ACME @ IETF117

24-JUL-2023 17:30-18:30

NOTE WELL

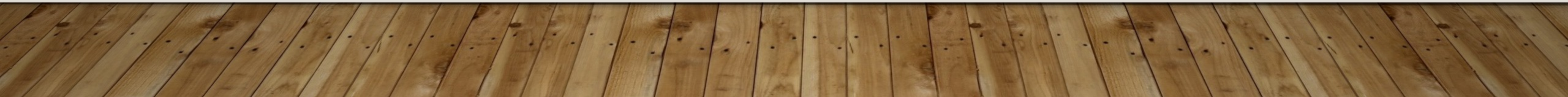
This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)



3 AGENDA

- Note Well, Agenda Bashing, and Technical Issues
- Document Status
- Presentations:
  - DNS Account Challenge (Omidi)
  - ARI (Frank)
  - ACME Onion (Misell)
  - ACME Auto Discovery (vanBrouwershaven, Ounsworth)
- AOB

4 DOCUMENT STATUS (1/3)

- ACME-Onion
  - Adopted. First WG version submitted 22-June
  - Presentation today
- ACME-DNS-Account-Challenge
  - Renamed from ACME-DNS-Account-01
  - Presentation today
- ACME-Client
  - Version -06 submitted

5 DOCUMENT STATUS (2/3)

- ACME-ARI
  - Not updated ; have presentation
- ACME-Integrations
  - New versions 14-17 ; changed from Informational to PS
  - Approved – in RFC Editor's queue
- ACME-Subdomains
  - In AUTH48 (for roughly 240 hours)
- ACME-Authority-Token-TnAuthList
  - Approved before IETF 116; still in RFC Editor's queue

6 DOCUMENT STATUS (3/3)

- ACME-Authority Token
  - Approved before IETF 116 ; still in RFC Editor's queue
- ACME-DTN-NodeId (validation extension)
  - Publication requested, but
  - Stuck since October…
- No RFC published for almost 2 years.
- Should be different by 118.

7

PRESENTATION SLIDES GO HERE

DNS-ACCOUNT-CHALLENGE

Antonis Chariton - Amir Omidi - James Kasten
Stanislaw Janikowski - Fotis Loukos

Background

DNS-01

- Is awesome!
- Has limitations :(

DNS-ACCOUNT-CHALLENGE

Domain Validation Delegation

- Decentralization
- Adoption
- Resilience
- Beyond https?
- Not replacing DNS-01

Updates

Errors

- Community support

KID

- Keep them stable
- Query parameters, etc.

