“IKEv2 Rekey optimization SA &TS Payloads support ”

IKEv2 Optional SA&TS in Child Exchange draft-kampati-ipsecme-ikev2-saPayloads -ts-payloads-opt-00

https://tools.ietf.org/html/draft-kampati-ipsecme-ikev2-sa-ts-payloads

By:
Sandeep Kampati ,

Meduri S S Bharath

www.huawei.com

HUAWEI TECHNOLOGIES INDIA Pvt Ltd

HUAWEI

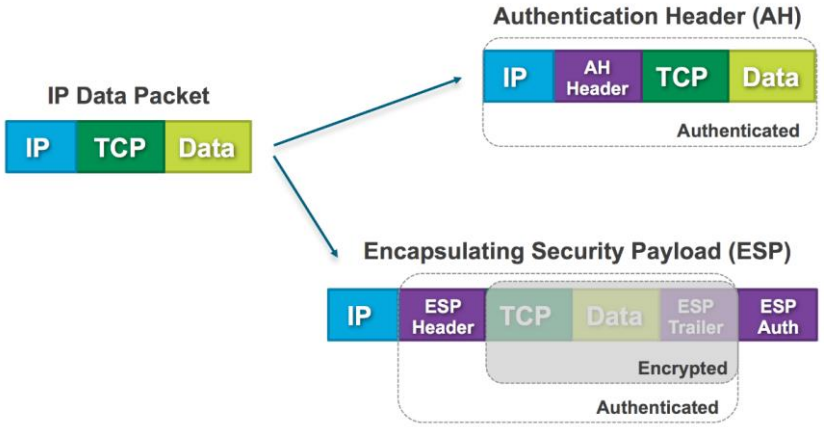
What is IPSec?

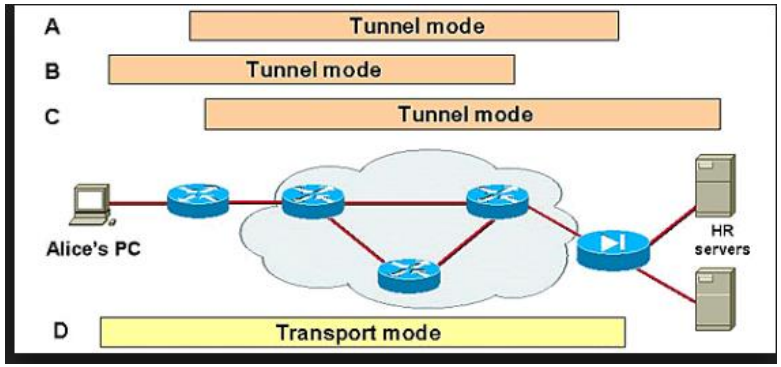
- **IP Security is a set of protocols and standards to support the securing of data at the IP layer.**

- **Supports authentication and encryption of traffic.**
  - Certifies the originator of the packet.
  - Protects the data from interception and tampering while in transit.

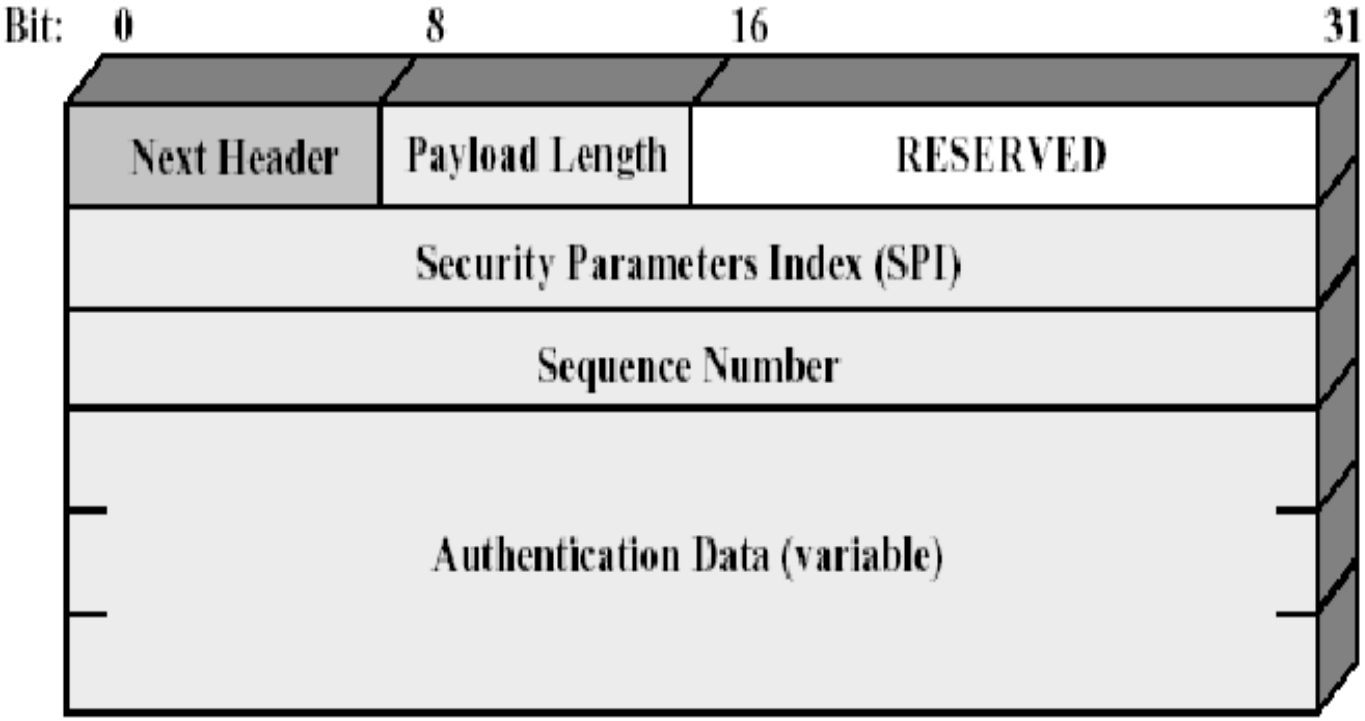
IPSec Basic features

- **IPsec provides security services at the IP layer by enabling a system to select required security protocols.**
  - Integrity.
  - Authentication.
  - Anti replay Service.
  - Confidentiality.
- **IPsec uses 2 protocols to provide these services.**
  - AH (**Authentication Header**)
  - ESP **(Encapsulating Security Payload)**
- **Each Protocol supports 2 modes**
  - Tunnel Mode
  - Transport Mode





AH Header

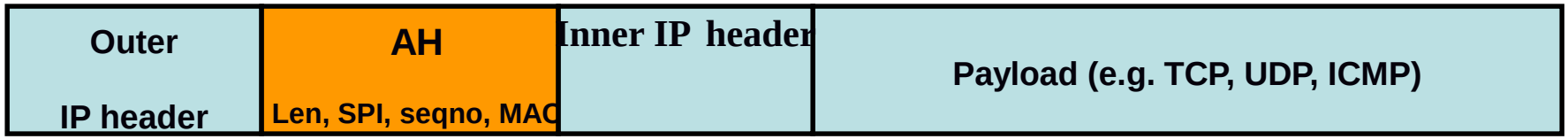

Bit:
0
8
16
31
Next Header
Payload Length
RESERVED
Security Parameters Index (SPI)
Sequence Number
Authentication Data (variable)

AH Protocol – Transport and Tunnel

AH in transport mode:

