Tech-invite

http://www.tech-invite.com

IPSec Guide

ISAKMP & IKE Formats

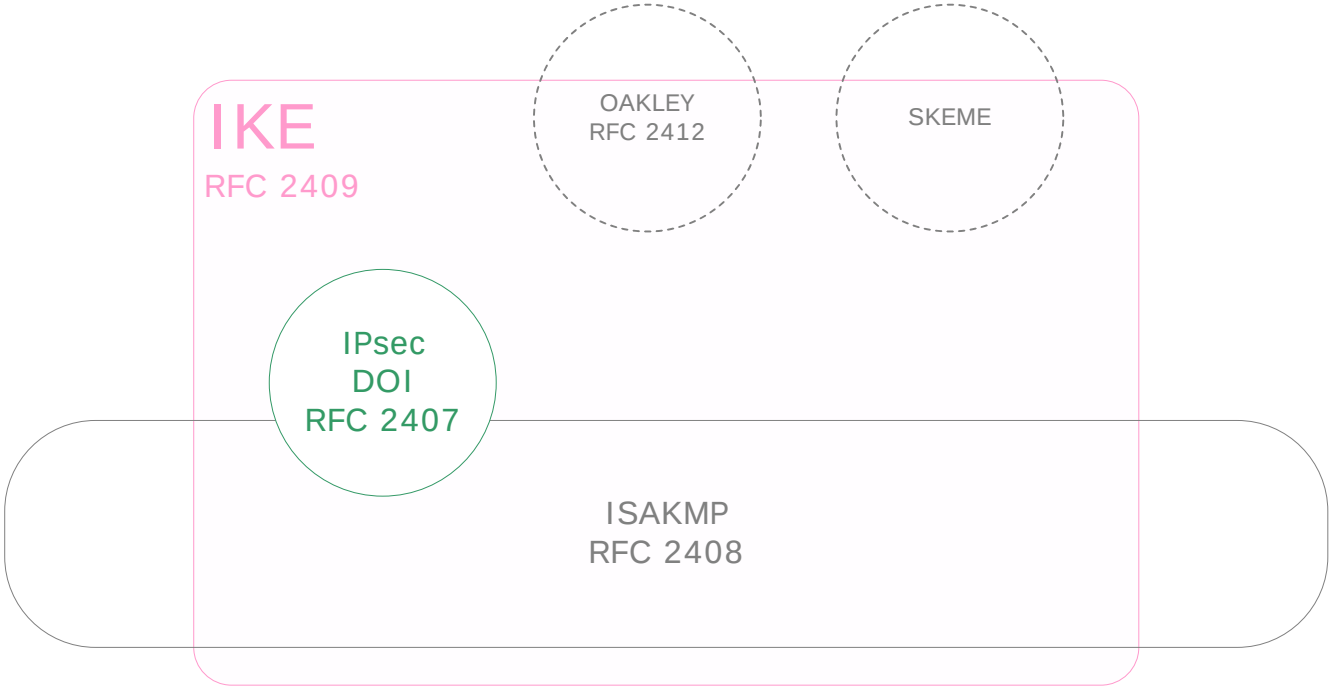
V1.0 – March 2, 2005

This document illustrates IKE message formats. These formats result from ISAKMP framework definition (RFC 2408) refined by IPSec DOI (domain of interpretation, defined in RFC2407) for phase 2 attributes, and finally appendix A of RFC 2409 (IKE) for phase 1 attributes.