Questions | Feedback

ACME Renewal Information

draft-ietf-acme-ari-01

Samantha Frank, Let’s Encrypt
IETF 117, 2023-07-24

Since IETF 116

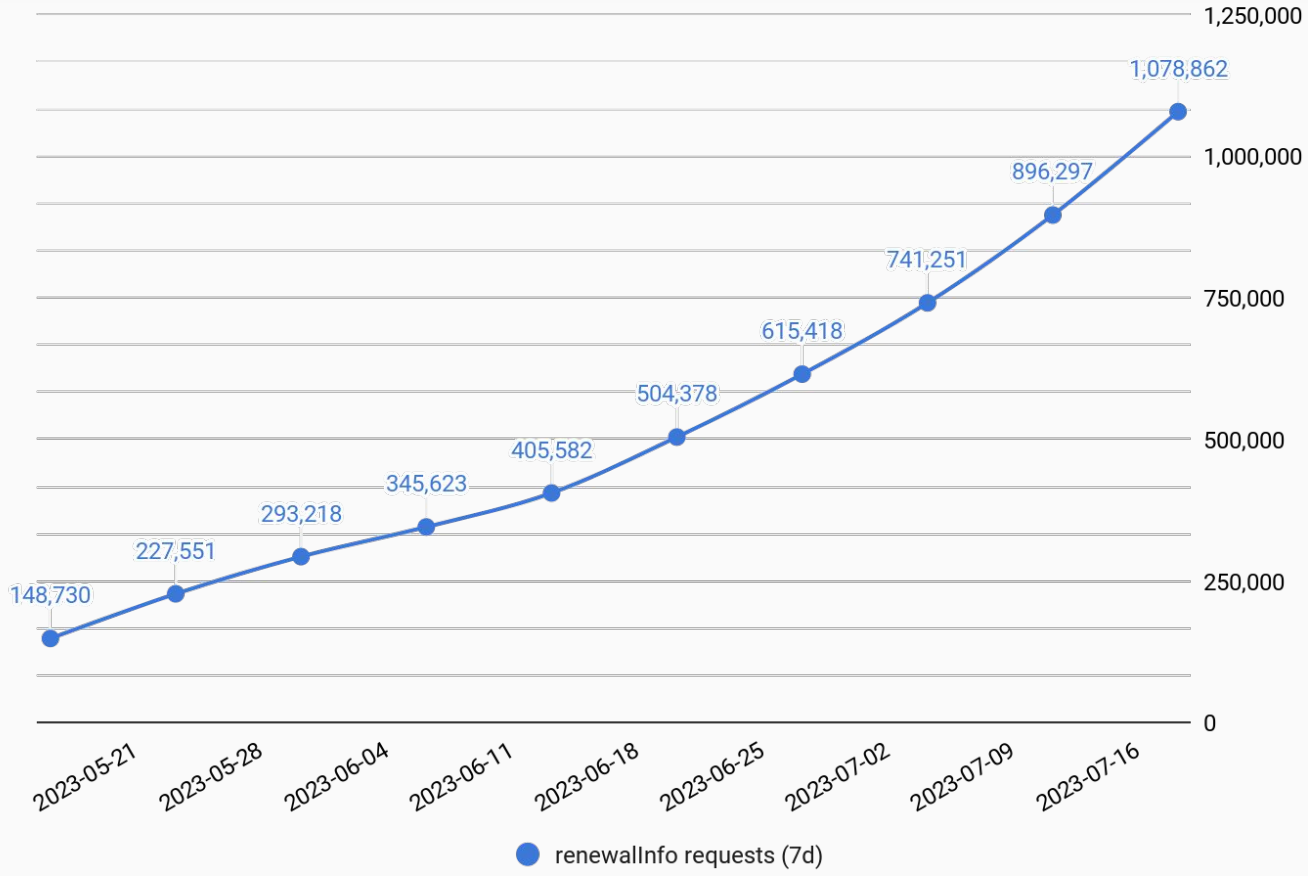
- No changes to the draft specification

- Fully implemented by Let’s Encrypt
- Fully implemented by Google Trust Services
- Under evaluation by Certainly (Fastly)

Current Work

- Client adoption
  - eggsampler/acme (Go)
  - go-acme/lego (Go)
  - Let’s Encrypt is contributing to multiple clients

ARI Endpoint Usage



Open Questions

- Construction of the unique certificate ID
  - OCSP CertID
  - base64url(Authority Key Identifier + Serial)

- Reducing request volume
  - Batch endpoint
    - GET
    - POST-as-GET
  - Include current CertID in newOrder requests

- Simplifying client logic
  - Single timestamp instead of window
  - Bypassing rate limits for renewals during window

ACME FOR ONIONS

`draft-ietf-acme-onion`

Q MISELL, GLAUCA DIGITAL

IETF 117, Monday 24th of July 2023

Fedi: @q@glauca.space
Email: q@as207960.net

SINCE IETF 116

- Adopted 🎉
- Reference CA implementation
  acmeforonions.org
- Certbot plugin for `onion-csr-01`
  certbot-onion
- Tor Spec Proposal `343-rend-caa`

WHY EVEN HAVE X.509 CERTIFICATES FOR TOR HIDDEN SERVICES?

- Secure cookies
- Content Security Policy
- HTTP/2
- PCI DSS
- Security-in-depth

GOALS

Define extensions to ACME to automate the issuance of X.509 certificates for Tor hidden services in line with the accepted methods in the CA/BF BR.

NON-GOALS

Any method not accepted by the CA/BF.

CURRENT STATE OF THINGS

- DigiCert (EV only)
- HARICA

CA/BF BR APPENDIX B

- § 3.2.2.4.18 - Agreed-Upon Change to Website v2
- § 3.2.2.4.19 - Agreed-Upon Change to Website - ACME
- § 3.2.2.4.20 - TLS Using ALPN
- § B.2.b - Special CSR

IDENTIFIER TYPE

```
{
  "type": "dns",
  "value": "bbcweb3hytmz...rad.onion"
}
```

Clients can be oblivious to the fact that the identifier is a Tor hidden service with "http-01" or "tls-alpn-01" validation methods.

