INTERMEDIATE Exchange Update

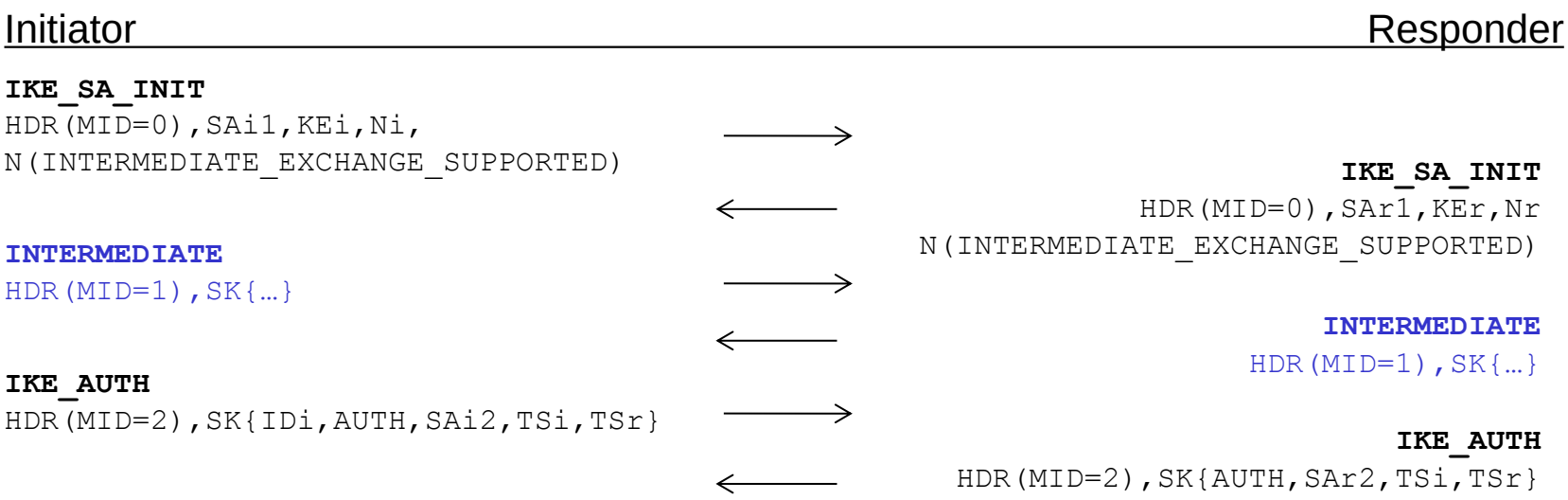
draft-smyslov-ipsecme-ikev2-aux-02

Valery Smyslov
svan@elvis.ru

IETF 104

Exchange Overview

One or more INTERMEDIATE (ex IKE_AUX) Exchanges may take place between IKE_SA_INIT and IKE_AUTH. Their use is negotiated via exchange of `INTERMEDIATE_EXCHANGE_SUPPORTED` notifications:



The exchanges can be used to transfer large amount of data prior IKE_AUTH (e.g. QSKE public keys), since standard IKE Fragmentation works for them

Changes from -01 version

- Exchange renamed from IKE_AUX to INTERMEDIATE
  - IANA Considerations are updated
- Exchange authentication is changed so, that all INTERMEDIATE exchanges messages are included (via PRF) in AUTH payload calculation
  - thanks to Scott Fluhrer for this suggestion

Old INTERMEDIATE Exchange Authentication

- Previously each party included only her own INTERMEDIATE messages into the AUTH payload computation

```
InitiatorSignedOctets = RealMessage1 | AUX_I | NonceRData | MACedIDForI
ResponderSignedOctets = RealMessage2 | AUX_R | NonceIData | MACedIDForR

AUX_I = [AUX_PRF_I_1 [| AUX_PRF_I_2 [| AUX_PRF_I_3]]] ...
AUX_R = [AUX_PRF_R_1 [| AUX_PRF_R_2 [| AUX_PRF_R_3]]] ...

AUX_PRF_I_n = prf(SK_pi_n, IKE_AUX_I_n_H [| IKE_AUX_I_n_E])
AUX_PRF_R_n = prf(SK_pr_n, IKE_AUX_R_n_H [| IKE_AUX_R_n_E])
```

IKE_AUX_[I/r]_n_H – part of the message from the beginning of IKE header till the end of Encrypted payload header

IKE_AUX_[I/r]_n_E – content of Encrypted payload before encryption and possible fragmentation (not including payload header, IV, ICV, Pad Length and Padding)

New INTERMEDIATE Exchange Authentication

- Authentication is changed so that all INTERMEDIATE messages are included into the AUTH payload calculation by each party

```
InitiatorSignedOctets = RealMessage1 | NonceRData | MACedIDForI [| IntAuth]
ResponderSignedOctets = RealMessage2 | NonceIData | MACedIDForR [| IntAuth]

IntAuth = IntAuth_1 | [| IntAuth_2 [| IntAuth_3]] ...

IntAuth_n = IntAuth_n_I | IntAuth_n_R
IntAuth_n_I = prf(SK_pi_n, [IntMessage_n_I_P |] IntMessage_n_I_A)
IntAuth_n_R = prf(SK_pr_n, [IntMessage_n_R_P |] IntMessage_n_R_A)
```

IntMessage_n_[I/R]_P – content of Encrypted payload before encryption and possible fragmentation (not including payload header, IV, ICV, Pad Length and Padding)

IntMessage_n_[I/R]_A – part of the message from the beginning of IKE header till the end of Encrypted payload header

Impact of New INTERMEDIATE Exchange Authentication

- Strengthens authentication of INTERMEDIATE exchanges, preventing any kind of replay attacks
- Changing the order of authentication inputs to signature calculation simplifies implementations
- Swapping the order of authentication inputs to calculation of **`IntAuth_n_[I/R]`** simplifies implementations

Thank you!

- Comments?
- Questions?
- Way forward?