EMSK Key Hierarchy

draft-ietf-hokey-emsk-hierarchy-00.txt

Joe Salowey
Madjid Nakhjiri
Vidya Narayanan
Laksminath Dondeti
Proposal for EMSK Hierarchy

EMSK

USRK

CK

DSRK

DSUSRK

CK
KDF Prototypes

KDF( key, usage label, domain label, opt data )

USRK = KDF(EMSK, usage label, null, opt data)

DSRK = KDF(EMSK, dsrk@ietf.org, domain label, opt data)

DSUSRK = KDF(DSRK, usage label, domain label, opt data)

Note: dsrk@ietf.org is a usage label, not a domain label.
Hierarchy Branches

• Domain independent root
  – Usage specific root key (USRK) derived from EMSK

• Domain specific root
  – Domain specific root key (DSRK) derived from EMSK
  – Domain specific usage specific keys (DSUSRK) derived from a DSRK

• Usage definition defines if keys may be derived from the USRK, the DSUSRK or both

• Cryptographic usage keys (CK) are derived according to usage definition