Derivation, delivery and management of EAP based keys for handover and re-authentication

draft-ietf-hokey-key-mgm-00
IETF 69, July 2007

Madjid Nakhjiri
Yoshihiro Ohba
Contents

- EMSK based USRK (HOKEY) and DSRK derivation
  - Remove DSRK derivation (refer to emsk-hierarchy)?
  - Includes DSUSRK. To be removed??

- Generic Delivery Architecture (3 party)

- Generic Delivery Signaling (3 party)

- EMSK based keys for delivery protection

- USRK and DSRK based HOKEY hierarchies
  - Using [hokey-emsk-hierarchy]
  - DSHRKs
  - Delivery mechanisms for both.
Hokey key hierarchy alternatives

- **HOKEY Key hierarchy:**
  - **USRK based: EMSK->HRK->DHRK**
    - Derive HRK, deliver to Hokey server (domain independent, or home), derive DSHRK for each domain Hokey server.
  - **DSRK based: EMSK->DSRK->DHRK**
    - Derive DSRK, deliver to domain AAA server, derive DSHRK for the domain, deliver to domain Hokey server.
  - **DSUSRK based**
    - Derive DSHRK from EMSK directly, deliver to domain HOKEY server (removed from Joe’s draft?)
Key Hierarchy

EMSK

USRK (HRK)  To be removed in 01?

DSUSRK (DSHRK)  Keys

DSUSRK

DSRK  IK, CK

DIK, DCK  DSUSRK (DSHRK)

Keys

Keys

EMSK

USRK (HRK)  To be removed in 01?

DSUSRK (DSHRK)  Keys

DSUSRK

DSRK  IK, CK

DIK, DCK  DSUSRK (DSHRK)

Keys

Keys
Key Delivery architecture

EAP server

To be removed in 01?

USR-KH

USRK

DSRK

DSUSR-KH

DSUSR-KH

EMSK

USR-KH

DSR-KH
Delivery of USRK to USR-KH
(HRK to HOKEY server)

0) KH ID

1) Int [IK, (peer ID, KH ID, N, ...)]

2) Int(KIUS, Pid, KH id)
   Int [IK, (peer ID, KH ID, N,..)]
   Verify MACs and KH IDs

3) Enc (KCUS, Pid, KH id, USRK, lifetime, ...)
   Int [IK, (peer ID, KH ID, N+1,USRKname, lifetime, ...)]

4) Int [IK, (peer ID, KH ID, N+1,USRKname, lifetime, ...)]
   Install USRK

Int [K, X]=X || MIC(K, X),
Delivery of DSRK to DSR-KH

MN/ Peer

0) KH ID

1) Int [IK, (peer ID, KH ID, N, ...)]

DSR-KH

2) Int(KIDS, Pid, KH id)

Int [IK, (peer ID, KH ID, N,..)]

2) Int [IK, (peer ID, KH ID, N,..)]

Verify MACs and KH IDs

EAP server

3) Enc (KCDS, Pid, KH id, DSRK, lifetime, ...)

Int [IK, (peer ID, KH ID, N+1, DSRKname, lifetime, ...)]

4) Int [IK, (peer ID, KH ID, N+1, DSRKname, lifetime, ...)]

Install DSRK
Yoshi’s comments

- Use nonce or time stamps for key exchange?
- Use server ID instead of domain ID? DSRK?
- Carry Key Type (USRK, DSRK, DSUSRK) along
- Carry one ID only, not both up and downlink ID
Future work/Issues

- Remove DSUSRK branch??
- Align key derivation details with hokey-emsk-hierarchy
  - Uses both usage and domain label (to fix)
- Derivation of keys at lower layers of hierarchy
  - Authenticator root keys