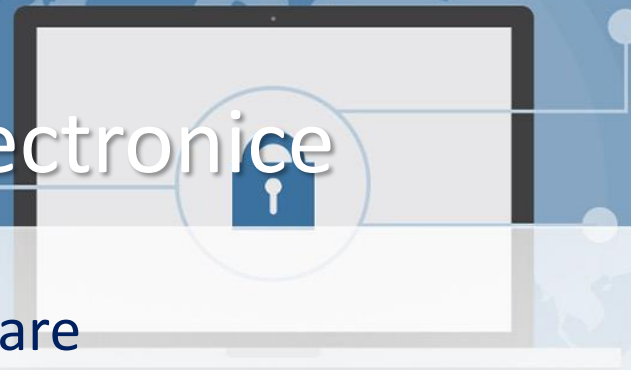
Criptografie și Securitate Cibernetică

RCC - CSC 6

Conținut

- Securitatea poștei electronice (eMail)
  - PGP - Pretty Good Privacy
  - MIME - Multipurpose Internet Mail Extension
  - S/MIME - Secure/Multipurpose Internet Mail Extension
  - DKIM - DomainKeys Identified Mail
- Securitatea IP
  - Elemente de securitate IP (IPsec)
  - Politici de securitate IP
  - Încapsularea datelor
  - Soluții de securitate combinate
  - Internet Key Exchange
  - Soluții criptografice

Securitatea poștei electronice



- Elemente specifice de securizare
  - PGP - Pretty Good Privacy
  - MIME - Multipurpose Internet Mail Extension
  - S/MIME - Secure/Multipurpose Internet Mail Extension
  - DKIM – DomainKeys Identified Mail

PGP – Pretty Good Privacy

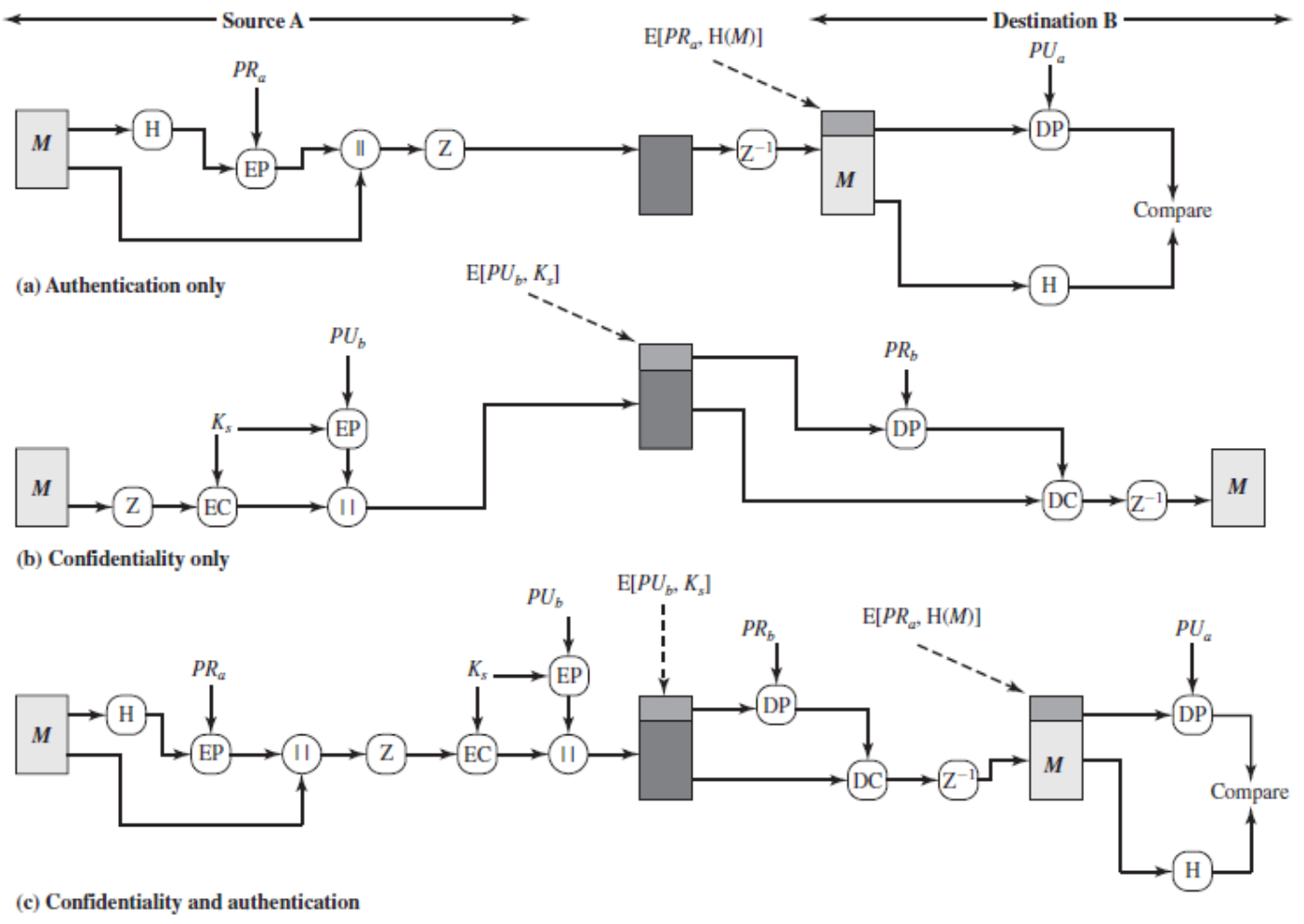
- Caracteristici
  - serviciu de confidenţialitate şi autentificare
  - pe bază de algoritmi criptografici pe blocuri
    - RSA, DSS, Diffie-Hellman criptare cu cheie publică
    - CAST-128, IDEA, and 3DES pentru criptare simetrică
    - SHA-1 pentru codare hash
  - integrat la nivelul unei aplicații de uz general, independentă de sistemul de operare, cu un set minimal de comenzi, ușor de utilizat
  - disponibil ca sursă și documentație pe Internet
  - disponibil gratuit pe diverse platforme
  - preluat de versiuni comerciale
  - RFC 3156; MIME Security with OpenPGP