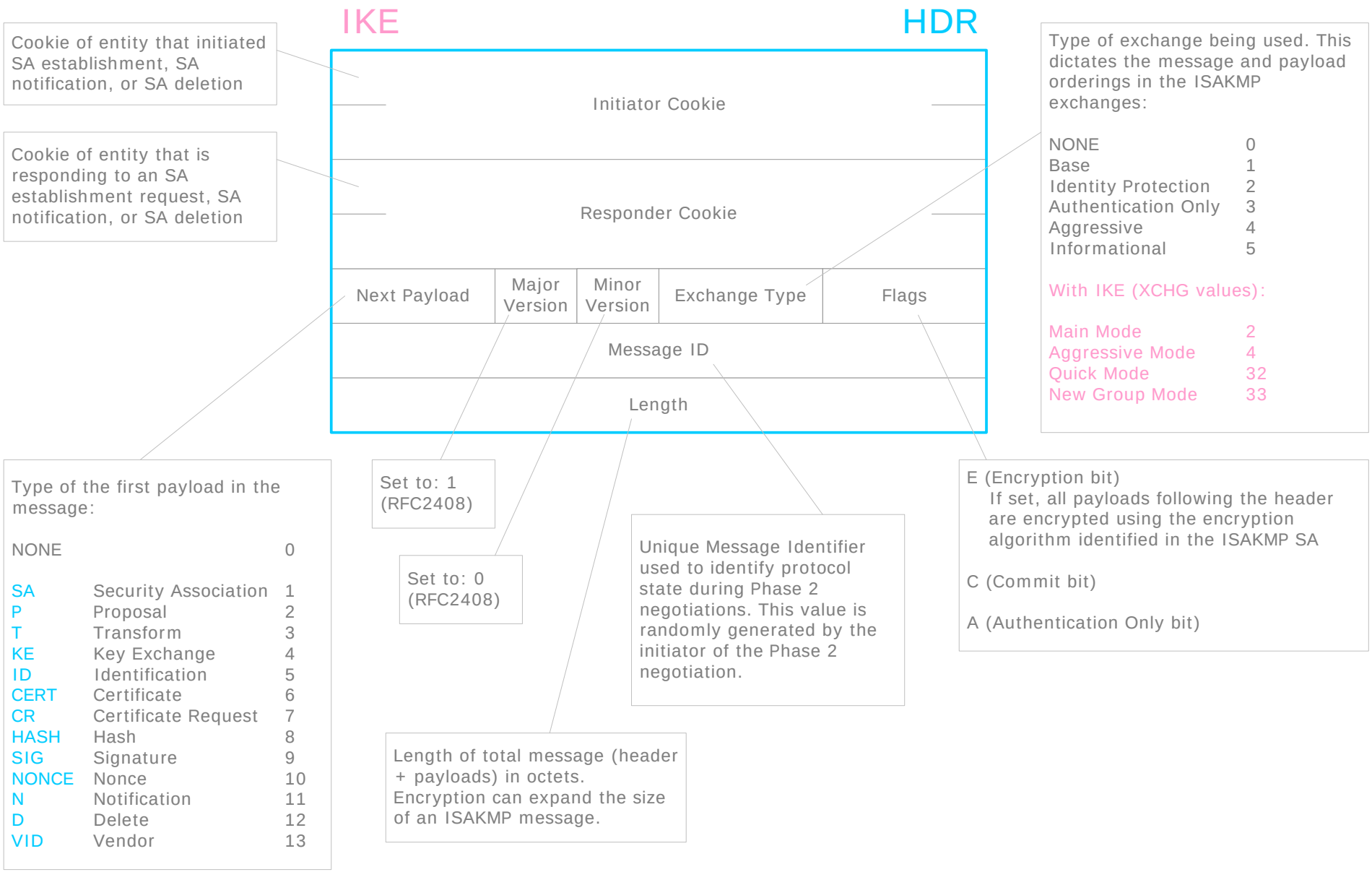
Color codes are used consistently throughout this document for relevant information sources.

