OmniPublish

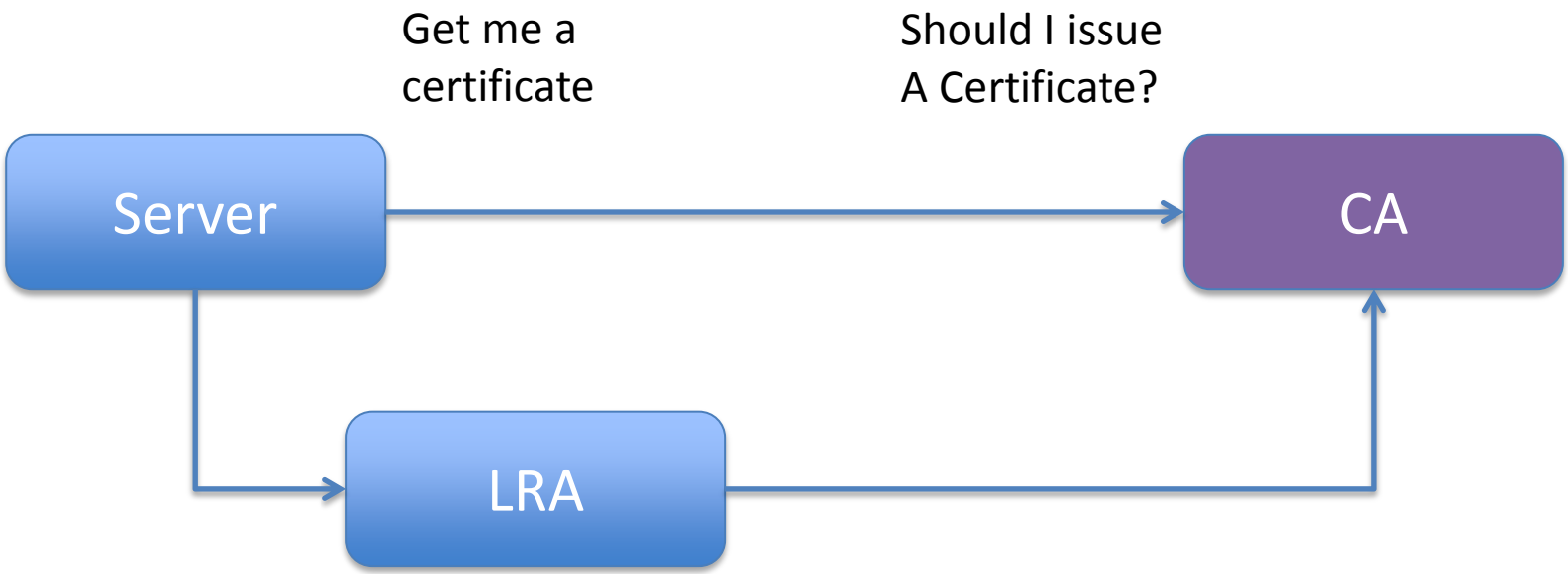
Phillip Hallam-Baker

History

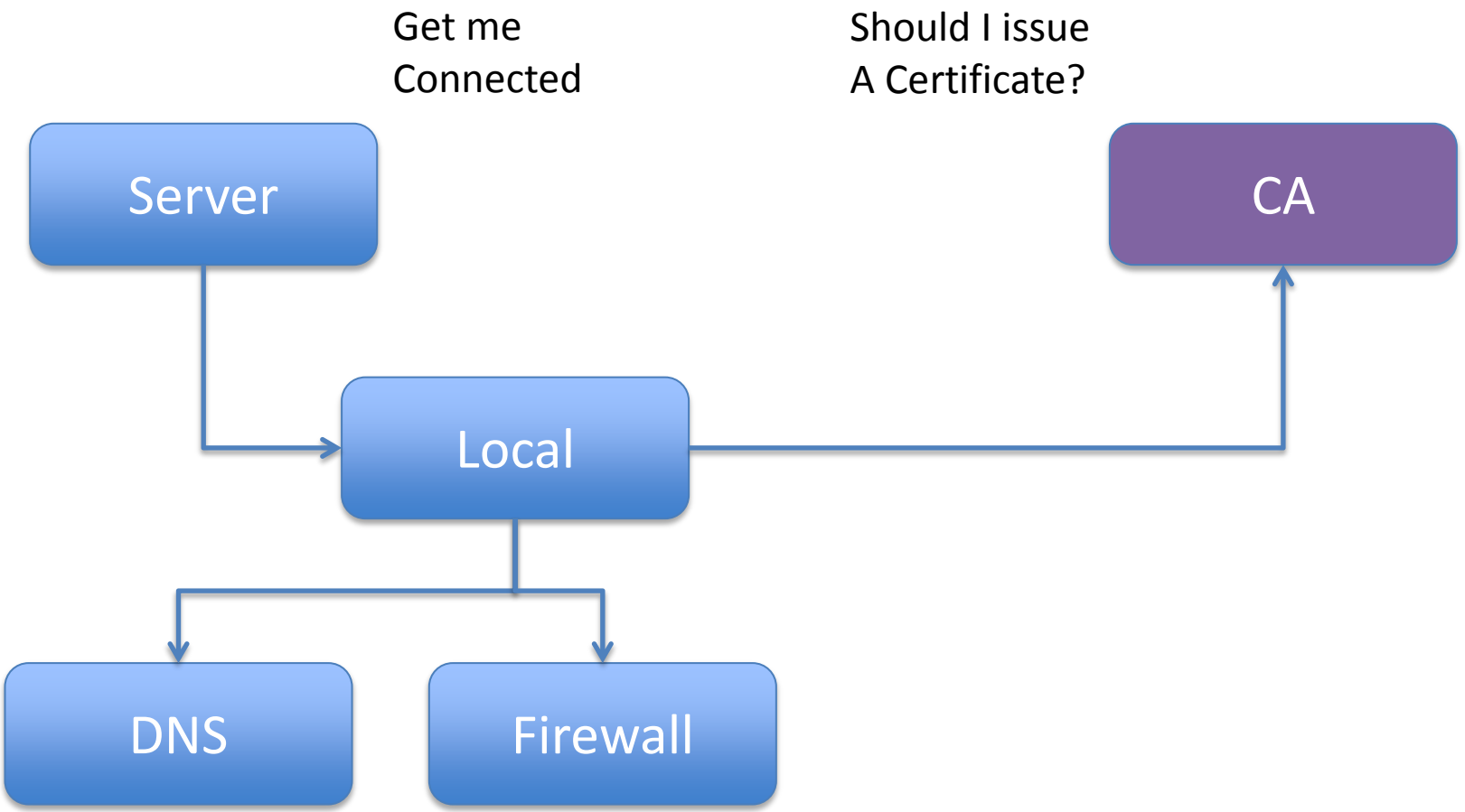
- Proposed May 2014
- Current draft
  - hallambaker-acme-omnipublish-00

- Constraint
  - How do we do automated certificate issue
  - Given IETF/W3C have tried this 4 times already

The Problem – PKI Space



The Real Problem



Consequences - Client

- ACME Request
  - Give me a TLS certificate for example.com
    - [Proof I should get it]
- Omnipublish request
  - I will offer SMTP for *@example.com
  - Give me what I need
    - [Except the private key]
  - Make the necessary network configurations

Consequences – Local Agent (LRA)

- Local Agent / LRA is the entity that validates
  - Hosts / Services are transient.
  - Do not want to do EV validation every 6 hours
- Single point of configuration for network
  - Makes it easy to deploy / manage new features
    - Choice of algorithm
    - Publish security policy in DNS (e.g. DANE)

ACME vs OmniPublish

ACME

- Low level, PKIX
- Defines CA conversation
- JSON / HTTPS
- DV Validation
  - Generate CSRs

OmniPublish

- High Level
- Defines Client end
- JSON / HTTPS
- DV Validation
  - Generate CSRs
- Account based Validation
  - [Paid DV / OV / EV]

Next Steps

- Approach I, Competition
  - "These are different protocols, separate SDOs"
- Approach II, Cooperation
  - ACME is a subset of OmniPublish
  - Needs some change in ACME approach
    - Account based
    - Separate Validation / Issue processes completely
  - Probably 90% of code will carry over