eduroam Trust mangement

Overview

- eduroam is
  - Wi-Fi roaming consortium
  - for users in education and research only
  - Based on IEEE 802.1X and EAP
  - transmitted over RADIUS proxies

- Eduroam has
  - > 1K hotspots in Europe
  - > 1M European users

Trust management (classic)

- Request routing by NAIs with domain names
- RADIUS aggregation by proxies: one per ccTLD
- ccTLD proxies aggregated to world region proxies (3; Europe, Asia-Pacific, Americas)
- Connection of new participants via OOB signalling of pair (IP-address;shared-secret)
- Sync which world region hosts which ccTLD: OOB sync between world region operators
- gTLD realms don't come easy (at all)!

Trust management (new)

- 1st step: replace RADIUS with RadSec, keep hierarchical aggregation
- 2nd step: dynamic discovery (DNS) + PKI to short-cut or eliminate hierarchy
- accomodates gTLD realms much more easily
- Eliminates SPOFs
- replaces OOB transmission of shared secret with OOB certificate requests

Challenges

- Requires PKI management for multiple existing CAs (PMA, policy OIDs)
- This is not supposed to start a flame war!
  - Some people dislike PKI concept.
  - But we think this works for us.
- Problem: if PKI doesn't work – what are the options?
  - There aren't any.
  - Having options is a luxury I'd like to have.
  - Moonshot KNP can be one.