ACME @ IETF 115

10 November 2022

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

I E T F®

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)

Resources for IETF 115 in London

- Agenda https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information: https://www.ietf.org/how/meetings/115/preparation
- If you need technical assistance, see the Reporting Issues page: http://www.ietf.org/how/meetings/issues/

Agenda

- Note Well, Technical difficulties, and Administrivia
- Document Status (chairs)
- Current work items:
  - draft-ietf-acme-dtnnodeid-10 (Sipos)
- (Potential) new work:
  - draft-bweeks-acme-device-attest-01 (Weeks)
  - draft-todo-chariton-dns-account-01-01
- AOB

Document Status

- No new RFCs (3rd meeting in a row) ☹
- acme-client has been allowed to expire
- acme-ari: -00 WG draft submitted
- acme-authority-token
  - Version -09 submitted last month
  - Approved!
- acme-authority-token-tnauthlist
  - Versions -09 and -10 submitted since Philadelphia
  - Still has DISCUSSes that require a revision

Document Status

- dtnnodeid
  - Latest revision from September
  - Presentation today
  - Still waiting on IANA registry changes
- acme-integrations
  - Version -10 from September
  - AD evaluation
  - Revised I-D needed

Document Status

- acme-subdomains
    - No new revision
    - In IETF LC

draft-ietf-acme-dtnnodeid

ACME DTN Node ID Validation

IETF 115 ACME WG

Brian Sipos
JHU/APL

Current Status of Draft

- Latest is https://www.ietf.org/archive/id/draft-ietf-acme-dtnnodeid-10.html
- Changes since -09:
  - Corrected typos
  - Added aside paragraphs to explain the experimental nature of each aspect of the validation method
  - COSE Hash Algorithms is now RFC 9054
- Known issues remaining:
  - The companion document to update the IANA sub-registry for Bundle Protocol is up for DTN WG adoption

draft-bweeks-acme-device-attest

draft-bweeks-acme-device-attest

Brandon Weeks
IETF 115

Changes since IETF 114

- Clarifying that verification procedures are out of scope
- IANA registry creation for attestation statement formats
  - Borrowed from draft-wallace-lamps-key-attestation-ext

Drafts encapsulating attestation statements (evidence)

- draft-bweeks-acme-device-attest
- draft-fossati-tls-attestation
- draft-wallace-lamps-key-attestation-ext

Implementations of the current draft

- iOS / tvOS
- step-ca certificate authority

draft-todo-chariton-dns-account-01

DNS-ACCOUNT-01

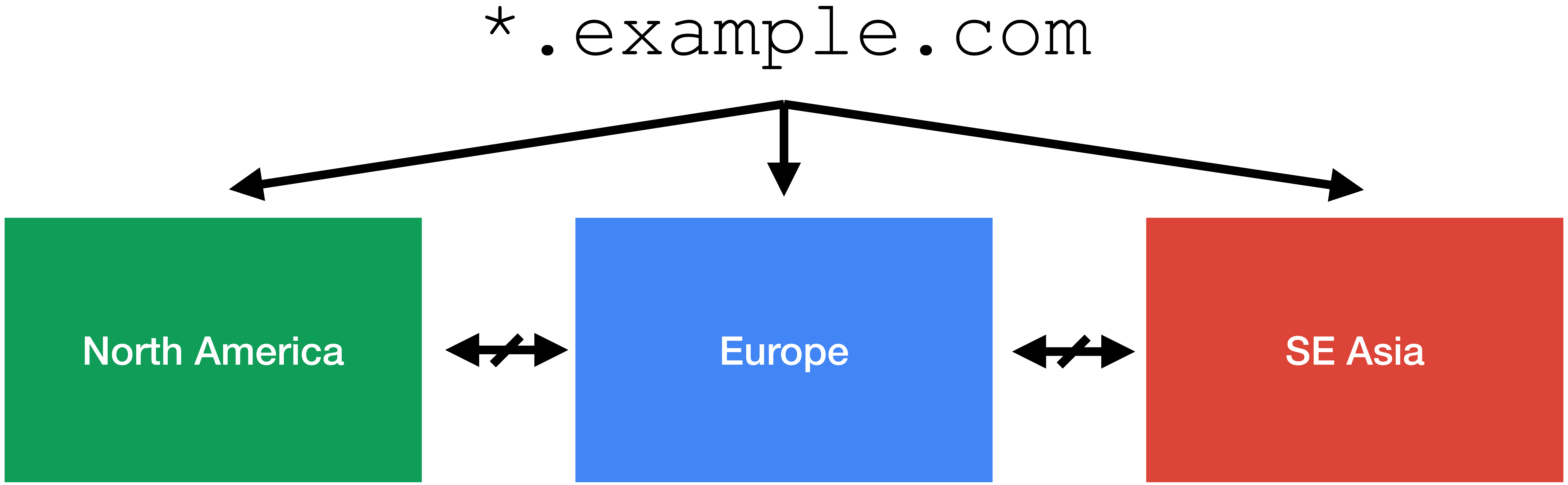
Antonios Chariton, Amir Omidi, James Kasten,
Fotios Loukos, Stanisław Janikowski

