ACME @ IETF118

8-NOV-2023 13:00-14:00

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)

Agenda

- Note Well, Agenda Bashing, and Technical Issues
- Document Status
- Presentations:
  - ACME for Onions (Misell)
  - ACME Auto Discovery (Ounsworth, Van Brouwershaven)
- AOB

Document status

Last time at the ACME meeting...

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.**

Document Status (1/2)

- draft-ietf-acme-subdomains was published as RFC 9444.
  - Thanks to Owen, Richard, Tim and Michael for all the work.
- draft-ietf-acme-authority-token and draft-ietf-acme-authority-token-tnauthlist were published as RFC 9447 and RFC 9448 respectively.
  - Thanks to Jon, Mary, David and Chris for the work.
  - Thanks to Rich Salz for shepherding them.
- These three RFCs bring ACME's total to 10 RFCs.

- ACME-ONION got a revision last month. Presentation today.

Document status (2/2)

- ARI got revision -02 in August. No discussion on the list since then. No presentation today.
- ACME-Client got revision -07 in Augutst. No discussion on the list. No presentation today.
- DTN-nodeId revision -11 in August. Publication requested, but still stuck waiting for Roman for 383 days.
- Device Attestation got revision -01 in July. No discussion on list.
- ACME integrations in RFC editor's queue. Waiting for an ANIMA draft and a LAMPS draft
- Account-Challenge – no new draft since last time. No discussion

- draft-vanbrouwershaven-acme-auto-discovery – revision -02 from last month. Presentation today
- draft-giron-acme-pqcnegotiation – revision -02 from July. No discussion or presentation.

presentation

ACME for Onions

ACME FOR ONIONS

draft-ietf-acme-onion

Q MISELL, GLAUCA DIGITAL

IETF 118, Wednesday 8th of November 2023

Fedi: @q@glauca.space

Email: q@as207960.net

CURRENT STATE OF THINGS

- Adding the CA/BF methods to ACME is uncontroversial
- CAA isn't quite there

WHY CAA?

- Consistency with every other TLD
- Reduce chances of mis-issuance
- Enforce organisational policy
- Publish IODEF endpoint/contact details

HOW DID -00 DO THIS?

Extra field in the Tor hidden service descriptor

IMPLEMENTATION CHALLENGES

- CAs need to run a Tor client
- Audits for the Tor client
- Client memory safety

SOLUTION: CAA OVER ACME

Tor directory authorities are already untrusted in the security model.

The HS descriptor is verified purely using the service's public key.

The ACME client can send the signed CAA records in the ACME exchange without reducing cryptographic guarantees.

`inBandOnionCAARequired` to signal the CA requires this method.

WHERE TO PUT CAA?

1. In the challenge response, or
2. In the finalize call

IN THE CHALLENGE RESPONSE

- Constrains all protocol modifications to one API method.
- Certificate must be issued within 8 hours of a challenge response.

IN THE FINALIZE CALL

- Allows issuance at any time
- Allows using other validation methods

```
{
  "csr": "MIIBPTCBxAIBADBFMQ...FS6aKdZeGsysoCo4H9P",
  "onionCAA": {
    "5anebu2...2qd.onion": {
      "caa": "caa 128 issue \"...",
      "expiry": 1697210719,
      "signature": "u_iP6JZ4JZB...pxAA=="
    }
  }
}
```

```
"onion-caa|" || expiry || "|" || caa
```

Is this the right way to do it?

QUESTIONS?