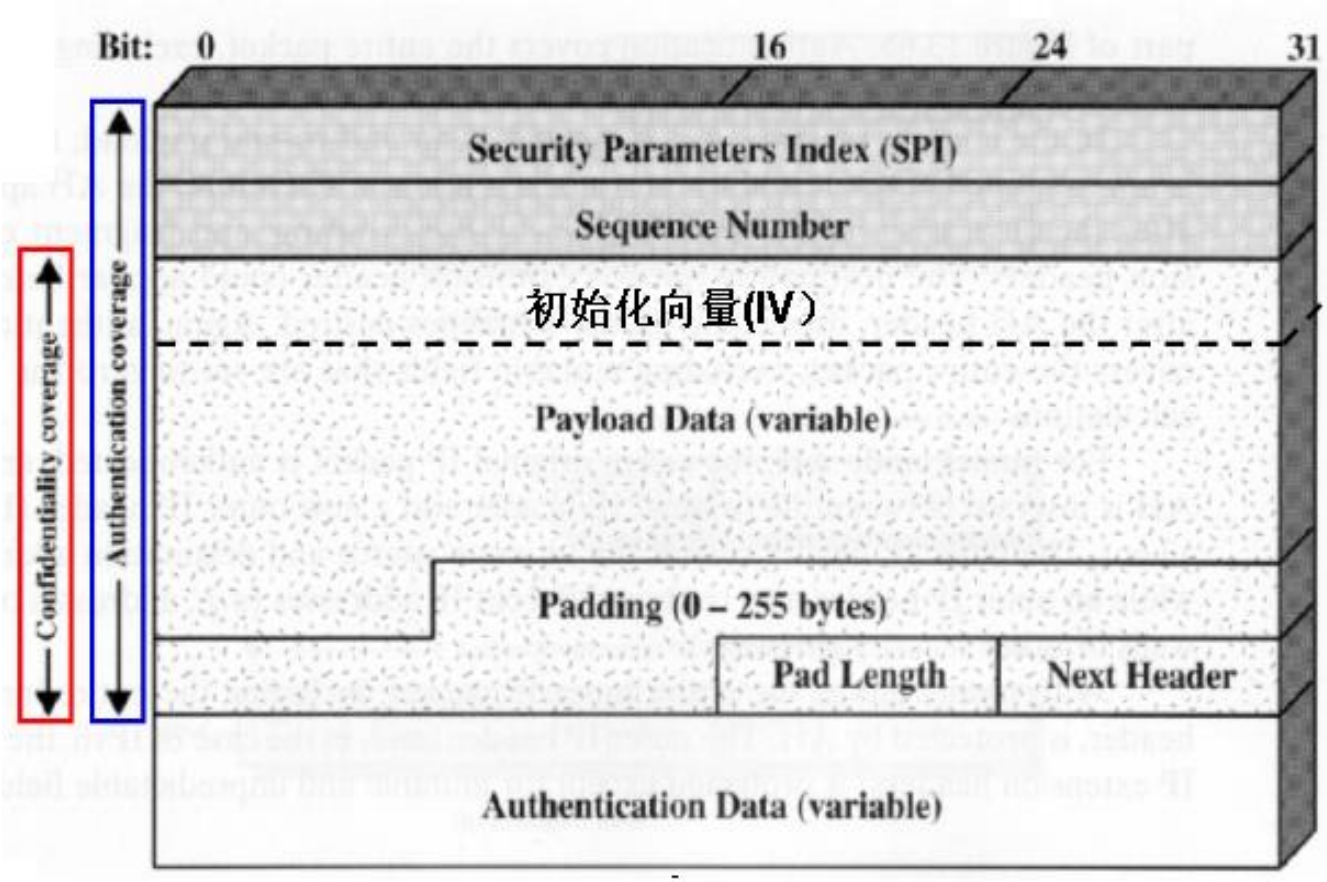
Authentication scope - all immutable fields

AH in tunnel mode:



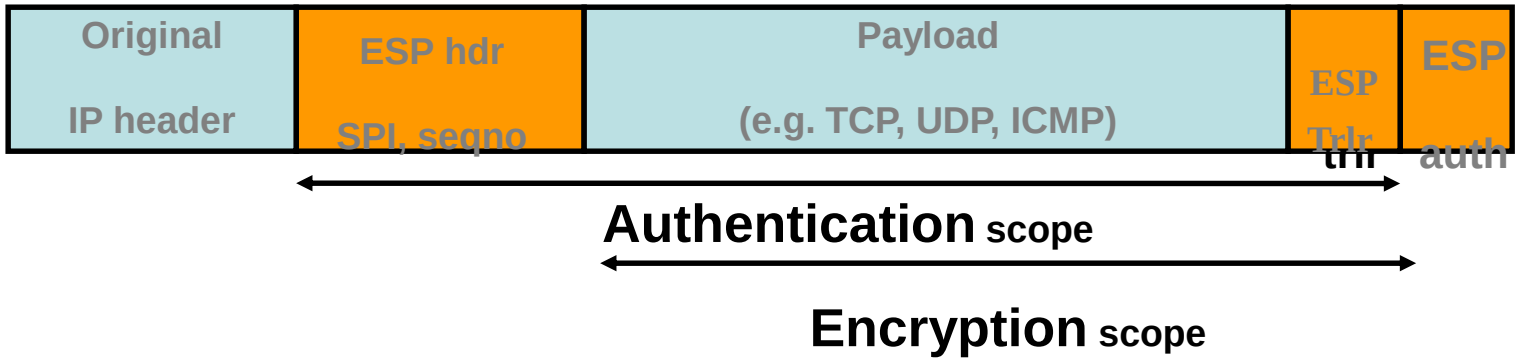
Authentication scope - all immutable fields

ESP Protocol

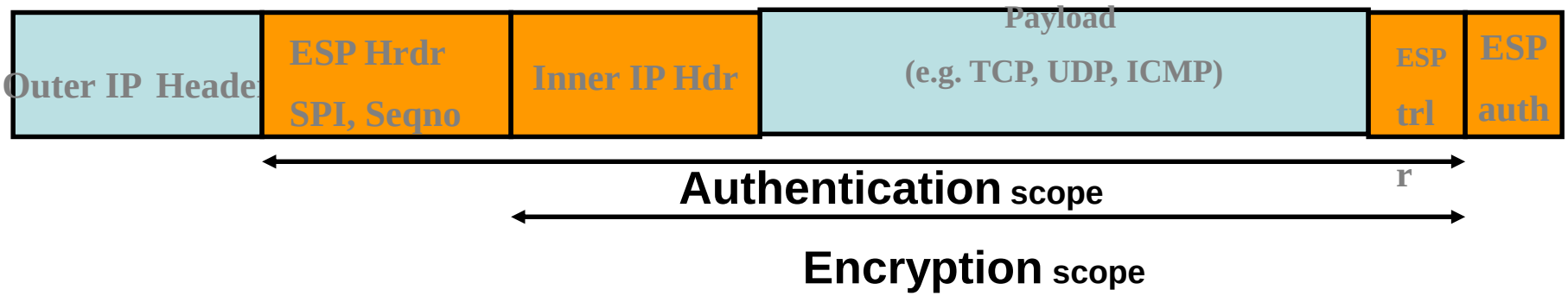


ESP Protocol – Transport and Tunnel

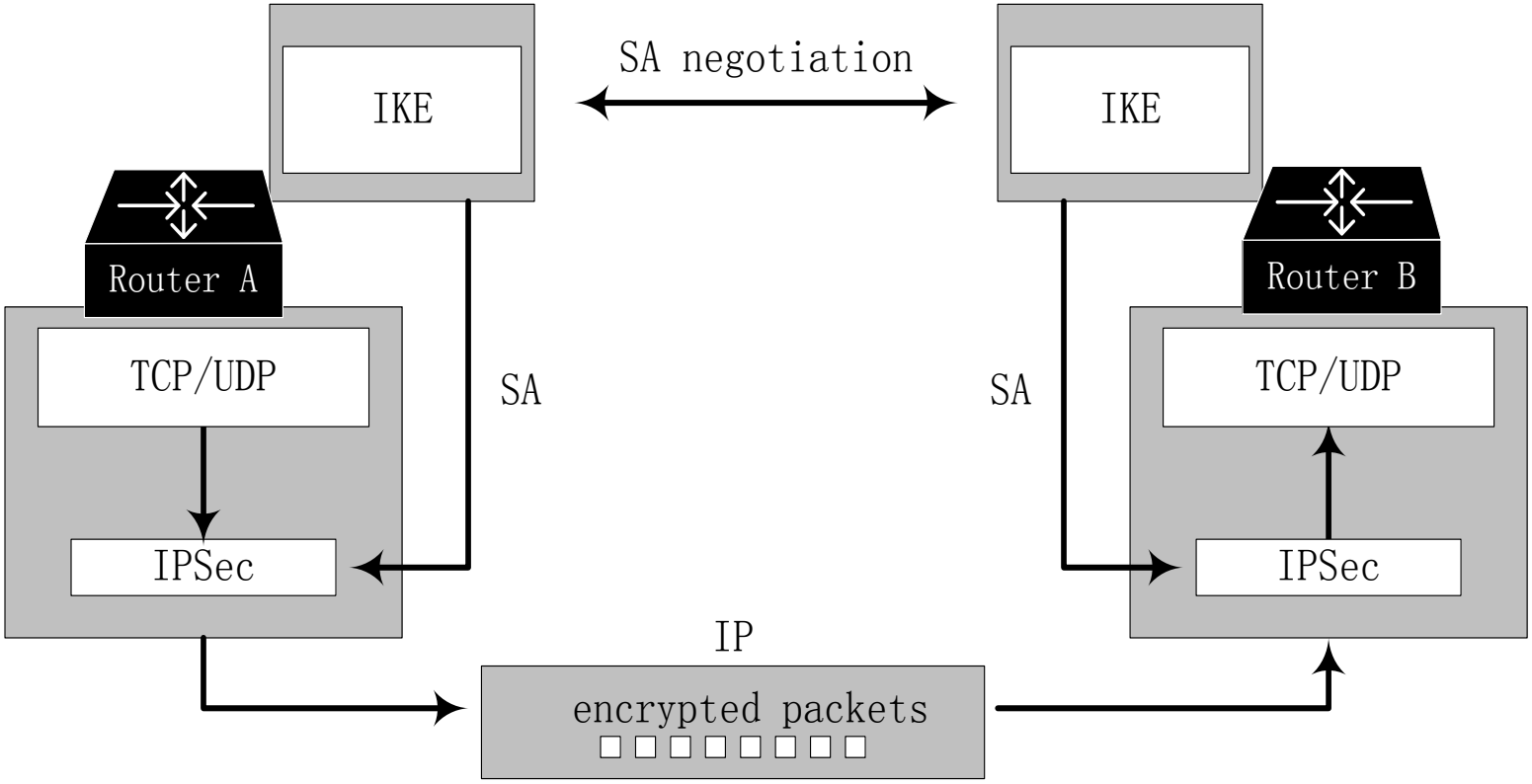
ESP in transport mode:



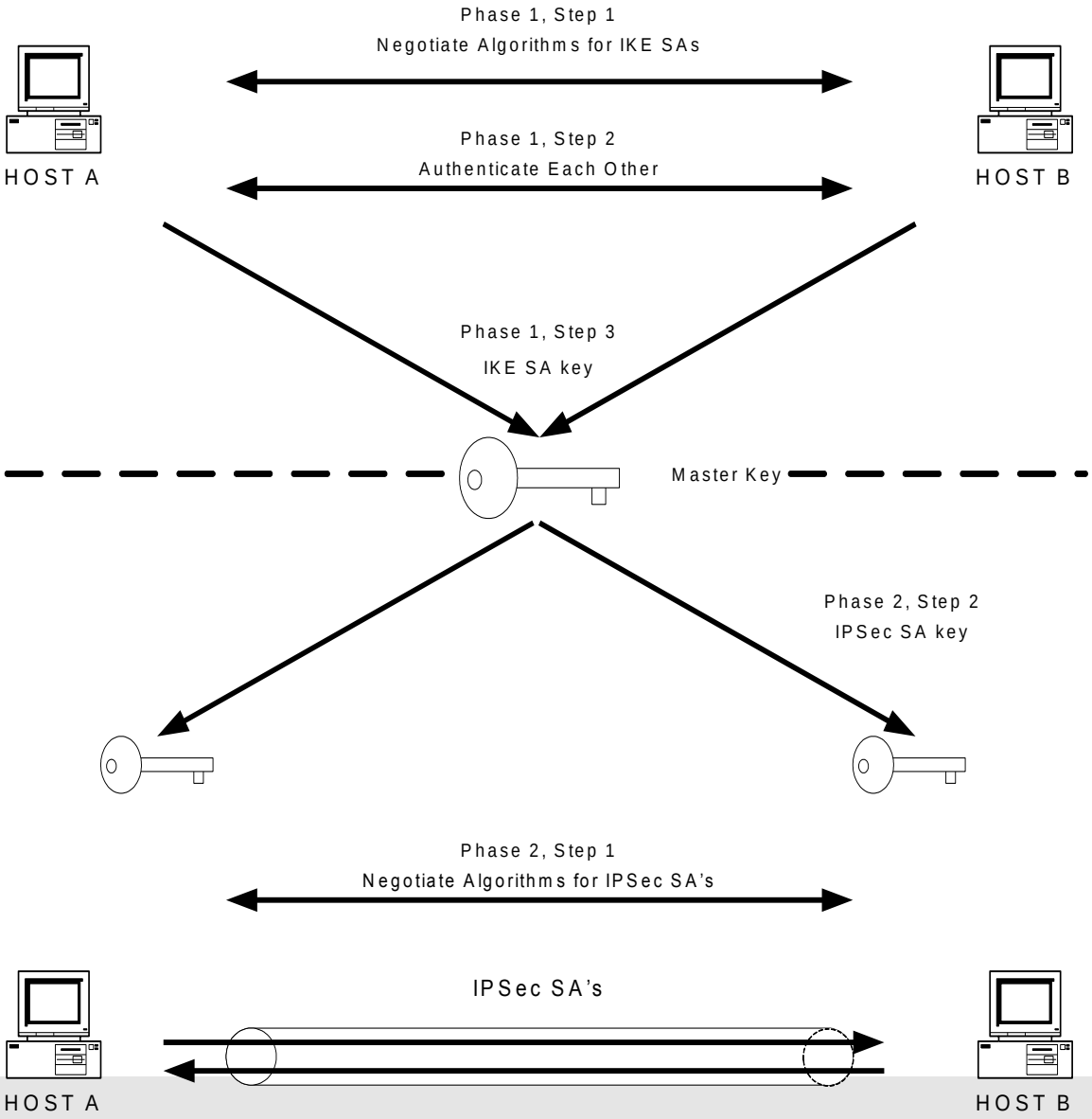
ESP in tunnel mode:



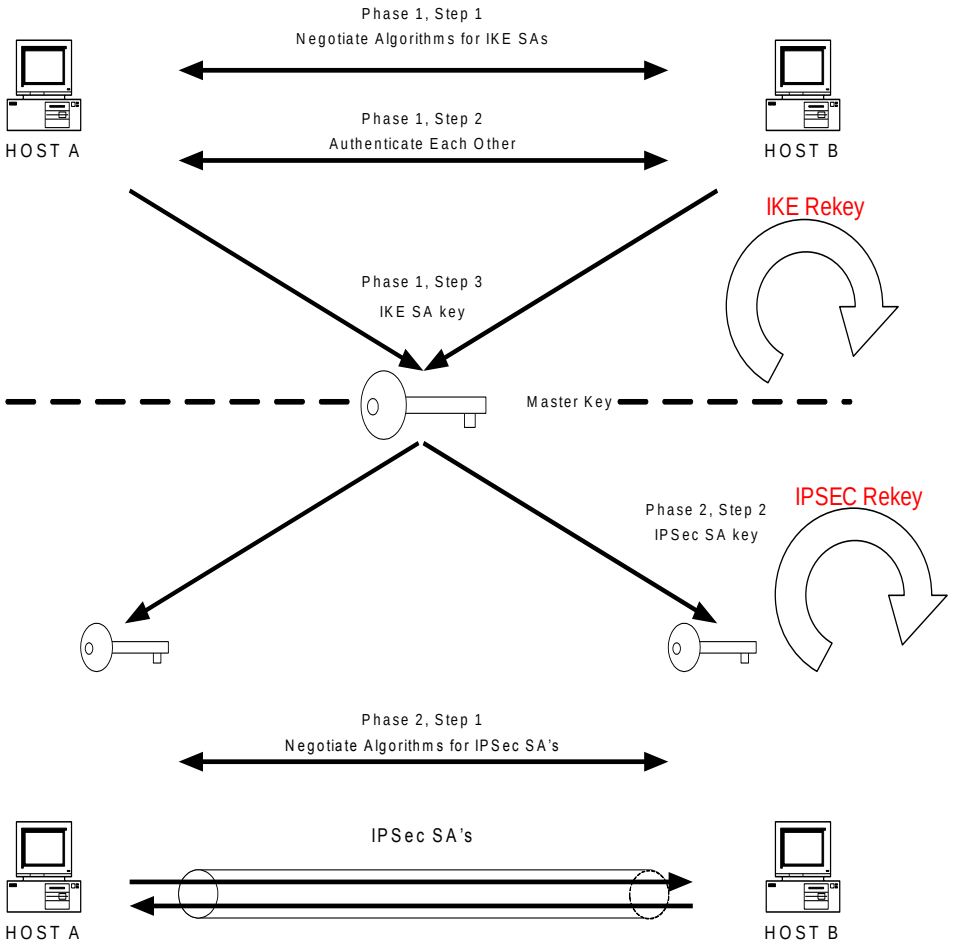
Relationship between IPsec and IKE



Overview


Phase 1, Step 1
Negotiate Algorithms for IKE SAs
Phase 1, Step 2
Authenticate Each Other
HOST A
HOST B
Phase 1, Step 3
IKE SA key
Master Key
Phase 2, Step 2
IPSec SA key
Phase 2, Step 1
Negotiate Algorithms for IPSec SA's
IPSec SA's
HOST A
HOST B

