

# ACME AUTO DISCOVERY

draft-vanbrouwershaven-acme-auto-discovery

---

Mike Ounsworth, Paul van Brouwershaven

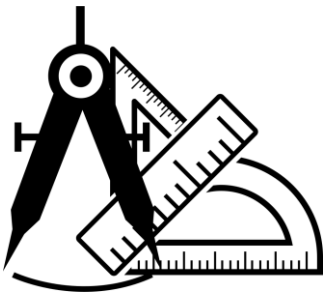
24 July 2022

Automated Certificate Management Environment Working Group  
IETF 117 – San Francisco



**ENTRUST**

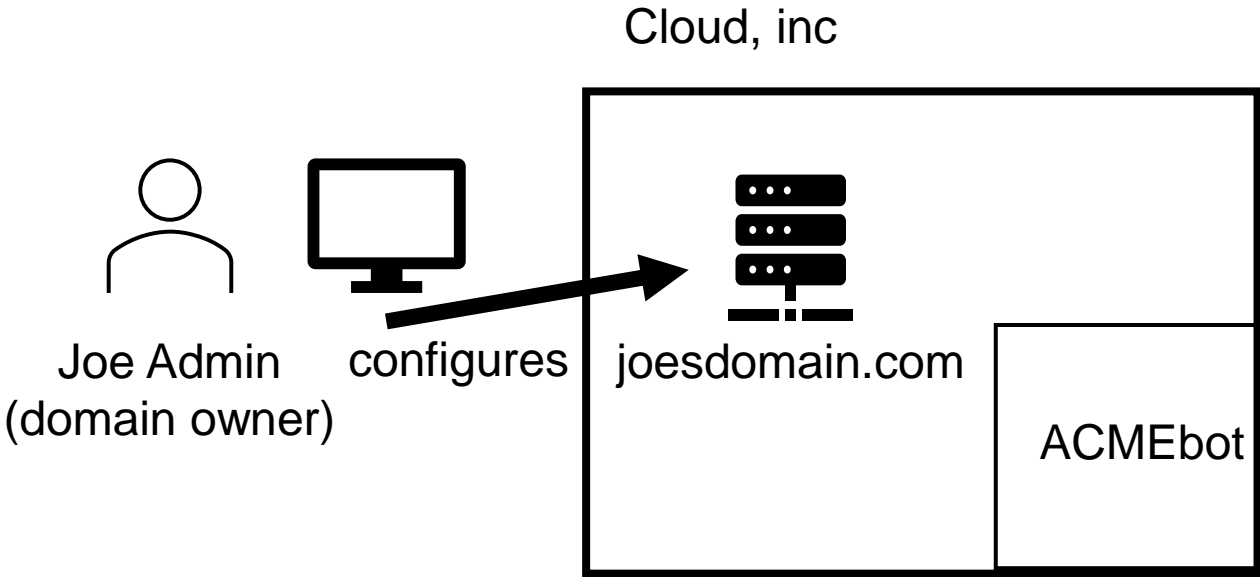
SECURING A WORLD IN MOTION



# PUT YOUR EDGE-CASE FINDERS AWAY!

Our motivating use case is:

- ▶ Public domains (ie publicly-accessible, public DNS, etc),
- ▶ Hosted on public cloud providers,
- ▶ Where the domain owner has a preferred public CA.



# DIGITALOCEAN (CSP) - LOAD BALANCER

resource name or public IP (Ctrl+B) Create

## New certificate

Use Let's Encrypt Bring your own certificate

Automatically encrypt traffic up to the Load Balancer with a free Let's Encrypt certificate. Choose domains using the search box below. We'll generate and auto-renew the certificate. [Learn more](#)

Search for a domain on DigitalOcean

Include all subdomains (wildcard certificate)

Select specific subdomains

Name this certificate \*

Generate Certificate

You can use Let's Encrypt (ACME), provide some configuration, but you **can not** specify your own ACME server or account binding.

source name or public IP (Ctrl+B) Create

## New certificate

Use Let's Encrypt Bring your own certificate

[How to create an SSL certificate](#)

Name \*

Certificate \*

Private key \*

Certificate chain

Save SSL Certificate

Or you can upload a custom certificate.

