Interfacing between IKEv2/IPsec & MIPv6 by simple PF_KEY extensions

Minpeng Qi, Haitao Li, Ke Xu (CERNET)

Hui Deng (China Mobile)

Peng Yang (Hitachi China R&D)

Examples for this interfacing Problem

- Bootstrap in foreign network:
  - To protect BU/BA, HoA-to-HA SAs should be set up by IKEv2 daemon. HoA is not routable before successful registration. So, IKEv2 daemon needs to operate over CoA at this stage. However, it can not probe the CoA during bootstrap.
- Handover to another foreign network
  - IKE SA and Tunnel-mode IPsec SAs should be updated by nCoA. But, IKEv2 daemon also can not probe the nCoA.

Problem

- When mobile nodes bootstrap in foreign network or handover to a new network, IKEv2/IPsec can not probe the changing of care-of-address, which is related to security associations.
- Previous related works:
  - draft-sugimoto-mip6-pfkey-migrate-03
  - draft-arkko-pfkey-reference-00

Design consideration

- Update the SA during handover without signaling between MN and HA
- Minimum modification on OS kernal, IKEv2 and MIPv6
- Light-weight signaling inside OS kernal
- Easy to implement in all the OS
- Easy to extend
- Easy to re-key

Our proposal: Mobile Security Reference Database (MSRD)

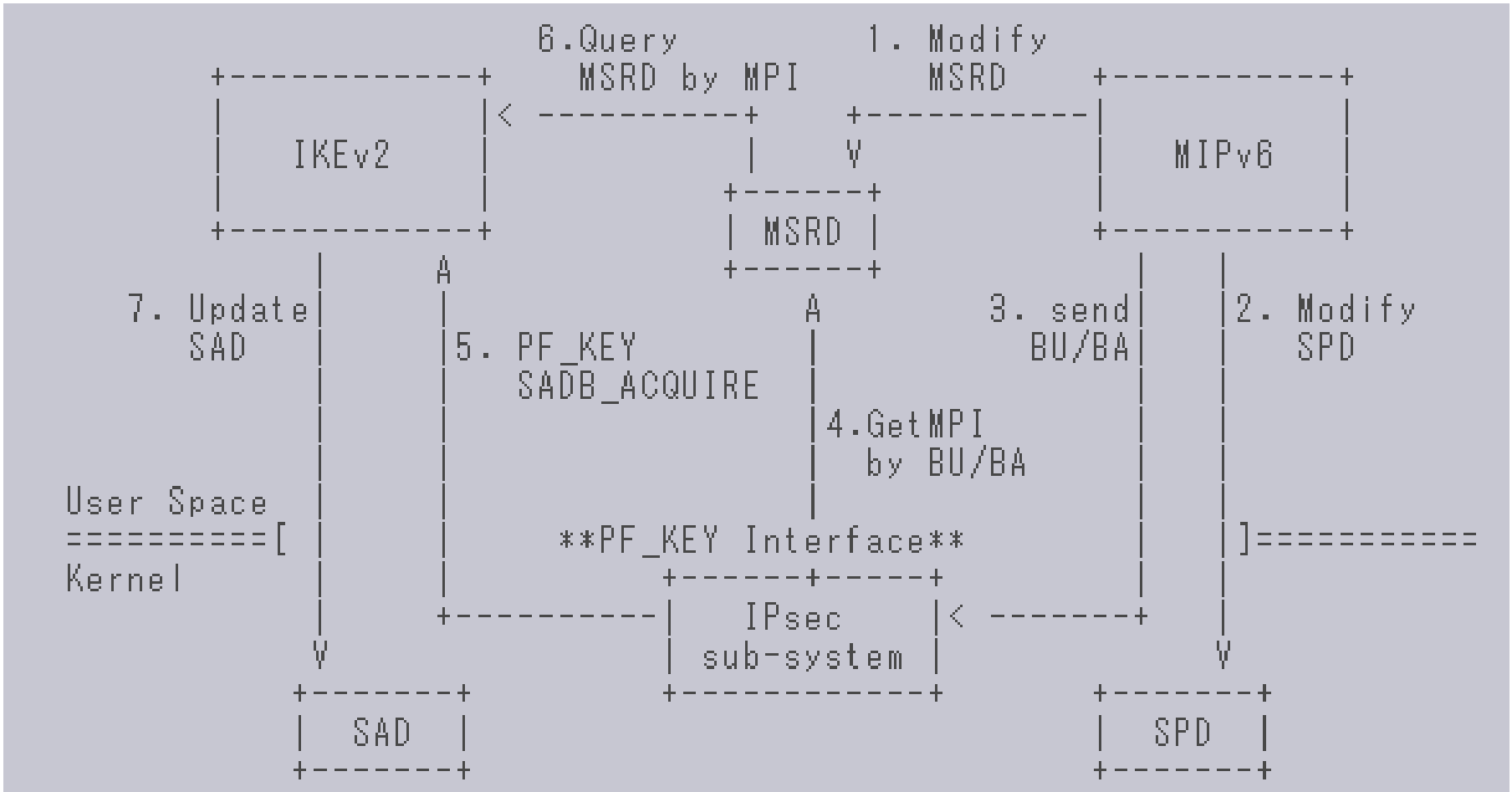
- Store the mobility information in somewhere (MSRD), which is reachable for IKEv2 and OS kernel.
  - Minimum modification on OS kernel.
  - Light-weighted signaling inside OS kernel
  - Easy to be extended
- Indexed by mobile protocol index (MPI)
- MIPv6 deamon will store the mobility related paramters in this database. (especially CoA)
- IKEv2 and OS kernel could fetch the information by simple MSRD API.