17 pages

IPSec / IKE – Structure



IPSec / IKE – ISAKMP Header Format



IPSec / IKE – Generic Payload Header Format

IKE Generic Payload Header

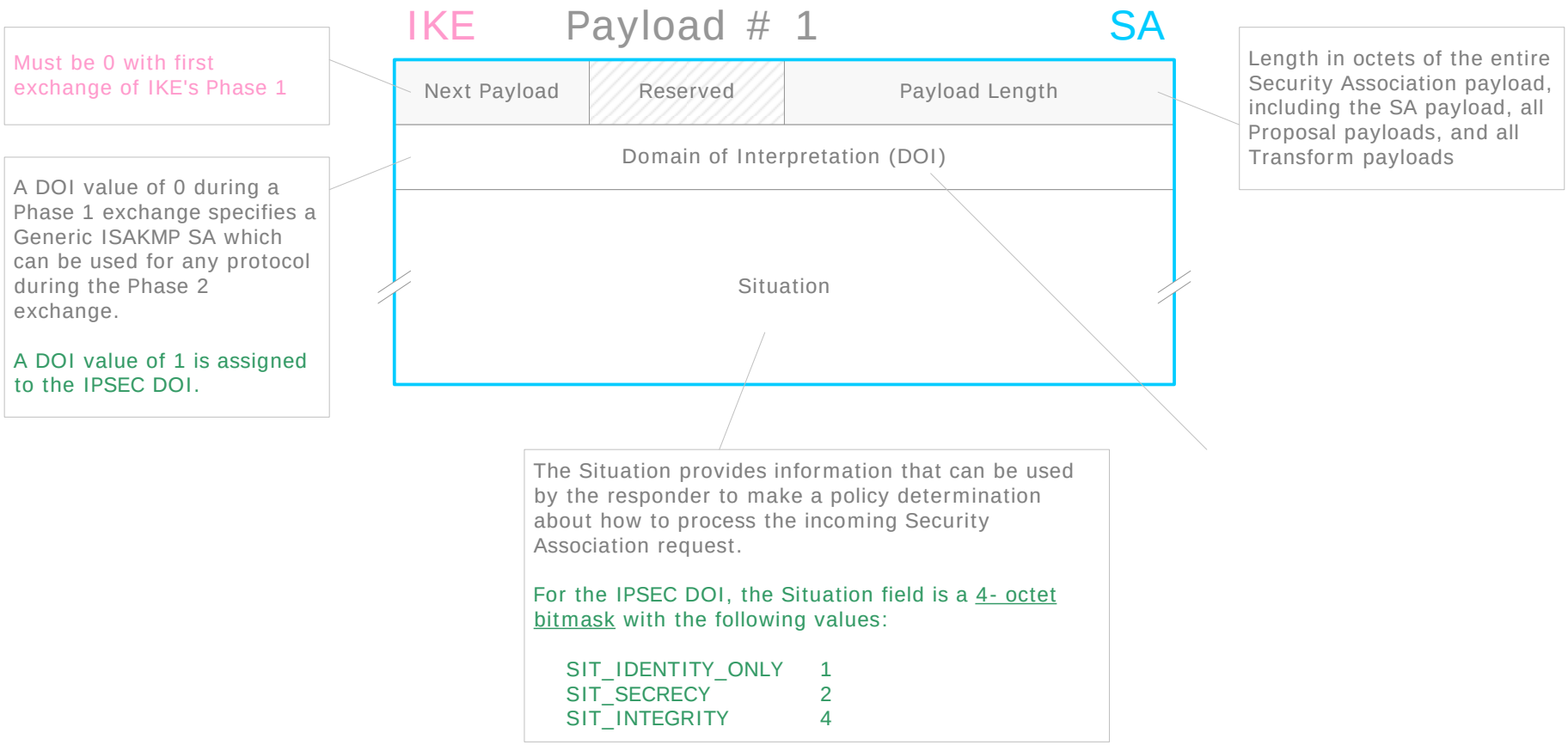
Next Payload	Reserved	Payload Length

This field provides the "chaining" capability

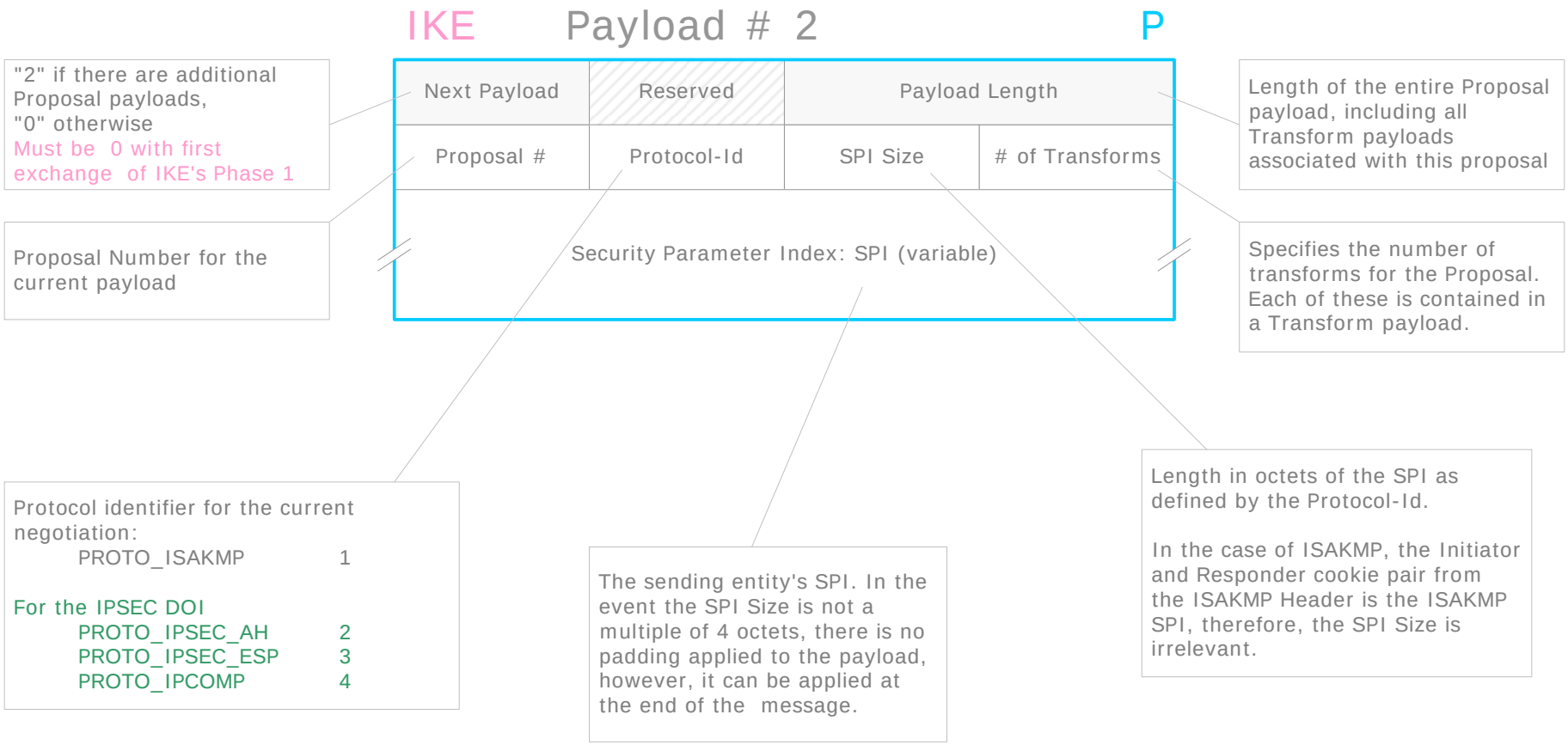
	No Next Payload	0
SA	Security Association	1
P	Proposal	2
T	Transform	3
KE	Key Exchange	4
ID	Identification	5
CERT	Certificate	6
CR	Certificate Request	7
HASH	Hash	8
SIG	Signature	9
NONCE	Nonce	10
N	Notification	11
D	Delete	12
VID	Vendor	13

Length in octets of the current payload, including the generic payload header

IPSec / IKE – Security Association (SA) Payload Format



IPSec / IKE – Proposal (P) Payload Format



IPSec / IKE – Transform (T) Payload Format

"3" if there are additional T payloads, "0" otherwise

Identifies the Transform number for the current payload. If there is more than one transform proposed for a specific protocol within the Proposal payload, then each Transform payload has a unique Transform number

Transform identifier for the current negotiation.