DNS-01

_acme-challenge.example.com

```
_acme-challenge.example.com
IN CNAME
challenge-solver.example.org
```

Multi-Region Deployments



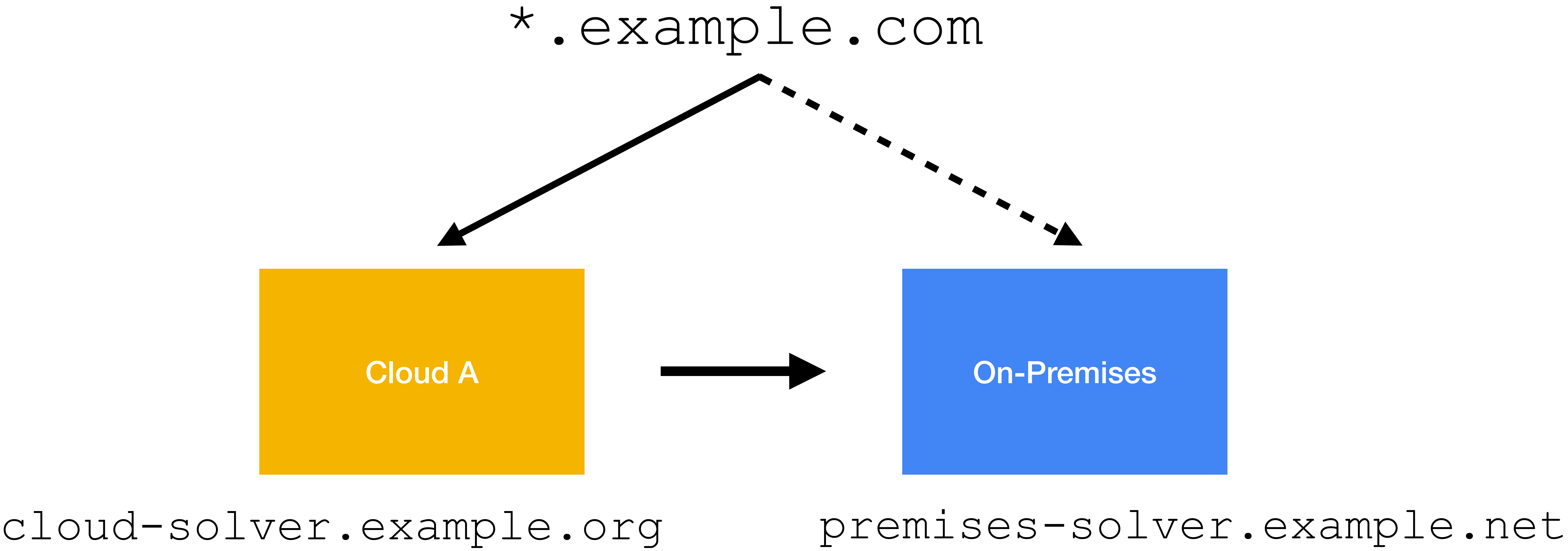
*.example.com

North America

Europe

SE Asia

0-Downtime Migrations



Things to avoid

- Manual work
- Copying of private keys around
- Downtime
- Dependencies between autonomous regions

```
_acme-challenge.example.com
IN CNAME
challenge-solver.example.org
```

```
_acme-challenge.example.com
IN CNAME
challenge-solver.example.org
challenge-solver.example.net
```

DNS-ACCOUNT-01

_acme-challenge_aqsjotdikmbjarmm

acme-challenge****aqsjotdikmbjarmm

#1

`_acme-challenge_aqsjotdikmbjarmm`

```
aqsjotdikmbjarmm

base32(sha256(AccountResourceURL)[0:9])
```

aqsjotdikmbjarmm

base32(sha256(AccountResourceURL)**[0:9]**)

#2

```
_acme-challenge_aqsjotdikmbjarmm
IN CNAME
solver01.example.org

_acme-challenge_igdhq74wtezyyhzv
IN CNAME
solver02.example.net
```

WebPKI

CA/B F BR 3.2.2.4.7

Resources

- Latest HTML Draft
  - https://daknob.github.io/draft-todo-chariton-dns-account-01/
- Latest TXT Draft
  - https://daknob.github.io/draft-todo-chariton-dns-account-01/draft.txt
- Datatracker
  - https://datatracker.ietf.org/doc/draft-todo-chariton-dns-account-01/

AOB