Q MISELL, GLAUCA DIGITAL

Slide deck available at magicalcodewit.ch/ietf118-slides/

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

presentation

ACME Auto Discovery

ACME Auto Discovery

draft-vanbrouwershaven-acme-auto-discovery

Mike Ounsworth, Paul van Brouwershaven

ACME WG

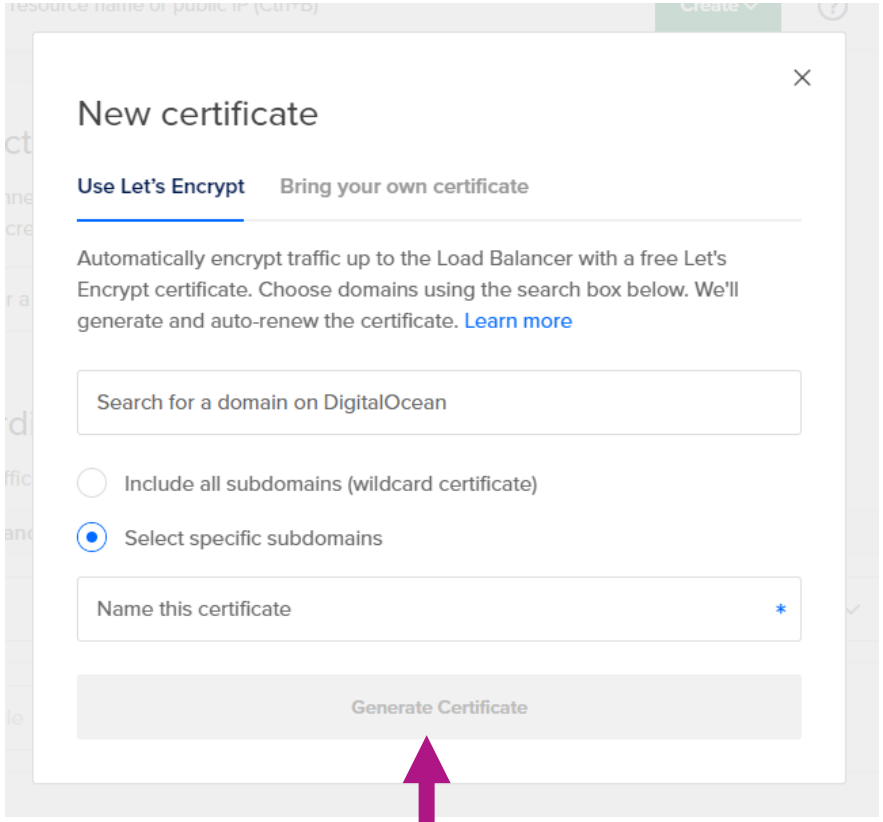
IETF 118 – Prague | November 2023

ENTRUST

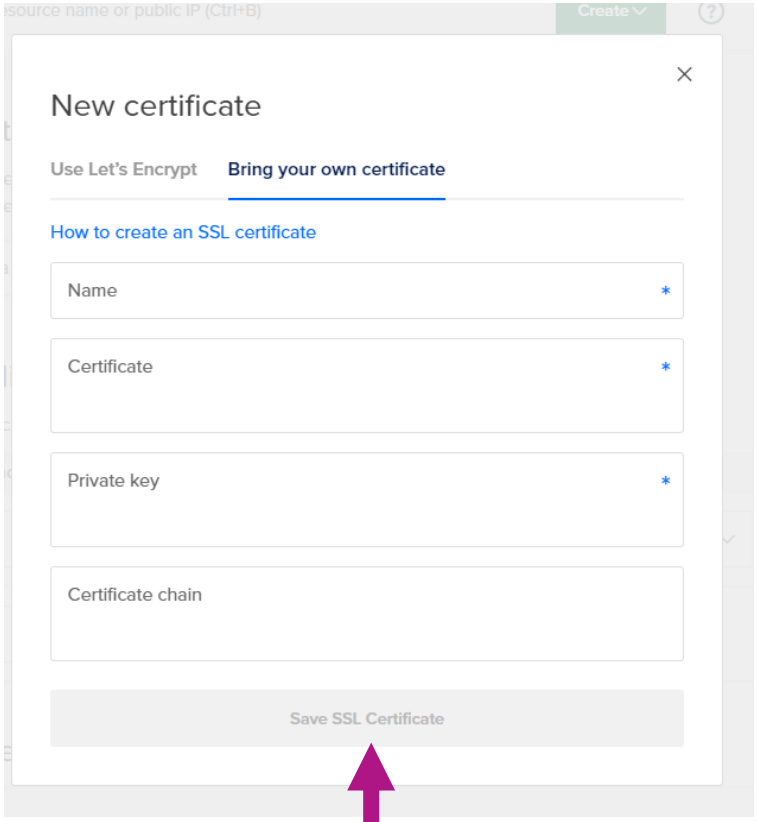
SECURING A WORLD IN MOTION

Problem refresher from 117

DIGITALOCEAN - 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.

