Forelesning 9

Email-sikkerhet
&
Internett-sikkerhet (IPSec)

Pretty Good Privacy

PGP by Leslie Fish

The G-men all are cryin'
And tearin' out their hair,
'Cause there's a new cryptography
That's shown up everywhere.
Nobody can break it,
However good they be.
Everybody's PC got the PGP.

There's no way to crack it,
Not if you take a year.
All the spooks & wiretappers
Are cryin' in their beer.
They can't spy on citizens
Here or oversea
When every home computer's got the PGP.

So go say what you want to,
Of love or war or hate,
Kinky sex, or dirty words,
Or overthrow the state.
Nobody can stop you.
Speech is really free
When everybody's PC got the PGP.

It guarantees who's callin'
And just who gets the call.
If you ain't got your code-phrase,
You can't get in at all.
Oh, there ain't nothin' like it
To keep your privacy.
Half the world's computers got the PGP.

Bless the man who made it,
And pray that he ain't dead.
He could've made a million
If he'd sold it to the feds,
But he was hot for freedom;
He gave it out for free.
Now every common citizen's got PGP.

Hva gjorde Phil Zimmermann?

- Valgte ut ”de beste” krypto-algoritmene som byggeklosser
- Integrerte disse i en lettfattelig applikasjon
- Lot programpakken, dokumentasjon og kildekode være fritt tilgjengelig på Internett
- Gjorde en avtale om en 100% kompatibel rimelig, kommersiell versjon

Et lite skår i gleden

- Viacrypt gikk inn i Network Associates (NAI)
- NAI bestemte seg i mars 2002 for å droppe PGP som produkt
- Det er nå dannet et nytt selskap (PGP Corporation – www.pgp.com) som har ansvar for salg og markedsføring av PGP
- Får man fremdeles PGP gratis?

Hvorfor ble PGP så populær?

- Fritt tilgjengelig på en rekke plattformer
- Basert på algoritmer som har tålt nitidig analyse av forskere og offentligheten
- Stort spennvidde for bruksområder, fra store konsern til privatpersoner
- Ikke utviklet av, og ikke kontrollert av noen statlig organisasjon eller ”standard-institusjon”

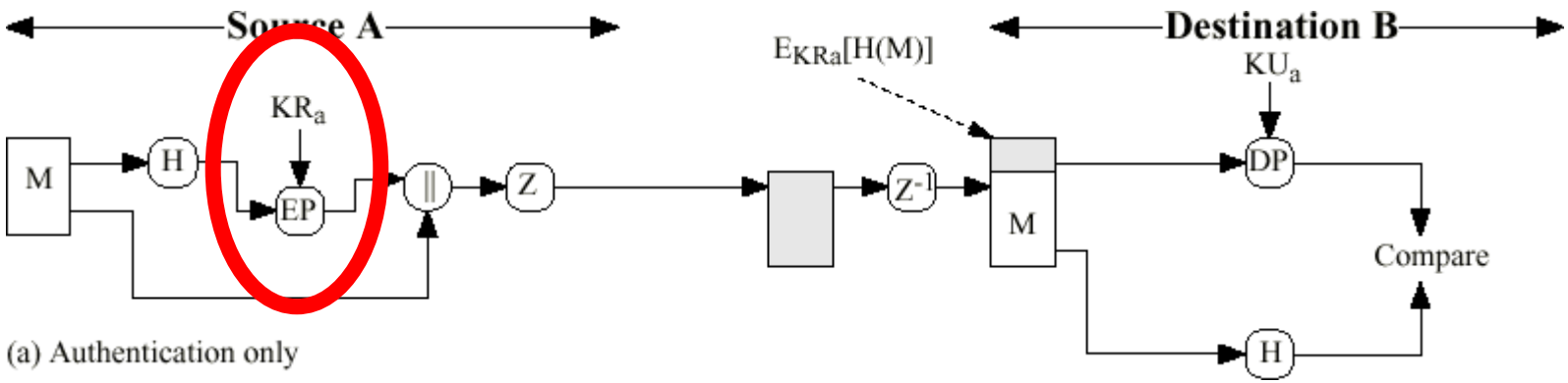
PGP notasjon

- K_S – symmetrisk sesjonsnøkkel
- KR_a – privat nøkkel til bruker A
- KU_a – offentlig nøkkel til bruker A
- EP – offentlig-nøkkel kryptering
- DP – offentlig-nøkkel dekryptering
- EC – konvensjonell kryptering
- DC – konvensjonell dekryptering
- H – hash-funksjon
- || - konkatenering
- Z – komprimering
- R64 – konvertering til Radix64-format

PGP Tjenester

Funksjon	Algoritme
Digital signatur	DSS/SHA *eller* RSA/SHA
Meldingskryptering	CAST *eller* IDEA *eller* 3DES *med* RSA *eller* ElGamal
Komprimering	ZIP (Lempel-Ziv)
Epost-kompatibilitet	Radix-64
Segmentering	-

PGP autentisering

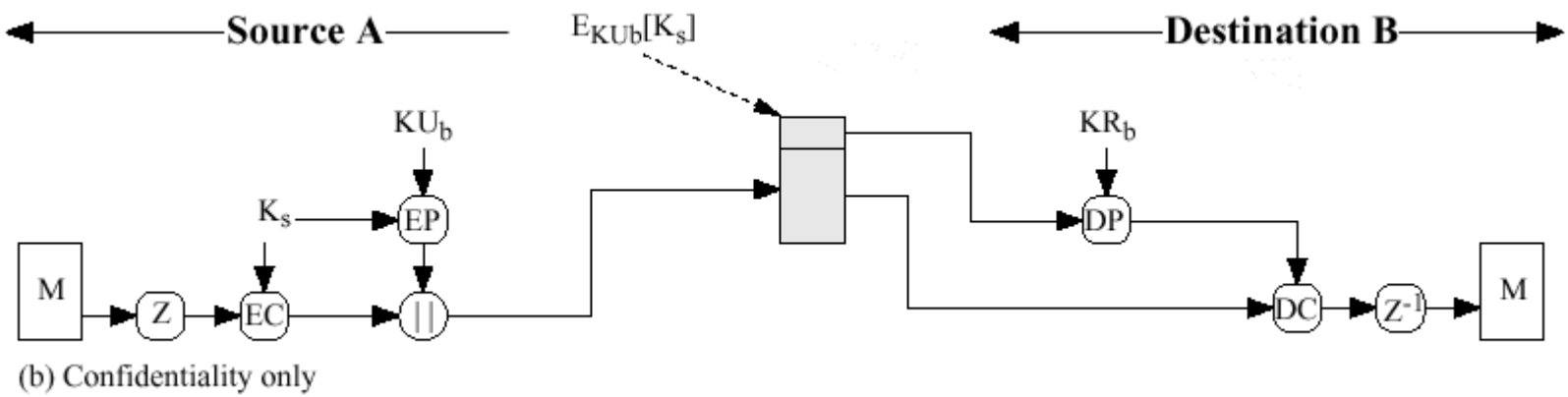


Signering

Separate signaturer

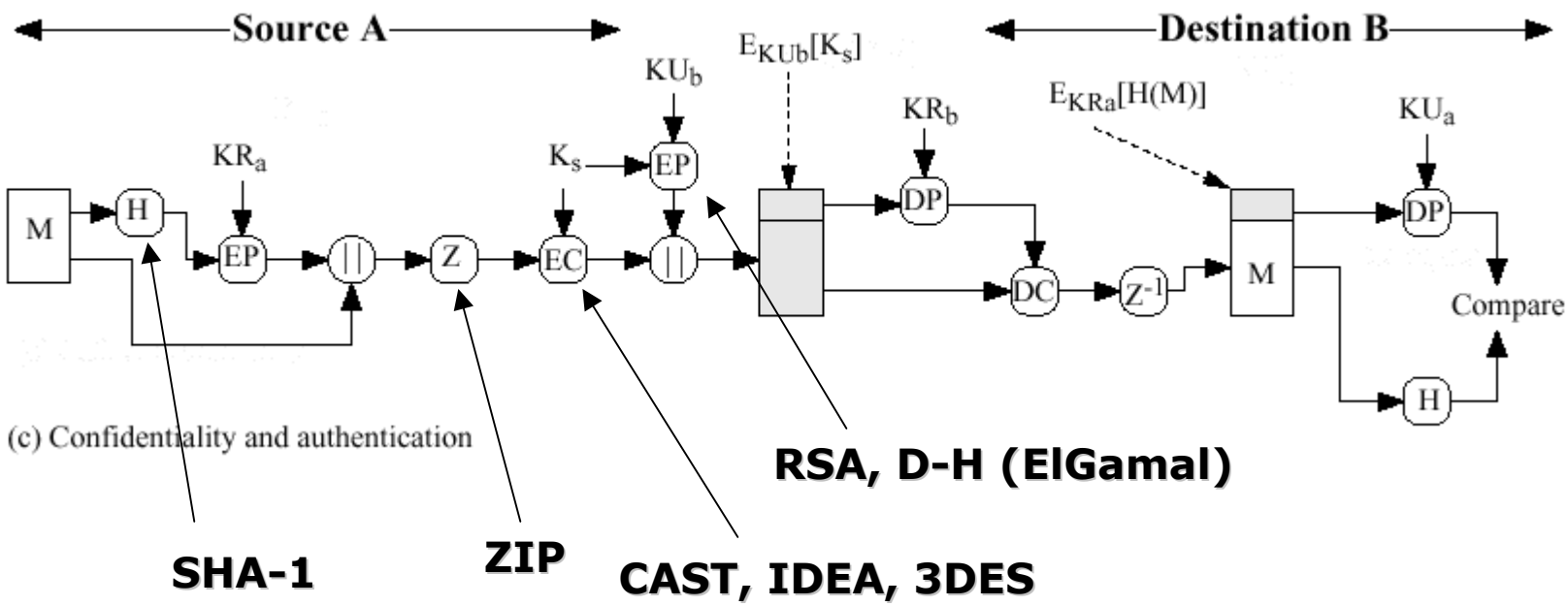
- PGP kan også signere filer uavhengig av mail-funksjonen
- Kan signere tekst, dokumenter, programmer...
- Signaturene kan være separate filer som kan sendes med; muliggjør at flere kan signere samme dokument uavhengig av hverandre (ingen nøsting)

