Tech-invite

http://www.tech-invite.com

IPSec Guide

IKEv2 Formats

V1.0 – March 2, 2005

18 pages

IKEv1

- ISAKMP Header
- ISAKMP Payloads

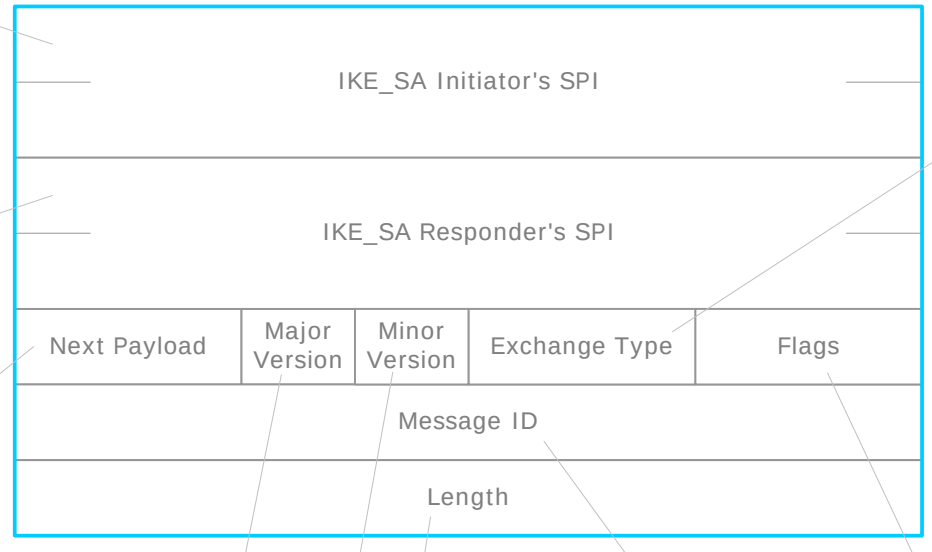
-	Generic Header
1	Security Association
2	Proposal
3	Transform
4	Key Exchange
5	Identification
6	Certificate
7	Certificate Request
8	Hash
9	Signature
10	Nonce
11	Notify
12	Delete
13	Vendor ID

IKEv2

- Header
- Payloads

-	Generic Header
33	Security Association
34	Key Exchange
35-36	Identification
37	Certificate
38	Certificate Request
39	Authentication
40	Nonce
41	Notify
42	Delete
43	Vendor ID
44-45	Traffic Selector
46	Encrypted
47	Configuration
48	Extensible Authentication Protocol

IKEv2 – Header Format



Type of exchange being used.

This constrains the payloads sent in each message and orderings of messages in an exchange:

IKE_SA_INIT	34
IKE_AUTH	35
CREATE_CHILD_SA	36
INFORMATIONAL	37

Type of payload that immediately follows the header:

SA	Security Association	33
KE	Key Exchange	34
IDi	Identification - Initiator	35
IDr	Identification - Responder	36
CERT	Certificate	37
CERTREQ	Certificate Request	38
AUTH	Authentication	39
Ni, Nr	Nonce	40
N	Notify	41
D	Delete	42
V	Vendor	43
TSi	Traffic Selector - Initiator	44
TSr	Traffic Selector - Responder	45
E	Encrypted	46
CP	Configuration	47
EAP	Extensible Authentication	48

Set to: 2

Set to: 0

Message identifier used to control retransmission of lost packets and matching of requests and responses. It is essential to the security of the protocol because it is used to prevent message replay attacks.

Length of total message (header + payloads) in octets.

Indicates specific options that are set for the message:

I Initiator (bit 3)
It is used by the recipient to determine which eight octets of the SPI was generated by the recipient.

V Version (bit 4)
Indicates that the transmitter is capable of speaking a higher major version number of the protocol than the one indicated in the major version

R Response (bit 5)
Indicates that this message is a response to a message containing the same message ID.