extension to PF_KEY interface

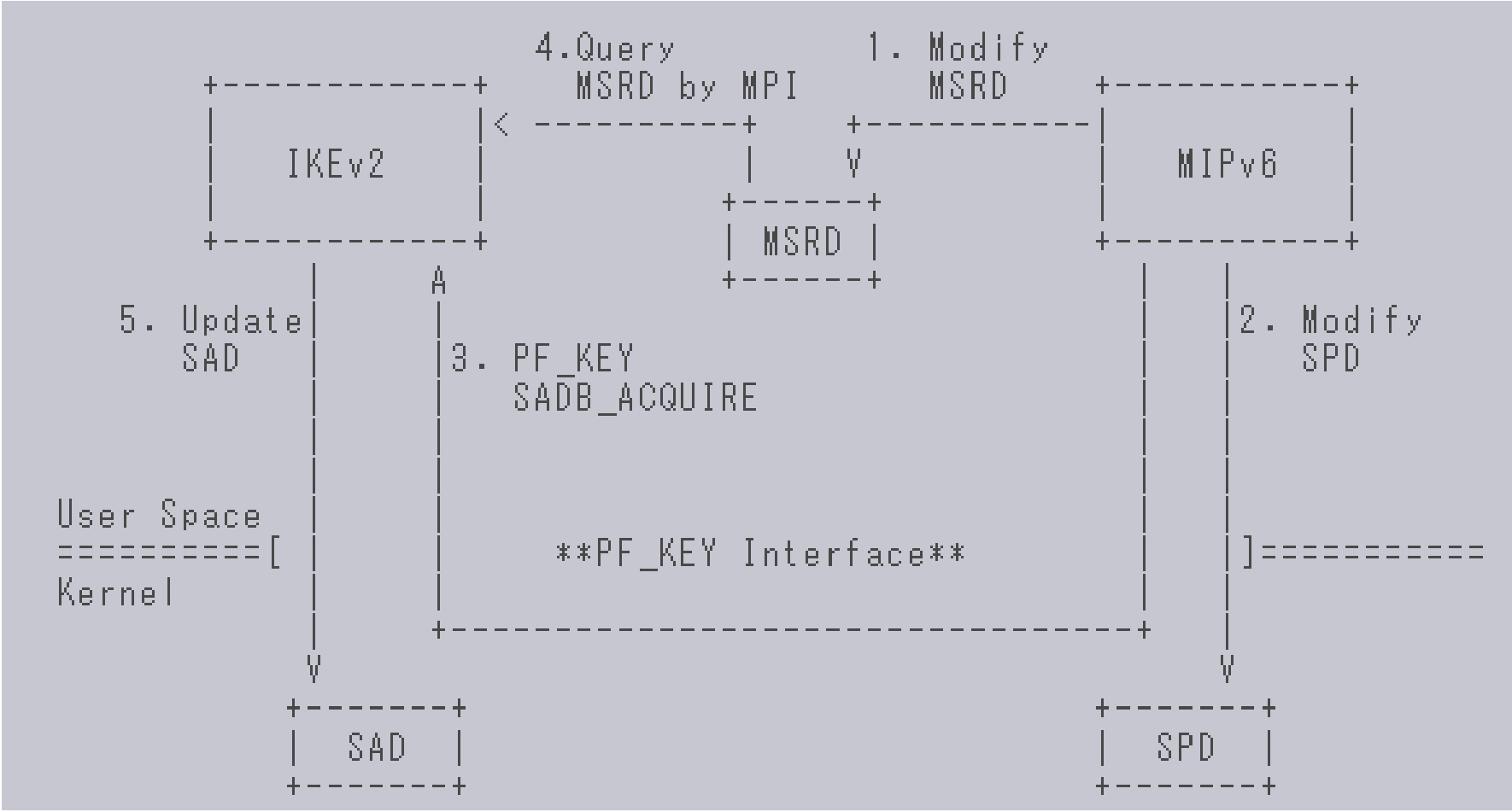
- Original SADB_ACQUIRE message
  < base, address(SD), address(P)*, identity(SD)*, sensitivity* proposal >
- Extended SADB_ACQUIRE message in this draft
- < base, address(SD), address(P)*, identity(SD)*, sensitivity*, proposal, ref* >
- definition of SADB_X_REF for 'ref'

```
struct sadb_x_ref {
    uint8_t  sadb_ref_ver;          //version
    uint8_t  sadb_ref_type;         //type
    uint16_t sadb_ref_type_ext;  //sub type
    uint16_t sadb_ref_len;          //length
    uint16_t sadb_ref_reserved;  //length
    uint64_t sadb_ref_mpi;          //index in MSRD
                        };  /* SADB_X_REF header */
```