For IPSEC DOI, depending on Protocol-Id in Proposal:

- With PROTO_ISAKMP:
  - KEY_IKE 1
- With PROTO_IPCOMP:
  - IPCOMP_OUI 1
  - IPCOMP_DEFLATE 2
  - IPCOMP_LZS 3
- With PROTO_IPSEC_AH:
  - AH_MD5 2
  - AH_SHA 3
  - AH_DES 4
- With PROTO_IPSEC_ESP:
  - ESP_DES_IV64 1
  - ESP_DES 2
  - ESP_3DES 3
  - ESP_RC5 4
  - ESP_IDEA 5
  - ESP_CAST 6
  - ESP_BLOWFISH 7
  - ESP_3IDEA 8
  - ESP_DES_IV32 9
  - ESP_RC4 10
  - ESP_NULL 11

IKE Payload # 3 T

Next Payload	Reserved	Payload Length
Transform #	Transform-Id	Reserved
SA Attributes		

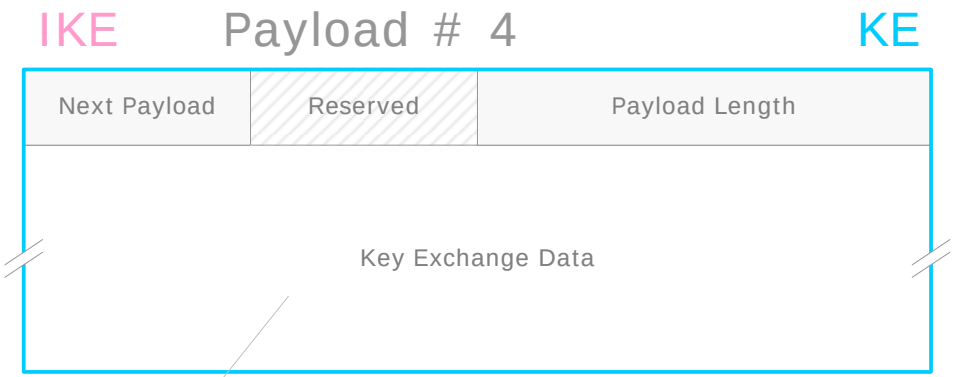
With IKE, during phase 1, some important attribute types & values:

	Type	Values	
Encryption Algorithm	1		
		DES-CBC	1
		IDEA-CBC	2
		3DES-CBC	5
Hash Algorithm	2		
		MD5	1
		SHA	2
Authentication Method	3		
		Pre-Shared Key	1
		DSS signatures	2
		RSA signatures	3
		Encryption with RSA	4
		Revised Encryption with RSA	5
Group Description	4		
		768-bit MODP	1
		1024-bit MODP	2
		EC2N group on GF[2^155]	3
		EC2N group on GF[2^185]	4
Life Type	5		
		seconds	1
		kilobytes	2
Life Duration	12		

With IPSec Protocols, during Quick Mode phase 2, some important attribute types & values:

	Type	Values	
SA Life Type	1		
		seconds	1
		kilobytes	2
SA Life Duration	2		
Group Description (PFS negotiation)	3		
		768-bit MODP	1
		1024-bit MODP	2
		2048-bit MODP	14
		...	
Encapsulation Mode	4		
		Tunnel	1
		Transport	2
Authentication Algorithm	5		
		HMAC-MD5	1
		HMAC-SHA	2
		DES-MAC	3
		KPDK	4

IPSec / IKE – Key Exchange (KE) Payload Format



The Diffie-Hellman public value, as per the Diffie-Hellman Group Type and Description attributes in the negotiated transform.

IPSec / IKE – Identification (ID) Payload Format

IKE Payload # 5 ID

Next Payload	Reserved	Payload Length
ID Type	Protocol ID	Port
Identification Data		

Value specifying an associated port (e.g. 500, with UDP). A value of 0 means that the Port field should be ignored