3

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 risks becoming a single 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?

4

ENTRUST

PROBLEM

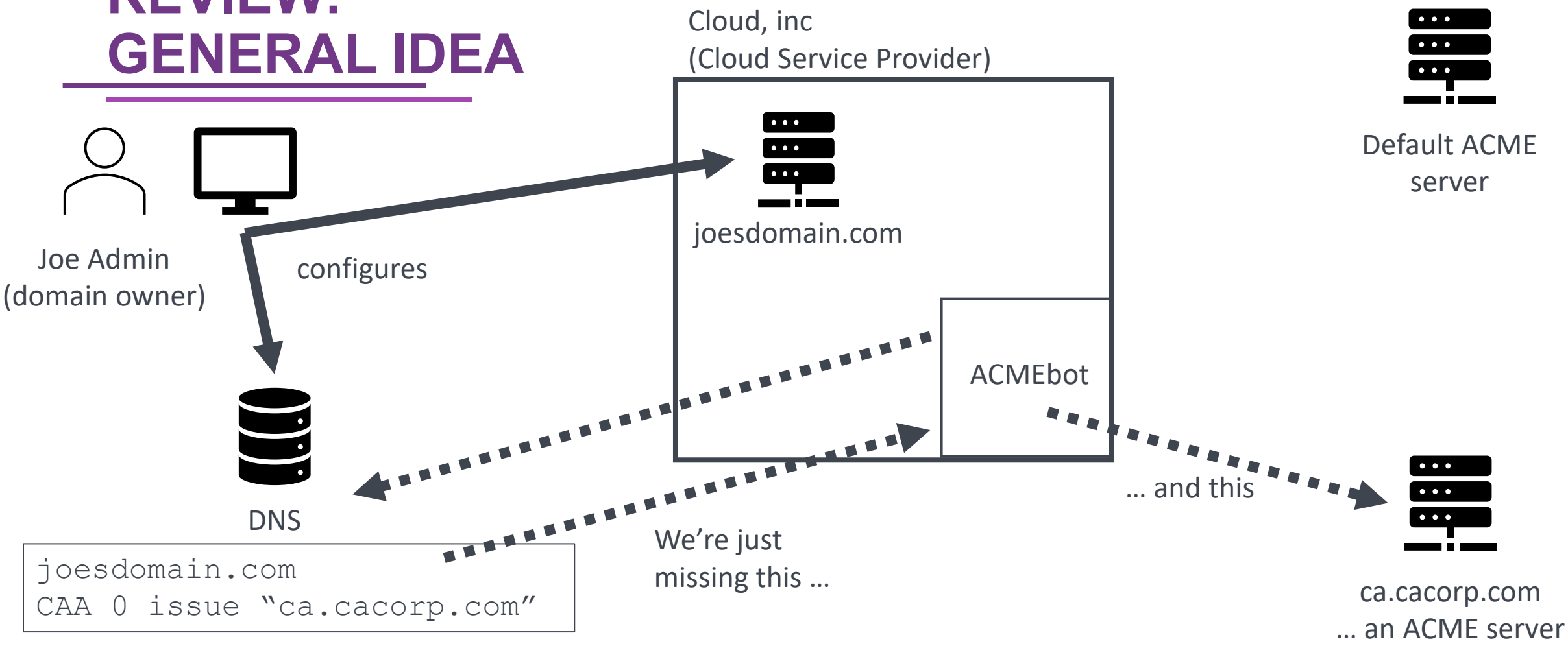
- A certificate with a validity of 90-days ‘requires’ automation
  - Renewing a certificate manually 4-6 times will not be ‘appreciated’
- When subscribers can’t specify their preferred ACME server, the **default** will become the norm!
- If the default is the norm, we **lack issuer diversity** which risks becoming a single 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?