IKE Rekey & Ipsec Rekey



IKE rekey will

recreate new keys

for IKE tunnel

IPSEC Rekey will

recreate new keys

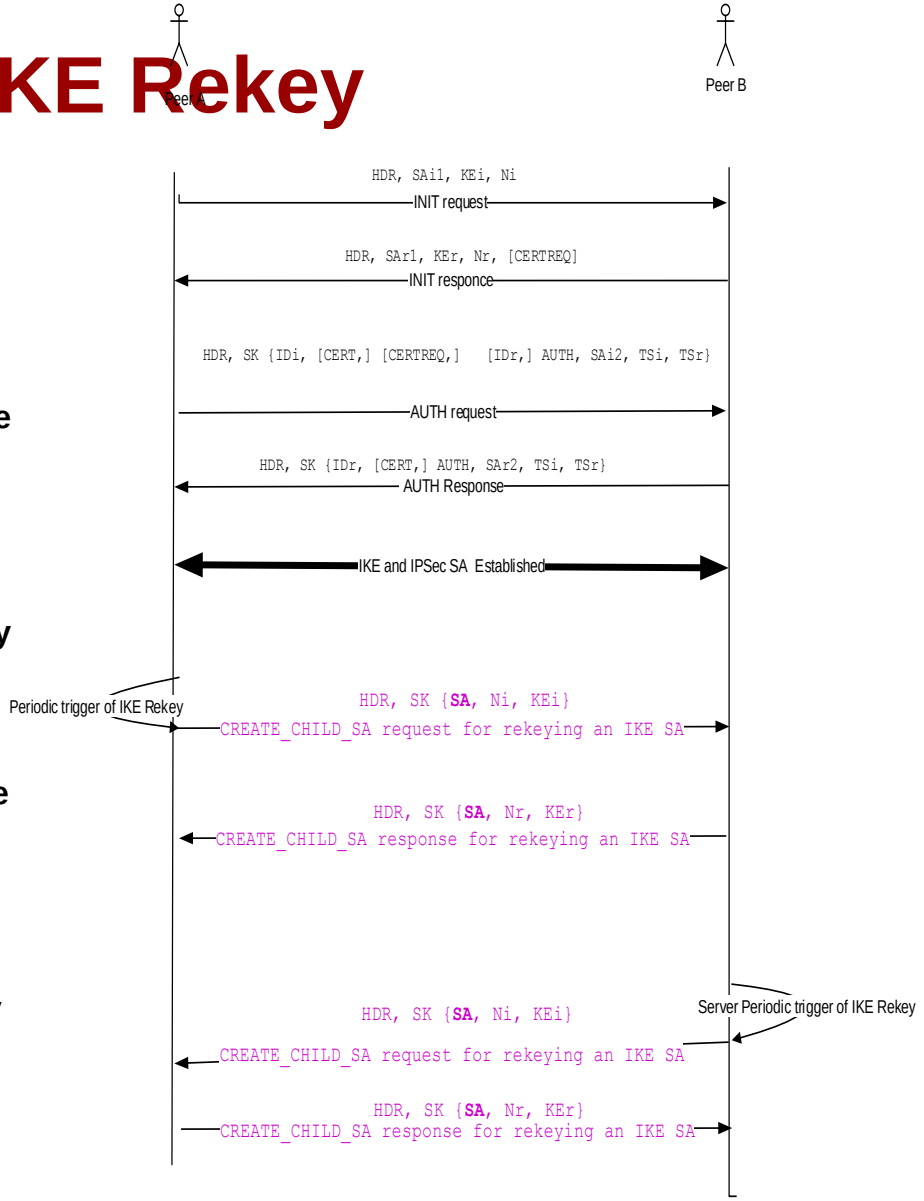
for IPSEC tunnel

Most of deployment Scenarios they configure for 1 hour

Initial SA creation & IKE Rekey

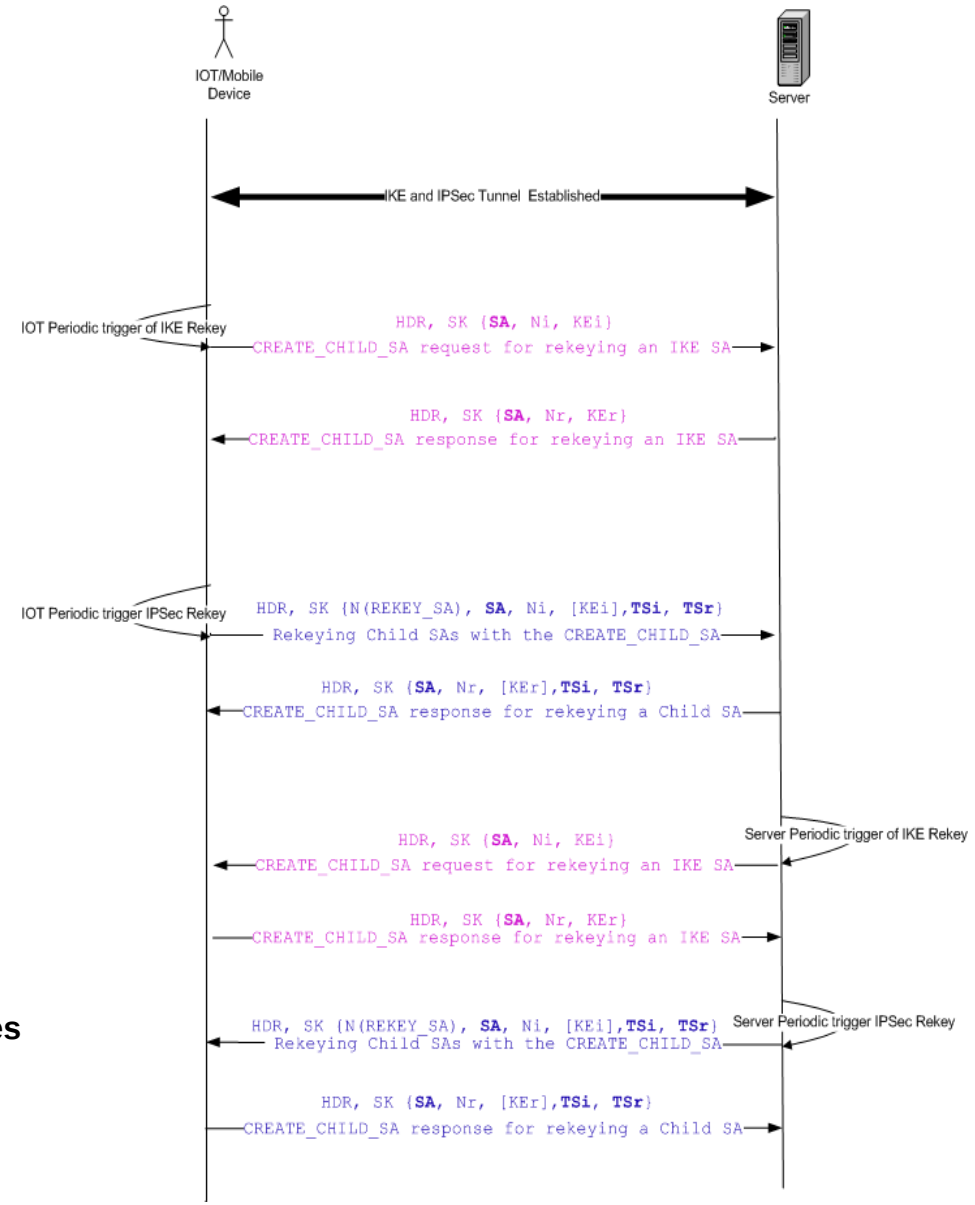
- **As per RFC7296 IKE tunnel is created and IPSEC (AH/ESP) tunnel is created after INIT and AUTH exchanges.**
- **IKE rekey contains SA payloads which contains single/multiple cryptographic suite. Most of time this suits are not changed at rekey time. Minimum size of (single set of cryptographic suite)SA payload 52 bytes.**
- **In IKESA payload size will increase exponentially for multiple cryptographic suite.**
- **IKE rekey are triggered periodically which consume bandwidth and power to process those payloads**

- **Key Problem:** when there is no configuration changes, still we will send SA payloads in IKE Rekey which is of no value but will consuming more bandwidth, processing time and power.



IKE Rekey

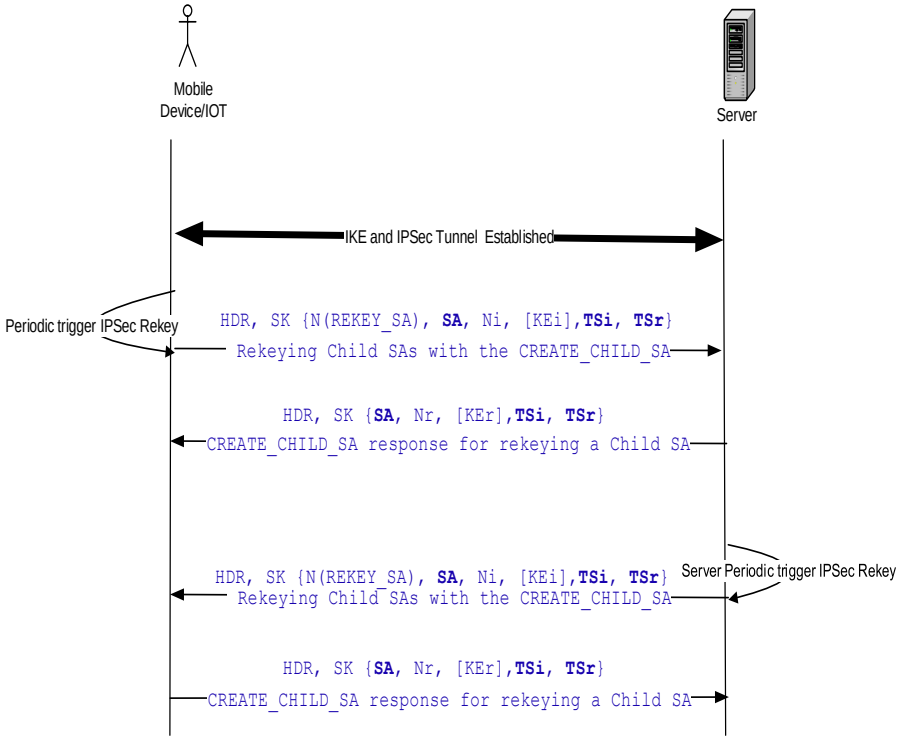
- IKE rekey contains SA payloads which contains single/multiple cryptographic suite. Most of time this suits are not changed at rekey time. Minimum size of (single set of cryptographic suite)SA payload 52 bytes.
- IPSEC rekey contains SA payloads which contains single/multiple cryptographic suite and TSi & TSr payloads . Most of time these are not changed at rekey time. Minimum size of SA payload 40 bytes, each TS size 24 bytes (2*24 = 48 bytes).
- In IKE/IPSEC SA payload size will increase exponentially for multiple cryptographic suite.
- IKE /IPSEC rekey are triggered periodically which consume bandwidth and power to process those payloads
- Existing all devices if there is any change in Tsi or TSr they are deleting SA and recreating it.