NEW `onion-csr-01` VALIDATION METHOD

Implements CA/BF BR § B.2.b

Clients prove control over the .onion domain by signing a CSR with the private key of the .onion domain.

OVERVIEW OF THE TOR HIDDEN SERVICE DESCRIPTOR

OUTER LAYER

Fetched with the service's blinded public key

```
hs-descriptor 3
descriptor-lifetime ...
descriptor-signing-key-cert
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
revision-counter ...
superencrypted
-----BEGIN MESSAGE-----
...
-----END MESSAGE-----
```

FIRST LAYER ENCRYPTED DATA

Encrypted with the service's (non-blinded) public key

```
desc-auth-type x25519
desc-auth-ephemeral-key ...
auth-client ...
auth-client ...
auth-client ...
encrypted
-----BEGIN MESSAGE----
...
-----END MESSAGE-----
```

SECOND LAYER ENCRYPTED DATA

Encrypted with data from `auth-client`

```
create2-formats 2
introduction-point ...
onion-key ntor ...
auth-key
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
enc-key ntor ...
enc-key-cert
-----BEGIN ED25519 CERT-----
...
-----END ED25519 CERT-----
introduction-point ...
```

CLIENT AUTHENTICATION

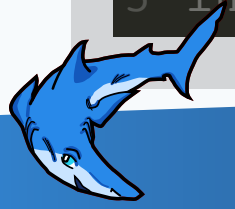
Tor allows hidden services to restrict which clients can connect using client authentication.

New `authKey` field to allow hidden service operators to allow the CA's Tor client to read their hidden service descriptor to issue certificates.

CAA RECORDS

.onion domains aren't in the DNS, so standard CAA records can't be used. Instead, CAA records are encoded in the BIND zone file format the second layer hidden service descriptor.

```
1 create2-formats 2
2 single-onion-service
3 caa 128 issue "test.acmeforonions.org;validationmethods=onic
4 caa 0 iodef "mailto:security@example.com"
5 introduction-point AwAGsAk5n...
```



CAA INTERACTION WITH CLIENT AUTHENTICATION

New field in the first layer hiiden service descriptor to signal that there are CAA records in the second layer descriptor.

```
1 desc-auth-type x25519
2 caa-critical
3 auth-client ...
```

QUESTIONS?

Q MISELL, GLAUCA DIGITAL

Slide deck available at
magicalcodewit.ch/ietf117-slides/

Fedi: @q@glauca.space
Email: q@as207960.net

ACME AUTO DISCOVERY

draft-vanbrouwershaven-acme-auto-discovery

Mike Ounsworth, Paul van Brouwershaven

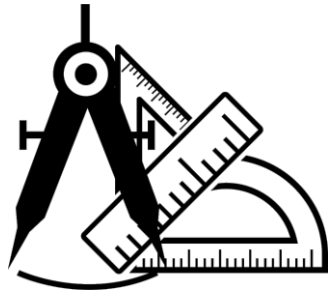
24 July 2022

Automated Certificate Management Environment Working Group
IETF 117 – San Francisco