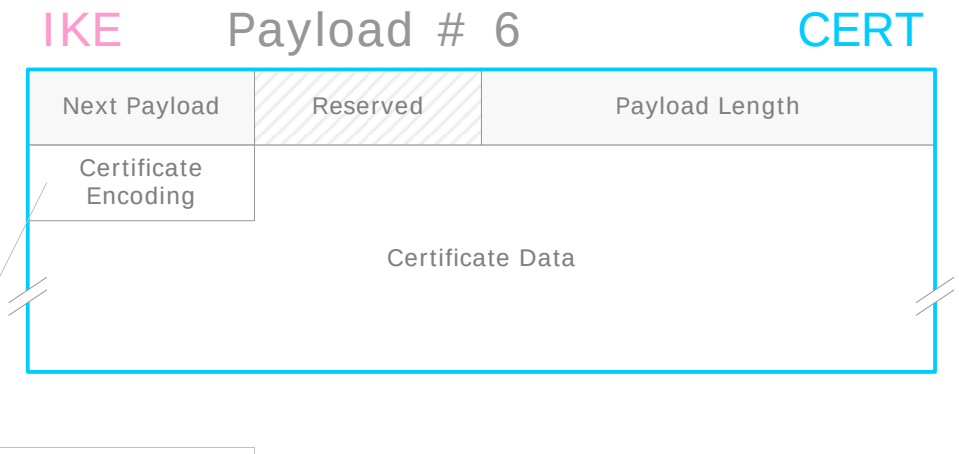
Value specifying an associated IP protocol ID (e.g. UDP/TCP). A value of 0 means that the Protocol ID field should be ignored

Value, as indicated by the Identification Type

Identification Type:

ID_IPV4_ADDR	1	(4-octet IPv4 address)
ID_FQDN	2	(fully-qualified domain name, e.g. "foo.bar.com")
ID_USER_FQDN	3	(fully-qualified username string, e.g. "user@foo.bar.com")
ID_IPV4_ADDR_SUBNET	4	(4-octet IPv4 address + 4-octet IPv4 network mask)
ID_IPV6_ADDR	5	(16-octet IPv6 address)
ID_IPV6_ADDR_SUBNET	6	(16-octet IPv6 address + 16-octet IPv6 network mask)
ID_IPV4_ADDR_RANGE	7	(4-octet beginning IPv4 address + 4-octet ending IPv4 address)
ID_IPV6_ADDR_RANGE	8	(16-octet beginning IPv6 address + 16-octet ending IPv6 address)
ID_DER_ASN1_DN	9	(binary DER encoding of an ASN.1 X.500 Distinguished Name)
ID_DER_ASN1_GN	10	(binary DER encoding of an ASN.1 X.500 General Name)
ID_KEY_ID	11	(opaque byte stream)

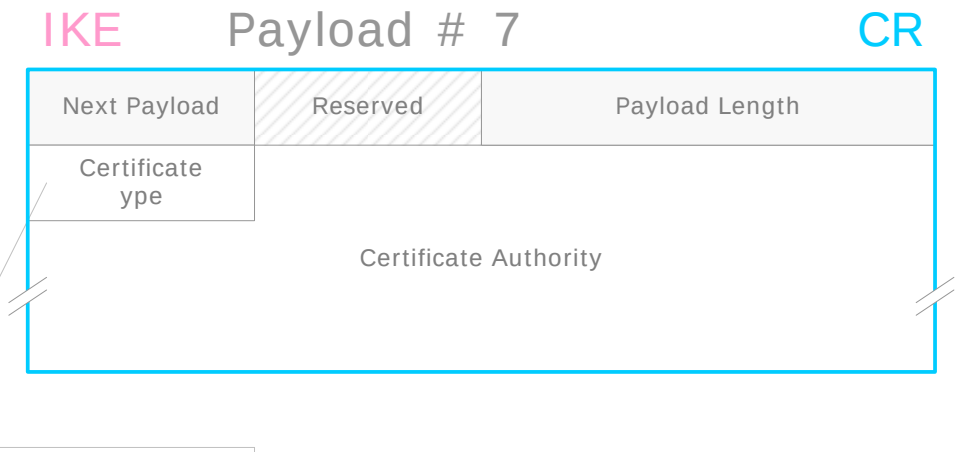
IPSec / IKE – Certificate (CERT) Payload Format



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
X.509 Certificate - Key Exchange	5
Kerberos Tokens	6
Certificate Revocation List (CRL)	7
Authority Revocation List (ARL)	8
SPKI Certificate	9
X.509 Certificate - Attribute	10