Key Problem: when there is no configuration changes still we will send SA &TS payloads in IKE/IPSEC Rekey which is of no value but will consuming more bandwidth, processing time and power.

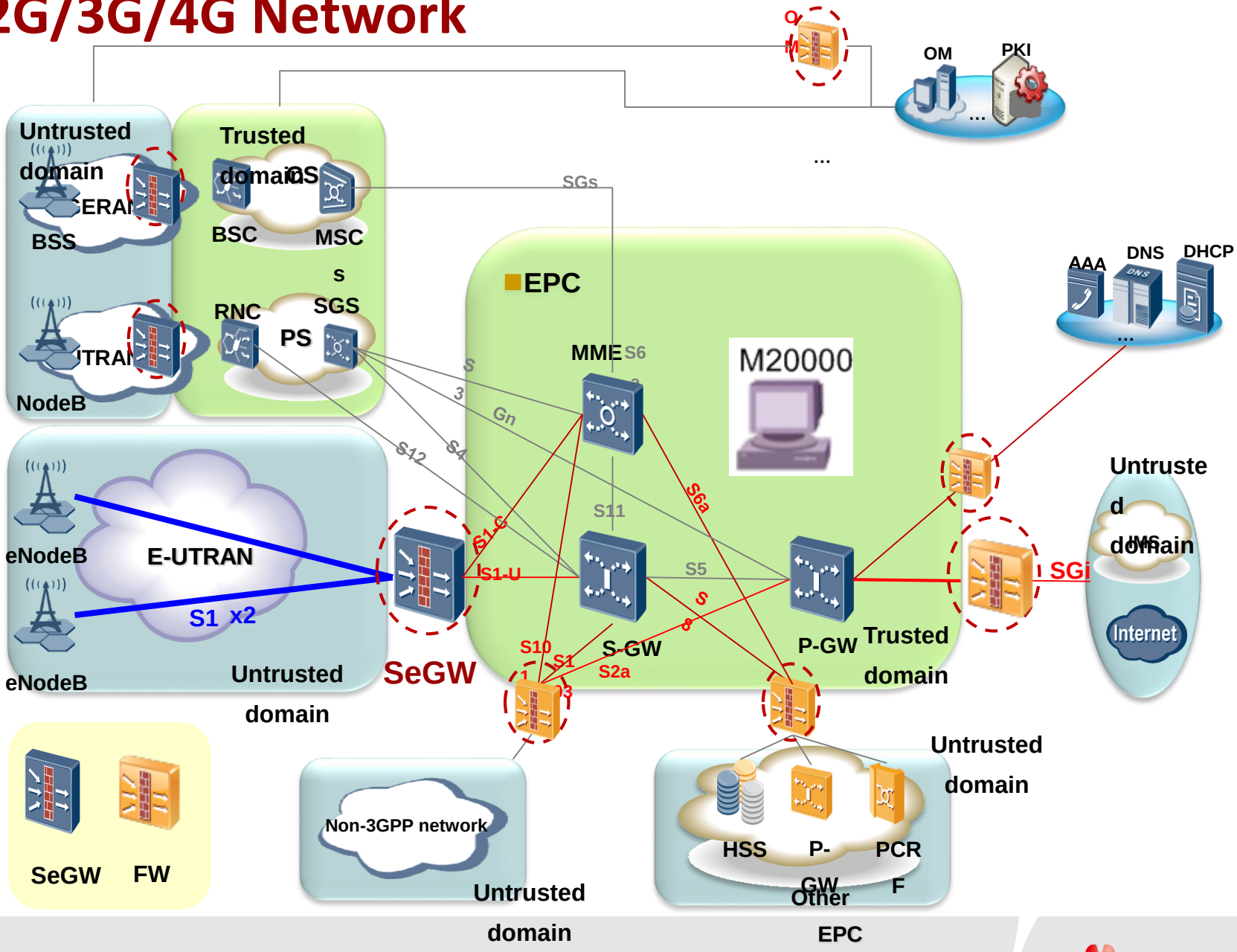
Ipsec Rekey

- **IPSEC rekey contains SA payloads which contains single/multiple cryptographic suite and TSi & TSr payloads . Most of time these are not changed at rekey time. Minimum size of SA payload 40 bytes, each TS size 24 bytes (2*24 = 48 bytes).**
- **In IPSEC SA payload size will increase exponentially for multiple cryptographic suite.**
- **IPSEC rekey are triggered periodically which consume bandwidth and power to process those payloads**
- **Existing all devices if there is any change in Tsi or TSr they are deleting SA and recreating it.**



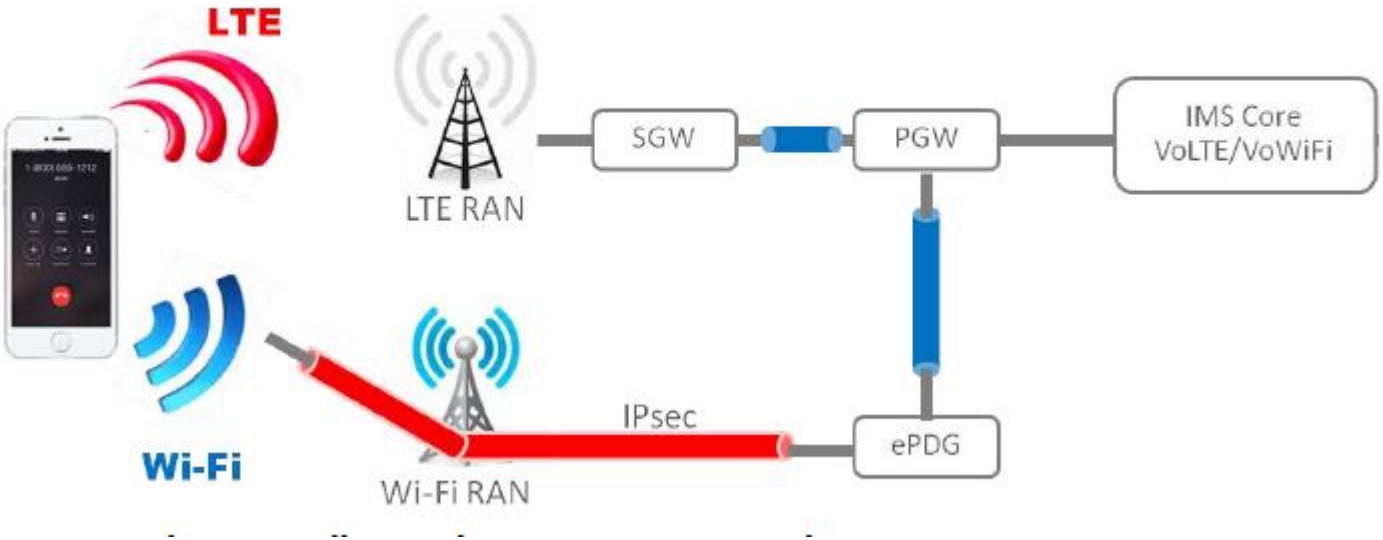
Key Problem: when there is no configuration changes, still we will send SA &TS payloads in IPSEC Rekey which is of no value but will consuming more bandwidth, processing time and power.

2G/3G/4G Network



HUAWEI

WiFi Calling architecture



Deployment Scenario

In 4G network security gateways/ePDG and in 5G networks cRAN/Cloud will support more than one 100000 IKE/IPSEC tunnels. So on an average, for every second we encounter many rekeys. This takes huge amount of bandwidth, packet fragmentation and more processing. This can be solved by introducing this solution.

This is useful in Internet of Things (IoT) devices which utilizing lower power consumption technology. The appendix A of [IPSEC-IOT- REQS] gives some estimate data.

