

# ACE Clients in Disadvantaged Networks

draft-secheverria-ace-client-disadvantaged-00

Ludwig Seitz (ludwig.seitz@ri.se)

IETF 104 ACE WG meeting  
March 29, 2019

# Disadvantaged Networks

- Conditions worse than for “constrained networks”
  - Disconnected, Intermittent, Limited (DIL)
  - High risk of sabotage, impersonation, device capture
- Scenarios: First responders, Law enforcement, Military
  - AS wants to revoke tokens for compromised RS
  - Clients want to check their tokens are still valid

# Alternatives

- Short token lifetime
  - AS stops making tokens for known compromised RS
  - Problems:
    - Waste of bandwidth for requesting new tokens
    - “Good” tokens may not be valid long enough
    - How to interpret denied token request?
- Token revokation & Client introspection
  - AS revokes tokens of known compromised RS
  - C checks tokens when AS in range

# Token Revocation and Client Introspection

- Problem: Attackers may learn token claims
  - Differentiate between clients and RS
    - AS only returns “Active” parameter for clients
- Problem: AS needs to decrypt the token
  - Need to find the key shared with the RS
    - include a “kid” in COSE wrapper

# Next Steps

- Is there WG interest to explore specific problems of disadvantaged networks?