Servicii PGP

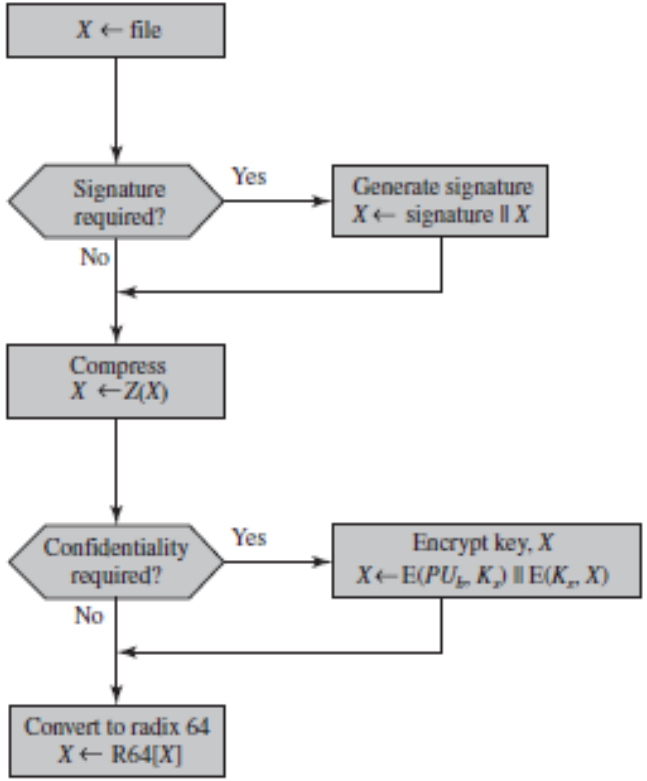
- PGP poate asigura 4 servicii
  - Autentificare
  - Confidențialitate
  - Compresie
  - Compatibilitate

