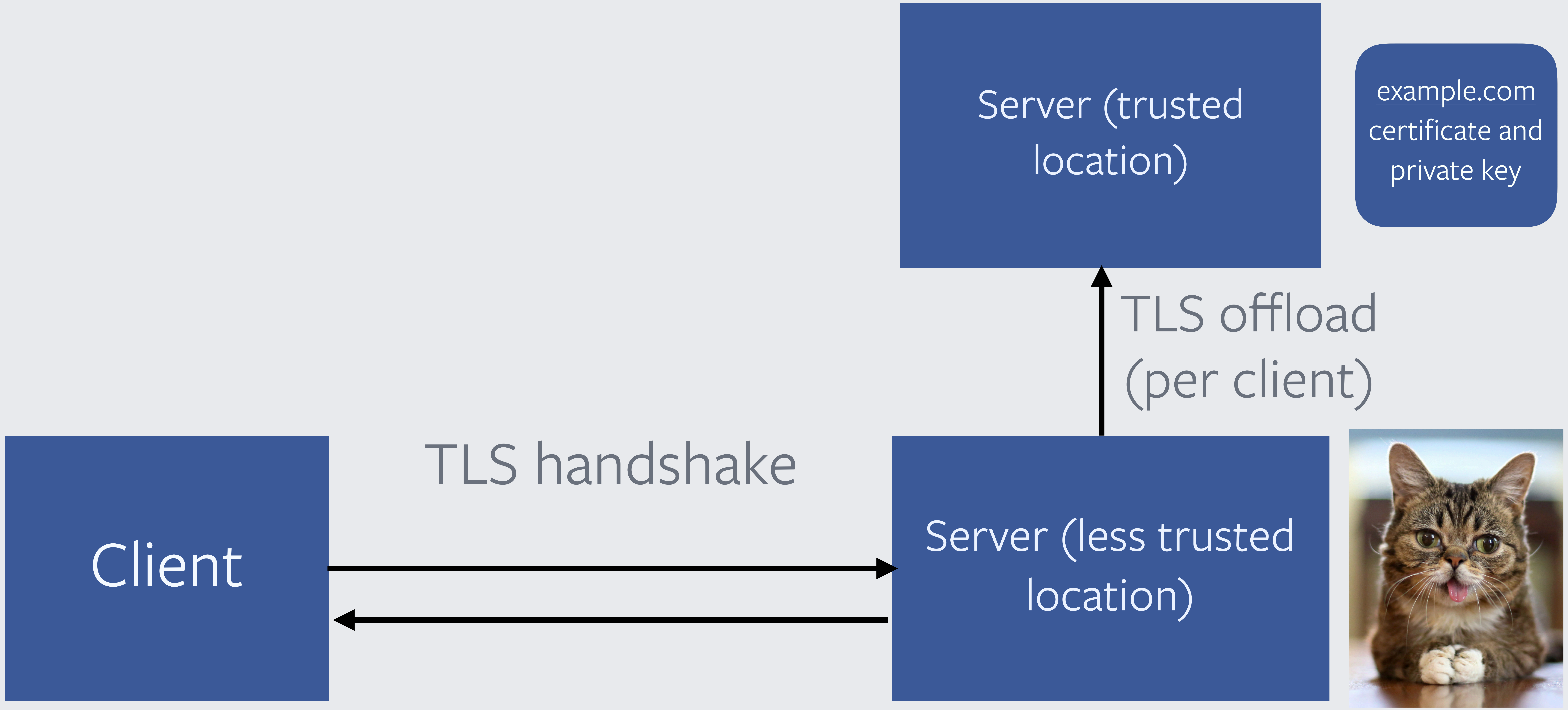
example.com certificate and private key

Client

TLS handshake

Server (less trusted location)