Most of devices they don't preferred to change suits frequently. Taking this advantage we can make SA and TS as optional payloads at time of IKE SA rekey and IPSEC SA rekey

Introduction to draft

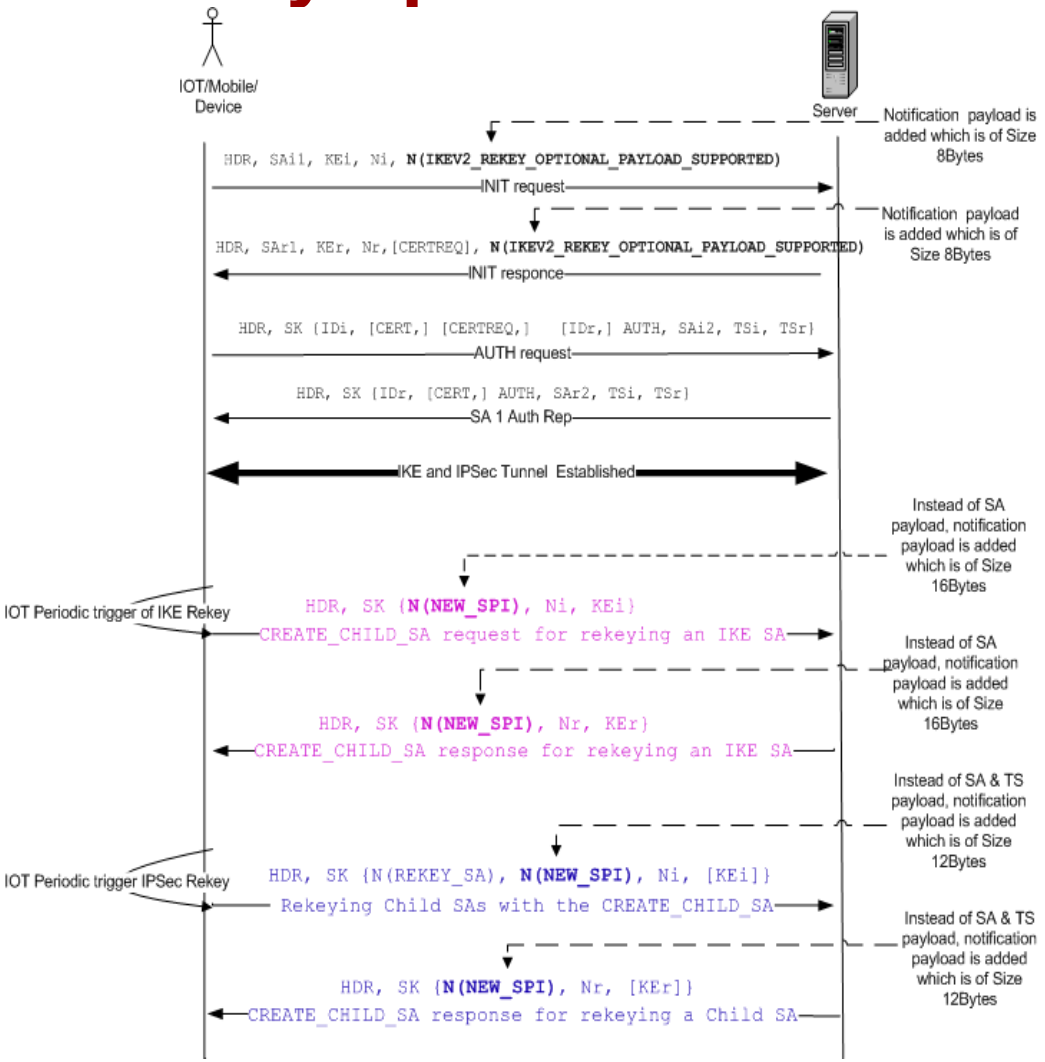
IKEv2 Optional SA&TS Payloads in Child Exchange draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt-00

https://tools.ietf.org/html/draft-kampati-ipsecme-ikev2-sa-ts-payloads

IKE rekey & IPSEC Rekey optimization

Scenario 1:

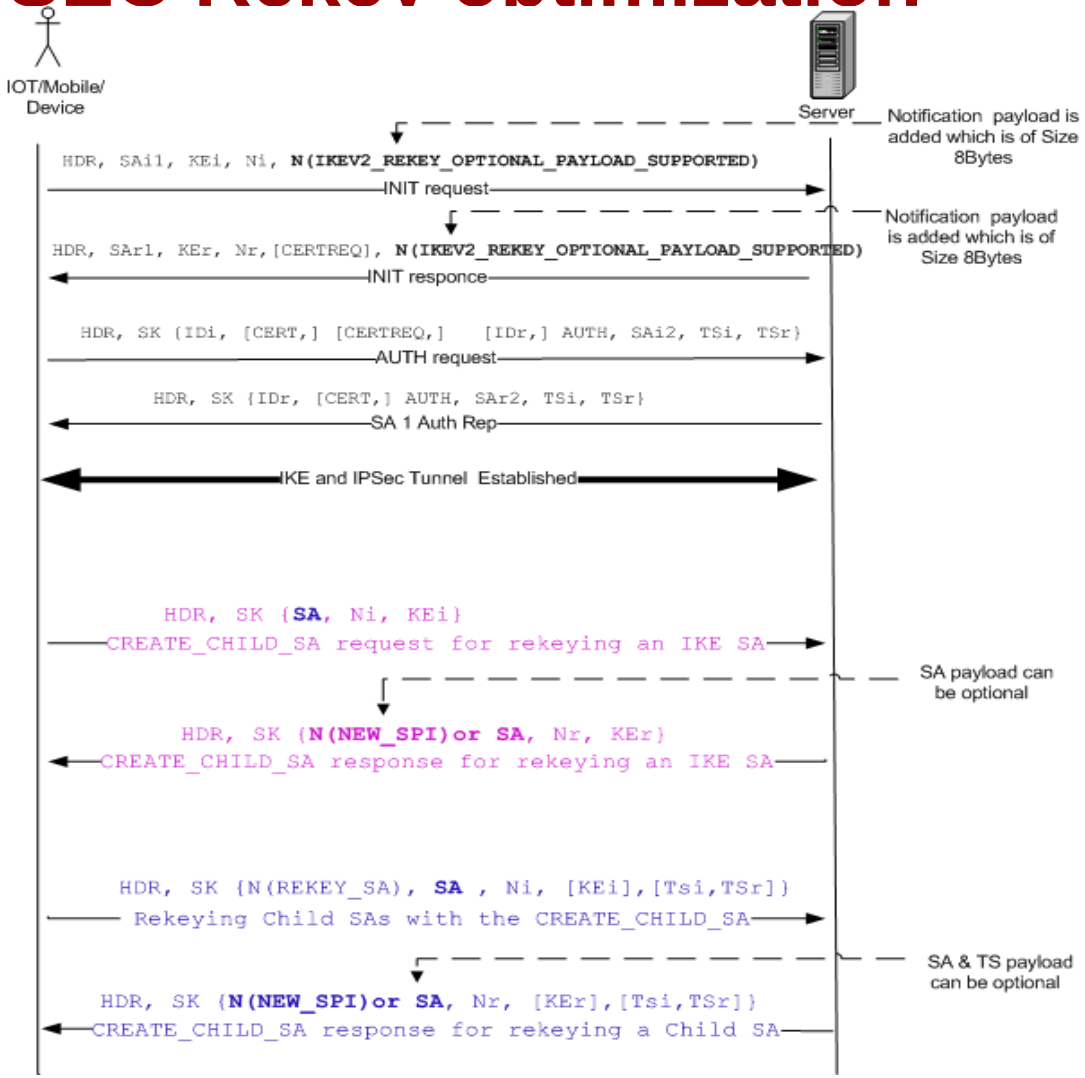
- At time of IKE rekey instead of SA payload we can use NEW_SPI notification payload which of size 16 bytes
- At time of IPSEC rekey instead of SA, TS payload we can use NEW_SPI notification payload which of size 14 bytes
- A new initiator/Responder SPI is supplied in the SPI field of the NEW_SPI notification payload.
- Due to NEW_SPI notification payload we saved minimum 36 bytes (number of bytes saving increase exponentially in multiple cryptographic suite) for each and every IKE rekey and reduced processing of complex validation and processing of SA payload
- Due to NEW_SPI notification payload we saved minimum 76 bytes (number of bytes saving increase exponentially in multiple cryptographic suite) for each and every IPSec rekey and reduced processing of complex validation and processing of SA ,TSi & TSr payloads