# FASTLY (CDN)

While “*Fastly-managed certificates use the ACME protocol to procure and renew TLS certificates from Let’s Encrypt, a non-profit certification authority, and GlobalSign, a commercial certification authority*”, they do not allow you to configure your own ACME server and key binding.

TLS domains   • TLS certificates 8   TLS configurations   TLS subscriptions 3   Mutual TLS

< Certificates / New

### Add a new key and certificate

Used for securing new domains

**Upload a new key (Optional)**  
Add new key for the certificate below as a security best practice

⤴ Drag your new private key file here to upload it securely or [browse for it](#).

**Upload the certificate file**  
Upload the new certificate file

⤴ Drag your new certificate file here to upload it securely or [browse for it](#).

Submit   Cancel

# AND SOME OTHERS WE CHECKED...

---

## › Content Delivery Network (CDN)

- Cloudflare
- Fastly
- Akamai

## › Cloud Service Provider (CSP)

- Azure
- Google Cloud
- AWS
- IBM Cloud
- DigitalOcean
- OVH
- Hertzner
- Vultr

## › PaaS

- WordPress
- Salesforce
- HubSpot

## › Control panels

- CPANEL / WHM
- Plesk

## › Appliances / other devices

- HP Officejet
- Reolink
- Ubiquiti / Unifi
- Synology



# PROBLEM

---

- › A certificate with a validity of 90-days ‘requires’ automation
  - Renewing a certificate manually 4-6 times will not be ‘appreciated’
- › When subscribers can’t specify their preferred ACME server, the default will become the norm!
- › If the default is the norm, we lack issuer diversity which will become a major point of failure.
- › (side-benefit: prioritized list of fallback ACME servers for a given domain)

How do we automate discovery of the domain owner’s preferred CA?