ENTRUST

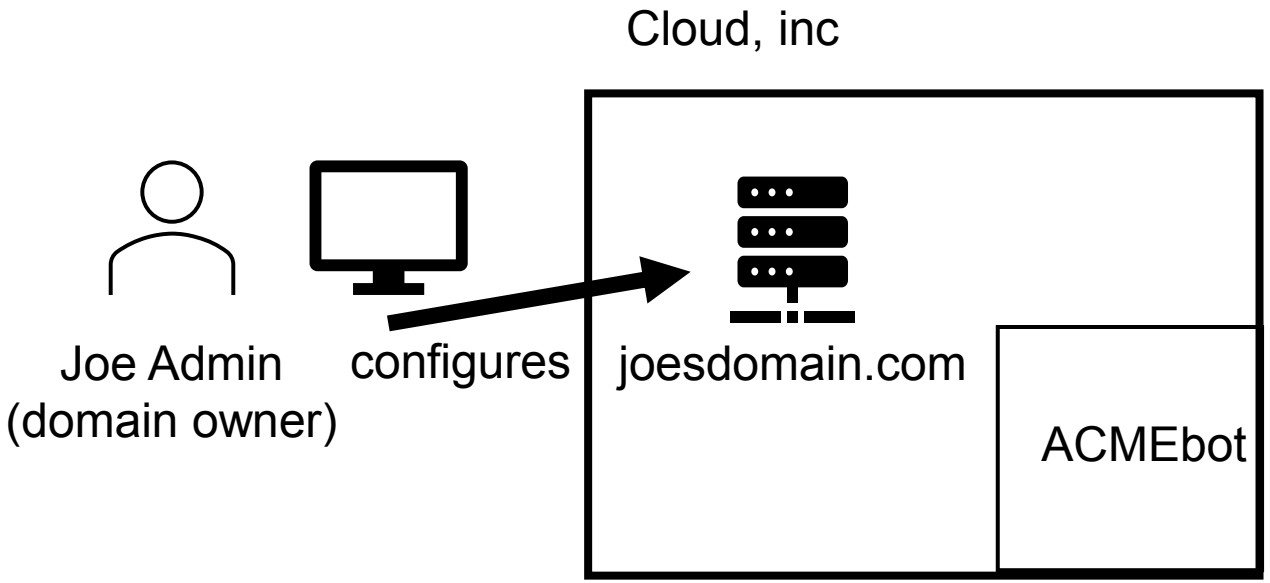
SECURING A WORLD IN MOTION

PUT YOUR EDGE-CASE FINDERS AWAY!



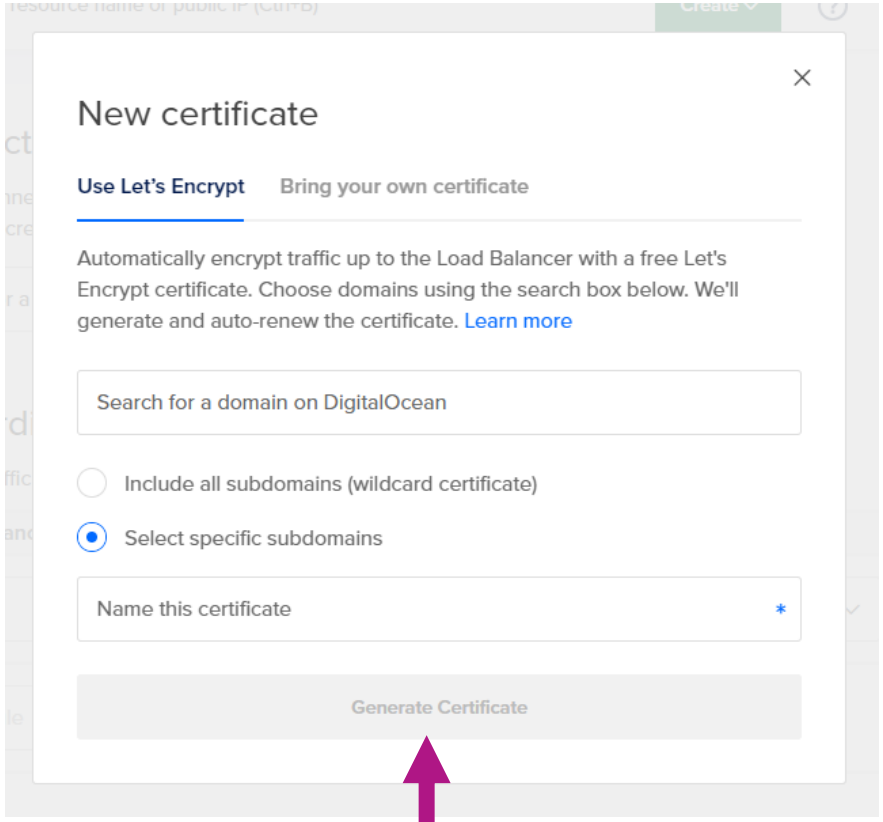
Our motivating use case is:

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

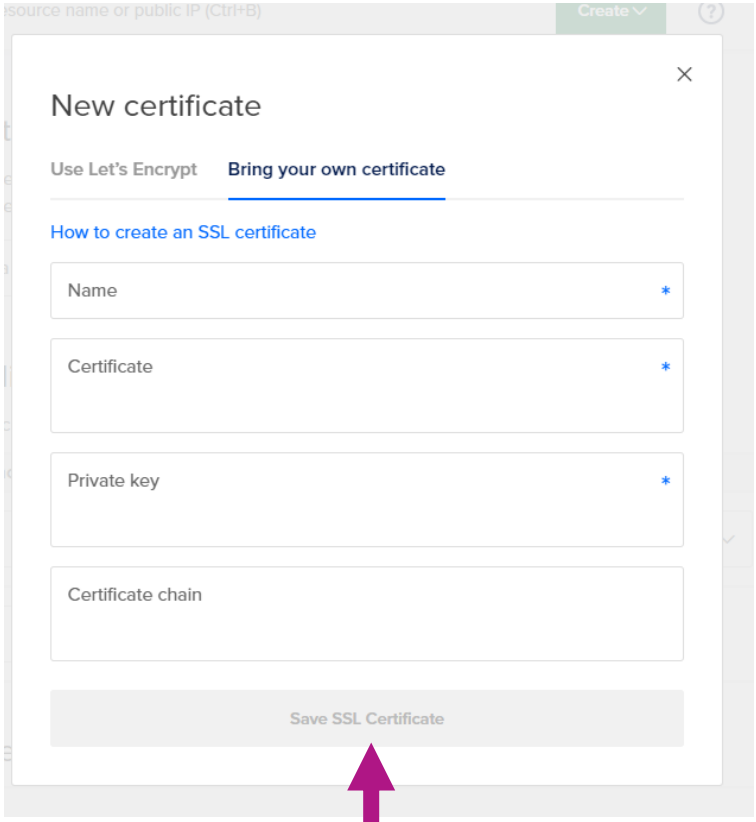


ENTRUST

DIGITALOCEAN (CSP) - LOAD BALANCER



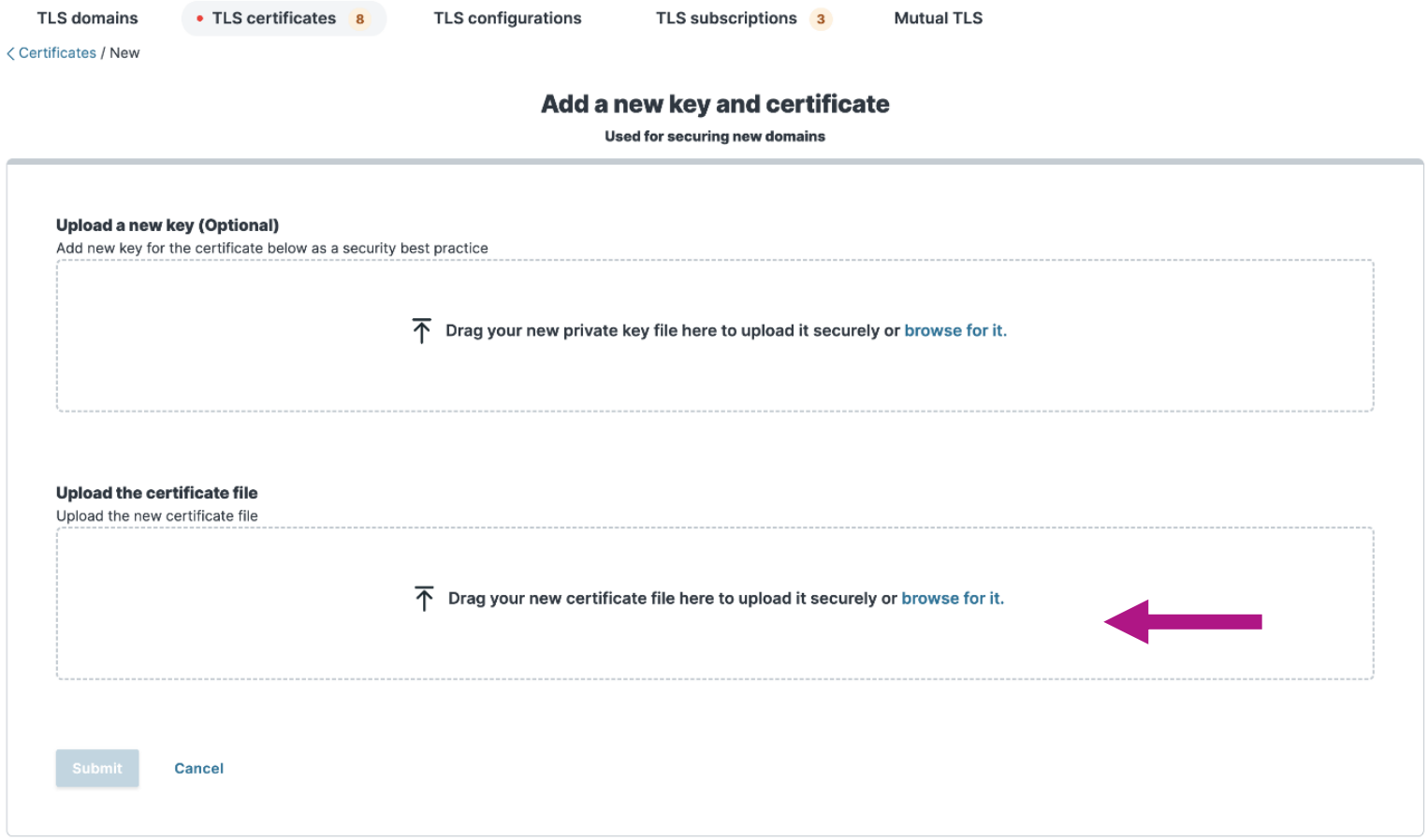
You can use Let's Encrypt (ACME), provide some configuration, but you **can not** specify your own ACME server or account binding.



