Confidentiality and Authorization

stephen.farrell@cs.tcd.ie

Assumptions

- No new crypto, just standard primitives
- A “pure” ICN approach without host-based networking
- Multiple mutually untrusting caches

- Caveat: I'm not up to date on the literature

Confidentiality

- If we want confidentiality then we have to encrypt
- If we encrypt we need key distribution in some form (D-H, key transport, ...)
- If we have key distribution we need to restrict access to keys
  - So we need authorization for confidentiality

Authorization

- If we need authorization we have to restrict access to data
- To do that we need
  - ACLs (or similar) and authentication at caches
    - => ACLs are public or encrypted
      - If public, does that meet requirement
  - Or
  - Encrypted content with keys released to authorized parties only
- In either case we need confidentiality

Conclusion

- Under the assumptions outlined...
- Confidentiality needs authorization
- Authorization needs confidentiality
  - Hmmm....