PGP konfidensialitet

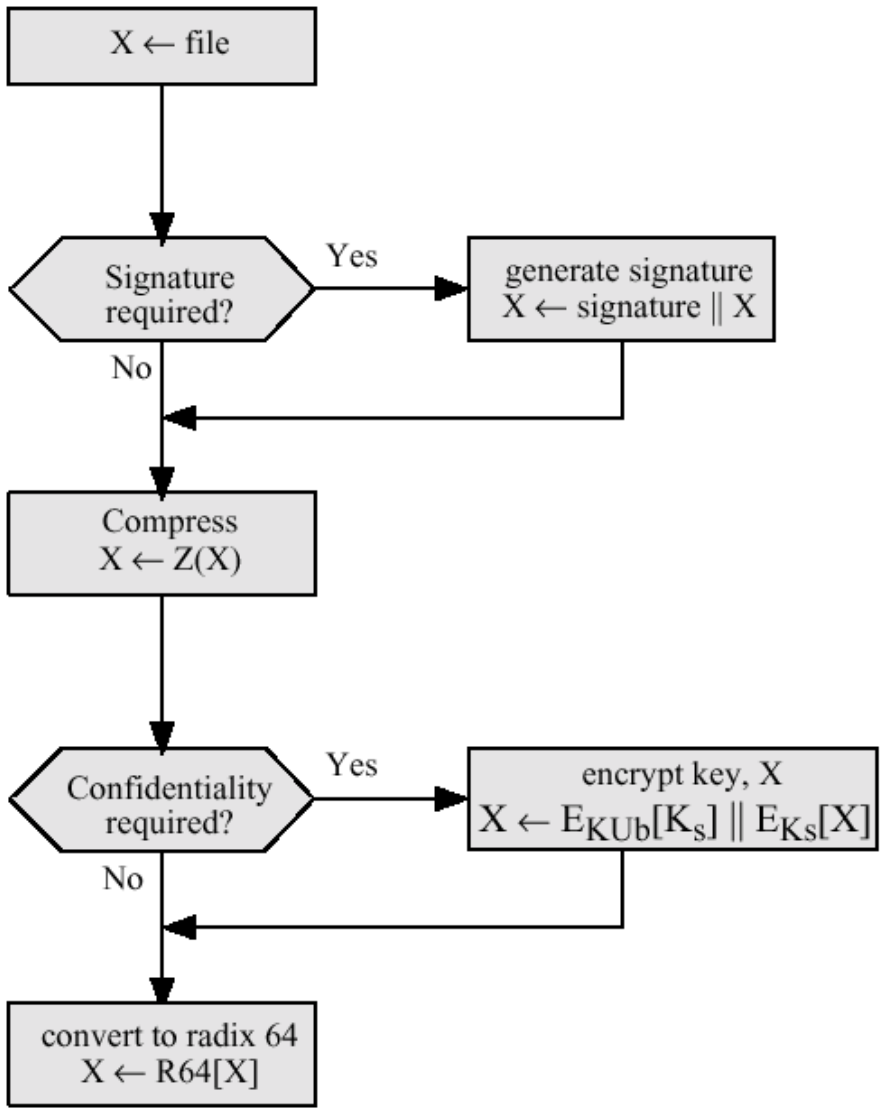


(b) Confidentiality only

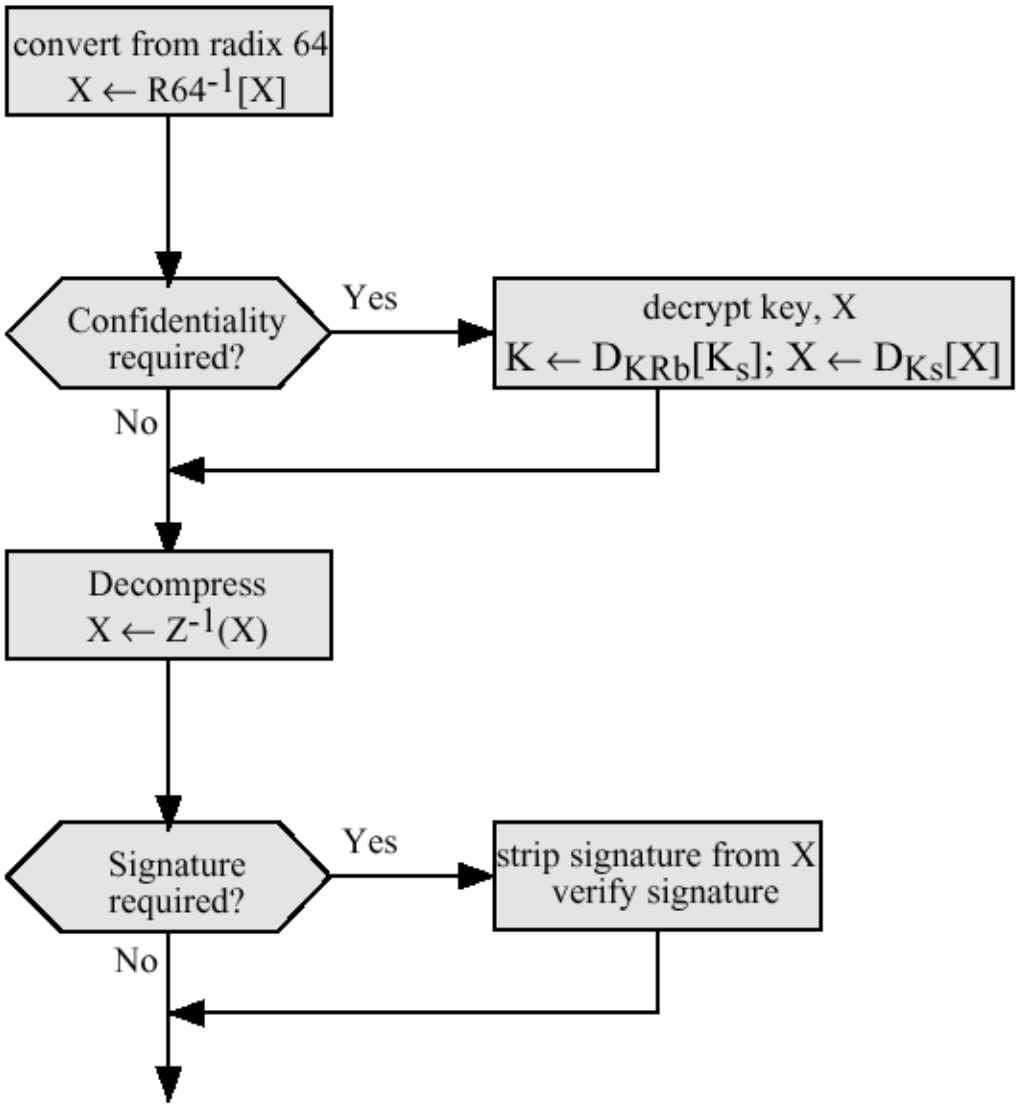
PGP autentisering & konfidensialitet



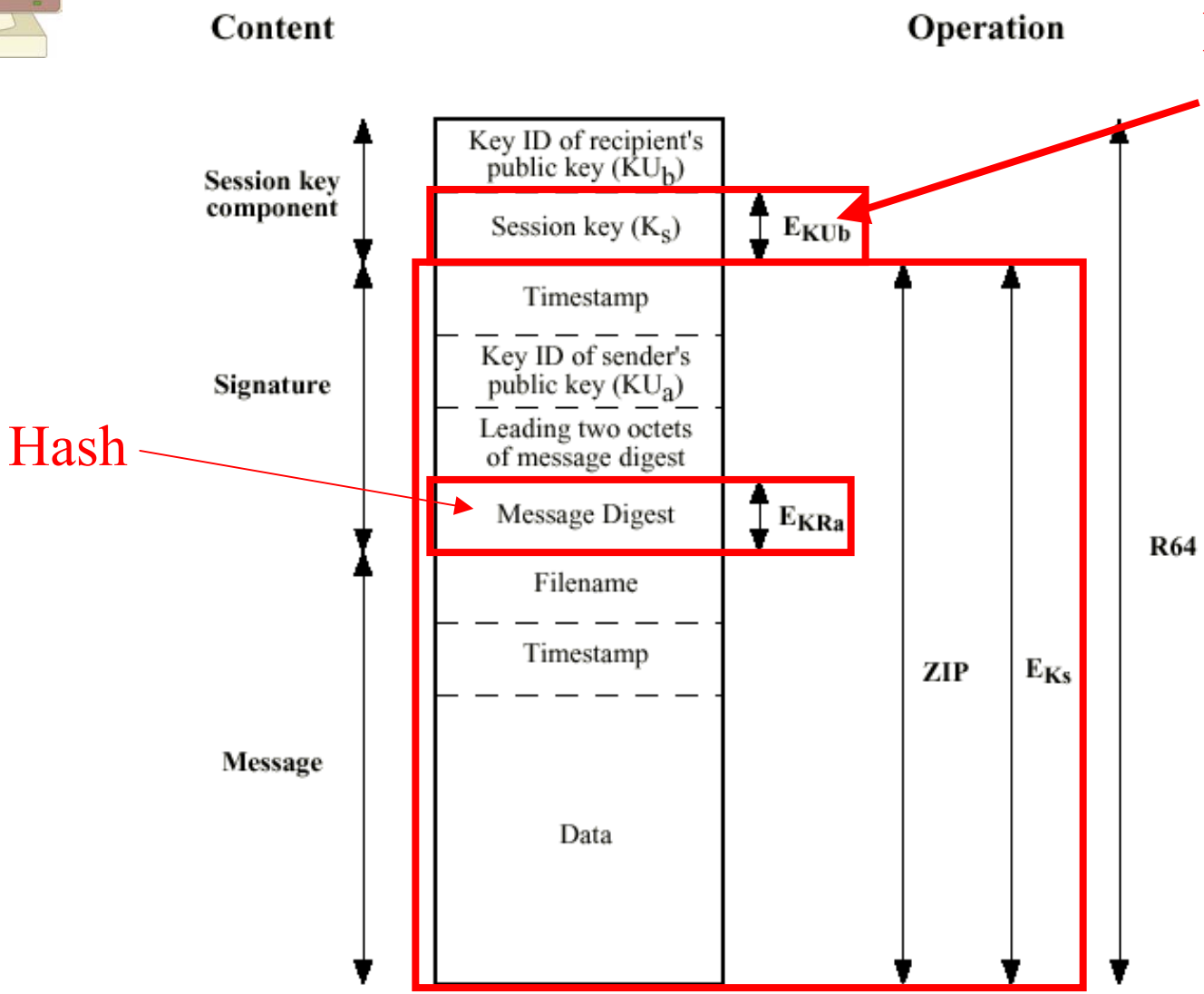
Sending av meldinger



Mottak av meldinger



PGP meldingsformat



Nøkkelringer

- Privat nøkkelring
- Offentlig nøkkelring

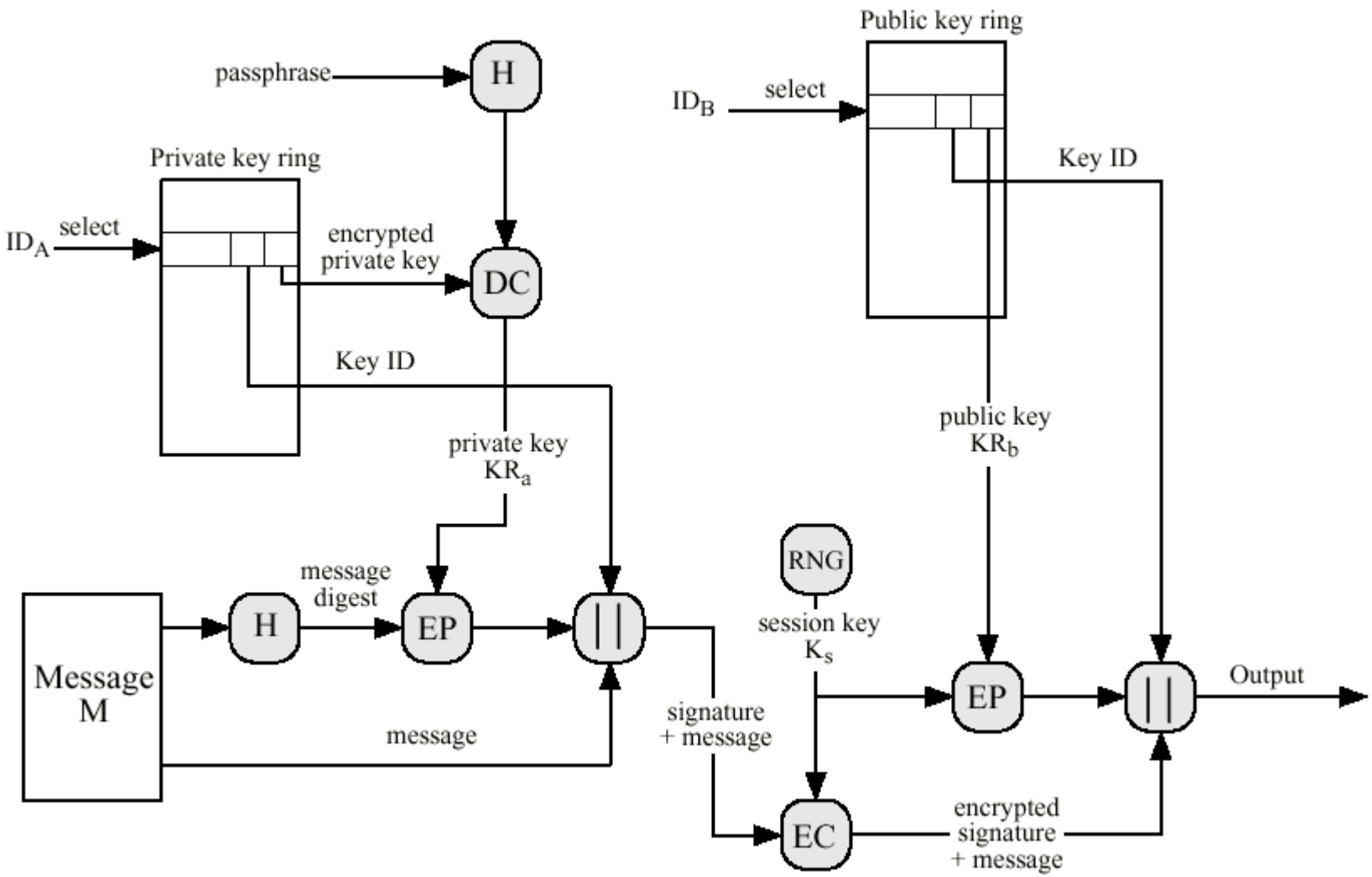
Privat nøkkelring

- Ditt nøkkelpar (privat,offentlig)
  - Timestamp
  - Key ID (siste 8 byte av offentlig nøkkel)
  - Offentlig nøkkel
  - Kryptert privat nøkkel
  - Bruker-ID (email-adresse)
- Evt. andre nøkkelpar for andre identiteter (f.eks. hjemme-adresse)
- Evt. gamle nøkkelpar

