Since IETF 117

- draft-ietf-acme-03
  - Changed computation of certificate identifier
  - Removed POST to renewalInfo endpoint
  - Add “replaces” field to Order objects

- draft-ietf-acme-04 (upcoming)
  - Lots and lots of small phrasing improvements
Certificate Identifier

- Difficult to extract CertID from existing OCSP implementations
- Requires access to the issuer cert

\[
\text{base64url(DER(ASN.1 OCSP CertID))}
\]

- Only requires information from the end-entity certificate
- Server can be counted on to know its own AKID value

\[
\text{base64url(AKID keyIdentifier) || . || base64url(DER(Serial))}
\]
Updating the Server

- Add a new field to Order request and response objects:
  
  "replaces": "aYhba4dGQEHhs3uEe6CuLN4ByNQ.AId1QyE",

- Removes the need for additional network roundtrip
- Gives server more useful information
- Carrot for client adoption: replacement orders may bypass rate limits
Editorial Improvements

- Compliant IANA Considerations section
- References to RFC3647 and RFC5280 up front
- Improvements to phrasing found by folks who already read draft-03
Acknowledgements

- Clients: Samantha Frank, Ilari Liusvaara, Matt Holt, and Wouter Tinus
- Servers: Freddy Zhang
- Editorial feedback: Rob Stradling and Amanda Barber
Open Questions

- Mandate 409 Conflict response code for “replaces” collisions?
  - and/or a new ACME error type?

- WG Last Call?