ERP for IKEv2

draft-nir-ipsecme-erx-02

What's ERP

- ERP (RFC 5296) was defined by Hokey
  - -bis document just ended LC
- ERP adds a quick re-authentication to EAP.
  - Do the full EAP method with an Authenticator
  - Subsequent EAP exchanges with other authenticators or the same are quicker
    - And don't require human intervention
  - Defines two new EAP packets:
    - Initiate (5)
    - Finish (6)

Use Case for VPN

- Mobile device uses 802.1x within the building.
  - Has an EAP session and a "rRK"
- The user leaves the building, and moves to the cellular network.
  - A VPN connection is now needed to access corporate resources.
- The VPN client establishes a tunnel, using the saved rRK with no user intervention.

What the Draft Contains

- Minor changes to the protocol
  - Client requests renegotiation, so EAP-Initiate message in first IKE_AUTH request
  - Gateway replies with EAP-Finish in first IKE_AUTH response
- Clarification that the new packets are allowed.
- Discussion of applicability of the Hokey scenario with multiple AAA domains.

Questions?