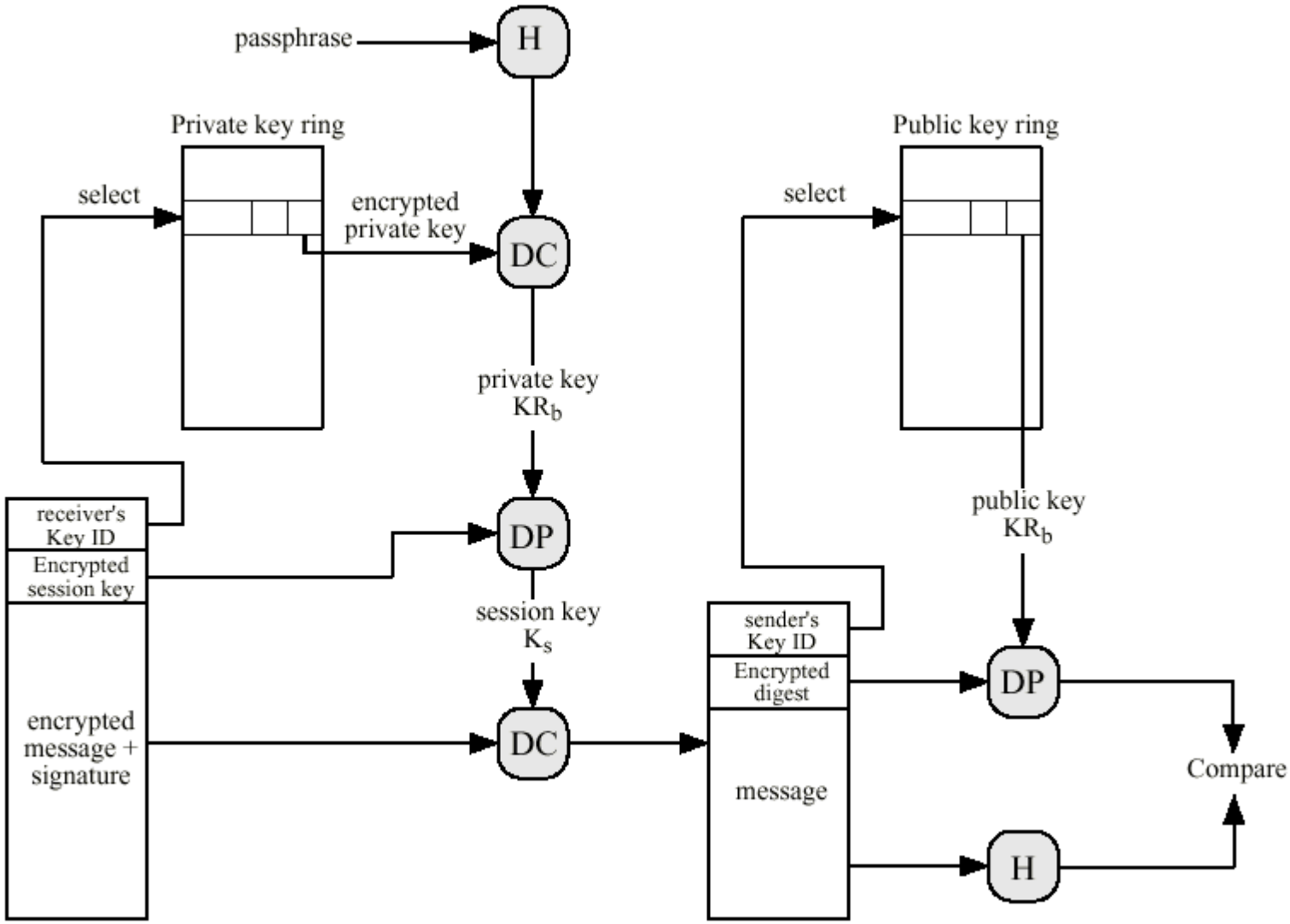
Offentlig nøkkelring

- Din egen samling av andres offentlige nøkler
- Hvert innslag består av
  - Timestamp
  - Key ID
  - Offentlig nøkkel
  - Bruker-ID
  - ”Trust”
  - Legitimitet
  - Signatur(er)

PGP meldingsgenerering



PGP meldingsdekryptering



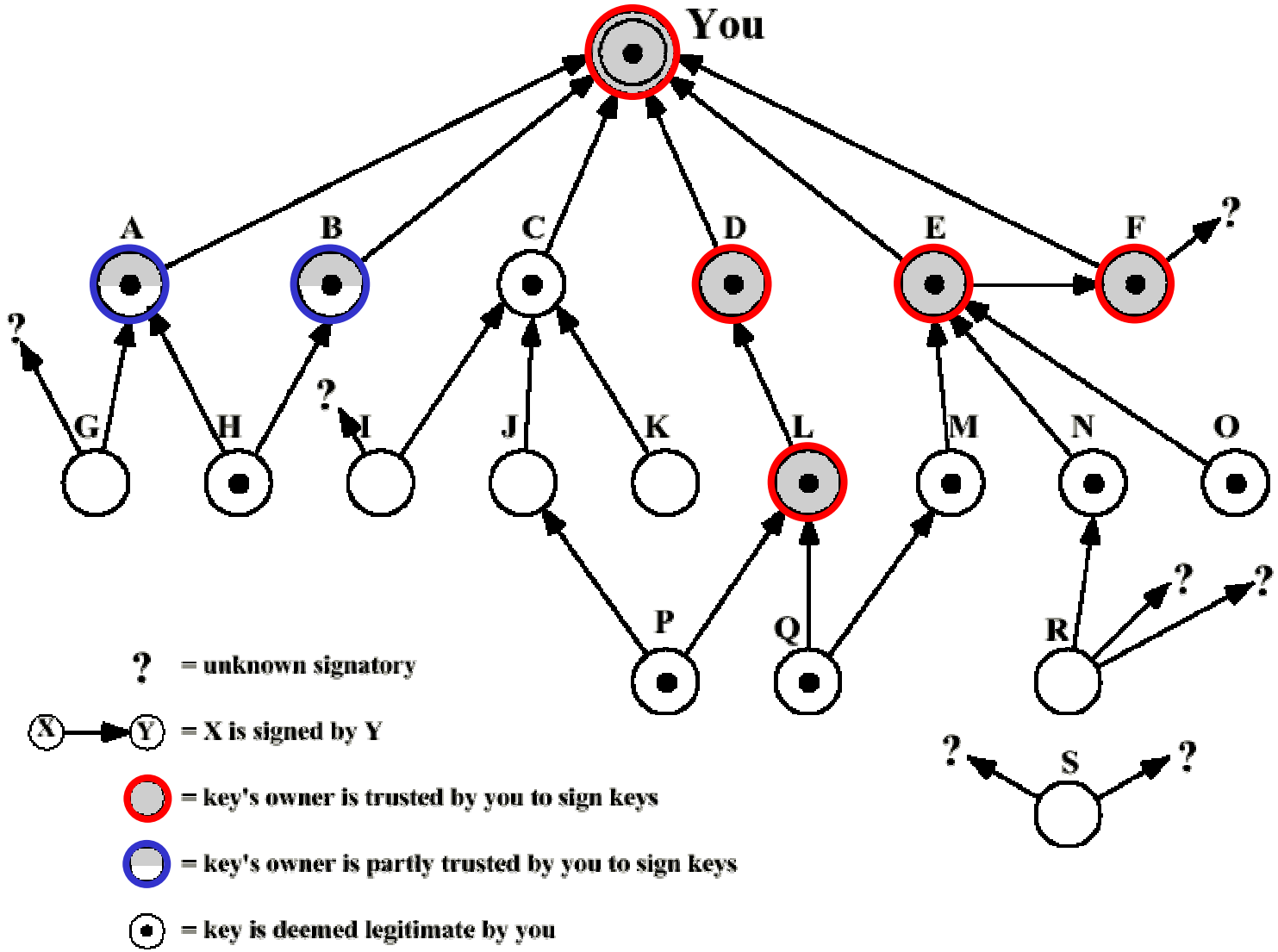
Distribusjon av offentlige nøkler

- Personlig (fysisk) utveksling
- Verifiser via telefon
  - Send nøkkel via email, verifiser ved å lese opp SHA-1 hash (fingerprint) på telefonen
- Få nøkkelen via en person du stoler på
- Få nøkkelen via en tiltrodd sertifiseringsmyndighet (sertifikat)

Nøkler fra noen du stoler på

- PGP har et eget ”trust”-system som gjør det mulig å automatisk godta nøkler som er signert av en eller flere personer du stoler på
- Avhengig av hvor mye (lite) du stoler på en person (eller nøkkel), kan du kreve at flere skal ha signert en ny nøkkel for at du skal godta den

PGP Trust


You
A
B
C
D
E
F
?
G
H
?
I
J
K
L
M
N
O
P
Q
R
?
?
S
?
? = unknown signatory
X
Y
= X is signed by Y
= key's owner is trusted by you to sign keys
= key's owner is partly trusted by you to sign keys
= key is deemed legitimate by you

Key Revocation

- Hvis en privat nøkkel fryktes kompromittert, utsteder man et ”ugyldig-gjørende” sertifikat for den korresponderende offentlige nøkkelen
- Sertifikatet signeres med den private nøkkelen
- Distribusjon av sertifikatet er opp til avsenderen!