# PROBLEM

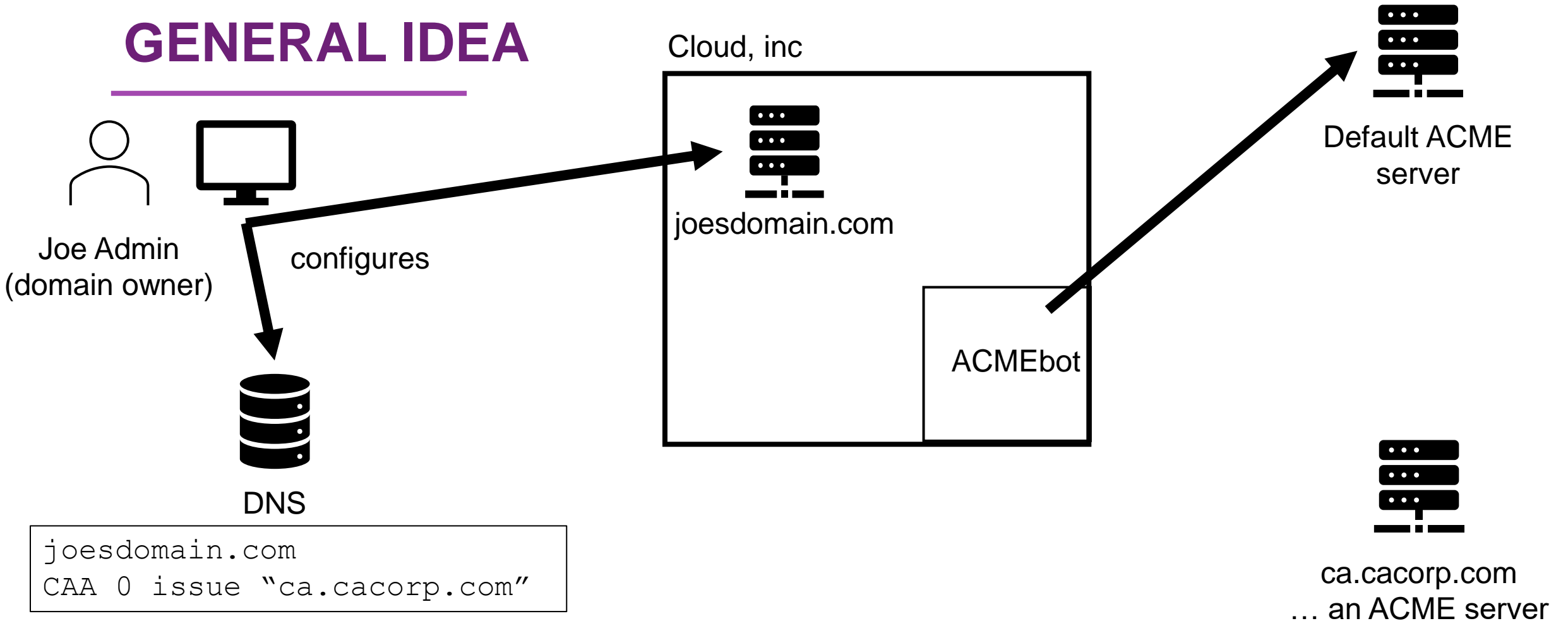
---

- › A certificate with a validity of 90-days ‘requires’ automation
  - Renewing a certificate manually 4-6 times will not be ‘appreciated’
- › When subscribers can’t specify their preferred ACME server, the default will become the norm!
- › If the default is the norm, we lack issuer diversity which will become a major point of failure.
- › (side-benefit: prioritized list of fallback ACME servers for a given domain)

How do we automate discovery of the domain owner’s preferred CA?



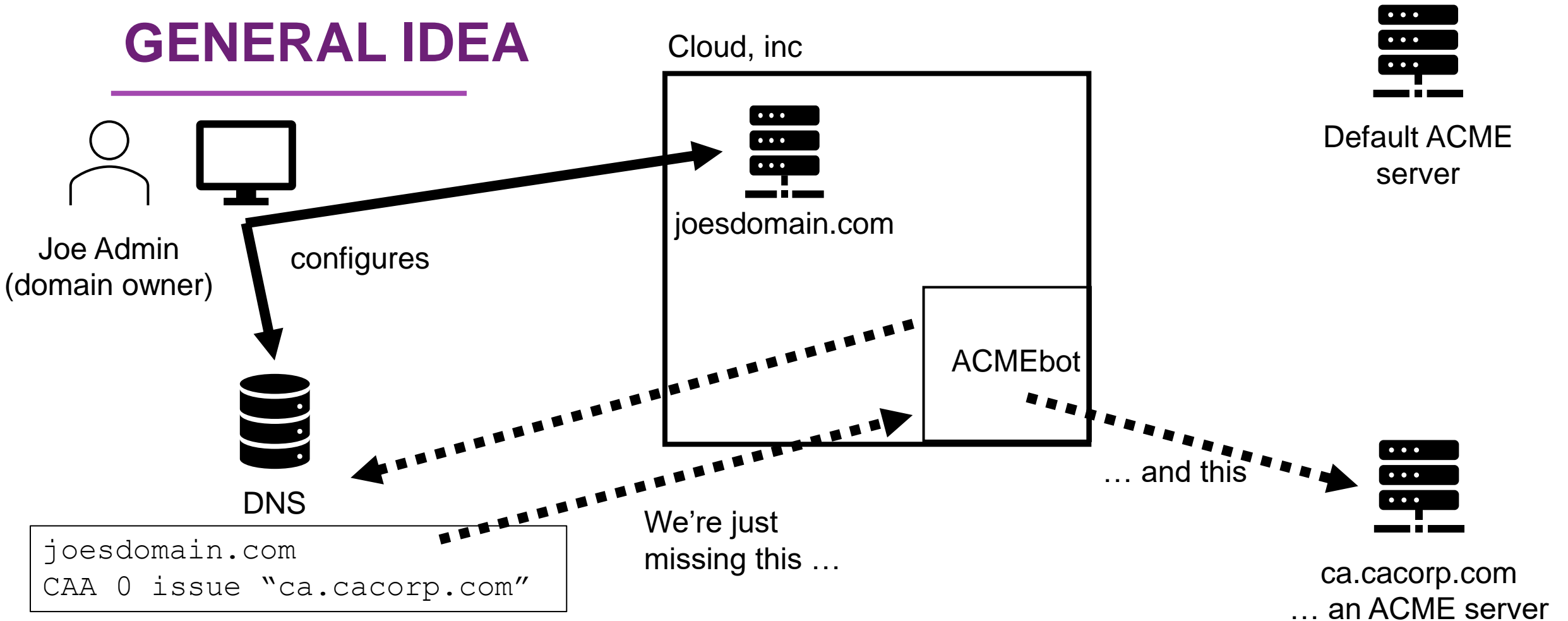
# GENERAL IDEA



```
joesdomain.com  
CAA 0 issue "ca.cacorp.com"
```