IKE rekey & IPSEC Rekey optimization

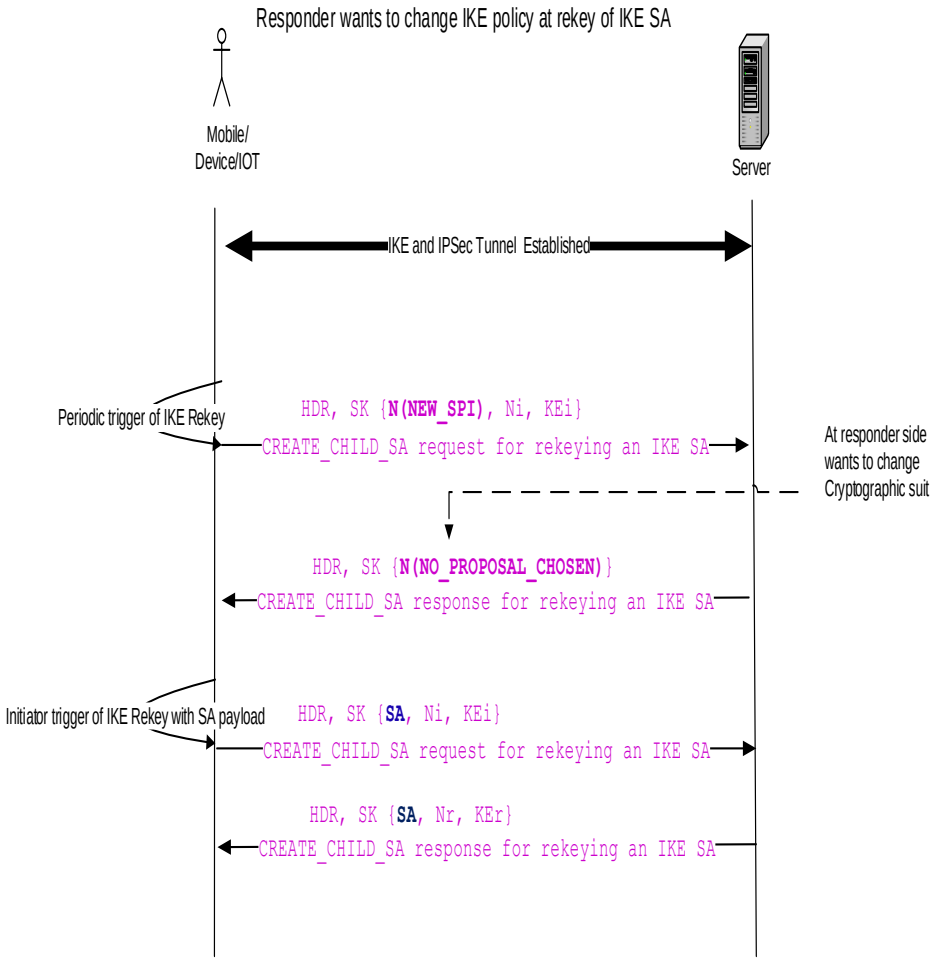
Scenario 2:

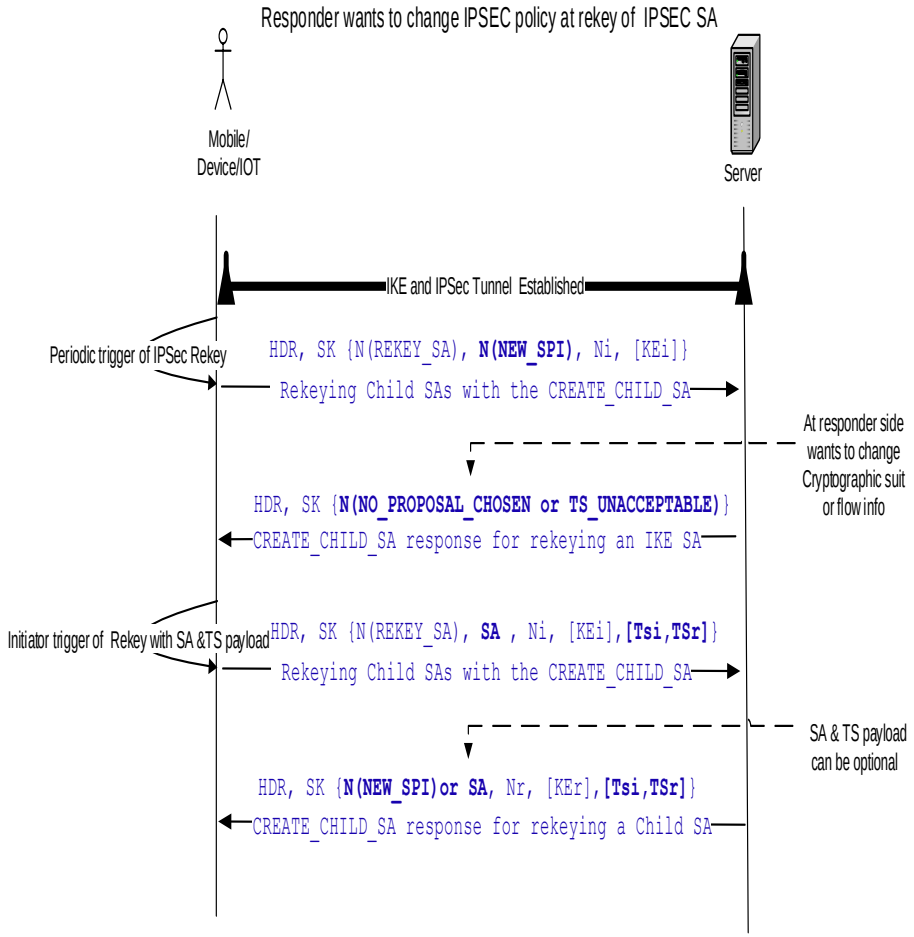
- At time of IKE rekey initiator can SA payload but responder can make it optional by sending NEW_SPI notification payload or SA payload
- At time of IPSEC rekey initiator can send of SA & optionally TS payloads but responder can make it optional by sending NEW_SPI notification payload or SA payload and optional TS payloads.
- Advantage of this solution to provide option at time of any policy changes.
- Due to NEW_SPI notification payload we saved minimum 36 bytes for each and every IKE rekey and reduced processing of complex validation and processing of SA payload
- Due to NEW_SPI notification payload we saved minimum 76 bytes for each and every IPSec rekey and reduced processing of complex validation ad processing of SA ,TSi & TSr payloads