S/MIME

S/MIME

- Introduserer mulighet for å sende krypterte/autentiserte meldinger i det eksisterende MIME-rammeverket
- Baserer seg i større grad på bruk av CA og X.509-sertifikater
- Finnes IETF-draft for oversetting mellom sikker X.400 (MMHS) og S/MIME

RFC 821, 822 og MIME

- RFC 821
  - SMTP
- RFC 822
  - Standard for ARPA Internet Text Messages
- RFC 2045-2049
  - MIME

- MIME Header
  - MIME-Version
  - Content-Type
  - Content-Transfer-Encoding
  - Content-ID
  - Content-Description

MIME Content Types

Type	Subtype
Text	Plain
	Enriched
Multipart	Mixed
	Parallel
	Alternative
	Digest
Message	rfc822
	Partial
	External-body

Type	Subtype
Image	jpeg
	gif
Video	mpeg
Audio	Basic
Application	PostScript
	octet-stream

MIME Transfer Encoding

- **7bit** – ASCII
- **8bit** - ISO 8859-1 (f.eks.)
- **binary** – non-ASCII, lange linjer
- **quoted-printable** – delen av data som består av tekst kan leses direkte
- **base64** – radix64
- **x-token** – navngitt ”ikke-standard”

Kryptoalgoritmer i S/MIME

Funksjon	**Krav**
Lag hash for signatur	**Må** støtte SHA-1 og MD5, **Bør** bruke SHA-1
Krypter hash for signatur	**Må** støtte DSS, Sender **bør** støtte RSA, Mottaker **bør** støtte RSA 512-1024
Kryptér sesjonsnøkkel	**Må** støtte Diffie-Hellman, avsender **bør** støtte RSA 512-1024, mottaker **bør** støtte RSA
Kryptér melding	Avsender **bør** støtte RC2/40 og 3DES, mottaker **må** støtte RC2/40, **bør** støtte 3DES

S/MIME Content Types

Type	Subtype	Parameter	Beskrivelse
Multipart	Signed		Signert i to deler
Application	pkcs7-mime	SignedData	Signert
		envelopedData	Kryptert
		degenerate signedData	Kun serifikat
	pkcs7-signature		Signaturdel av multipart
	pkcs10-mime		Registrer sertifikat anmodnng

Sertifikatprosessering

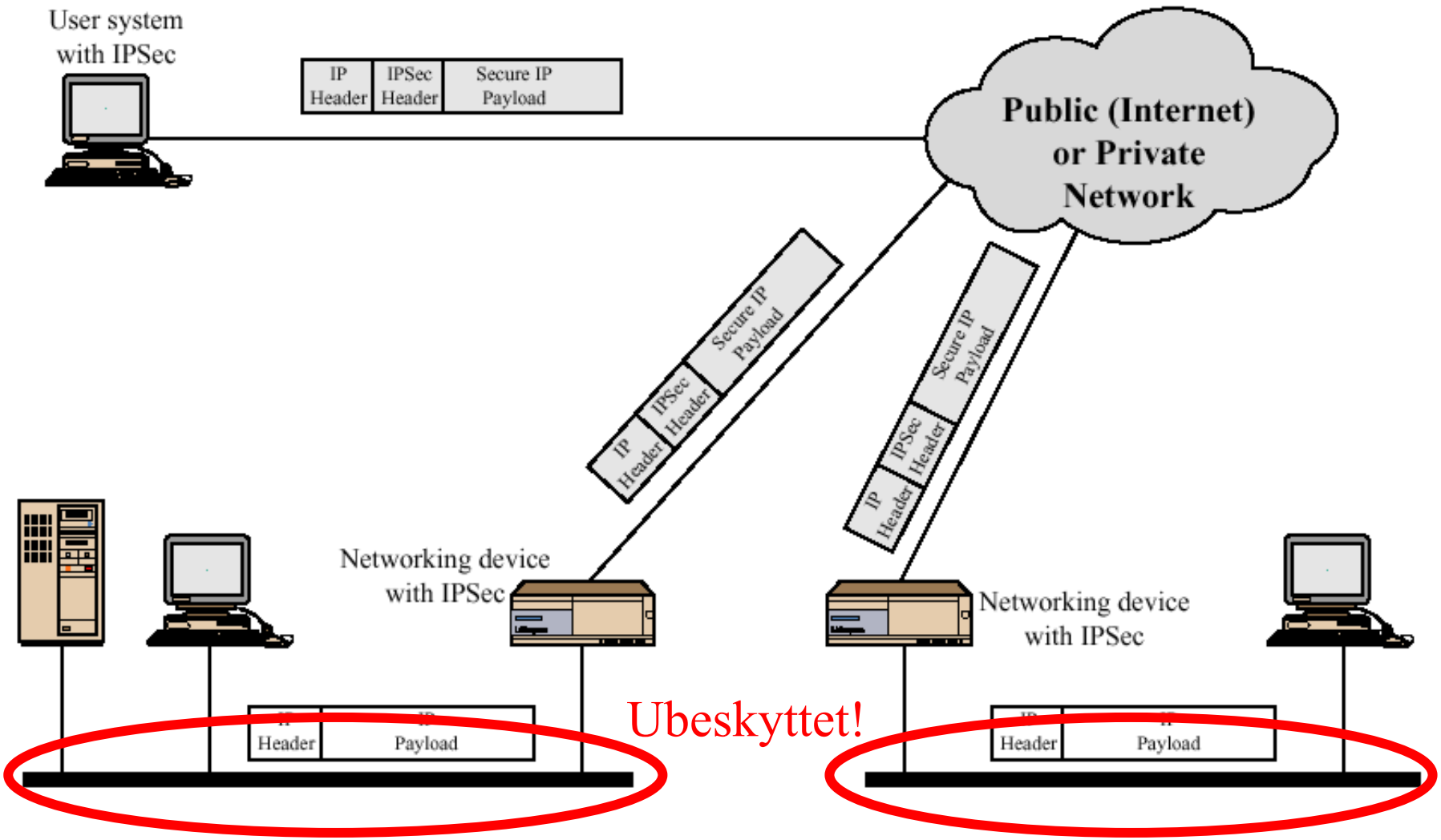
- S/MIME administratorer/brukere er selv ansvarlige for å vedlikeholde lister av gyldige sertifikater
- Alle sertifikater er utstedt av en CA

S/MIME Utvidede tjenester

- Signerte kvitteringer
  - Bekrefter mottak
- Graderingsinformasjon
  - Begrenset, Konfidensielt...
- Sikre maillister
  - Benytter en agent som håndterer alt det kjedelige arbeidet med kryptering per mottaker