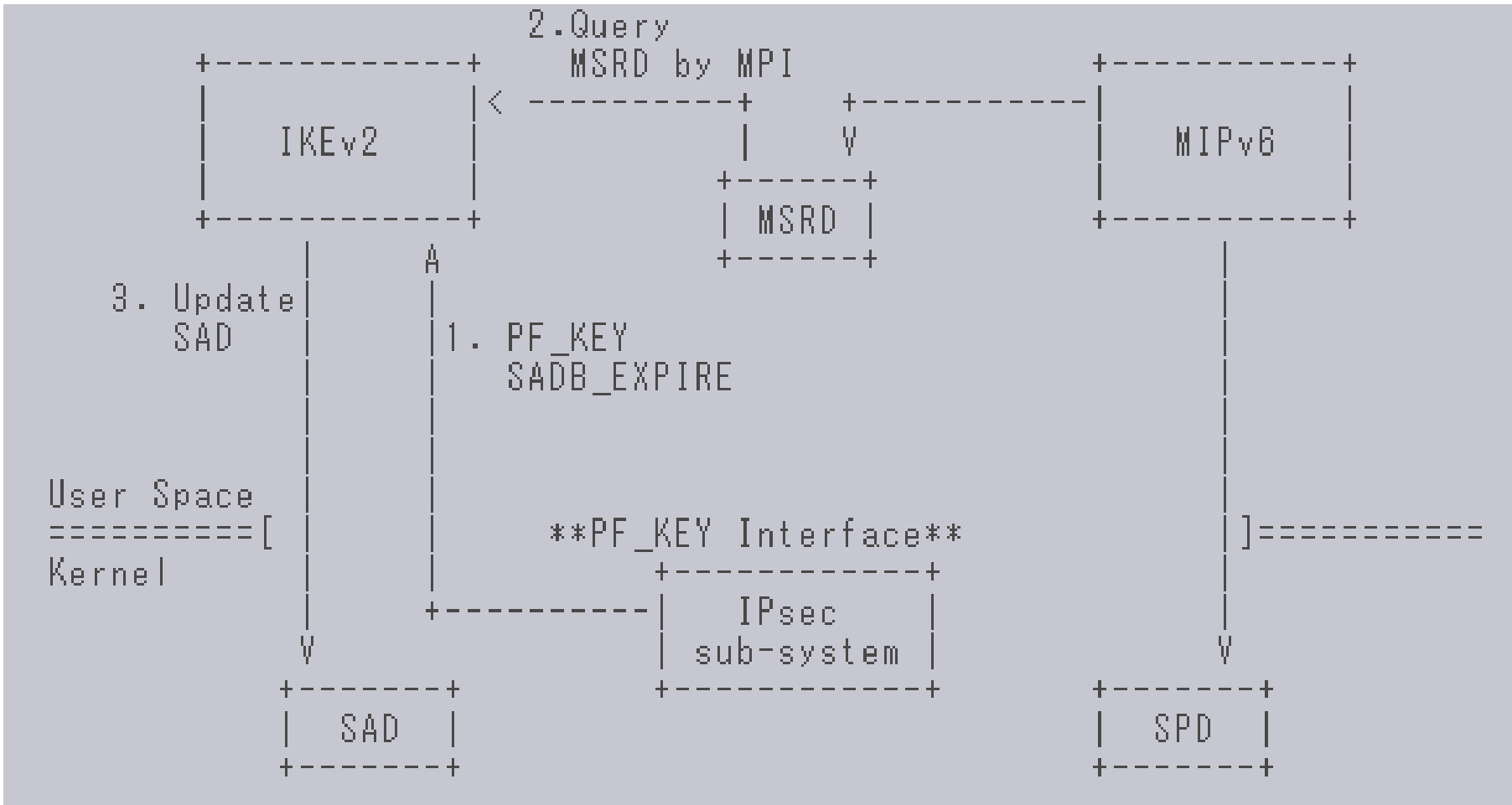
Treatment of transport SA for BU/BA during bootstrap