IKEv2 – Generic Payload Header Format

IKEv2 Generic Payload Header

Next Payload	C	Reserved	Payload Length

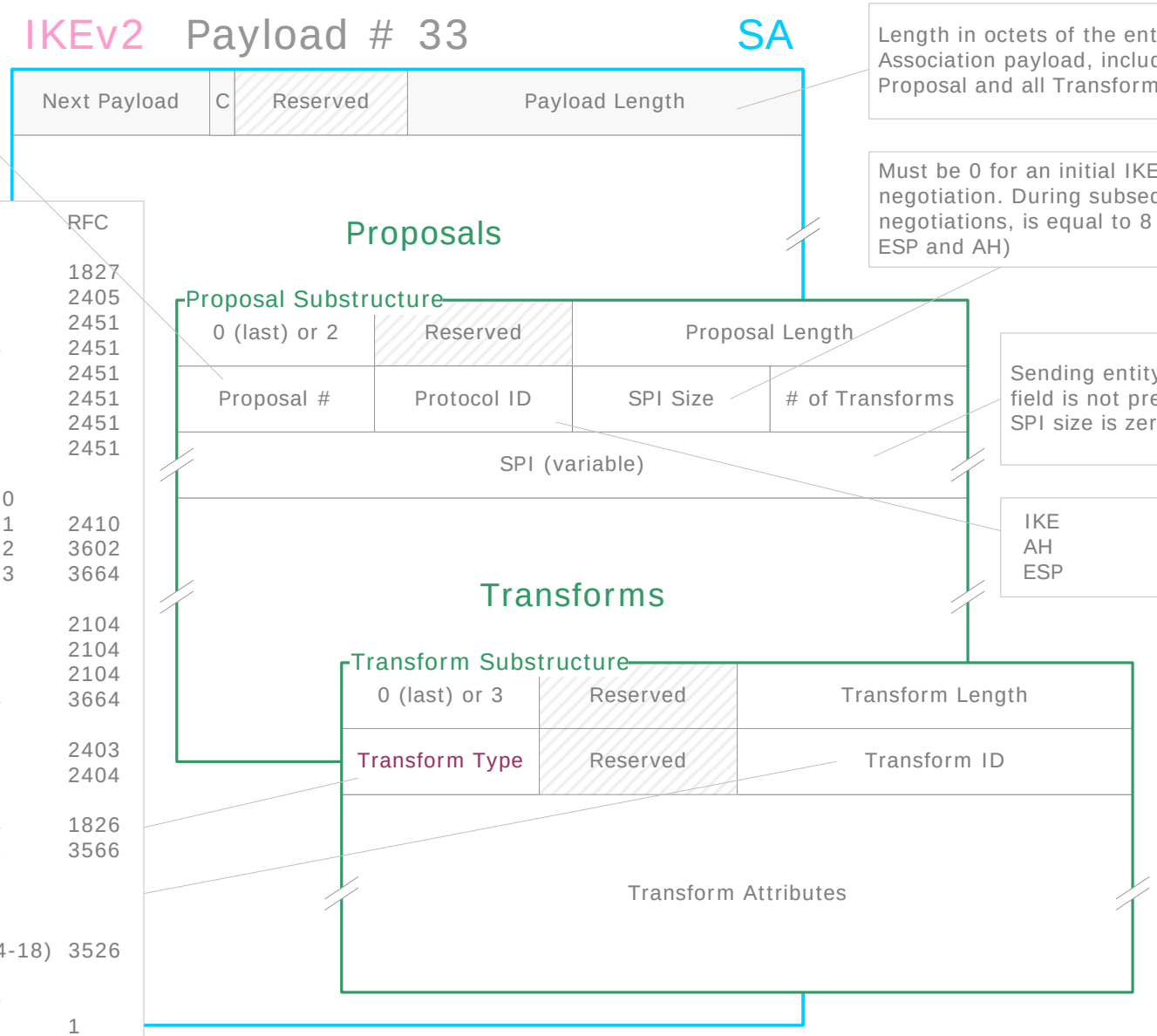
	No Next Payload	0
SA	Security Association	33
KE	Key Exchange	34
IDi	Identification - Initiator	35
IDr	Identification - Responder	36
CERT	Certificate	37
CERTREQ	Certificate Request	38
AUTH	Authentication	39
Ni, Nr	Nonce	40
N	Notify	41
D	Delete	42
V	Vendor	43
TSi	Traffic Selector - Initiator	44
TSr	Traffic Selector - Responder	45
E	Encrypted	46
CP	Configuration	47
EAP	Extensible Authentication Protocol	48

Critical bit: specifies the processing by the recipient in case the type of this payload is not understood:

0 payload skipped
1 message rejected

IKEv2 – Security Association (SA) Payload Format

First proposal in an SA payload must be #1. Subsequent proposals must either be the same as the previous proposal (indicating an AND) or one more than the previous proposal (indicating an OR)



Length in octets of the entire Security Association payload, including all Proposal and all Transform substructures