IPsec

IP-sikkerhet scenario

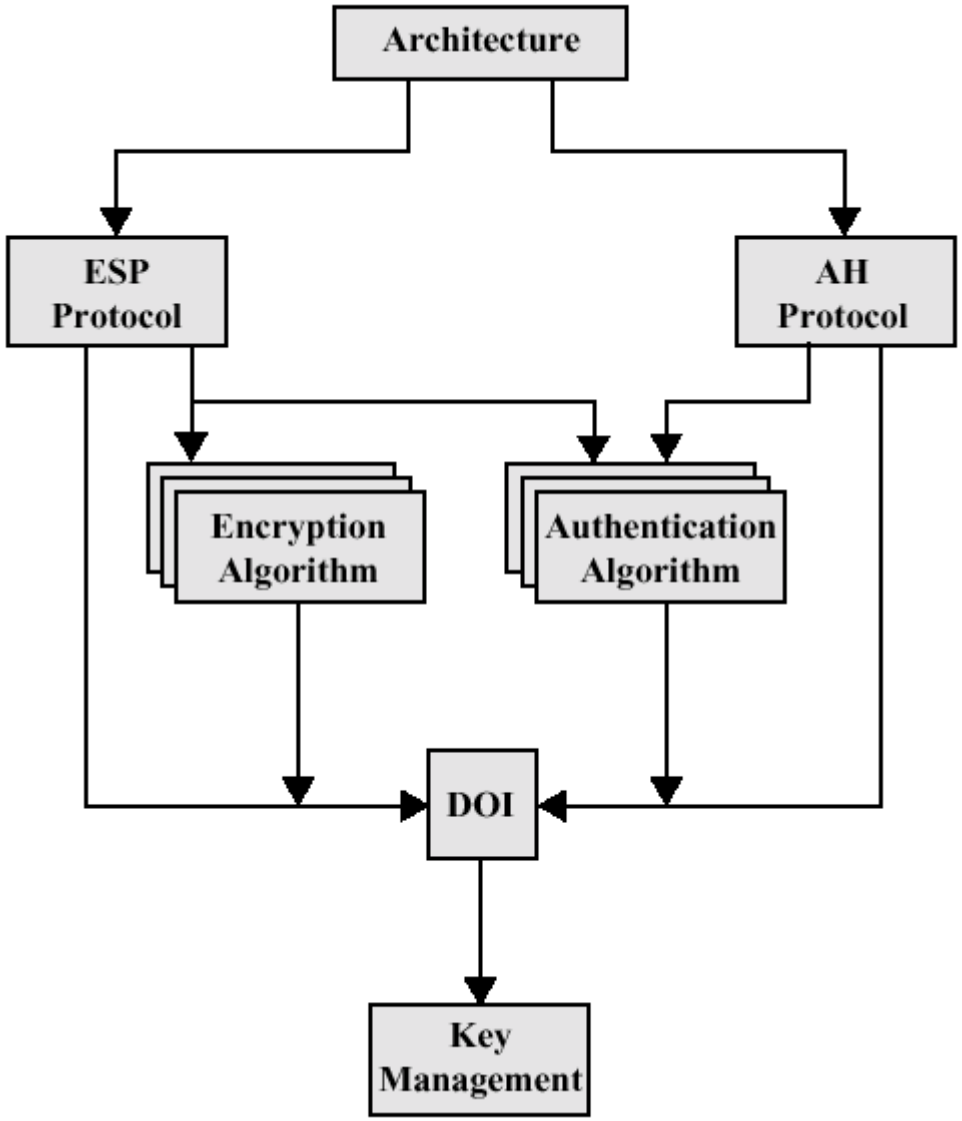


IPSec dokumenthierarki

ESP: Encapsulation Security Payload

AH: Authentication header

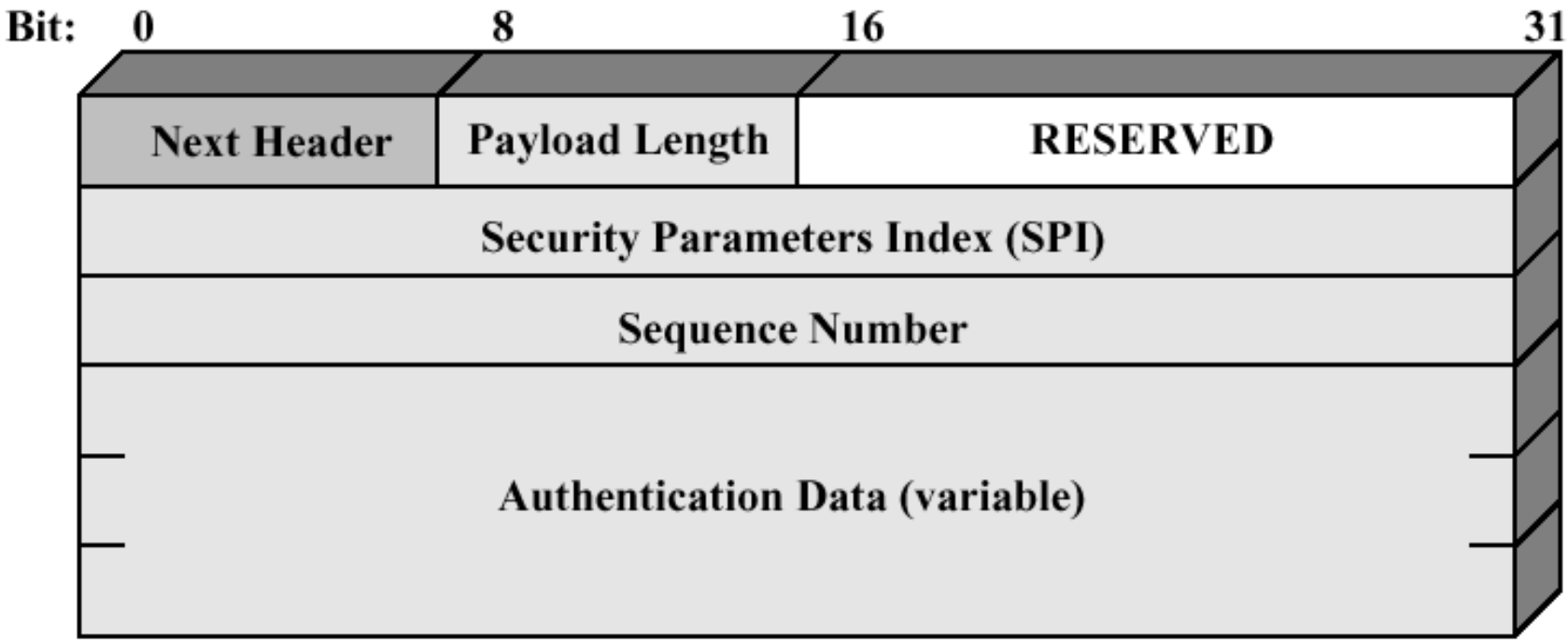
DOI: Domain of Interpretation



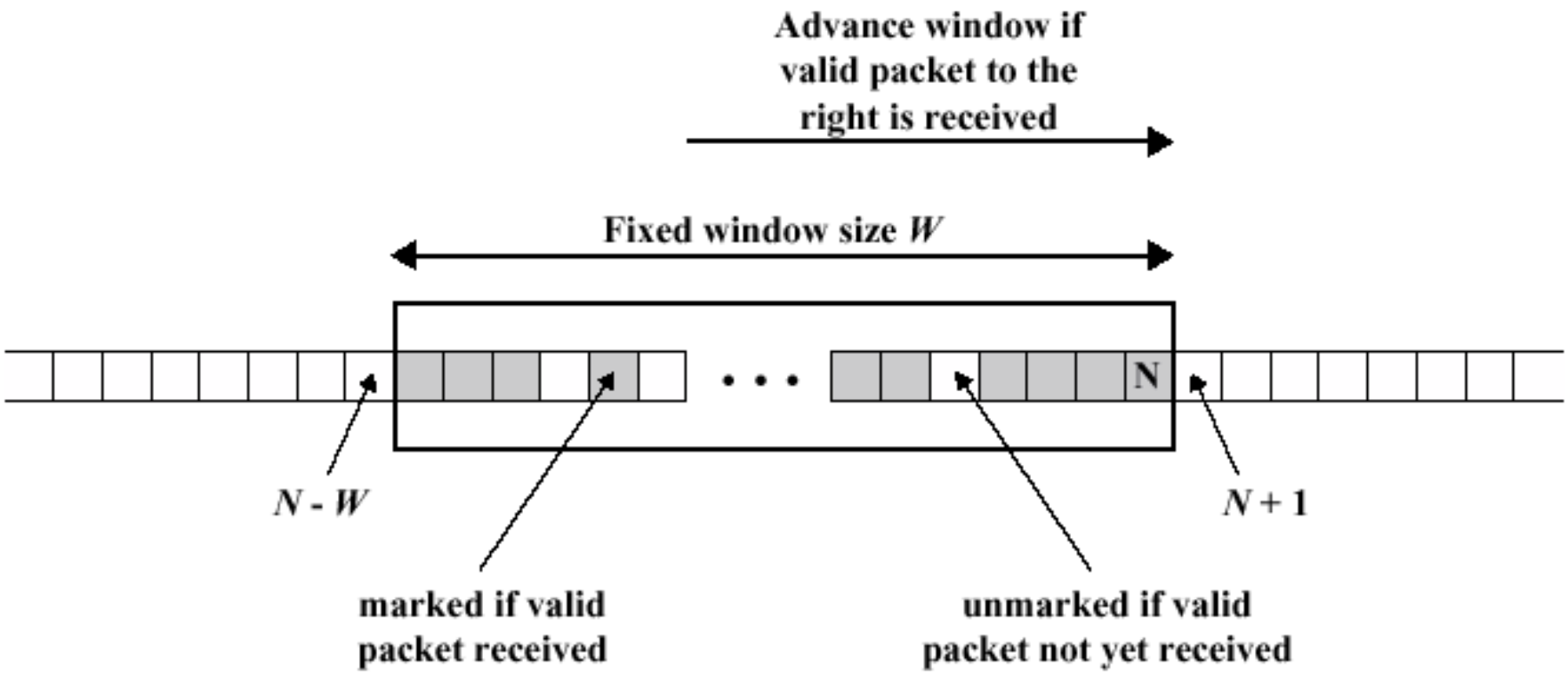
Sammenheng, SA og IP-trafikk

- Security Policy Database (SPD)
  - Destination IP
  - Source IP
  - UserID
  - Data Sensitivity Level
  - Transport Layer Protocol
  - IPSEC Protocol (AH/ESP)
  - Source/destination port
  - Type of Service (TOS)
  - (Litt annerledes for IPv6)