Brief overview



Server (trusted location)

example.com certificate and private key

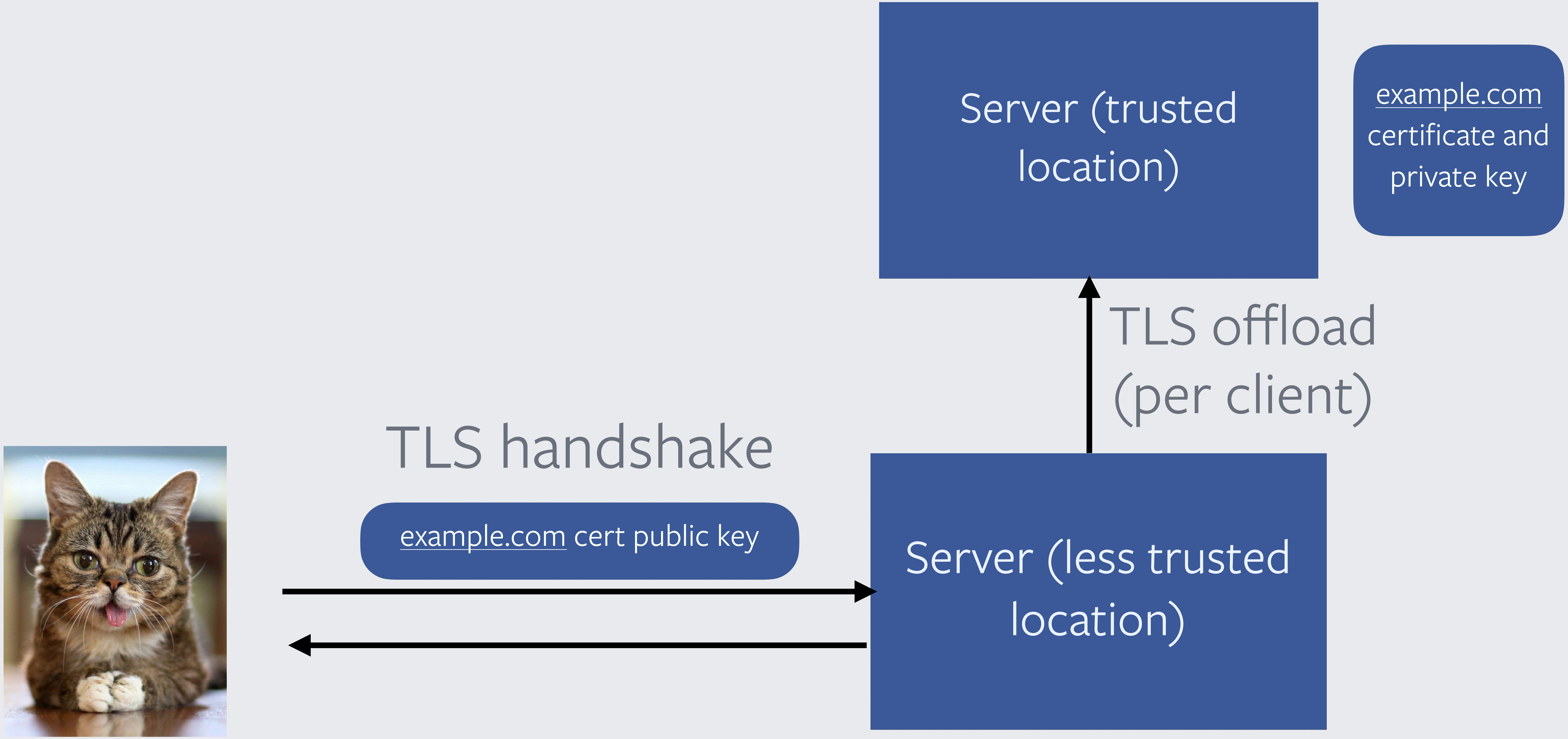
TLS offload (per client)

TLS handshake

Client

Server (less trusted location)