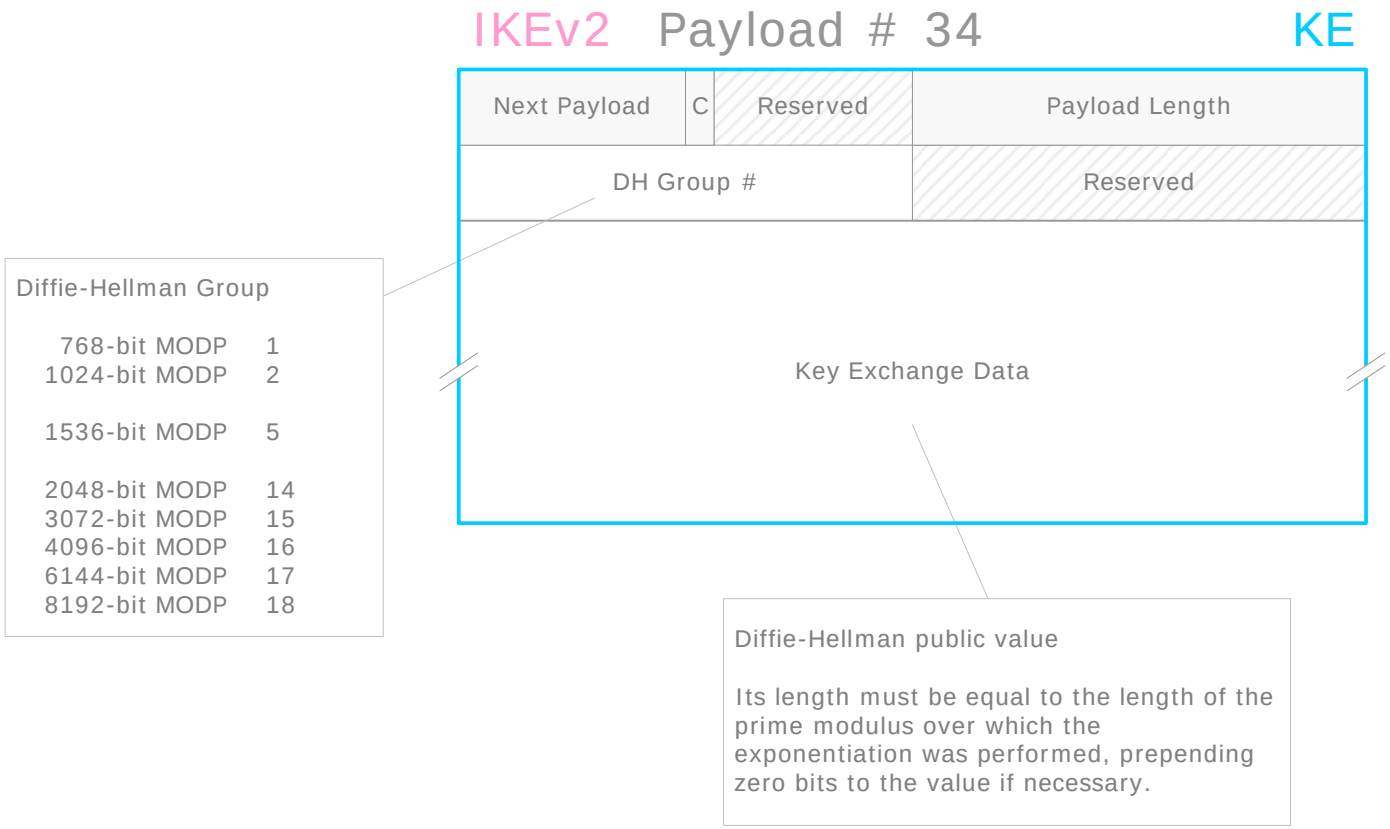
Must be 0 for an initial IKE_SA negotiation. During subsequent negotiations, is equal to 8 for IKE, 4 for ESP and AH)

Sending entity's SPI. This field is not present when the SPI size is zero.