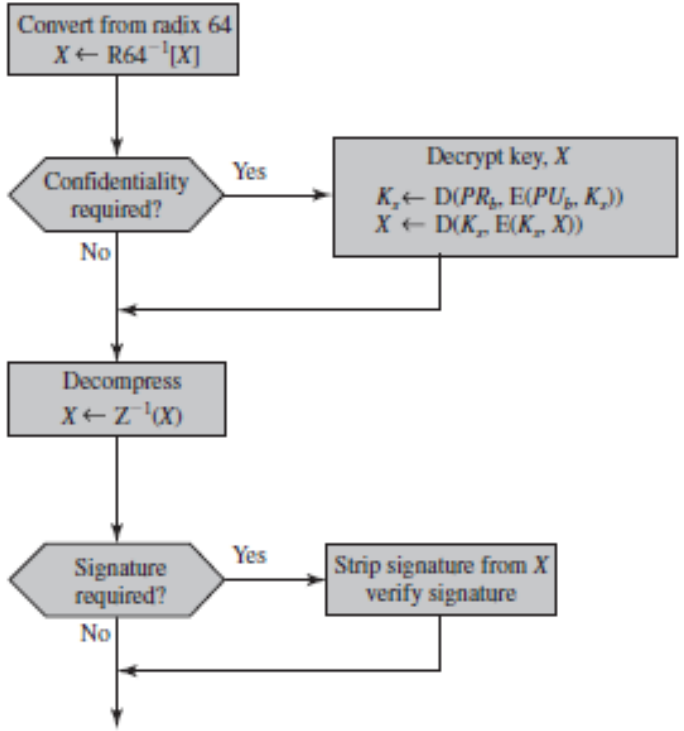
Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Funcții criptografice PGP



Mesaje PGP





- Diagrama logică pentru trimitere și recepție mesaje

S/MIME

- Secure/Multipurpose Internet Mail Extension (S/MIME)
  - Îmbunătățire la nivel de securitate a standardului MIME
  - Bazat pe RSA Data Security
  - Dedicat utilizării comerciale sau la nivel de organizație
- RFC 5322 (*Internet Message Format*)
  - Definește un format pentru mesajele text transmise prin sistemul de poștă electronică
  - Structură mesaj
    - Antet (header)
    - Conținut (body)

```
Date: October 8, 2009 2:15:49 PM EDT
From: "William Stallings" <ws@shore.net>
Subject: The Syntax in RFC 5322
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual
message body, which is delimited from the
message heading by a blank line.
```

MIME

- Multipurpose Internet Mail Extension (MIME)
  - Extensie a RFC 5322
  - Vizează limitări ale SMTP (Simple Mail Transfer Protocol)
    - Transmitere fișiere executabile sau binare
    - Transmitere mesaje cu caractere din alte limbi (8-biți)
    - Respingere mesaje peste o anumita dimensiune
    - Inconsistență de translatare ASCII – EBCDIC
    - Procesare mesaje X.400 (email ITU-T)
    - Implementări incomplete ale RFC 821 (SMTP)
      - Procesare caractere speciale (*carriage return, linefeed , space, tab*)
      - Trunchiere linii mai lungi de 76 de caractere

Elemente MIME

- Sunt folosite 5 câmpuri din antet
  - MIME-Version
    valoare 1.0., mesaj conform RFCs 2045 și 2046
  - Content-Type
    descrie datele din conținutul mesajului
  - Content-Transfer-Encoding:
    indică tipul de codare a mesajului, necesară pentru transport
  - Content-ID
    Indicator al entității MIME
  - Content-Description
    descriere text a obiectului din conținut
    (util pentru obiecte necitibile, ex. fișiere audio)

Tipuri de conținut MIME

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript format.
	octet-stream	General binary data consisting of 8-bit bytes.

Exemplu MIME (1)

```
MIME-Version: 1.0
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Subject: A multipart example
Content-Type: multipart/mixed;
     boundary=unique-boundary-1

This is the preamble area of a multipart message. Mail readers that understand multipart format should ignore
this preamble. If you are reading this text, you might want to consider changing to a mail reader that understands
how to properly display multipart messages.

--unique-boundary-1

     ...Some text appears here...
[Note that the preceding blank line means no header fields were given and this is text, with charset US ASCII.
It could have been done with explicit typing as in the next part.]

--unique-boundary-1
Content-type: text/plain; charset=US-ASCII

This could have been part of the previous part, but illustrates explicit versus implicit typing of body parts.

--unique-boundary-1
Content-Type: multipart/parallel;   boundary=unique-boundary-2

--unique-boundary-2
Content-Type: audio/basic
Content-Transfer-Encoding: base64
```

Exemplu MIME (2)

continuare...

