Alternative Approach for Mixing PPKs in IKEv2: Update

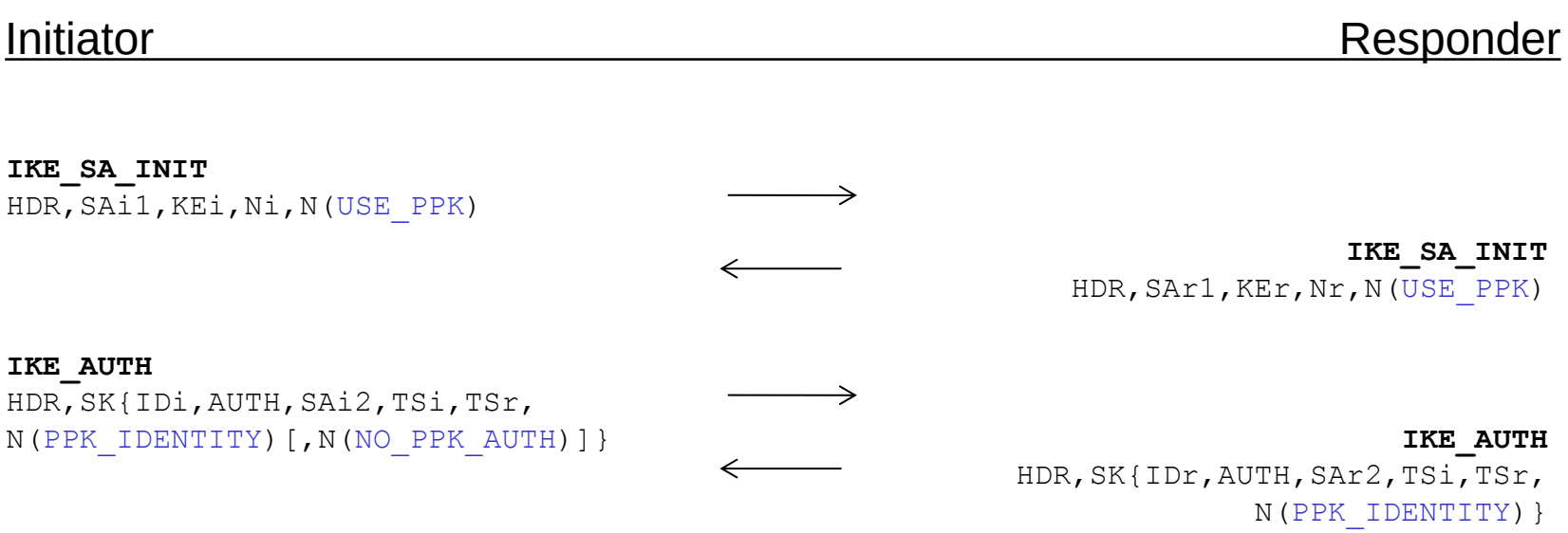
draft-smyslov-ipsecme-ikev2-qr-alt-09

Valery Smyslov
svan@elvis.ru

IETF 118

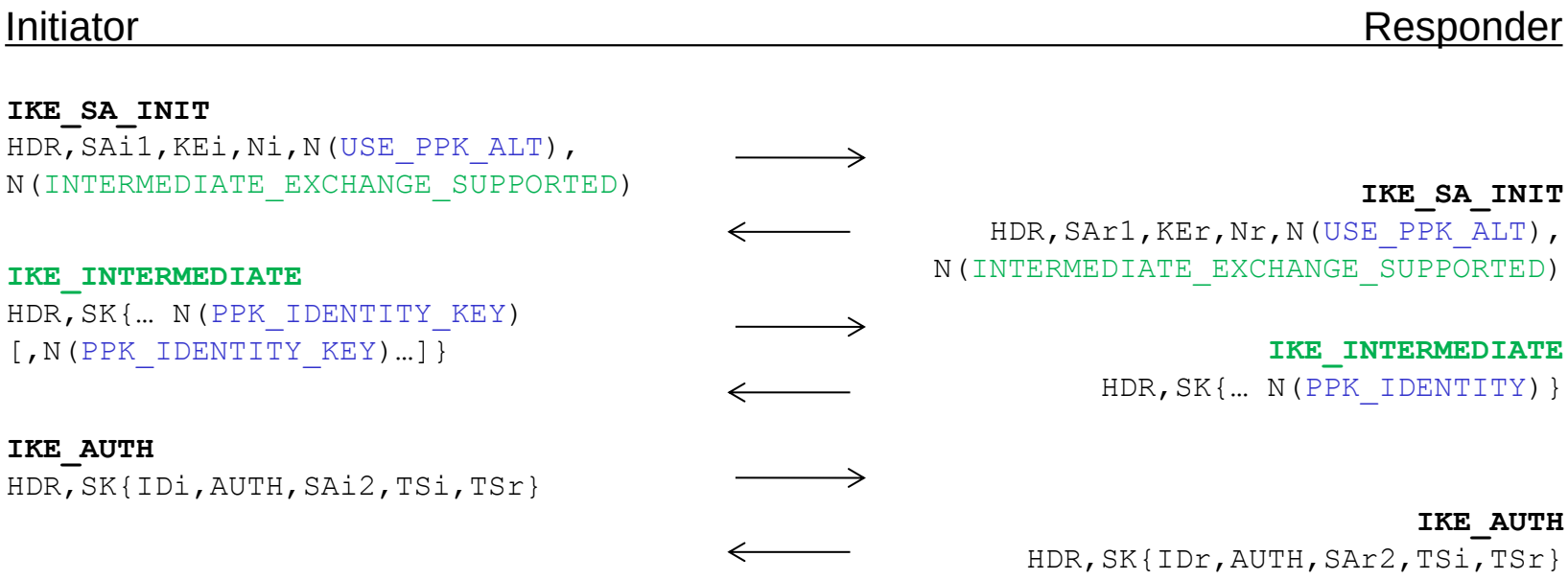
PPKs for IKEv2

Defined in RFC 8784:



Alternative Approach for PPKs in IKEv2

Proposed in draft-smyslov-ipsecme-ikev2-qr-alt:



Comparison

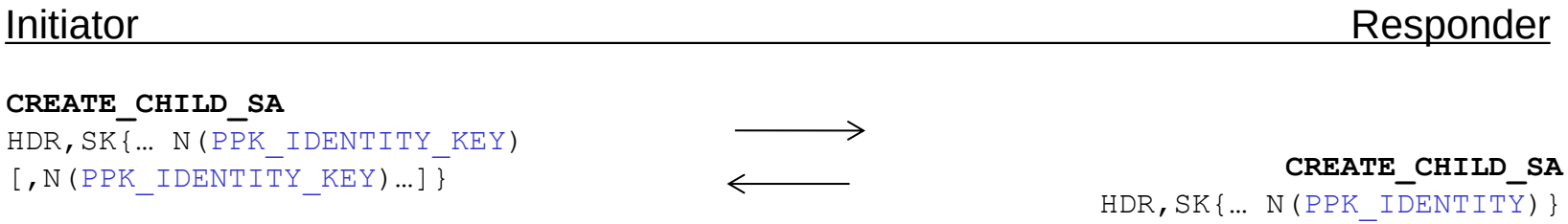
- Initial IKE SA is protected with PPK
- 3 IKE exchanges instead of 2
  - PPK_IDENTITY_KEY notification can be piggybacked if IKE_INTERMEDIATE is also used for other purposes
- 1 computation of AUTH instead of 2 if PPK is optional
- Initiator can propose several PPK_IDs
  - for each proposed PPK_ID a 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



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?