Latest changes

- Added a section on HTTPS delivery delegation requirements
- Rephrased HTTPS section
- Added a section on a Lurk in CDNI
HTTPS delivery requirements

- **on user side**
  - The end-user wants to have its content delivered over the CP domain whatever the CDN chosen
  - User agent: cert and domain must match

- **on CDN side**
  - A uCDN must designate the dCDN to deliver the requested content in a secure way
  - The uCDN and dCDN must be able to provide the CP/uCDN certificate to the user agent
  - A uCDN should not expose the CP private keys to the dCDN
  - A uCDN must provide the necessary credentials to the dCDN when delivering contents to the UA
Lurk interface for CDNI

- Lurk for CDNI would allow the Content provider (or uCDN) private keys to remain under his authority, while contents would be delivered by a dCDN using his certificate

- [https://tools.ietf.org/html/draft-mglt-lurk-tls-use-cases-00](https://tools.ietf.org/html/draft-mglt-lurk-tls-use-cases-00)

- Several use cases for CDNI
  - “Nominal”: KS under the uCDN authority
  - “Cascaded”: KS under the CP authority
  - ...
"Nominal" case for HTTPS delegation using Lurk

A uCDN delegates the HTTPS content delivery to a dCDN.

The uCDN doesn’t want to provide the dCDN with its private keys (i.e. for legal/security/… reasons)

Only the uCDN needs valid certificates received by the Content Provider (CP), whereas the dCDN would rely on security materials received from the uCDN Key Server (KS) for the TLS session establishment.

The dCDN will deliver HTTPS content to the user agent using the uCDN (or CP) certificate.
Discussion

- Architecture
- Certificates
- Security
- ...
Next steps

- Other “Lurk” use cases for CDNI
- Detail token based solutions