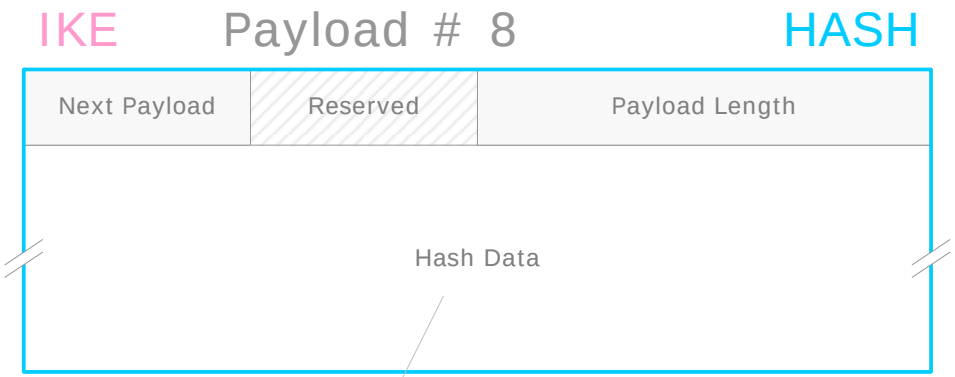
IPSec / IKE – Certificate Request (CR) Payload Format



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
X.509 Certificate - Key Exchange	5
Kerberos Tokens	6
Certificate Revocation List (CRL)	7
Authority Revocation List (ARL)	8
SPKI Certificate	9
X.509 Certificate - Attribute	10

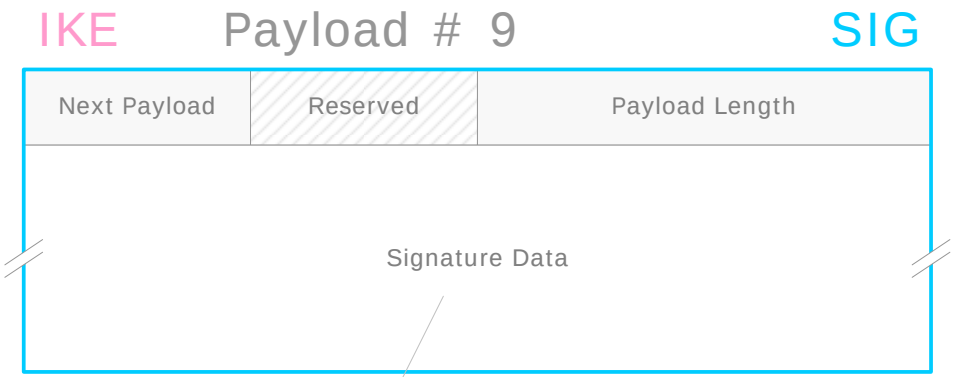
IPSec / IKE – Hash (HASH) Payload Format



Data generated by the hash function (selected during the SA establishment exchange), over some part of the message and/or ISAKMP state.

May be used to verify the integrity of the data in an ISAKMP message or for authentication of the negotiating entities.