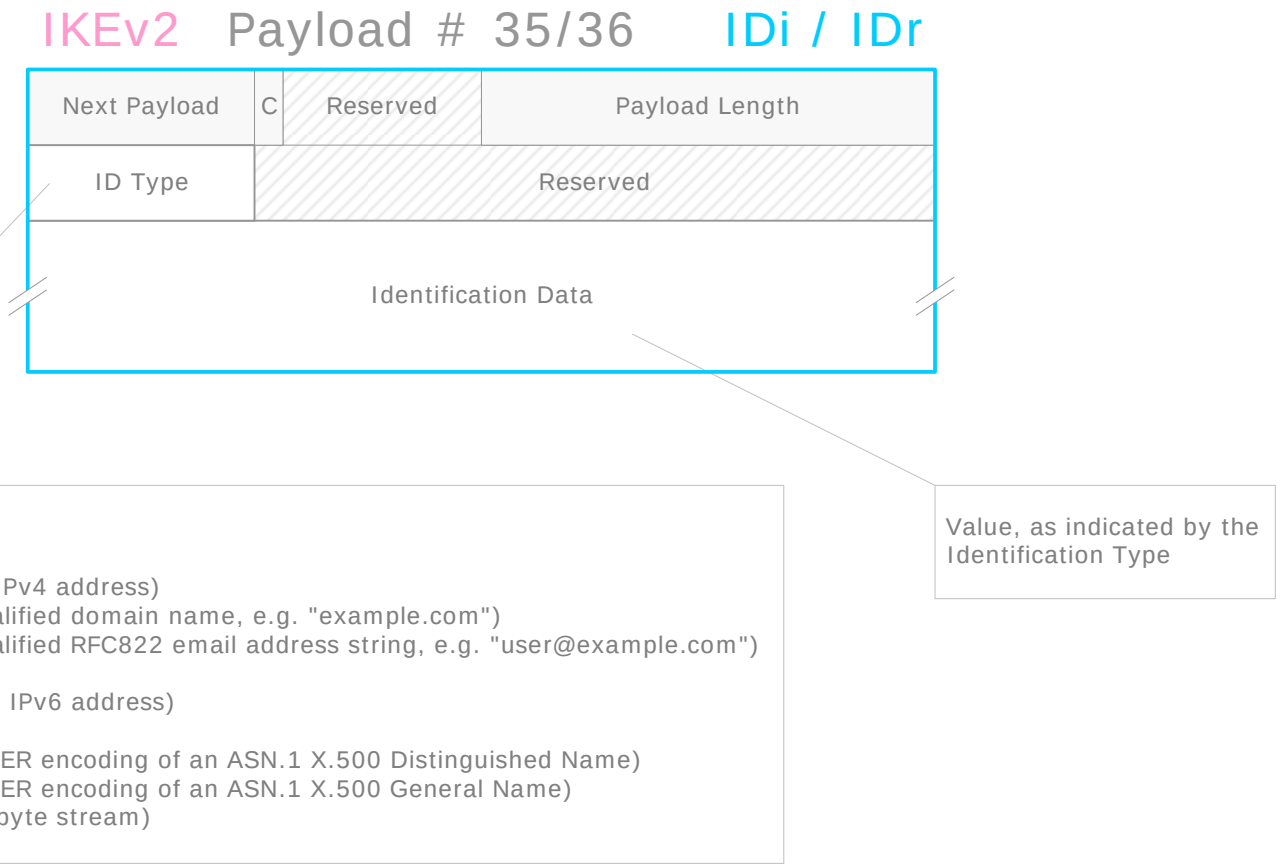
IKE	1
AH	2
ESP	3

			RFC
ENCR	Encryption Algorithm	1	
	ENCR_DES_IV64	1	1827
	ENCR_DES	2	2405
	ENCR_3DES	3	2451
	ENCR_RC5	4	2451
	ENCR_IDEA	5	2451
	ENCR_CAST	6	2451
	ENCR_BLOWFISH	7	2451
	ENCR_3IDEA	8	2451
	ENCR_DES_IV32	9	
	reserved	10	
	ENCR_NULL	11	2410
	ENCR_AES_CBC	12	3602
	ENCR_AES_CTR	13	3664
PRF	Pseudo-Random Function	2	
	PRF_HMAC_MD5	1	2104
	PRF_HMAC_SHA1	2	2104
	PRF_HMAC_TIGER	3	2104
	PRF_AES128_CBC	4	3664
INTEG	Integrity Algorithm	3	
	AUTH_HMAC_MD5_96	1	2403
	AUTH_HMAC_SHA1_96	2	2404
	AUTH_DES_MAC	3	
	AUTH_KPDK_MD5	4	1826
	AUTH_AES_XCBC_96	5	3566
D-H	Diffie-Hellman Group	4	
	768-bit MODP	1	
	1024-bit MODP	2	
	more MODP DH groups	(5, 14-18)	3526
ESN	Extended Sequence Number	5	
	No	0	
		Yes	1

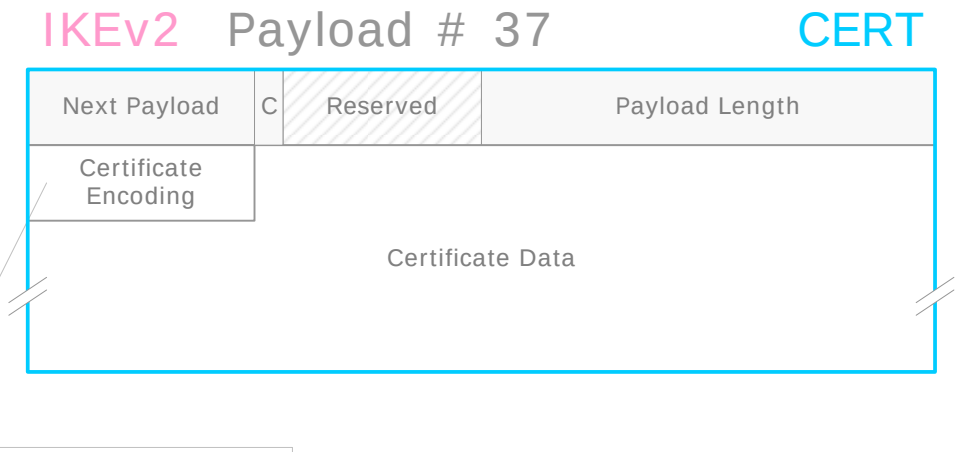
IKEv2 – Key Exchange (KE) Payload Format



IKEv2 – Identification (IDi or IDr) Payload Format



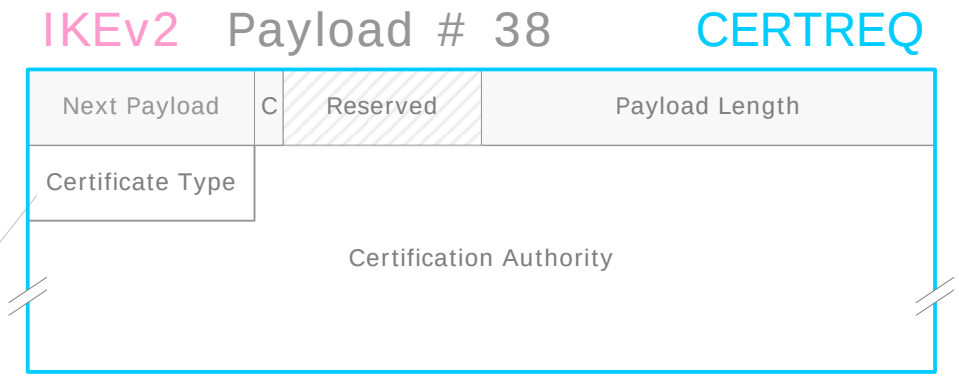
IKEv2 – Certificate (CERT) Payload Format