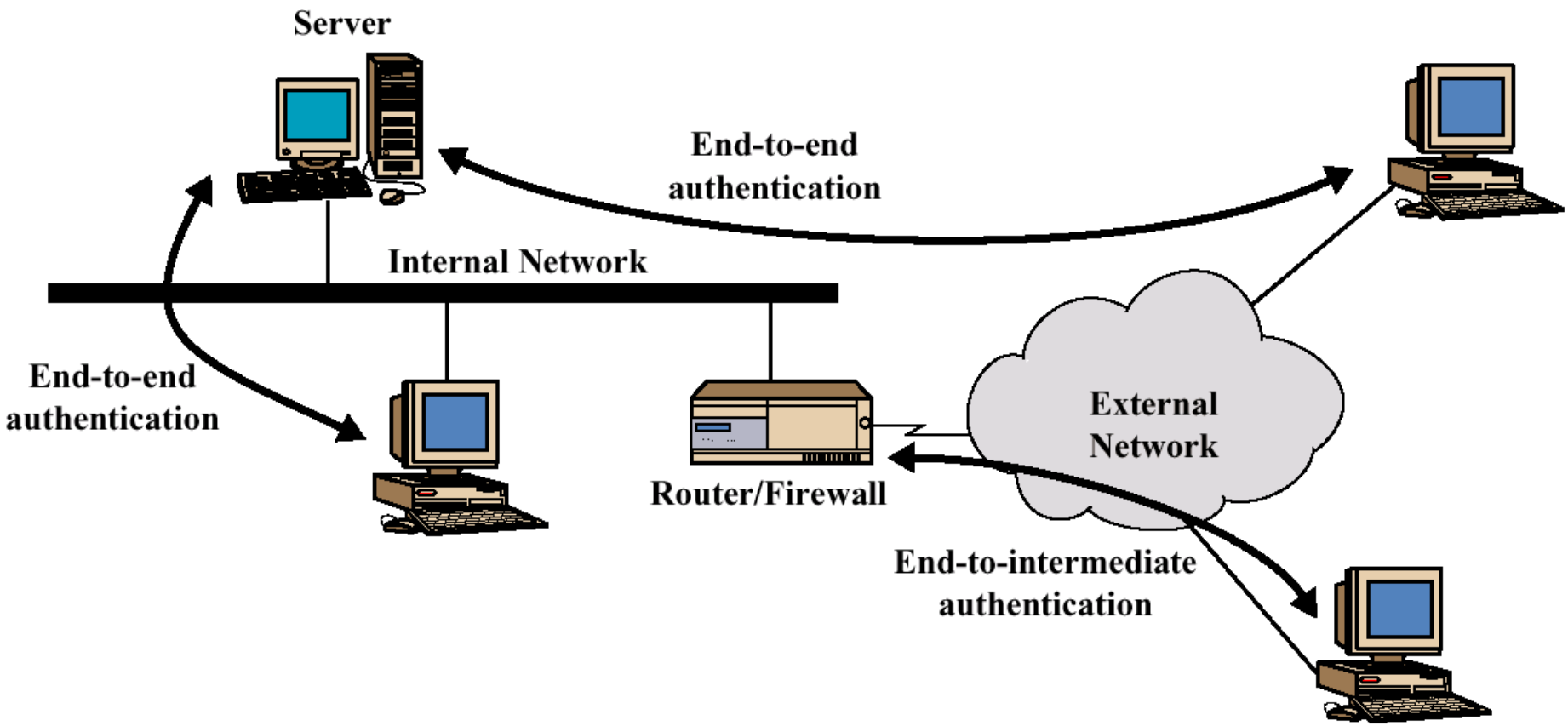
IPSec autentiseringsheader



Anti-replay mekanisme

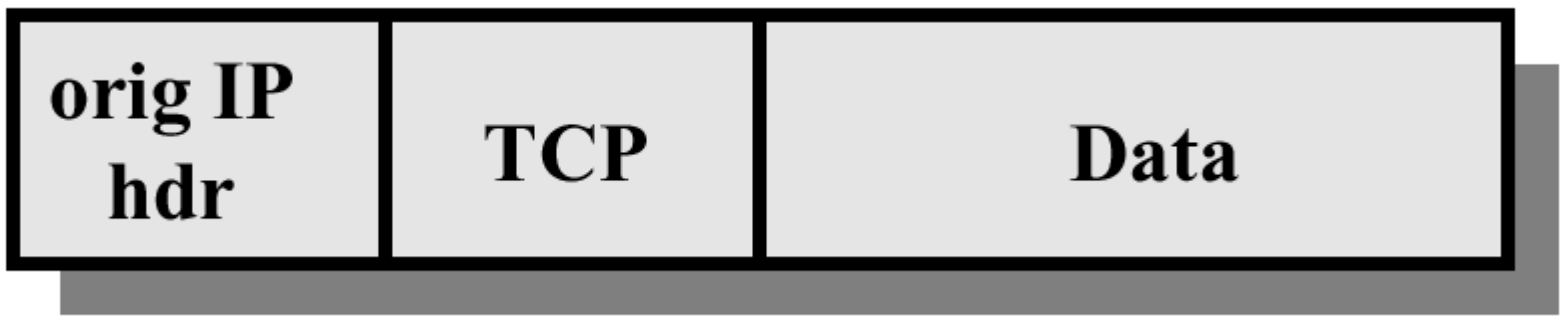


Ende-til-ende eller via andre

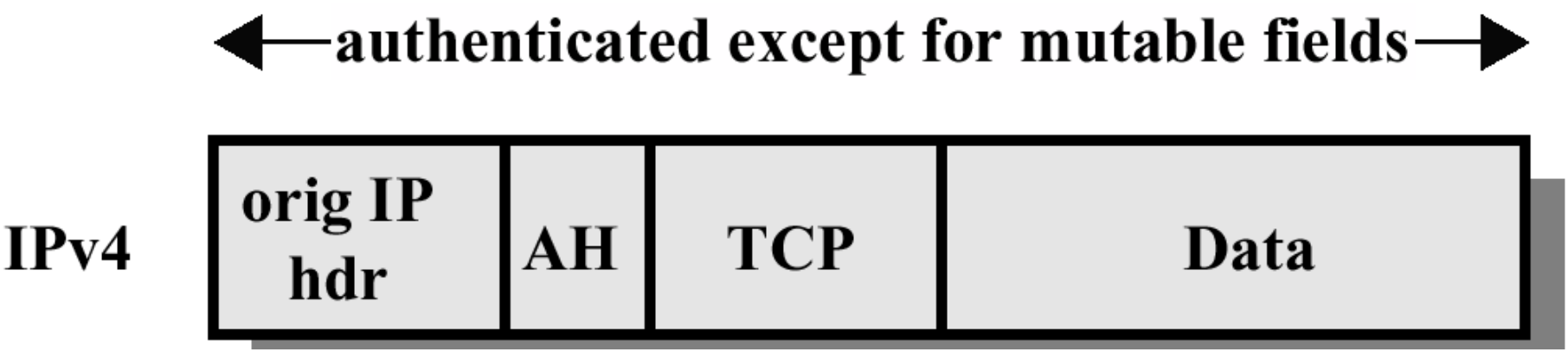


Pakkeformat uten Authentication Header

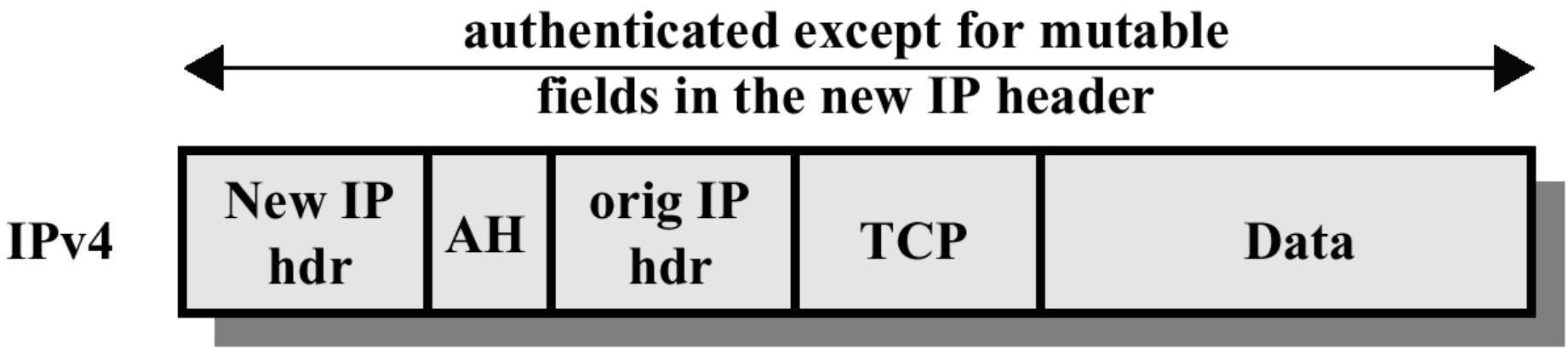
IPv4



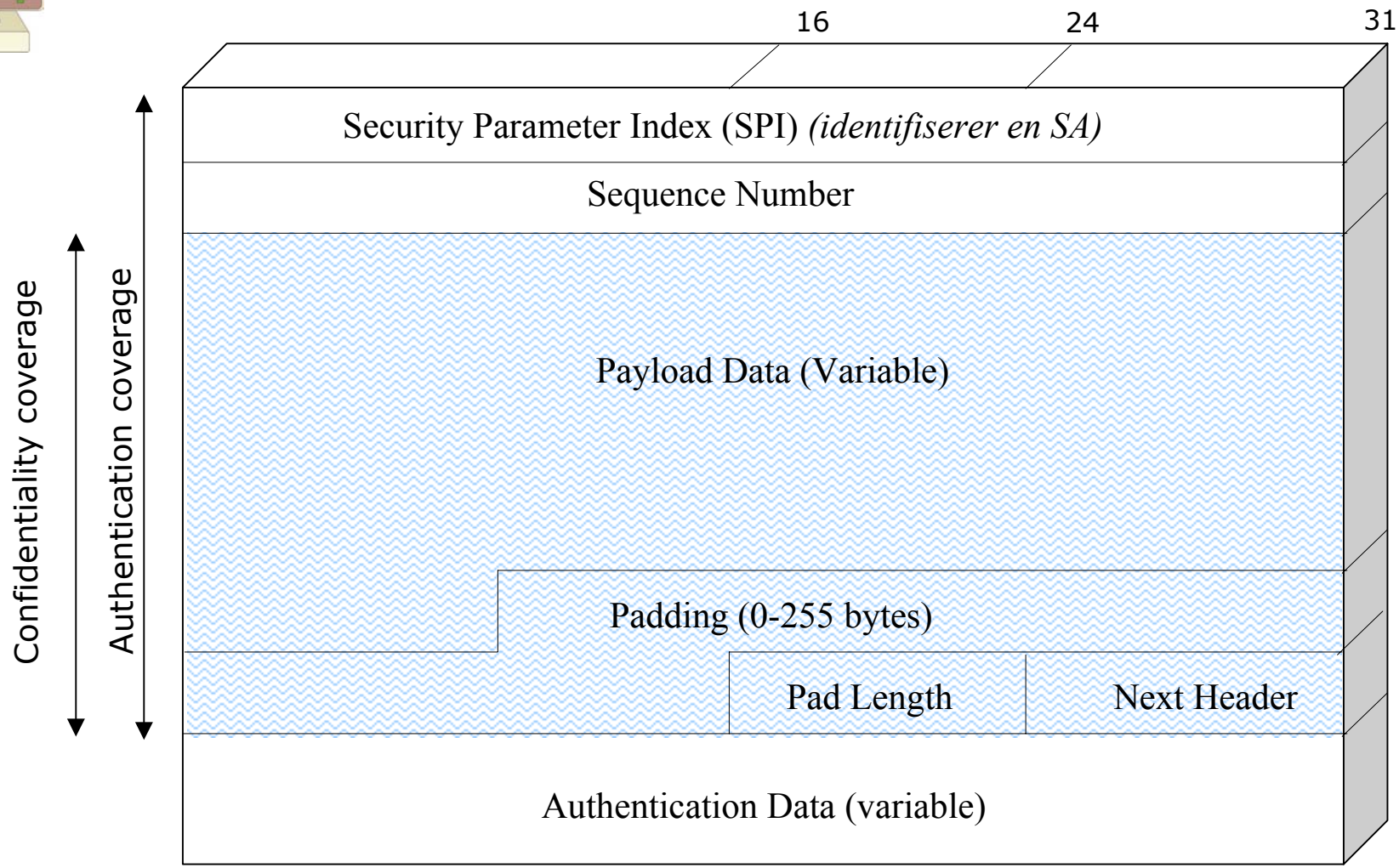
Transport Mode AH



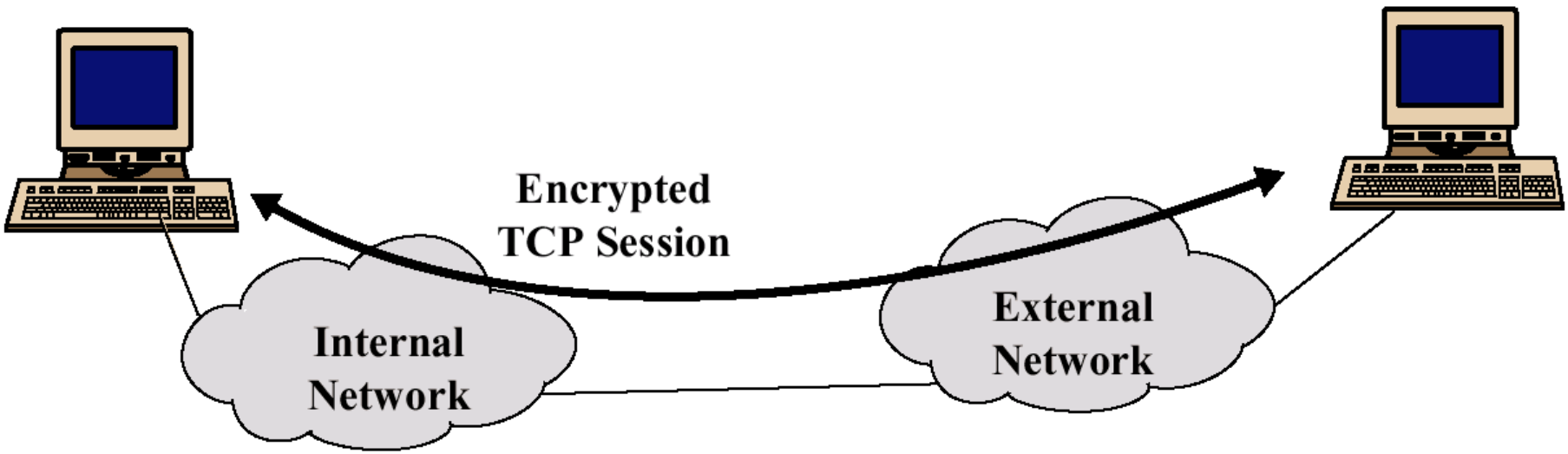
Tunnel Mode AH



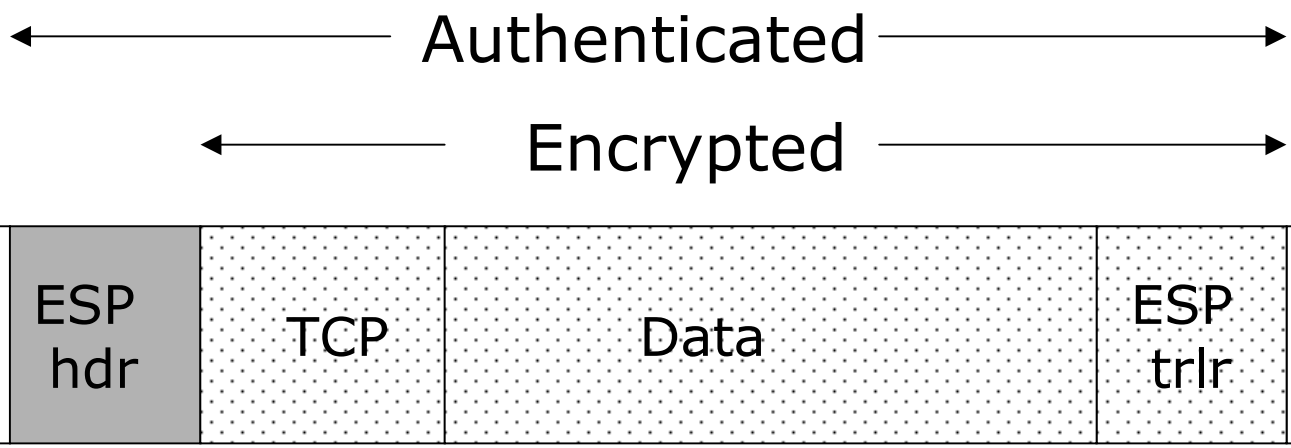
ESP pakkeformat



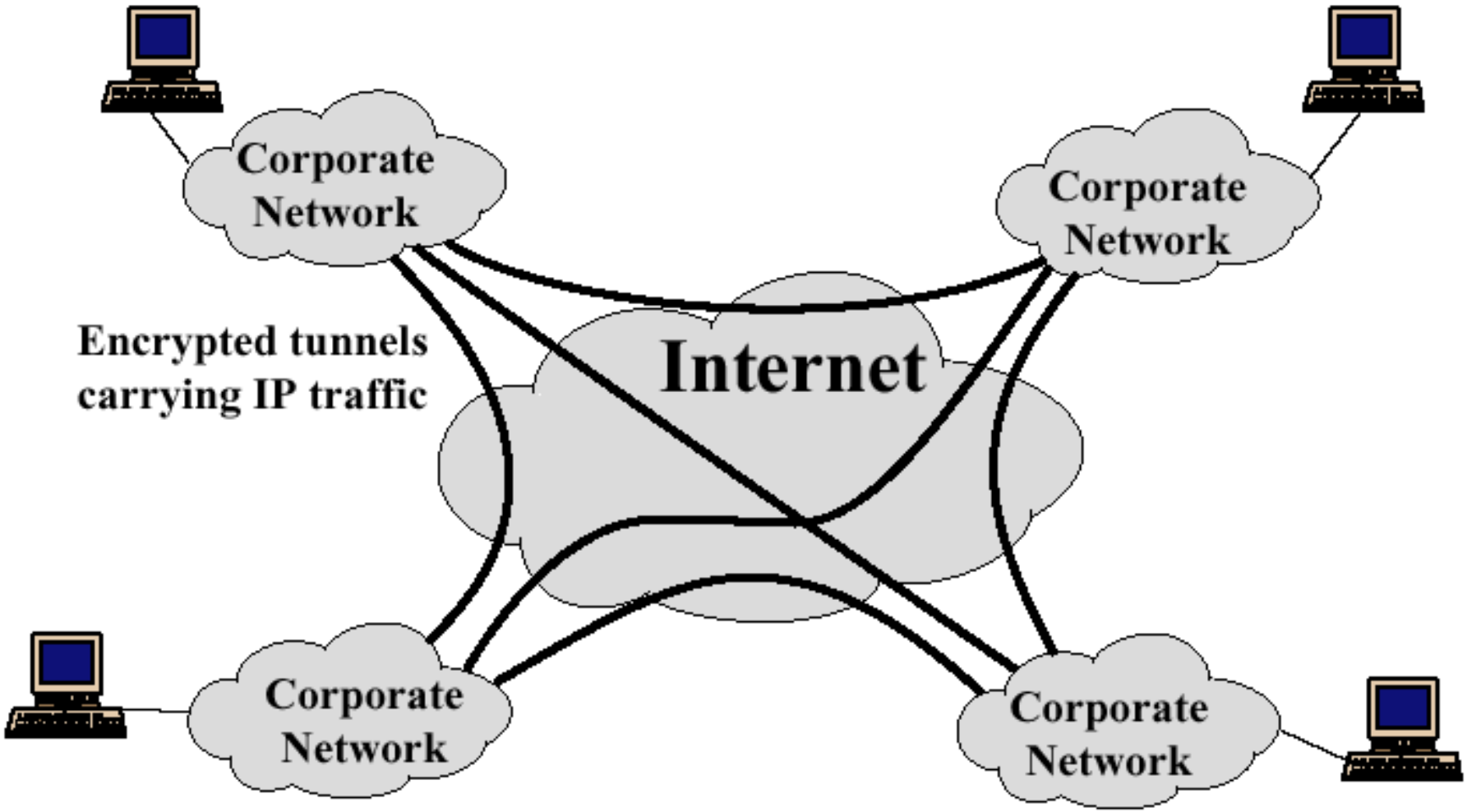
Transport mode ESP



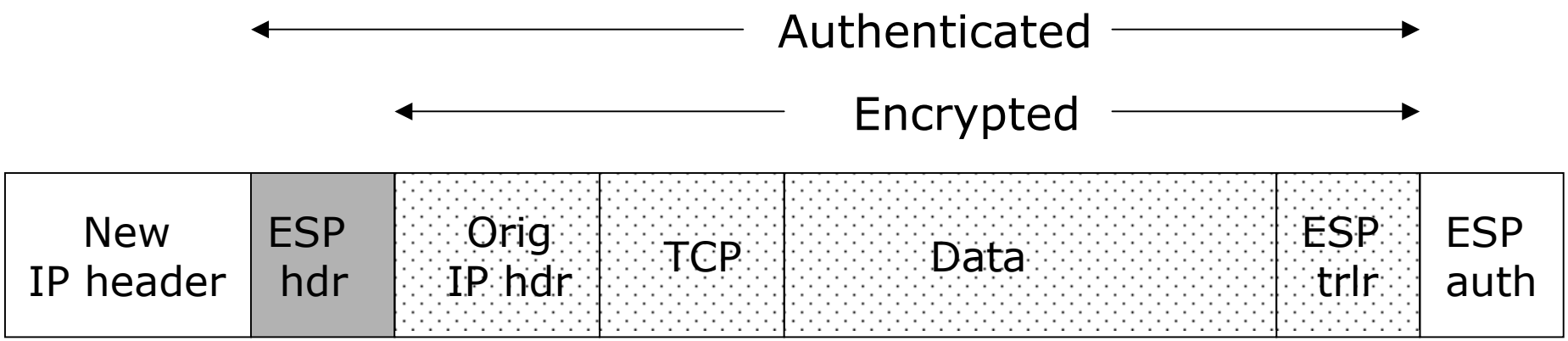
Transport Mode ESP pakkeformat



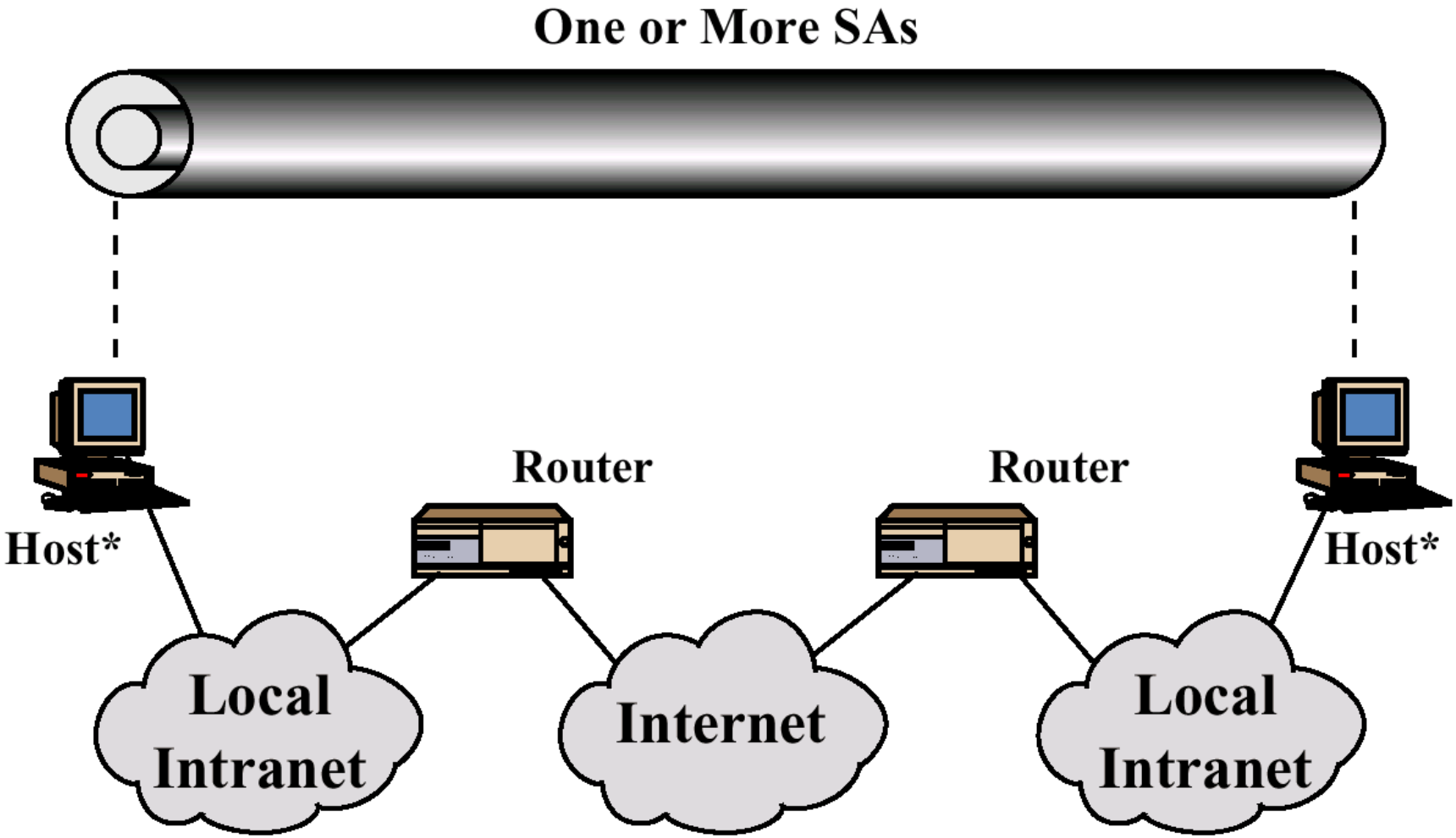
Et VPN via Tunnel Mode ESP



Tunnel Mode ESP pakkeformat

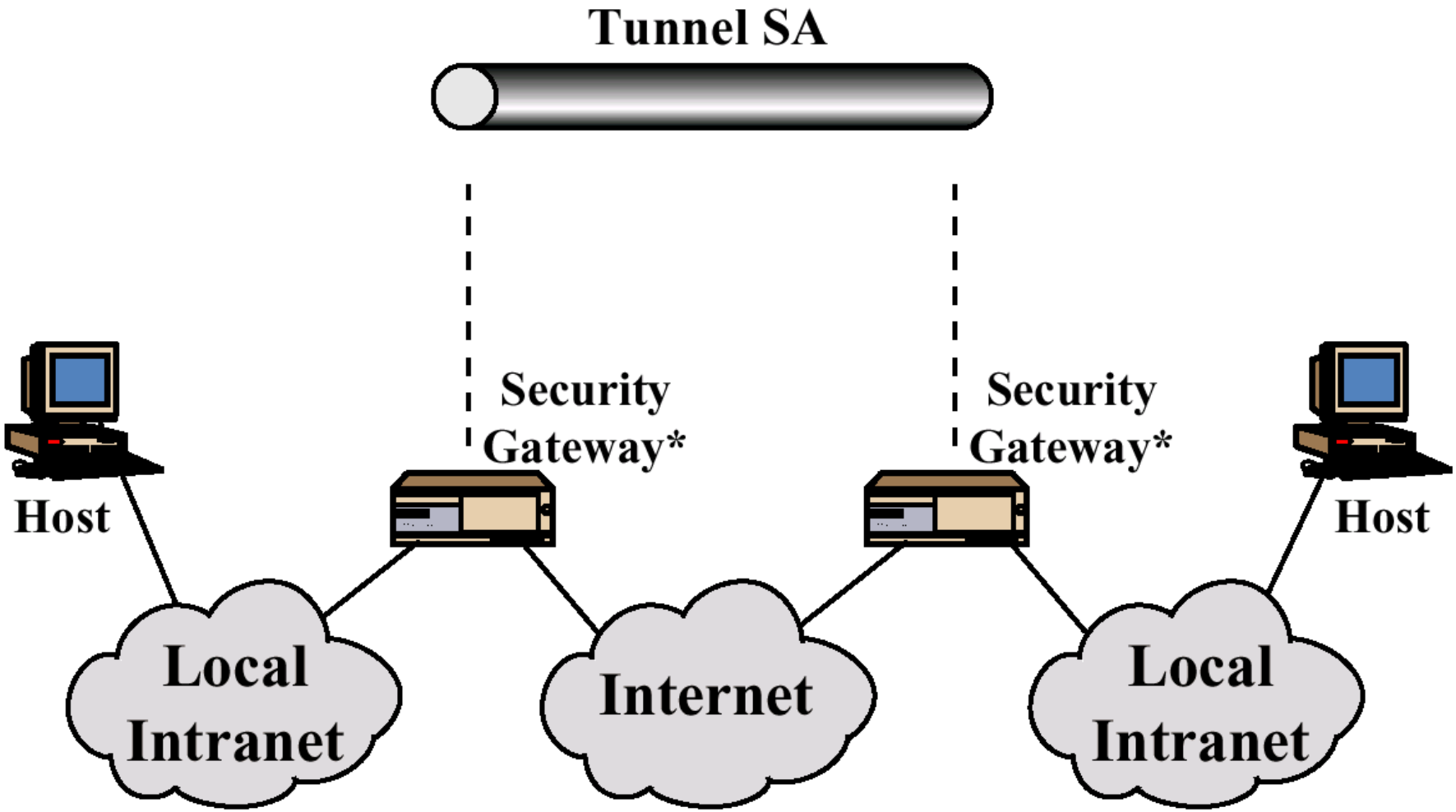


Security Assocations - Case 1



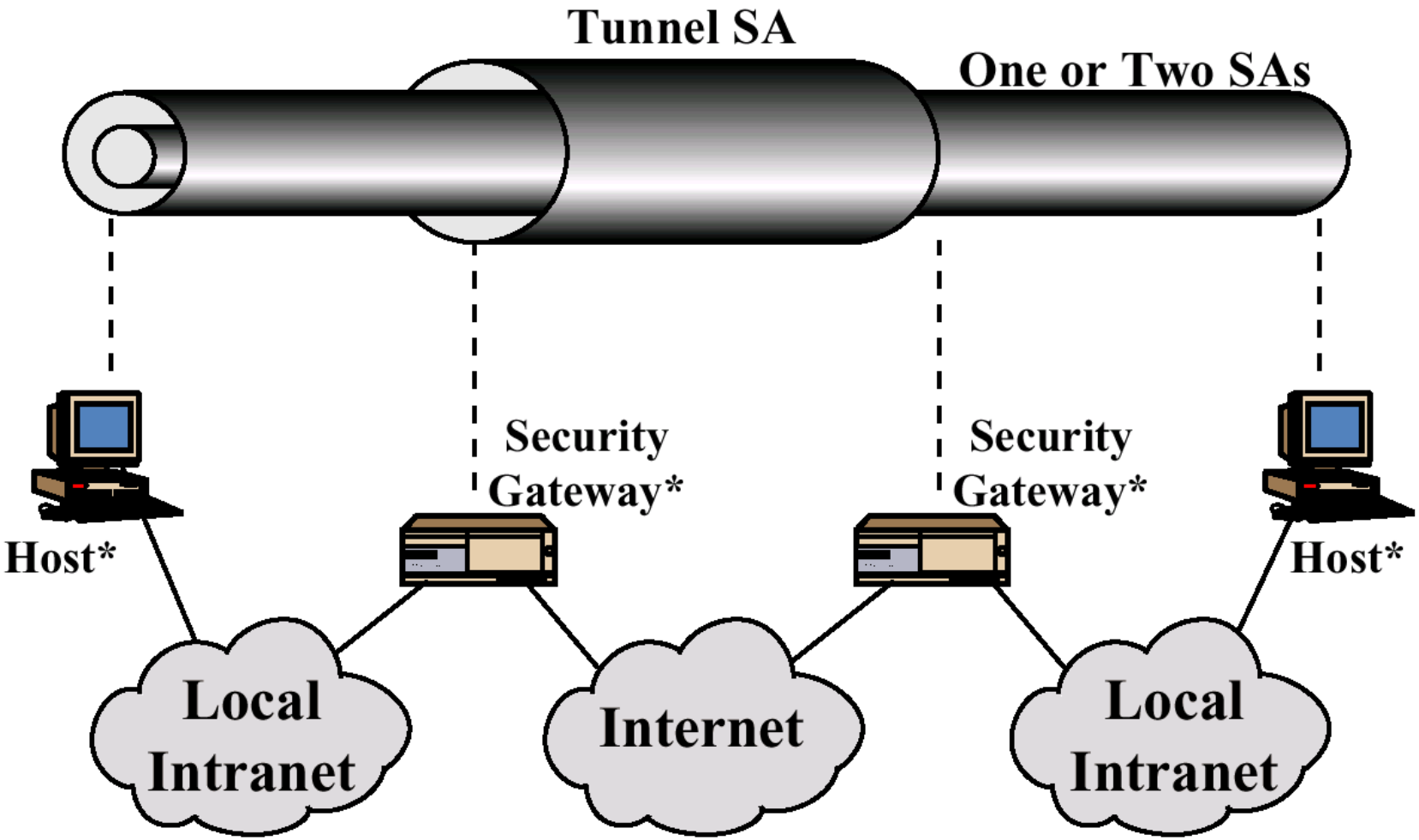
* = implementerer IPSec

Security Assocations - Case 2



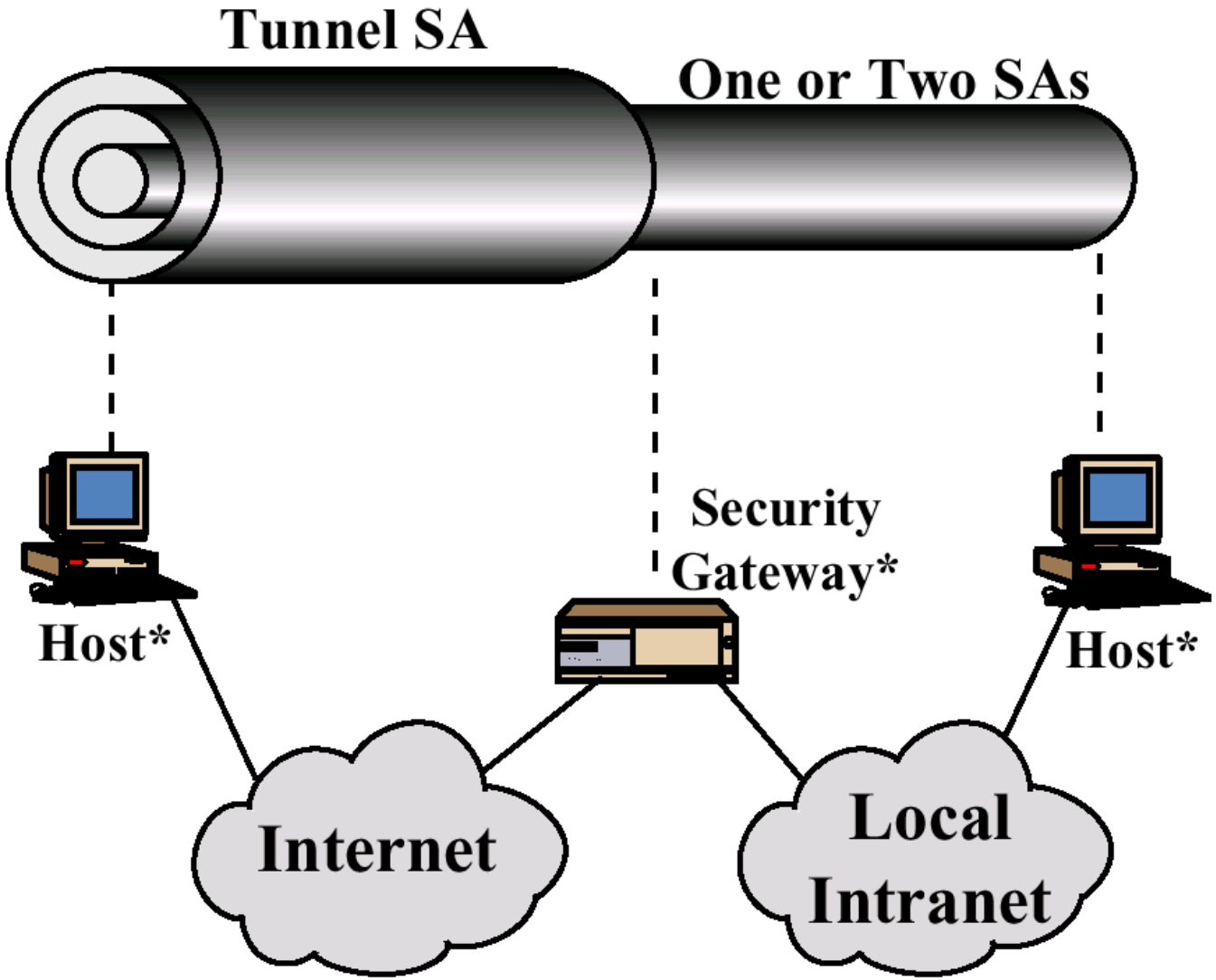
* = implementerer IPSec

Security Assocations - Case 3



* = implementerer IPSec

Security Assocations - Case 4



* = implementerer IPSec

Nøkkelhåndtering

- Manuell nøkkelhåndtering
