TLS-PSK

JUST USE SECRETS PSK

ALAN DEKOK, MAY 2023
NOT MUCH TO SAY

- The main issue with TLS-PSK is administrative interfaces
  - UI, API, etc.
- Feedback from the community has been that certificates are “hard”
  - Some more quantitative data would be useful
CHANGES FROM NORMAL RADIUS

- We need to the client to have an *identity* in addition to a *secret*
  - Identity was previously implicit in the network configuration
  - This TLS-PSK identity should not be automatically determined
    - e.g. IP address
  - Should not use the same secret for RADIUS and for TLS-PSK