Type of certificate or certificate-related information contained in the Certificate Data field

NONE	0
PKCS #7 wrapped X.509 certificate	1
PGP Certificate	2
DNS Signed Key	3
X.509 Certificate - Signature	4
Kerberos Tokens	6
Certificate Revocation List (CRL)	7
Authority Revocation List (ARL)	8
SPKI Certificate	9
X.509 Certificate - Attribute	10
Raw RSA Key	11
Hash and URL of X.509 certificate	12
Hash and URL of X.509 bundle	13

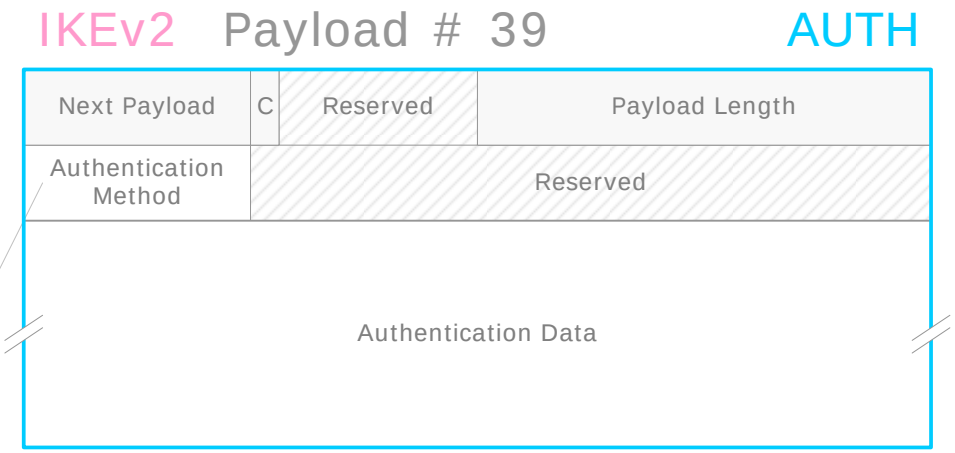
IKEv2 – Certificate Request (CERTREQ) Payload Format



Type of certificate or certificate-related information contained in the Certificate Data field

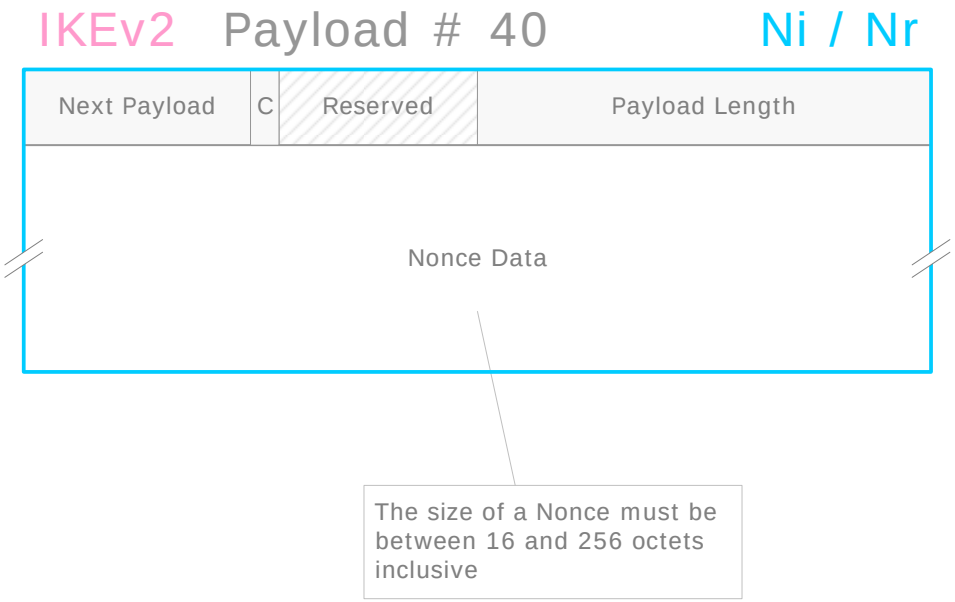
NONE	0
PKCS #7 wrapped X.509 certificate	1
PGP Certificate	2
DNS Signed Key	3
X.509 Certificate - Signature	4
Kerberos Tokens	6
Certificate Revocation List (CRL)	7
Authority Revocation List (ARL)	8
SPKI Certificate	9
X.509 Certificate - Attribute	10
Raw RSA Key	11
Hash and URL of X.509 certificate	12
Hash and URL of X.509 bundle	13

