TLS-PSK

JUST USE SECRETS PSK

ALAN DEKOK IETF 116
PSK IS GOOD

- Certificates are hard
  - They’re large, they expire, they require many certs to work
- PSK is simpler.
  - RFC 6614 and 7360 omitted discussion of PSK
- PSK has been implemented in FreeRADIUS for ~10 years
  - radsecproxy a little less
CHANGES FROM SHARED SECRET

- We need an *identity* in addition to a *secret*
- This identity should not be automatically created (e.g. IP address)
- System interfaces need to change (UI, API, etc)
- Should not use the same secret for RADIUS and for TLS-PSK
THE DOCUMENT

‣ Largely a discussion of why to use PSK

‣ And guidance on how to use it

‣ Open issues:
 ‣ credential sharing: good, bad, terrible?