... you would think there's enough info here to send ACMEbot to the Joe's preferred ACME server ...

# GENERAL IDEA



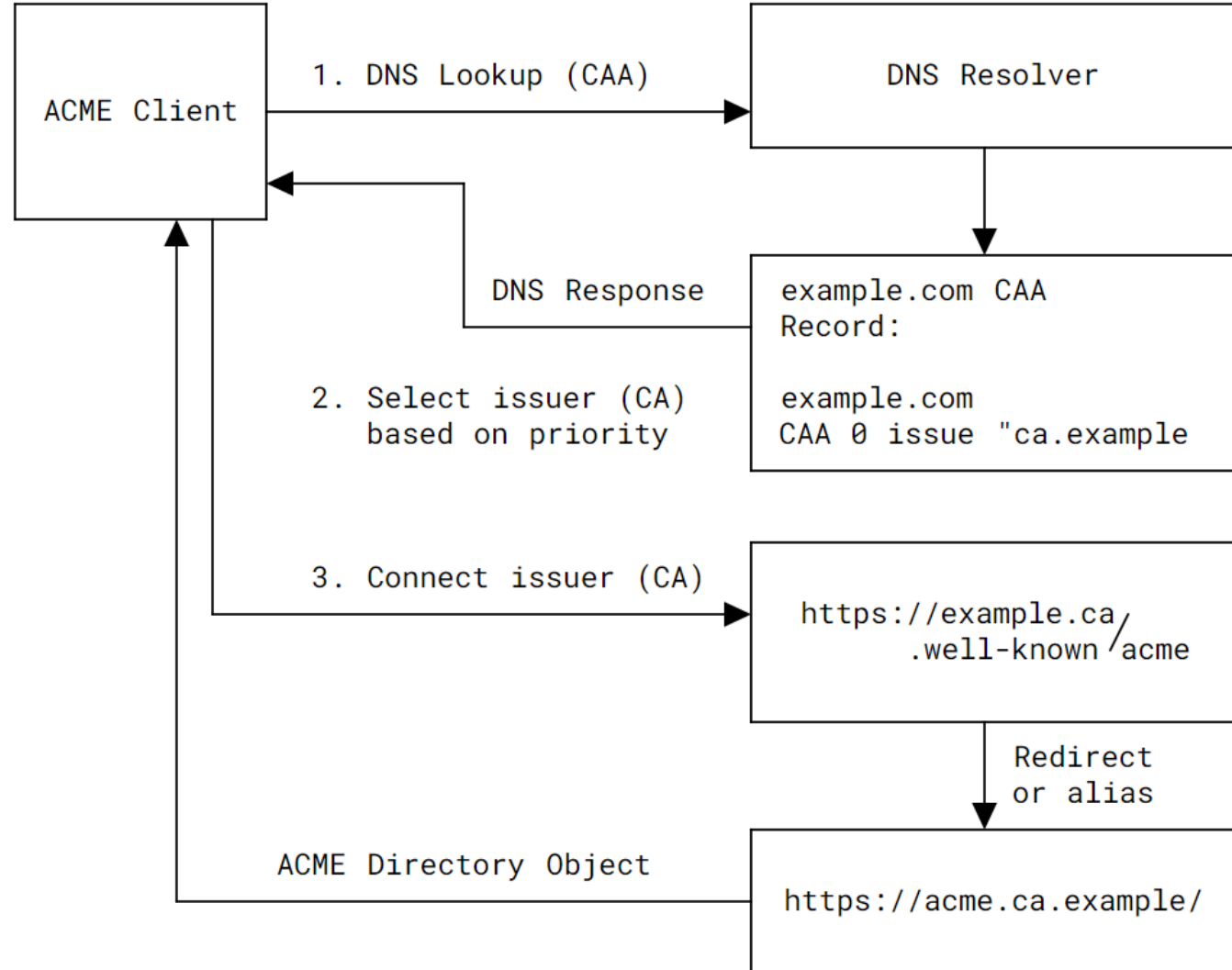
... you would think there's enough info here to send ACMEbot to the Joe's preferred ACME server ...