IKEv2 – Authentication (AUTH) Payload Format

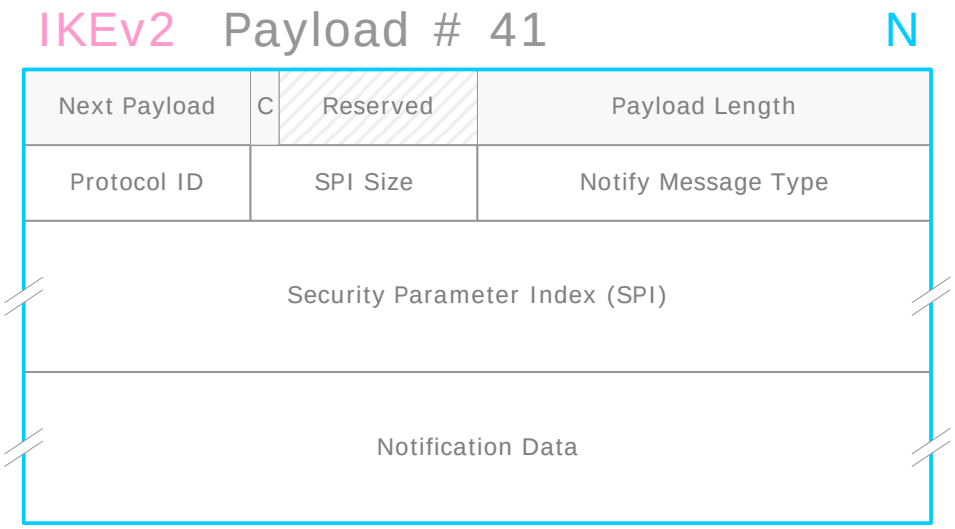


RSA Digital Signature	1
Shared Key Message Integrity Code	2
DSS Digital Signature	3

