ERICSSON

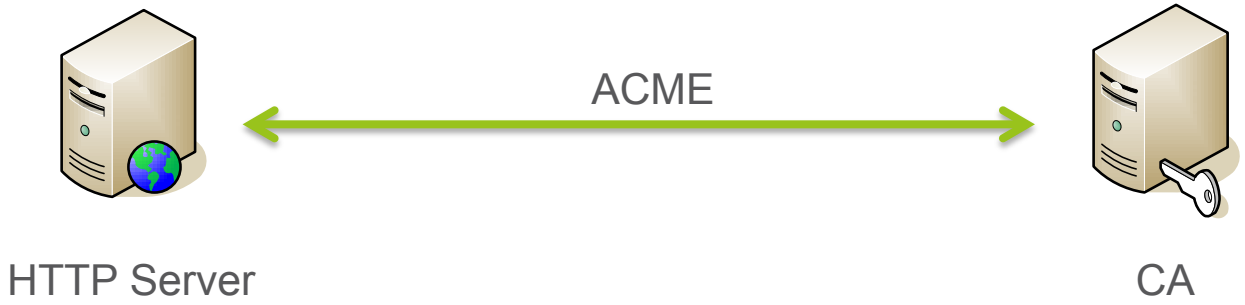
ACME USE CASES

DRAFT-MATTSSON-ACME-USE-CASES-00

JOHN MATTSSON

CERT MANAGEMENT OR I2CA

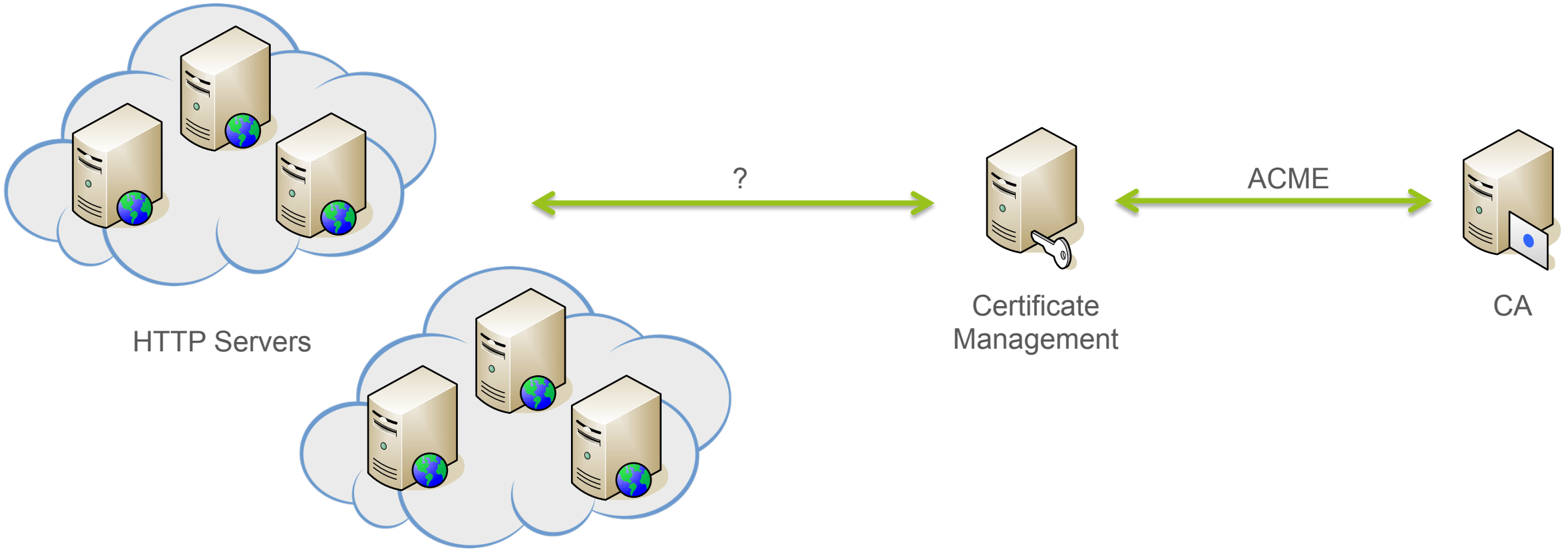
- With ACME, an origin can request certificates from a CA and the process can be automated.
- Current mechanisms in draft-barnes-acme are focused on the HTTP server directly contacting the certificate authority (CA).
  - “An ACME client therefore typically runs on a web server”.
  - “The ACME server runs at a certificate authority”.



- What should the use cases for ACME be?

USE CASES AND DELEGATION

- Everything except very small origins would probably like to have separation between the HTTP servers and the certificate management.