5

ENTRUST

REVIEW: GENERAL IDEA



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

6

ENTRUST

Current Status

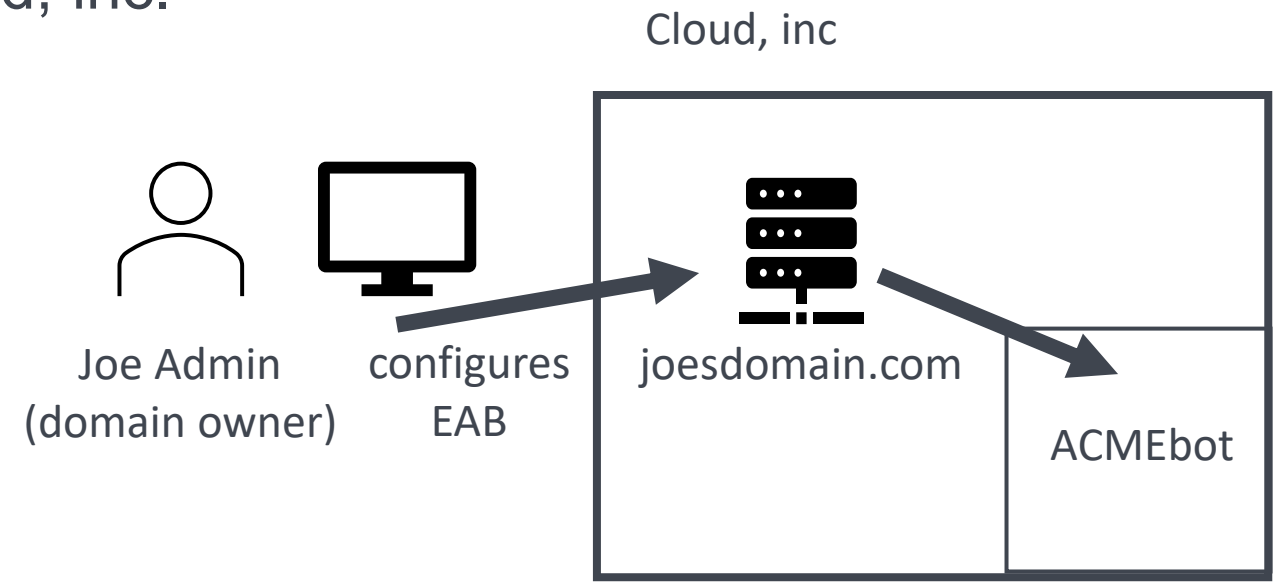
Status

- A new draft (-02) was released incorporating the feedback received.
- We have identified (and are attempting to solve) more challenges around the external/internal account binding mechanisms.
  - General problem: How to associate incoming ACME requests with the correct CA account?
  - Sub-Problem 1: The ACME account will be owned by the CSP and may either be re-used across all customers they manage, or may be a fresh account per ACME request.
    - So we cannot use ACME account to retrieve the appropriate CA account.
  - Sub-Problem 2: multiple CA accounts are authorized to issue for the same domain.
    - So we cannot use requested domain to retrieve the appropriate CA account.

ENTRUST

Problem 0: External Account Binding keys

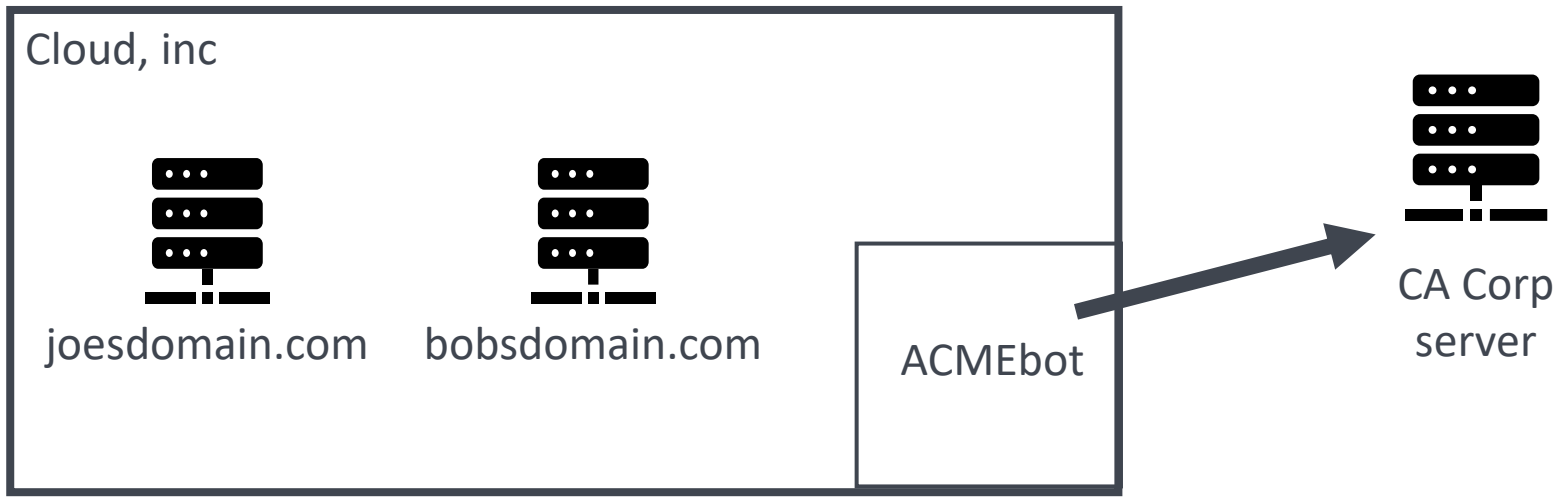
- ACME already has External Account Binding keys, but they can't be leveraged here because:
    1. Passing Joe's EAB key down to ACMEBot requires UI changes in Cloud, inc.
    2. Joe's EAB key may have more permissions than Joe really wants to share with Cloud, inc.



