acme-tls-alpn

tls-sni replacement

- tls-sni had unexpected interaction with major hosting providers
- Providers allowed users to claim arbitrary SNI names
- This allowed users to serve traffic for the tls-sni validation names despite not controlling the DNS name being validated
- A TLS layer validation method is still useful for a number of use cases
    - Clients embedded in non-web servers
    - Clients embedded in TLS terminators/balancers
    - Hosting providers managing TLS for customers

Method

1. Connect to host

2. Initiate a TLS handshake with a ClientHello containing a ALPN extension containing “acme-tls/1” and a SNI extension containing the name being validated

3. Verify the ServerHello contains a ALPN extension containing “acme-tls/1” and a self-signed certificate for the name being validated that contains a critical acmeValidation extension

4. Compare the contents of the acmeValidation extension with expected validation token

5. Close connection