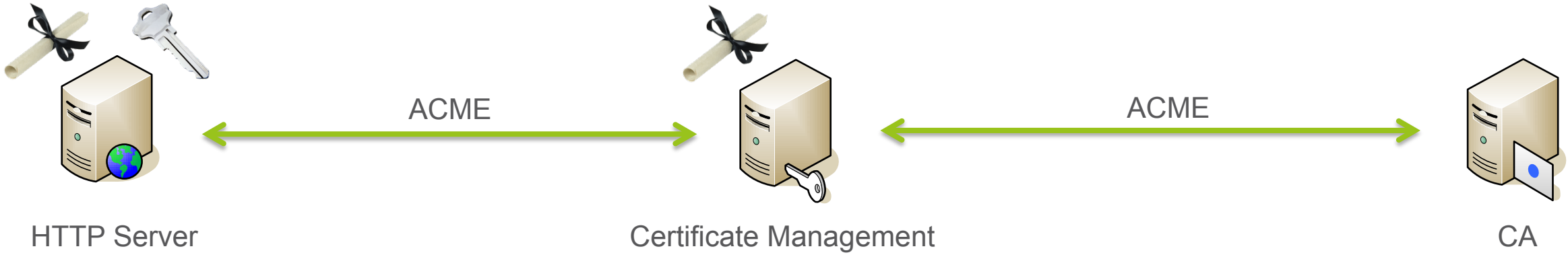
DELEGATION OPTIONS

- One option is to fetch public certificates and private keys from a central repository.

- A second option is to use a session key interface (e.g. draft-cairns-tls-session-key-interface)

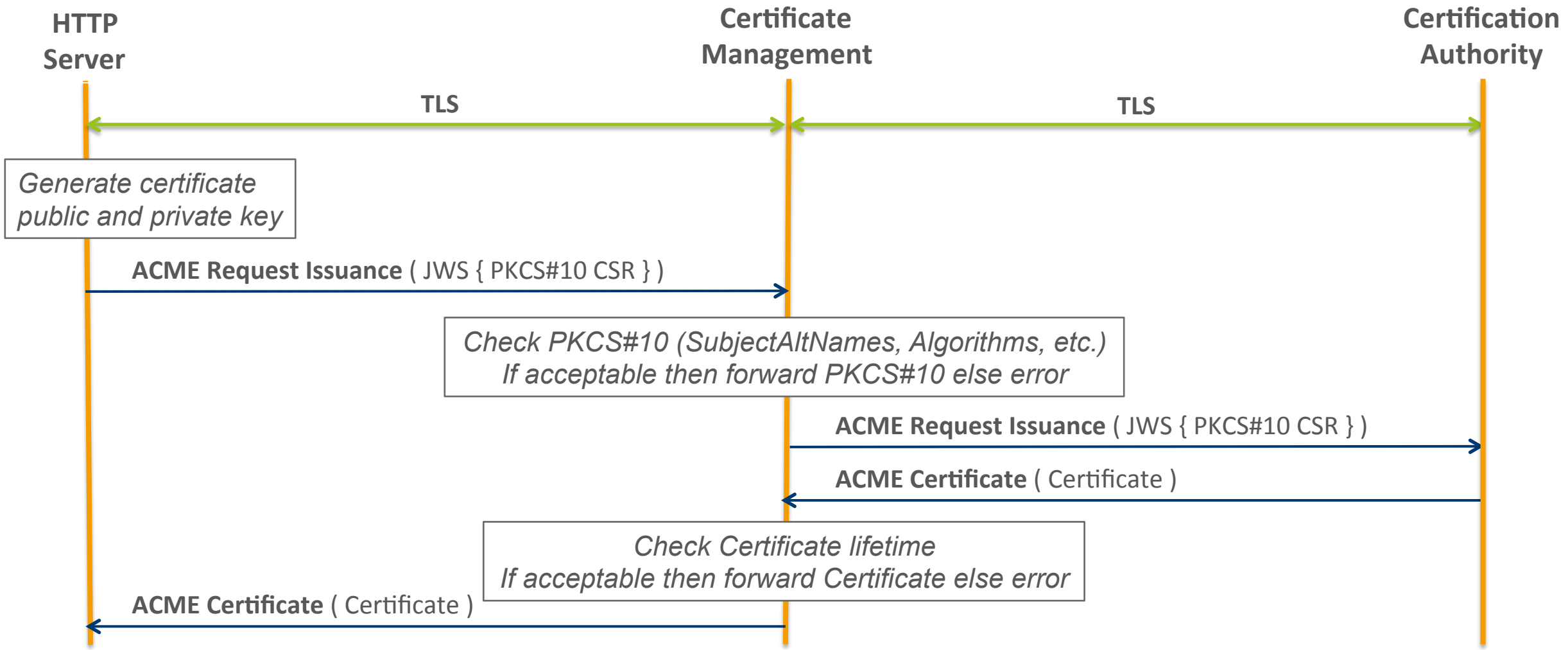
DELEGATION OPTIONS

- A third option is to “tunnel” ACME through the certificate management server.



- Assumption: the Certificate Management Server has previously registered with the CA and generated the key pair that is used for client authentication (in JOSE JWS).
- TLS and ACME is hob-by-hob (HTTP Server <-> Certificate Management <-> CA).
  - The Certificate Management Server above is both ACME Server and ACME Client.
  - CSR and Certificate is sent e2e (HTTP Server <-> CA)

DELEGATED ACME ("TUNNEL")



ANALYSIS

- ACME is currently not optimal for scenarios where the HTTP Server is not talking directly to the Certification Authority.
  - The Certificate Management can only chose to block or forward the **ACME Request Issuance** and the **ACME Certificate** messages.
  - ACME and PKCS#10 does not have any mechanism to let the Key Server determine the validity time of the certificate.

- We think tunneled ACME should be considered, and we think the above issues should be addressed.

ERICSSON