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.



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
  - Ubiquity / Unifi
  - Synology

ENTRUST

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?

ENTRUST

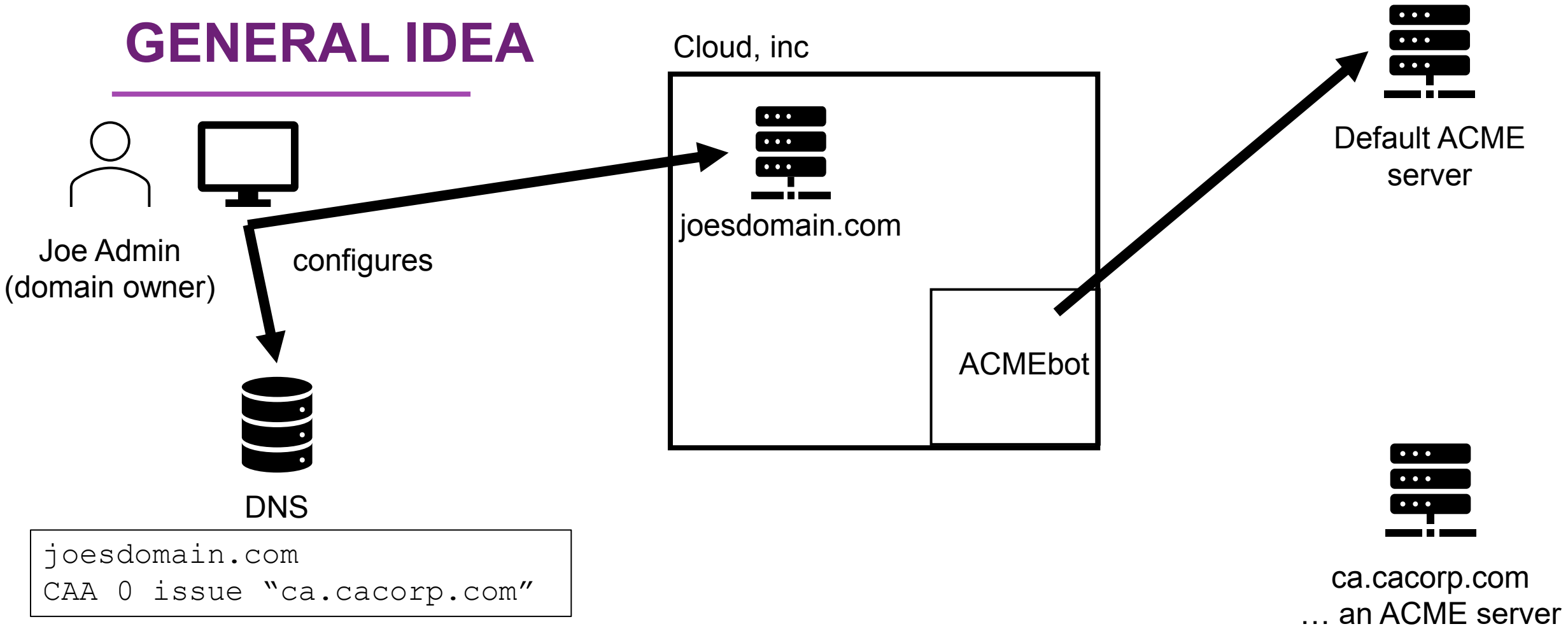
PROBLEM

- 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?

