Introduction

- Regarding TLS certificates, the LURK BoF feedback is that CSPs and CDN providers are reluctant to share private keys mainly because of legal and security issues about private keys.

- The CDNI working group is still looking for a solution that avoids the exchange of private keys between CDNs.

- We proposed a new draft to specifically based on LURK in CDNI: the objective is to propose a solution for delegating content delivery.
High level architecture

1. TLS clientHello
2. TLS serverHello
3. Certificate
4. ServerKeyExchange

... Continued

LURK (or whatever) Exchanges
Use Cases

- The draft presents 2 use cases
  - A: Origin certificate under the uCDN authority
  - B: Origin certificate under a 3\textsuperscript{rd} party authority
Next Steps

- It is likely that LURK key server interface is not going to be specified.

- Other approaches are being discussed at the IETF to provision adhoc certificates instead of keying information.

- Could those approaches be considered by the CDNI WG in a further work?

- Do we update the draft with these approaches?