Brief overview



Server (trusted location)

example.com certificate and private key

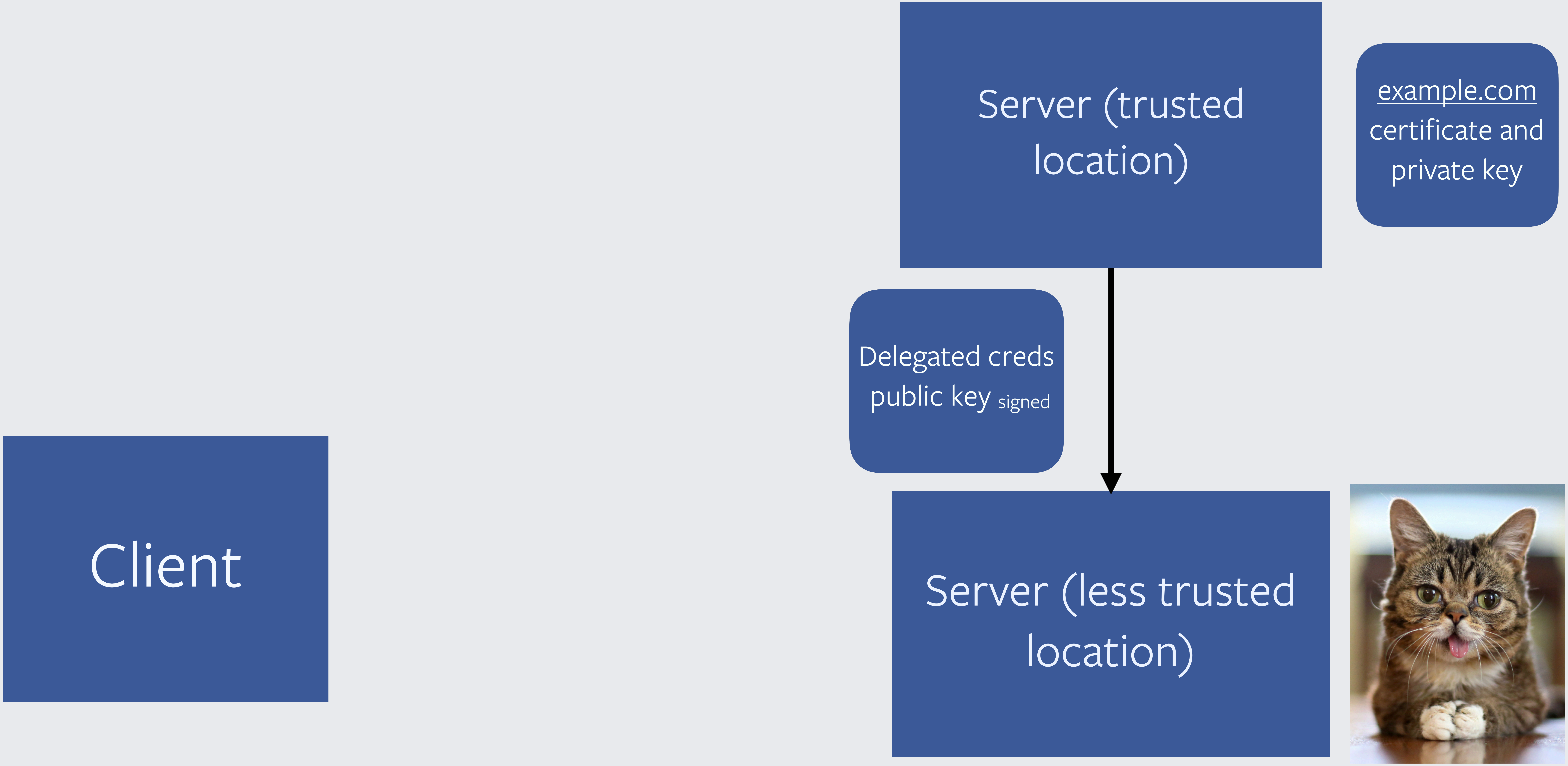
TLS offload (per client)

TLS handshake

example.com cert public key

Server (less trusted location)

Brief overview



Server (trusted location)