ENTRUST

Problem 1: ACME accounts are not unique per CA account

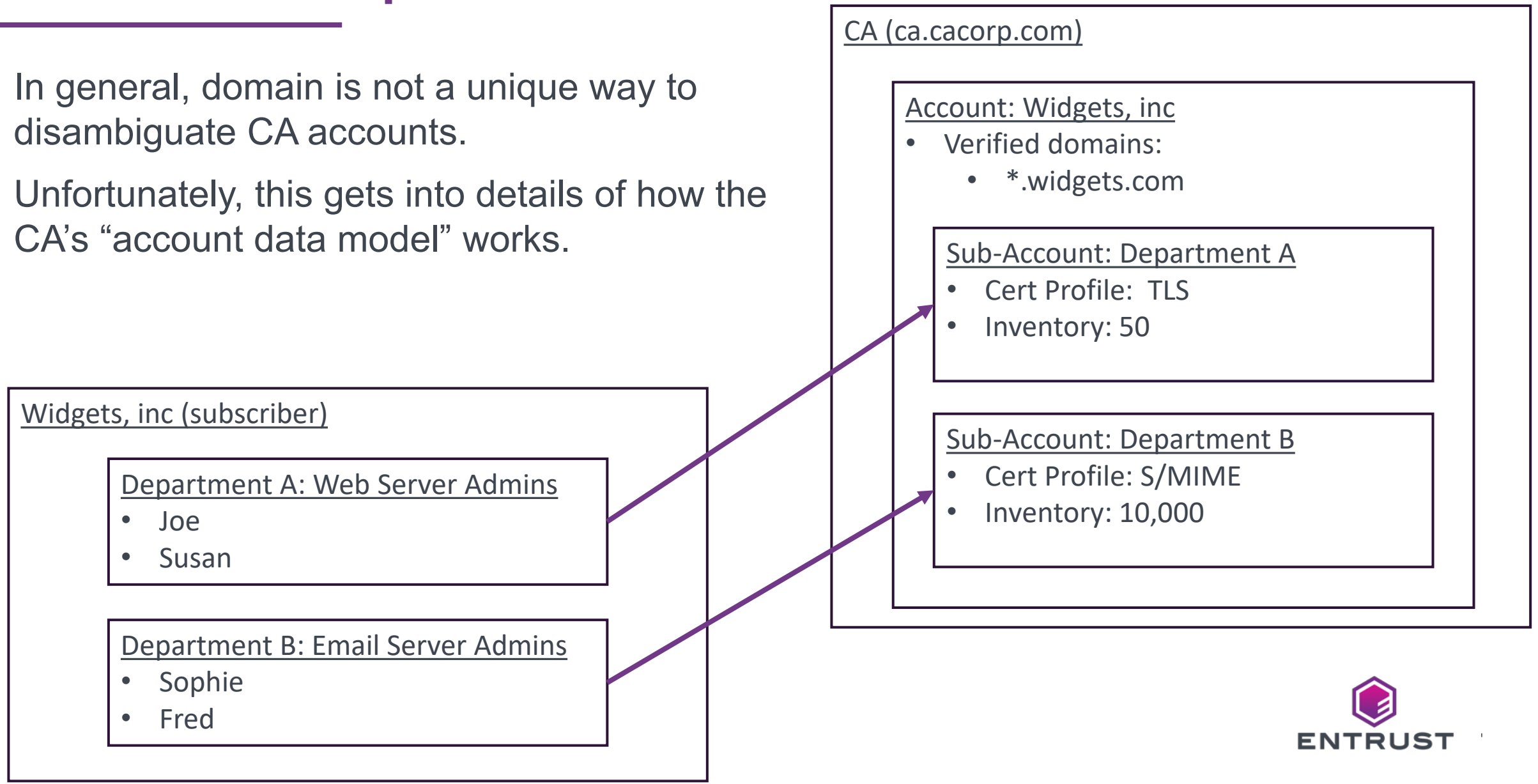
- Most service providers currently work by either having a single ACME account per CA, or generating throwaway ACME accounts – ex.: Certbot automatically creates a new account for each ACME server but doesn't know anything about users, actually, Cerbot creates the account keys in a shared config folder by default.
- This problem is described in section 9.3 of the security considerations of the draft.



