ACME FOR ONIONS
draft-ietf-acme-onion
Q MISSELL, GLAUCA DIGITAL

IETF 118, Wednesday 8\textsuperscript{th} 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
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