  - Administrator setter alle nøkler selv (bare aktuelt for små nettverk)
- Automatisk nøkkelhåndtering
  - ISAKMP/Oakley

Oakley Key Determination

- Videreføring av Diffie-Hellman:
- Brukere A og B blir enige om primtall q og primitiv rot (av q) α
- A velger tilfeldig integer X_A som sin private nøkkel, og sender $Y_A = \alpha^{X_A}$ til B
- B gjør tilsvarende
- $K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q = \alpha^{X_A X_B} \bmod q$

Oakley forts.

Forbedringer ved bruk av Oakley:

- Bruker cookies for å hindre DoS
  - Cookie avhenger av senderen (IP, port)
- Utveksler de globale D-H-parametrene
- Bruker nonces mot replay
- Autentiserer D-H-utveksling for å unngå man-in-the-middle
  - Digitale signaturer, PK krypto, eller SK krypto

ISAKMP

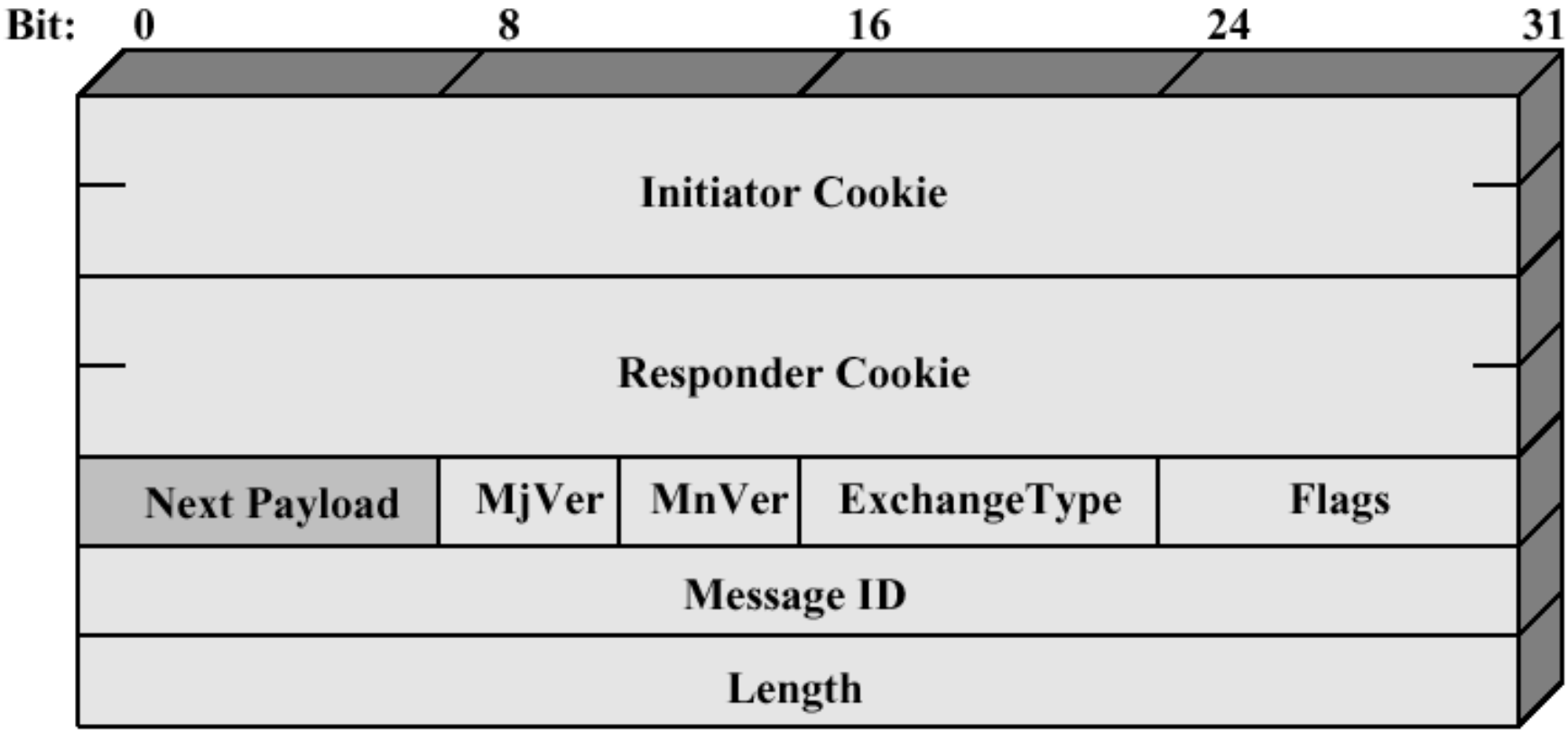
Internet Security Association and Key Management Protocol

Prosedyrer og formater for å

- opprette
- forhandle
- endre
- fjerne

sikkerhetsassosiasjoner (SA)

ISAKMP Header



Generell nyttelast header

ISAKMP Nyttelast-typer

- Security Association (SA) payload
- Proposal (P) payload