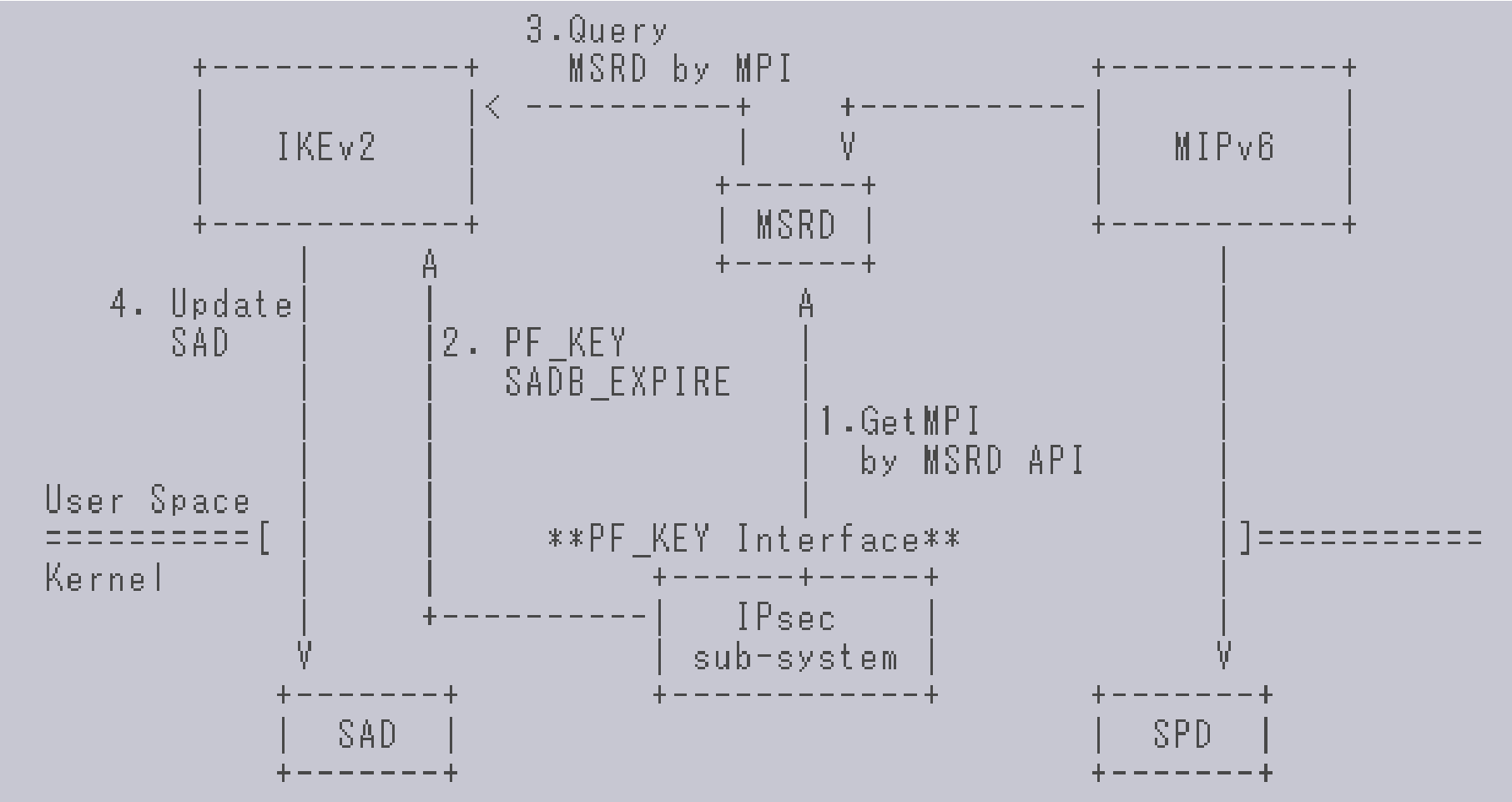
Update tunnel mode SAs during handover



Re-key (MPI stored in IKEv2)



Re-key (MPI not stored in IKEv2)



Related modifications

- IKEv2 software
  - Extract MPI from SADB_X_REF and build or update the SA according to the information in MSRD
- MIPv6 software
  - MSRD operation
  - Support the extended SADB_ACQUIRE
- OS kernel
  - Handling SADB_X_REF extension
  - Support MSRD query API if needed.

Question to Working group

- Shall we start this work item?