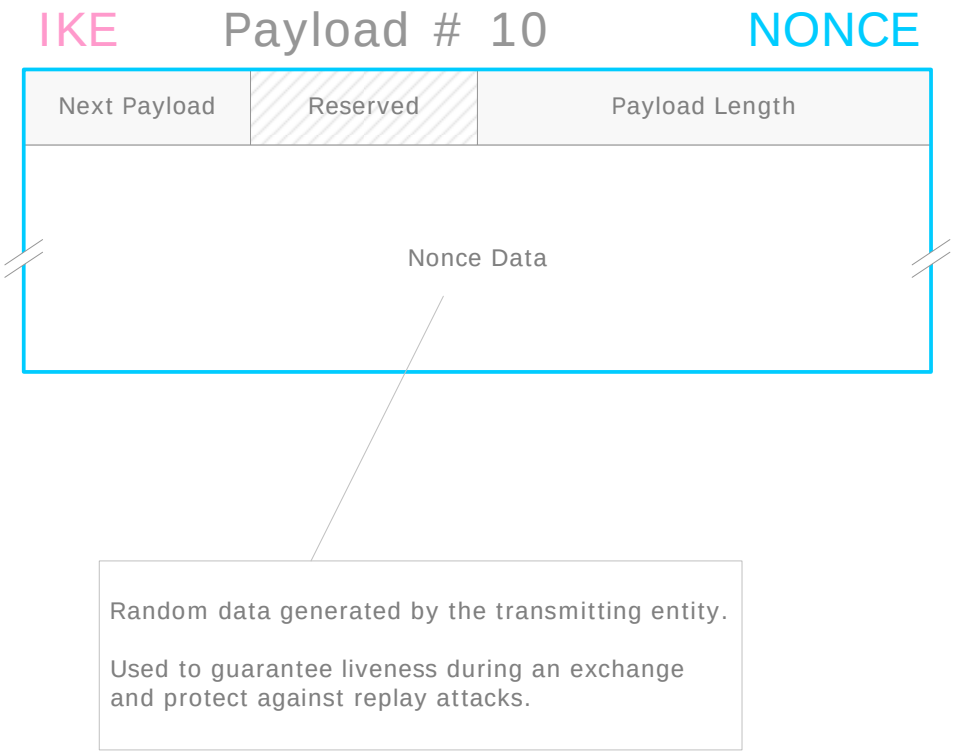
IPSec / IKE – Signature (SIG) Payload Format



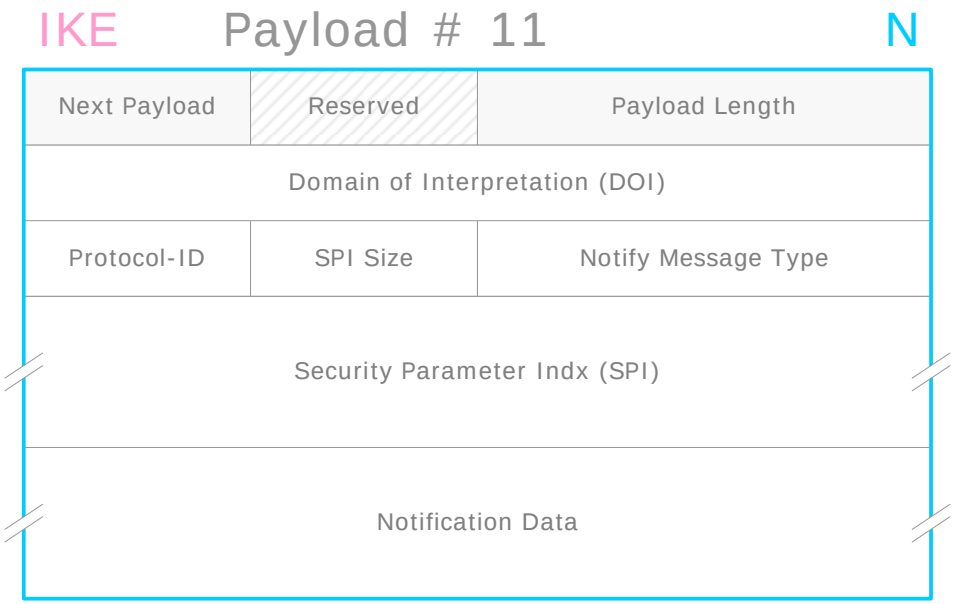
Data generated by the digital signature function (selected during the SA establishment exchange), over some part of the message and/or ISAKMP state.

Used to verify the integrity of the data in the ISAKMP message, and may be of use for non-repudiation services.

IPSec / IKE – Nonce (NONCE) Payload Format



IPSec / IKE – Notify (N) Payload Format



IPSec / IKE – Delete (D) Payload Format

IKE Payload # 12 D

Next Payload	Reserved	Payload Length
Domain of Interpretation (DOI)		
Protocol-ID	SPI Size	# of SPIs
Security Parameter Index(es) (SPI)		

IPSec / IKE – Vendor ID (VID) Payload Format