# ACME CLIENT BEHAVIOR

What's new in this draft?

- DNS CAA extensions:
  - Discovery: true/false
  - Priority: int
- The '.well-known/acme' URI
- Some suggested ACME client behaviour to tie it all together.
- Guidance to use Internal Account Binding (DV / email) instead of providing externalAccountBinding. (you probably don't want to give your ACME account key to your hosting provider)



# RUNNING CODE

---

*“I happened to be poking around the certbot codebase today and decided to try and implement this draft.*

*It turned out to be a much simpler task than I had expected*

*My fork of certbot with the implementation is available at*

*[https://github.com/as207960/certbot/tree/auto-discovery.](https://github.com/as207960/certbot/tree/auto-discovery)”*

Q Missel

Thanks Q!

<https://mailarchive.ietf.org/arch/msg/acme/JWQDZXSDa13zP57ytBI7bjEknKk/>

# ADOPT?

---

- › Is this useful?
  
- › draft-vanbrouwershaven-acme-auto-discovery

# POINTS RAISED ON-LIST

---



ENTRUST

# TERMS OF SERVICE

---

*Cloud, inc doesn't want to blindly accept the TOS of arbitrary ACME servers.*

*Raised by: Amir Omid, Seo Suchan*

Response: I think this is moot because it's actually Joe Admin who has the commercial relationship with the CA, we just need to make it clear that the ACME issuance is bound to Joe's ACME account, not Cloud, inc's.

Worth more discussion though.

<https://mailarchive.ietf.org/arch/msg/acme/6MPISpU3nD7SzKmnYcwyVeYqCiM/>

# CAN THIS BE SOLVED THROUGH HOSTER UI?

---

*“If the hosting provider already has a menu for upload certificate files, that menu could have a box for acme directory Uri too.”*

*Seo Suchan*

Response: Agree, that would be great if service provider would all do that.  
But they haven't.

So here is a mechanism that can be implemented in core ACME clients and will work regardless of service provider UI.

[https://mailarchive.ietf.org/arch/msg/acme/yCa3\\_ISEdgPWadr83MzV0Y8XwDo/](https://mailarchive.ietf.org/arch/msg/acme/yCa3_ISEdgPWadr83MzV0Y8XwDo/)



**ENTRUST**

SECURING A WORLD IN MOTION