Key Management Discussion

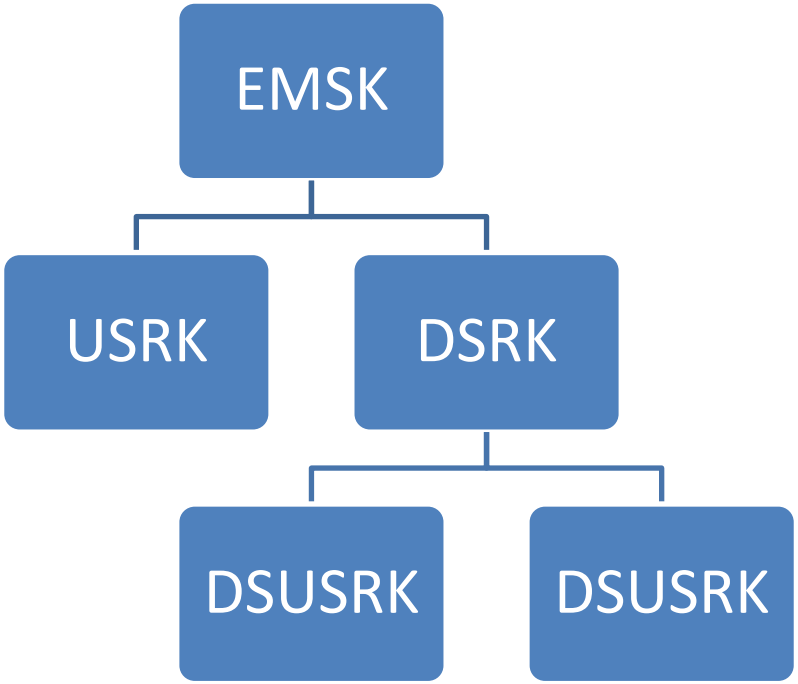
IETF 72

Dublin, Ireland

29 July 2008

Document Goal

- Interoperable delivery of USRK, DSRK, and DSUSRK
- Deliver to AAA entities using RADIUS or Diameter



IETF 70 Consensus

- AAA-based protocol transport
- Required support for hop-by-hop security associations in key transport
- Consistent with interpretation of RFC 4962

IETF 71 Discussion

- Need to define the remaining required security properties
- Key issue: requirement for peer consent
  - Does the peer have to authorize distribution of its keying material to AAA entities?
- ERX Authorization Attack
  - Problem: AAA domain can send bogus accounting records to bill you when you've never been in their domain
  - Solution: ERX bootstrap required when moving between domains to provide peer consent

IETF 71 Consensus Call

- Should HOKEY rely on AAA transport security?
  - Use existing encrypted attributes or [D]TLS tunnel
  - Strong room consensus for AAA transport
- Should HOKEY support non-AAA transports?
  - Support raw UDP, etc
  - No consensus
- Is peer consent a property we need to support?
  - Technical solution versus security considerations
  - Room consensus that peer consent is not required

IETF 71 key-mgm Document Plan

- Document Changes
  - Remove all encryption from existing key-mgm document; elimination of KDE0, KDE1, and KDE 4
  - Lay out security requirements for hop-by-hop security, apply to all transports
  - Define RADIUS attribute for key request and transport to meet HOKEY needs
- Documented as Issues 40, 41, 42
- Room consensus to pursue plan
- Overlap with existing document
  - draft-gaonkar-radext-erp-attrs

Subsequent List Discussion

- List discussion between Ohba and DeKok
  - Ohba: peer consent in key distribution provides a strong technical solution to the fraud problem
  - DeKok: ERX bootstrapping solution sufficient; same level of security as existing AAA deployments
- Consensus determination
  - List discussion consistent with room discussion
  - IETF 71 room consensus valid