ENTRUST

Problem 2: Multiple CA accounts for the same domain

- In general, domain is not a unique way to disambiguate CA accounts.
- Unfortunately, this gets into details of how the CA's "account data model" works.



ENTRUST

Potential Account Binding (AB) Mechanisms

External AB

- Not supported by Cloud Service Providers (CSP).
- Unlikely to gain support as it requires interface and implementation changes by the CSP.
- Requires a unique account per CSP customer.

Internal AB (email)

- Described in section 7.1.2 of the draft.
- Prone to phishing attacks.
- Easier to implement than the EAB as required information (email) is already known by the CSP.
- Requires a unique account per CSP customer.

Internal AB (DV)

- Described in section 7.1.1 of the draft.
- Does not require any CSP changes.
- Requires a unique account.

ENTRUST

Potential Account Binding (AB) Mechanisms

External AB

- Not supported by Cloud Service Providers (CSP)
- Unlikely to gain support as it requires interface and implementation changes by the CSP
- Requires a unique account per CSP customer

Internal AB (email)

- Described in section … of the draft
- Prone to phishi…
- Easier to imple… the EAB as re… information (e… already known…
- Requires a uniq… per CSP custom…

Int… AB (DV)

… 7.1.1

Design is still ongoing, we're not sure this is right yet.

More vendor input is needed here!

For example, is email really the right mechanism? What about a UUID in the CAA DNS record to disambiguate accounts? Or maybe {domain + cert profile} is unique? More design needed.

ENTRUST

Shared Account Binding

- Not described in the draft, looking for feedback
- Similar to where the CSP (Cloud Service Provider) is a reseller of the CA and uses one set of API credentials for multiple customers, except there would be no contract between the CA and the CSP
- The ACME key could identify the CSP, to allow CA customers to enable specific CSP
  - The CSP could publish its public key(s) in its well-known directory
  - The CSP could obtain a certificate for it's ACME key and include it in the x5u parameter of the JWK
    - less likely to see broad adoption, involves validation costs and renewal procedures
  - A challenge response with the account key email address could be performed (based on the CSP domain, e.g., @aws.com)
    - less likely to see broad adoption, requires (automated) acknowledgement on the CSP side
- Domain Control Validation determines if the CSP is authorized to issue this certificate

ENTRUST

Summary & Next Steps

- This draft **slowed down** when we realized there's a hard problem buried in here.
- We need more design iteration on how to disambiguate which CA account a given ACME request should be associated with – we may need to consider authentication and authorization separately.

- This may need **a design group** of CAs and CSPs to make sure we've captured and addressed the sticky cases properly (some of which may be CA-specific).

ENTRUST

Thank You

Mike.Ounsworth@entrust.com

Paul.vanBrouwershaven@entrust.com

entrust.com

AOB

Any Other Business