ENTRUST

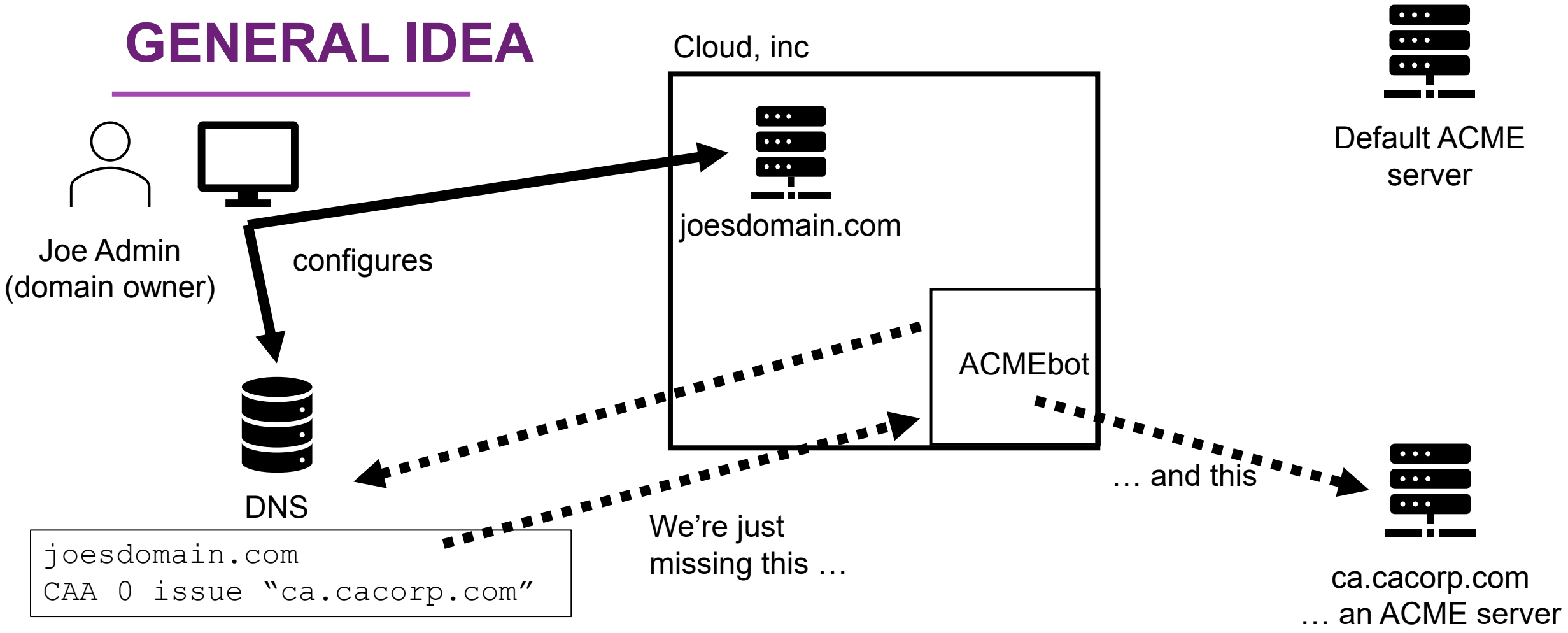
GENERAL IDEA



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

ENTRUST

GENERAL IDEA



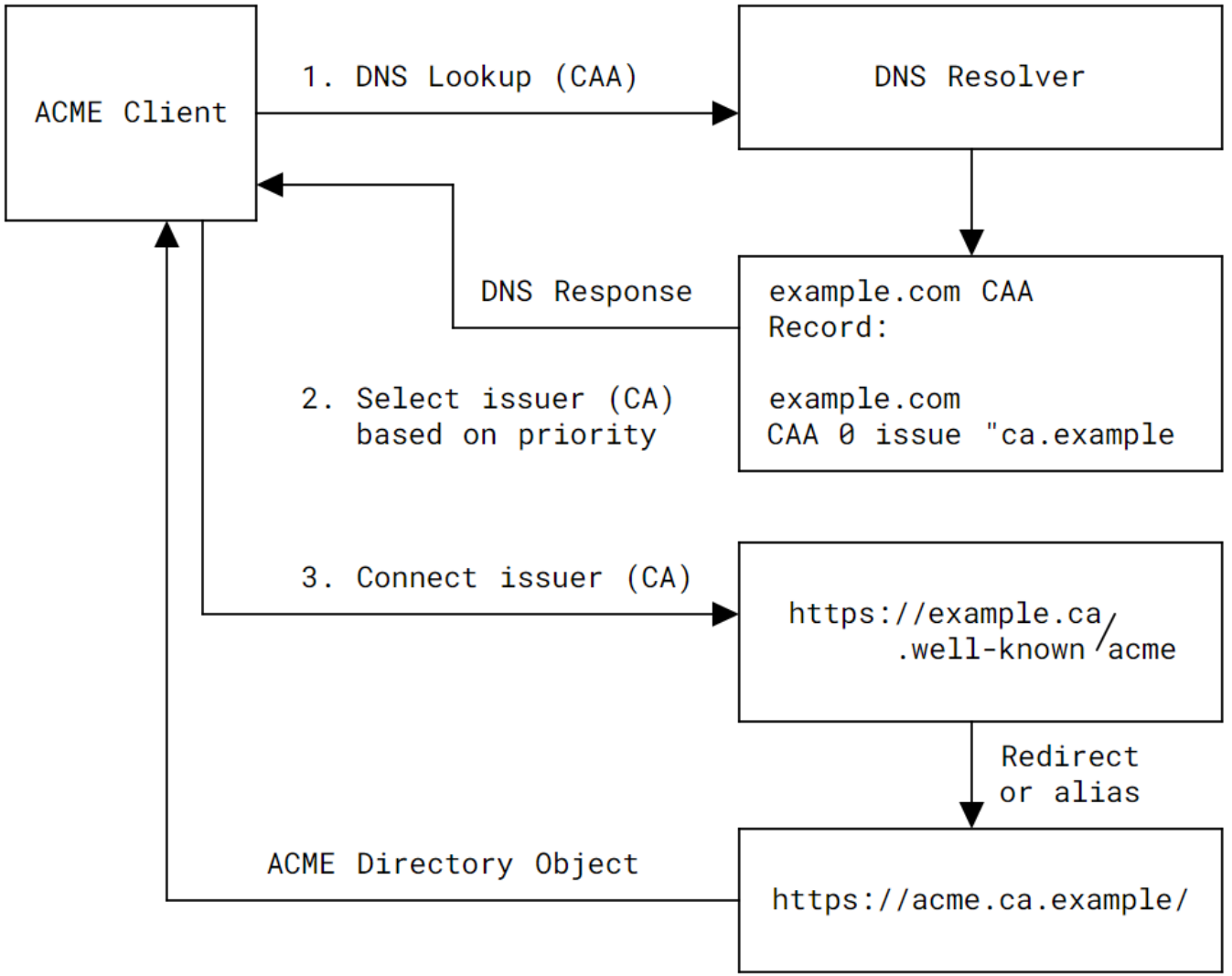
… you would think there's enough info here
to send ACMEbot to the Joe's preferred ACME server …

ENTRUST

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.”

Q Missel

Thanks Q!

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

ENTRUST

ADOPT?

- Is this useful?

- draft-vanbrouwershaven-acme-auto-discovery

ENTRUST

POINTS RAISED ON-LIST

TERMS OF SERVICE

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

Raised by: Amir Omidi, 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/

ENTRUST

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/

ENTRUST

8

AOB