

# Alternative Approach for Mixing PPKs in IKEv2: Update

`draft-smyslov-ipsecme-ikev2-qr-alt-09`

Valery Smyslov  
svan@elvis.ru

IETF 118

# PPKs for IKEv2

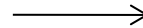
Defined in [RFC 8784](#):

Initiator

Responder

**IKE\_SA\_INIT**

HDR, SAi1, KEi, Ni, N(USE\_PPK)

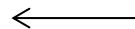


**IKE\_SA\_INIT**

HDR, SAR1, KEr, Nr, N(USE\_PPK)

**IKE\_AUTH**

HDR, SK{IDi, AUTH, SAi2, TSi, TSr,  
N(PPK\_IDENTITY) [, N(NO\_PPK\_AUTH) ] }



**IKE\_AUTH**

HDR, SK{IDr, AUTH, SAR2, TSi, TSr,  
N(PPK\_IDENTITY) }

# Alternative Approach for PPKs in IKEv2

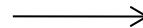
Proposed in [draft-smyslov-ipsecme-ikev2-qr-alt](#):

Initiator

Responder

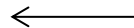
## **IKE\_SA\_INIT**

HDR, SAi1, KEi, Ni, N(USE\_PPK\_ALT),  
N(INTERMEDIATE\_EXCHANGE\_SUPPORTED)



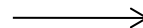
## **IKE\_SA\_INIT**

HDR, SAR1, KEr, Nr, N(USE\_PPK\_ALT),  
N(INTERMEDIATE\_EXCHANGE\_SUPPORTED)



## **IKE\_INTERMEDIATE**

HDR, SK{... N(PPK\_IDENTITY\_KEY)  
[, N(PPK\_IDENTITY\_KEY)...]}



## **IKE\_INTERMEDIATE**

HDR, SK{... N(PPK\_IDENTITY)}



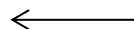
## **IKE\_AUTH**

HDR, SK{IDi, AUTH, SAi2, TSi, TSr}



## **IKE\_AUTH**

HDR, SK{IDr, AUTH, SAR2, TSi, TSr}



# Comparison

- Initial IKE SA is protected with PPK
- 3 IKE exchanges instead of 2
  - PPK\_IDENTITY\_KEY notification can be piggybacked if IKE\_INTERMEDIATE is also used for other purposes
- 1 computation of AUTH instead of 2 if PPK is optional
- Initiator can propose several PPK\_IDs
  - for each proposed PPK\_ID a call to prf is required

# New in -09

- Negotiation of alternative approach is now explicit and independent from RFC 8784
  - more clear protocol
  - initiator MAY propose both 8784 and alternative approach, responder MUST select one
- Use of PPKs in CREATE\_CHILD\_SA is defined
  - if PPK is changed before IKE SA expires (e.g. as result of QKD), then with RFC 8784 there is no way to use it other than delete IKE SA and re-create it from scratch
  - use PPKs in CREATE\_CHILD\_SA solves this problem (fresh PPK will only be used for confidentiality, not for authentication)

# PPKs in CREATE\_CHILD\_SA

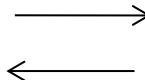
- Can be used for:
  - rekey IKE SA
  - rekey Child SAs
  - create additional Child SAs
- Diagram below omits content of CREATE\_CHILD\_SA messages for brevity

Initiator

Responder

**CREATE\_CHILD\_SA**

HDR, SK{... N(PPK\_IDENTITY\_KEY)  
[, N(PPK\_IDENTITY\_KEY)...]}



**CREATE\_CHILD\_SA**

HDR, SK{... N(PPK\_IDENTITY)}

# Session Keys Calculation

- For initial IKE SA

```
SKEYSEED` = prf+ (PPK, SK_d`)
{SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr} =
prf+ (SKEYSEED`, Ni | Nr | SPIi | SPIr)
```

- In CREATE\_CHILD\_SA

```
SK_d` = prf+ (PPK, SK_d)
```

- Rekey IKE SA:

```
SKEYSEED = prf (SK_d`, g^ir (new) | Ni | Nr)
```

- Rekey/create Child SA

```
KEYMAT = prf+ (SK_d`, [g^ir (new)] | Ni | Nr)
```

# Thanks

## WG adoption?