- Transform (T) payload
- Key Exchange (KE) payload
- Identification (ID) payload
- Certificate (CERT) payload
- Certificate request (CR) payload

Nyttelast-typer forts.

- Hash (HASH) payload
- Signature (SIG) payload
- Nonce (NONCE) payload
- Notification (N) payload
- Delete (D) payload
- AUTH payload?

ISAKMP utvekslinger

- ISAKMP er et rammeverk for meldingsutveksling. Følgende standard utvekslingstyper finnes:
  - Base Exchange
  - Identity Protection Exchange
  - Authentication Only Exchange
  - Aggressive Exchange
  - Informational Exchange

Base

Payload-typer definert tidligere!

(1) I→R: SA; NONCE

(2) R→I: SA; NONCE

(3) I→R: KE; ID_I;AUTH

(4) R→I: KE; ID_R;AUTH

I = Initiator

R = Responder

Identity Protection

(1) I→R: SA

(2) R→I: SA

(3) I→R: KE; NONCE

(4) R→I: KE; NONCE

Kryptert

(5) I→R: ID_I;AUTH

(6) R→I: ID_R;AUTH

Authentication Only

(1) I→R: SA; NONCE

(2) R→I: SA; NONCE; ID_R;AUTH

(3) I→R: ID_I;AUTH

Agressive

(1) I→R: SA; KE; NONCE; ID_I

(2) R→I: SA; KE; NONCE; ID_R;AUTH

Kryptert (3) I→R:AUTH

Informational

Kryptert

(1) I→R: N/D

Dagens website

- http://www.pgpi.org