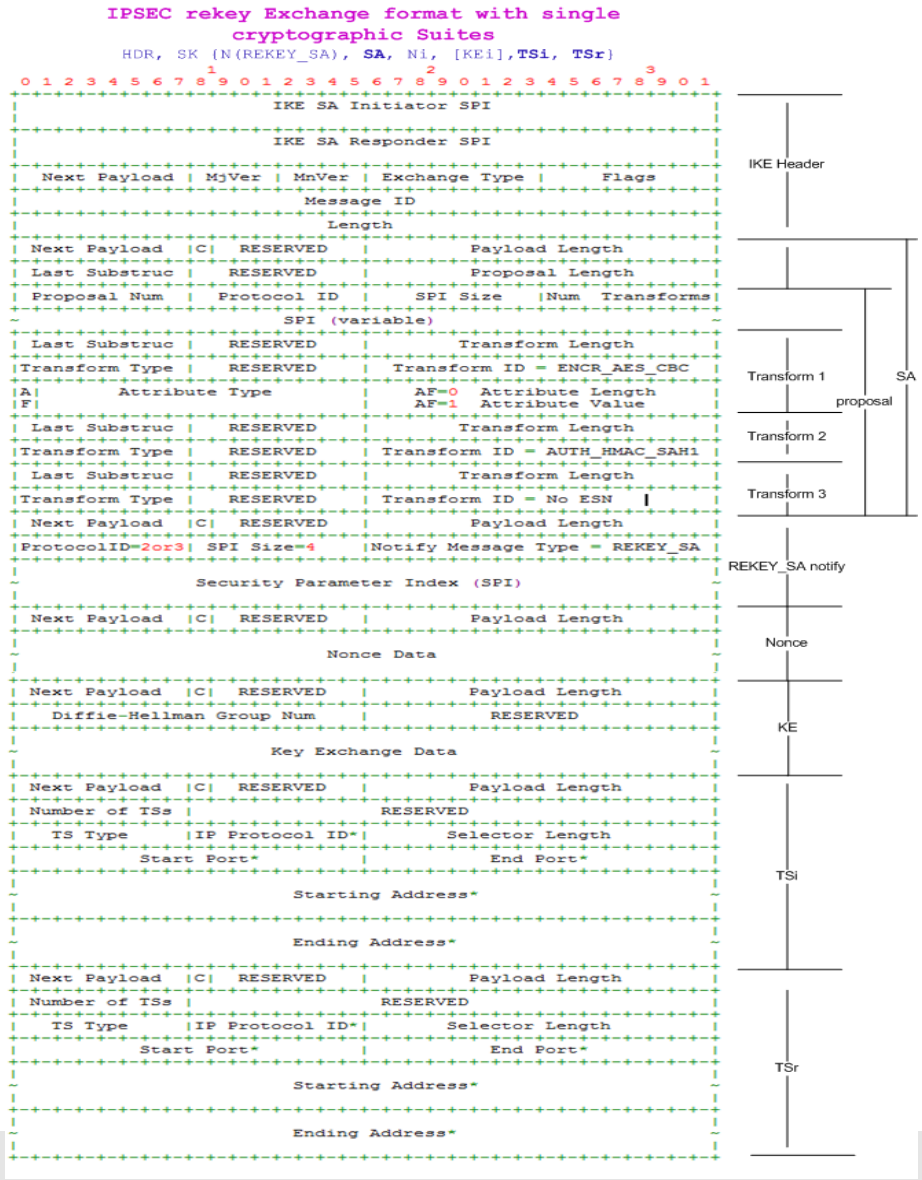
IKE rekey & IPSEC Rekey optimization

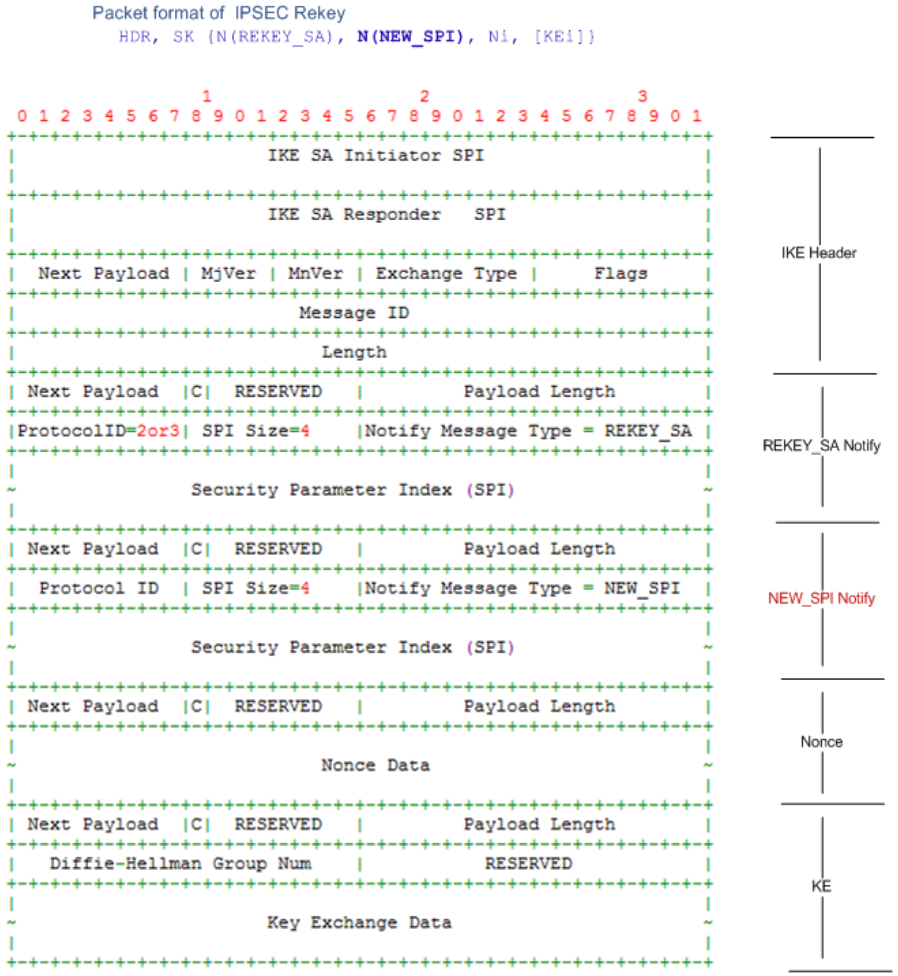
Scenario 3:





IPSEC rekey existing vs New Packet format

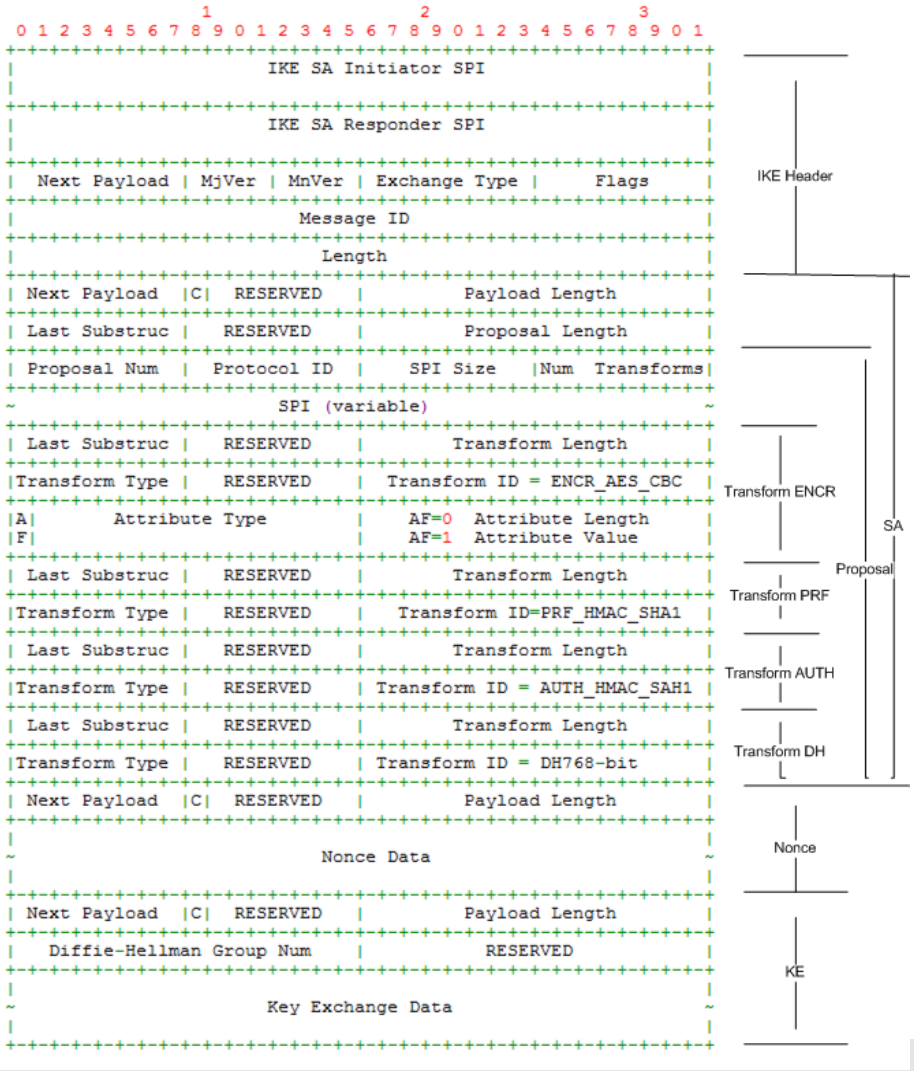




IKE rekey existing vs New Packet format

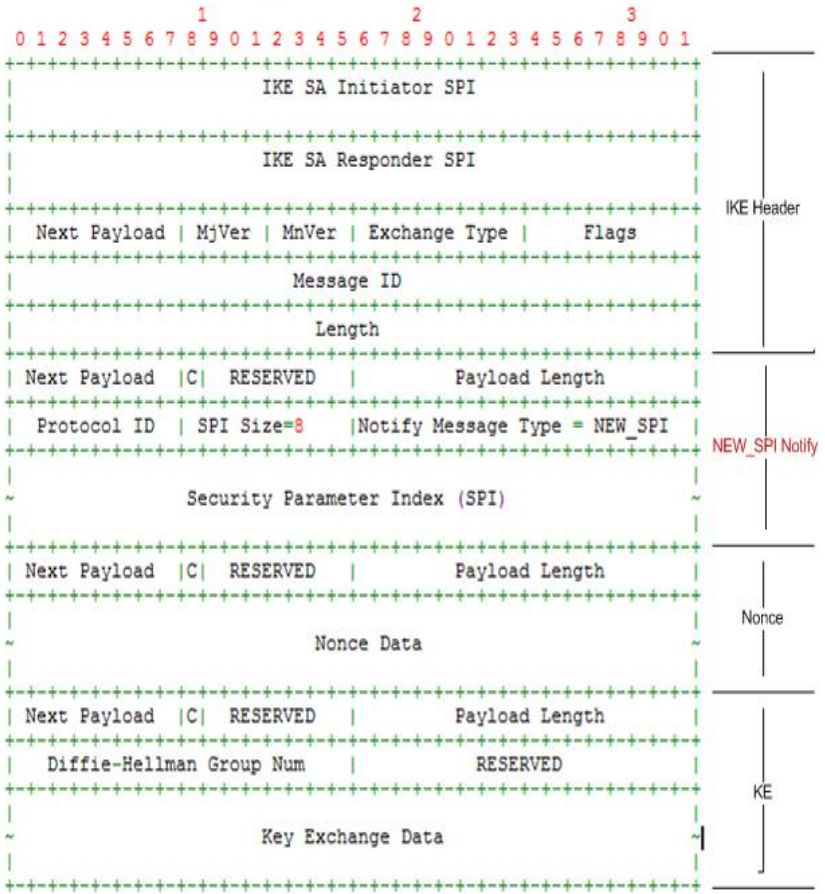
IKE rekey Exchange format with single cryptographic Suites

HDR, SK {**SA**, Ni, KEi}



Packet format of IKE Rekey

HDR, SK {**N(NEW_SPI)**, Ni, KEi}



Test Result

- **The proposed solution allows to reduced the IKEv2 rekey packet size.**
- **In our simulated test bed we observed**
  - When we configured 32 IKE cryptographic Suites. IPSEC 25 cryptographic Suites.
  - **IPSEC rekey**
    - IPSEC rekey total packet size before new solution 1036 bytes
    - IPSEC rekey total packet size with new solution 76 bytes
      - **Percentage we saved 92.66 %**
  - **IKE rekey**
    - IKE rekey total packet size before new solution 1532 bytes
    - IKE rekey total packet size with new solution 168 bytes
      - **Percentage we saved 89.03 %**

Thank You

www.huawei.com