IKEv2 – Nonce (Ni or Nr) Payload Format



IKEv2 – Notify (N) Payload Format

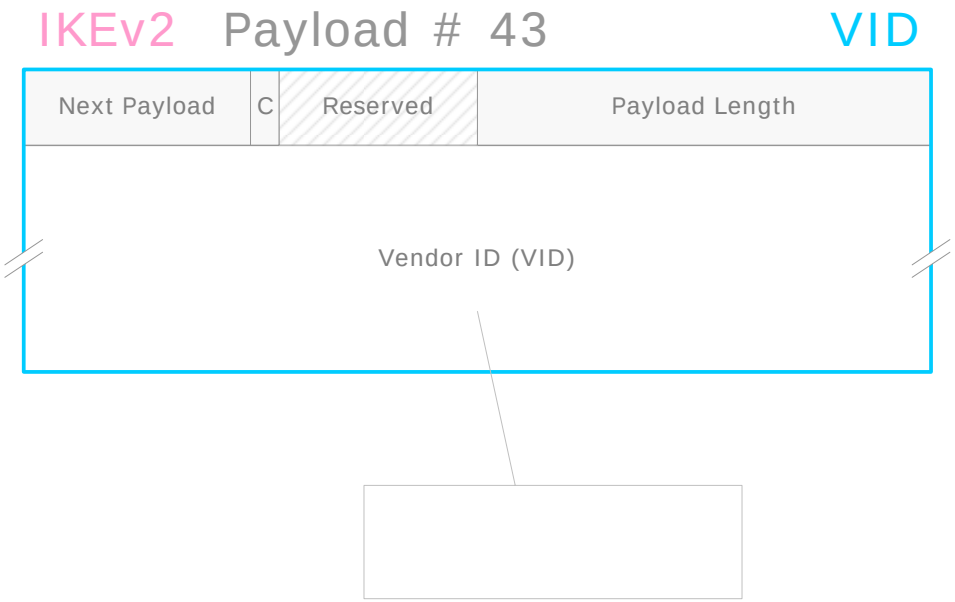


IKEv2 – Delete (D) Payload Format

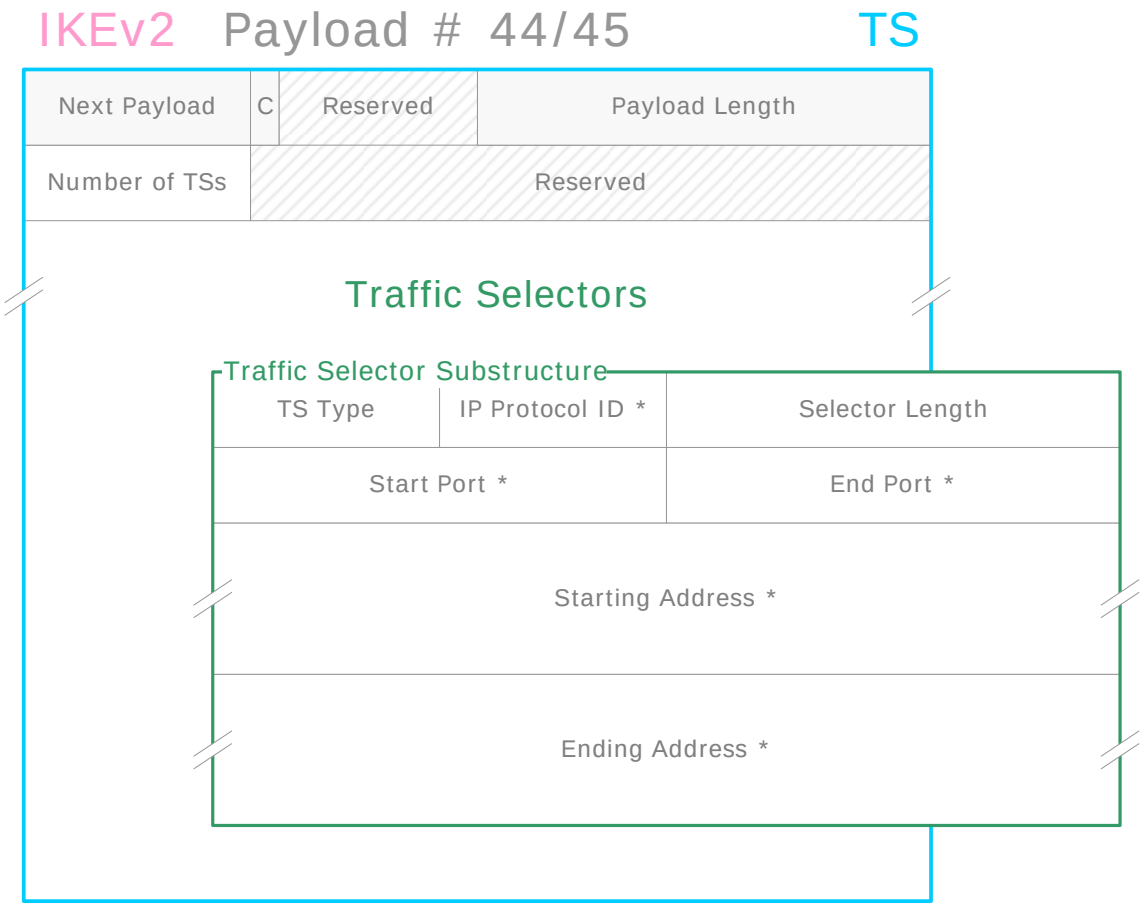
IKEv2 Payload # 42 D

Next Payload	C	Reserved	Payload Length
Protocol ID	SPI Size		# of SPIs
Security Parameter Index (es) (SPI)			

