Entity Key Discovery
< draft-miller-saag-key-discovery >

Matt Miller, Suhas Nandakumar

IETF 93

Problem Statement

- ***Given a thing that is encrypted …***
  - Single Object (file, email message)
  - Stream (MUC room, video conference)
- ***… How to find a key for that Thing?***

A Proposal

- Use WebFinger to query a URI for a key
  - ‘acct:’ for users
  - ‘key:’ for anything without a well known URI
- Response is URL where to find the Key
  - Holder could require authorization
- Key in JOSE format
  - Could be encrypted (JWE)

Next Steps

- Comments and reviews
- Key retrieval draft coming
- BoF?

END OF LINE