STAR Requests

draft-sheffer-star-requests@ietf.org
Outline

• Problem statement
• History
• How does STAR Requests work
• Next steps
Glossary

- **IdO**: Identity Owner (think Content Provider)
- **NDC**: Name Delegation Client (think CDN)
- **CA**: ...
Problem statement

• NDC need to terminate HTTPS using the IdO name and really want to avoid handover of IdO’s private key between IdO and NDC

• In CDN / CP case, the scope is DNS-based redirection, as opposed to HTTP 302 redirection or URL rewriting techniques

• STAR Request, coupled with a cert issuance protocol equivalent to ACME STAR, allows IdO-controlled name delegation without key sharing

• Why bother standardising it?

• IdO and NDC typically belong to different organisations
History

• STAR Requests was once one with ACME STAR (proposed as an alternative to the LURK / Keyless SSL style approach)

• Separated out at the time ACME STAR was adopted (because, strictly speaking, it is not an ACME extension)

• Now that ACME STAR enters WGLC, it looks like time is ripe for STAR Requests to find a home, so to have a complete solution for the name delegation problem
How does it work

- Bootstrap
- NDC requests name delegation
- IdO requests an ACME STAR cert from CA
- NDC polls STAR cert endpoint
- IdO terminates the name delegation
- NDC and IdO agree on a "CSR template" (including naming constraints, key sizes and algorithms, cert extensions, etc.)

- NDC and IdO set up a mutually authenticated channel (TLS with client certificates, VPN, IPsec, ...)

- IdO has an ACME account set up with an ACME CA
Requesting name delegation

- NDC generates key pair and fills the CSR template
- NDC sends the request including the CSR and proposed renewal timer and lifetime (these can be rewritten by the CA)
ACME STAR cert request

- IdO runs ACME + STAR extension with CA
STAR cert is issued

- IdO obtains the STAR cert endpoint from CA
- STAR cert endpoint is returned to the NDC
NDC fetches the STAR cert at regular intervals

- CA refreshes the STAR cert
- NDC fetches from the STAR cert endpoint at the agreed rate
IdO terminates the name delegation

- IdO terminates STAR certificate
- CA returns an error at next NDC fetch
- The cert expires shortly after
Next steps

- This is a security protocol, we'd really like to have in-depth security review (ISE could not be enough)

- ACME STAR is not necessary but it's sufficient (also, it's the only cert issuance protocol with the required characteristics that we can rely on at the moment)

- We think ACME WG is the most natural destination

- Discuss...