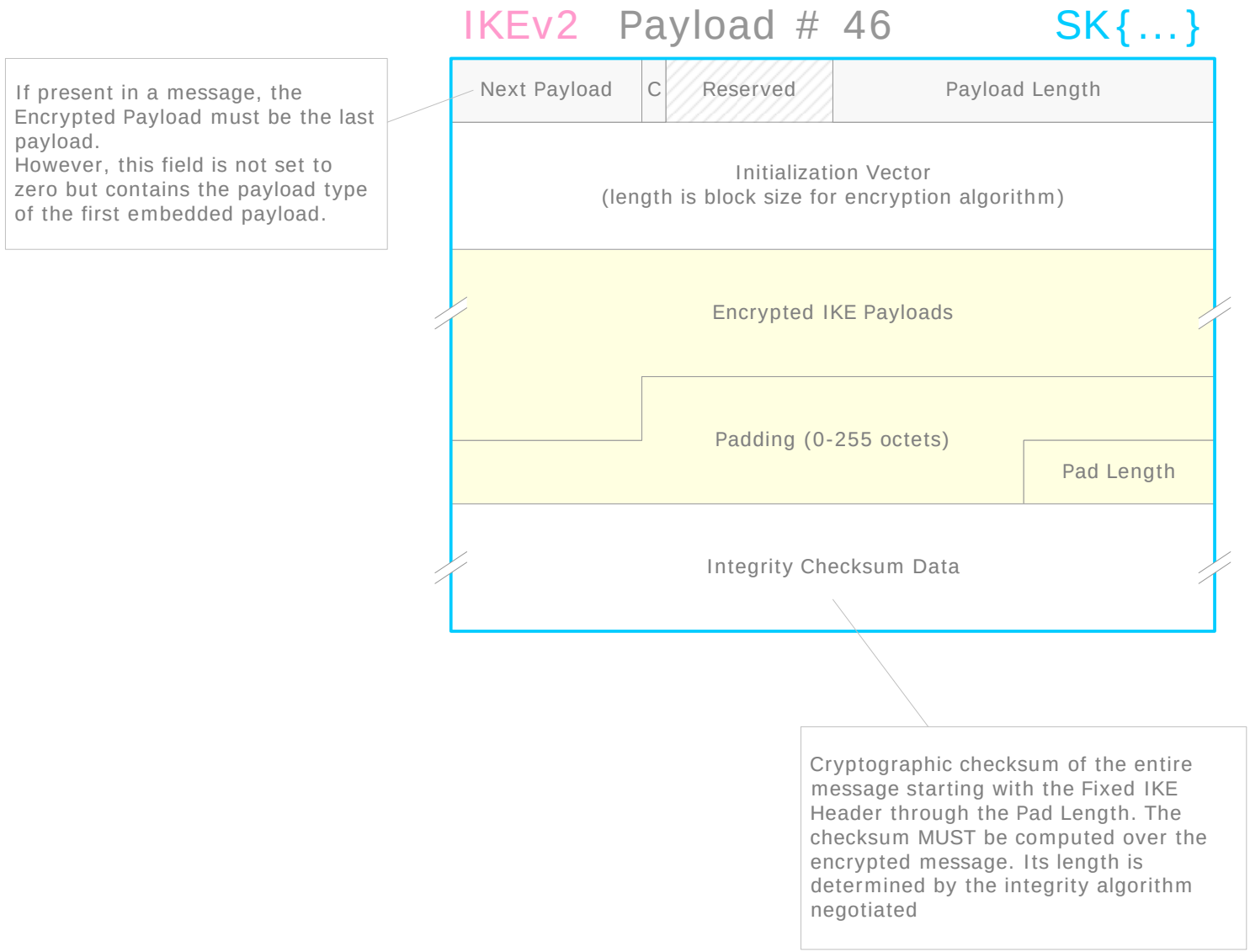
IKEv2 – Vendor ID (VID) Payload Format



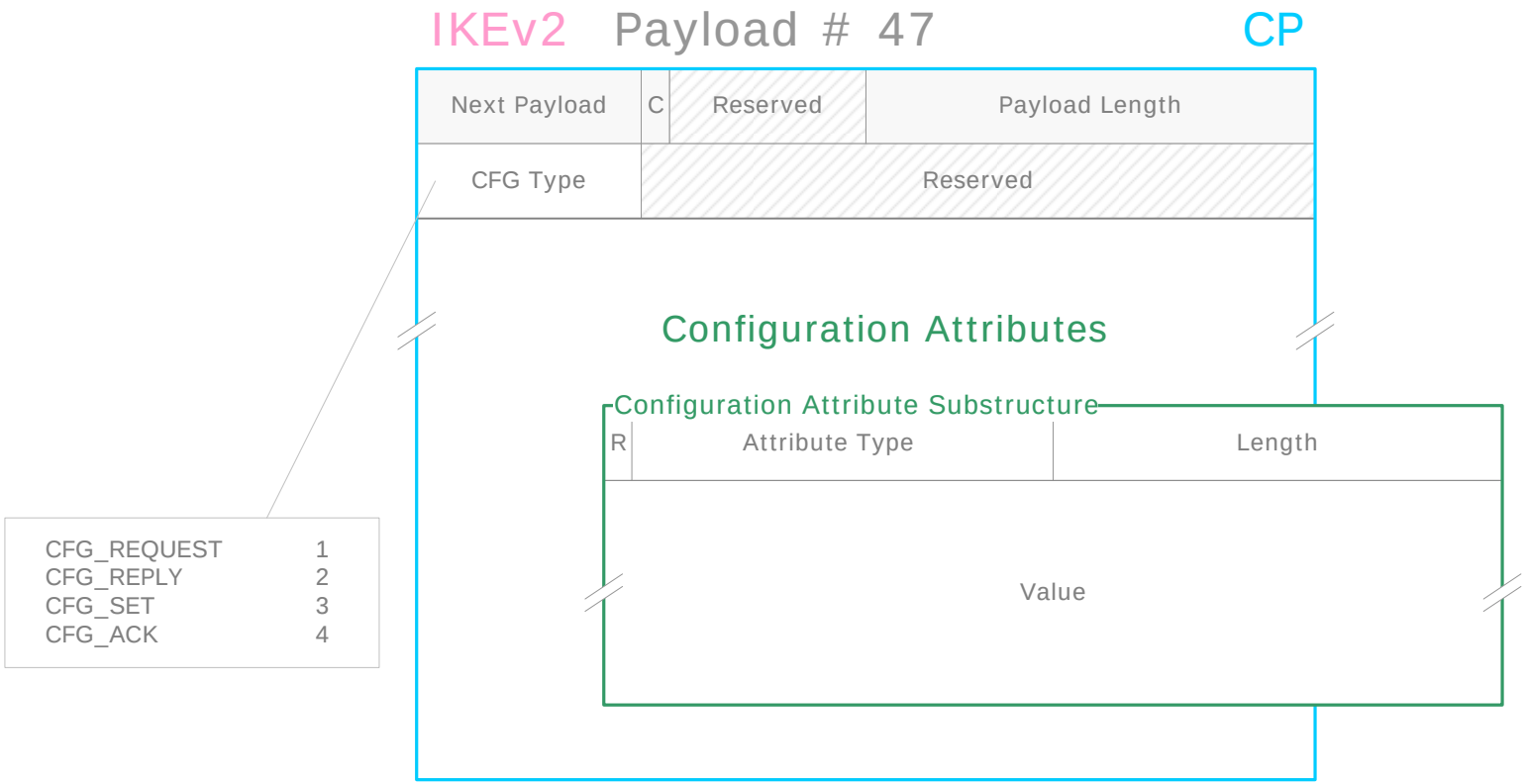
IKEv2 – Traffic Selector (TS) Payload Format



IKEv2 – Encrypted (SK{…}) Payload Format



IKEv2 – Configuration (CP) Payload Format



IKEv2 – Extensible Authentication Protocol (EAP) Payload Format