Usage Specific Root Keys (USRK)

IETF 67

Joe Salowey

jsalowey@cisco.com

Problem

- Allow multiple keys for multiple purposes to be derived from a single root key
- Prevent one usage from interfering from another
  - Cryptographic separation
  - Coordinated derivation
- Preserve the security of the EAP EMSK
  - Could be applicable to other keys

Some History

- Originally Application Master Session Keys (AMSK)
  - draft-salowey-eap-key-deriv (Salowey and Eronen, 2003)
- Refined to Usage Specific Root Keys (USRK)
  - draft-salowey-eap-emsk-deriv-01.txt (Salowey, Dondetti, Narayanan, and Nakhjiri, 2006)

USRK

- USRK is a root key for applications to use to derive keys for specific cryptographic purposes
- USRK derivation controlled by USRK framework
- URSK application specified in usage definition
  - Usage Specific Key usage
  - Management recommendations

USRK Framework

- **USRK = KDF(EMSK, label, optional data, len)**
  - EMSK from EAP
  - Key Label assigned by IANA for usage
  - Optional data
  - Key length
- PRF flexible
  - Default based on HMAC-SHA-256
  - Can be influenced by key exchanges and system configuration

Questions?