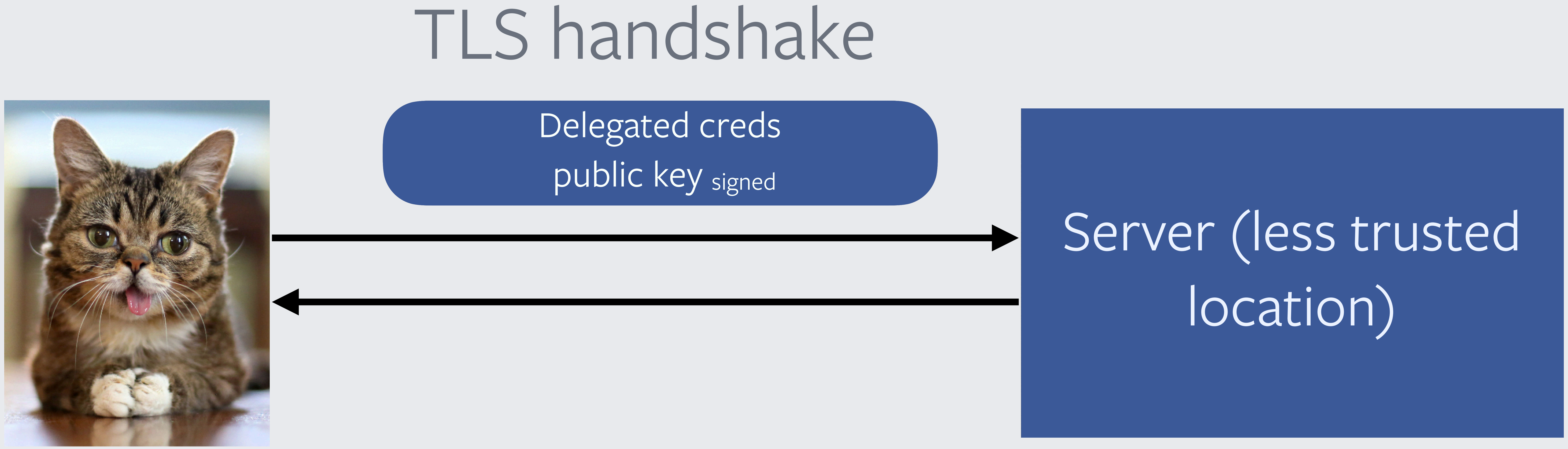
example.com certificate and private key

Delegated creds public key signed

Server (less trusted location)

Client

Brief overview



TLS handshake

Delegated creds
public key$_{\text{signed}}$

Server (less trusted location)

Major changes in draft-rescorla-tls-subcerts-01

- Delegated credentials are trimmed to the bare essentials
- Changed signature scheme
- Cleaned up draft to only have one option
- Added requirement for a new X509 extension

Bare essentials

```
struct {
  uint32 validTime;
  opaque publicKey<0..2^24-1>;
} DelegatedCredentialParams;

struct {
  DelegatedCredentialParams cred;
  SignatureScheme scheme;
  opaque signature<0..2^16-1>;
} DelegatedCredential;
```

Signature scheme

- A string that consists of octet 32 (0x20) repeated 64 times.
- ”TLS, server delegated credentials”.
- TLS ProtocolVersion
- End entity certificate used to sign the DelegatedCredential.
- SignatureScheme scheme.
- The DelegatedCredentialParams structure.

Draft cleanup

- Last draft presented several options
- Trimmed to the Delegated Credential structure

New X509 extension

- Comments from WG
- DelegationUsage X509 extension required on EE certificate

Hackathon results

IETF 98 hackathon we got interop between:

- Fizz (Facebook, C++)
- tls-tris (Cloudflare, Go)
- picotls (Fastly, C)

Open discussions

- We restrict lifetime to max 7 days. Does that work for everyone? Should we make this configurable?
- Delegated credentials can be taken from untrusted locations and used in trusted locations.