... base64-encoded 8000 Hz single-channel mu-law-format audio data goes here....

--unique-boundary-2
Content-Type: image/jpeg
Content-Transfer-Encoding: base64

... base64-encoded image data goes here....

--unique-boundary-2--

--unique-boundary-1
Content-type: text/enriched

This is <bold><italic>richtext.</italic></bold> <smaller>as defined in RFC 1896</smaller>

Isn't it <bigger><bigger>cool?</bigger></bigger>

--unique-boundary-1
Content-Type: message/rfc822

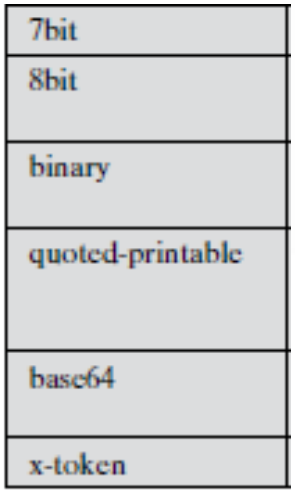
From: (mailbox in US-ASCII)
To: (address in US-ASCII)
Subject: (subject in US-ASCII)
Content-Type: Text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: Quoted-printable

... Additional text in ISO-8859-1 goes here ...

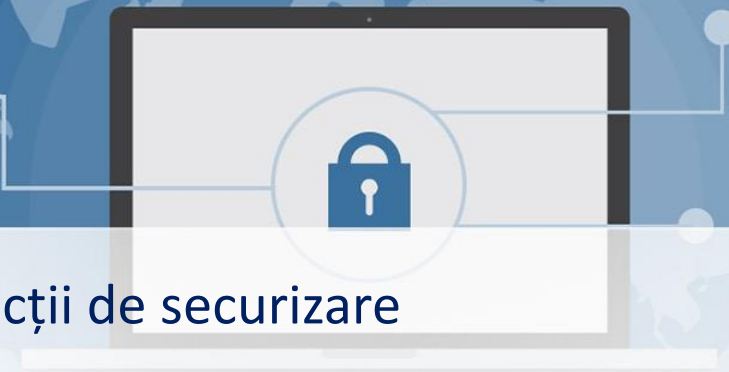
--unique-boundary-1--

Codare MIME

- Codarea conținutului mesajului pentru transport
  - Câmpul Content-Transfer-Encoding poate avea 6 valori
    - 7bit, 8bit și binary (fară codare, informare asupra tipul de date folosit)
    - x-token (scheme de codare specifice aplicațiilor sau proprietar)
    - 2 metode de codare efectivă
      - quoted-printable
        (introduce caractere „sfărșit de linie”
        pentru a delimita linii de maxim 76 de caractere)
      - base64 transfer encoding - radix-64
        (codarea datelor binare, folosita și de PGP)



Funcții S/MIME



- S/MIME oferă o serie de funcții de securizare
  - **Enveloped data**

    Criptare conținut mesaj și chei de criptare pentru unul sau mai mulți destinatari
  - **Signed data**

    Folosirea unei semnături digitale, codată împreună cu mesajul, folosind codarea base64
  - **Clear-signed data**

    doar semnatura este codată base64
  - **Signed and enveloped data**

    Combinații ale funcțiilor S/MIME

Algoritmi criptografici S/MIME

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.

- Funcții de securizare corelate cu algoritmi criptografici necesari implementării

Tipuri de conținut S/MIME

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs7-mime	signedData	A signed S/MIME entity.
	pkcs7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs7-mime	degenerate signedData	An entity containing only public-key certificates.
	pkcs7-mime	CompressedData	A compressed S/MIME entity.
	pkcs7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

- Sunt utilizate specificațiile sistemelor criptografice cu cheie publică

Exemple mesaje S/MIME

```
Content-Type: multipart/signed;
   protocol="application/pkcs7-signature";
   micalg=sha1; boundary=boundary42

–boundary42
Content-Type: text/plain

This is a clear-signed message.

–boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

–boundary42–
```

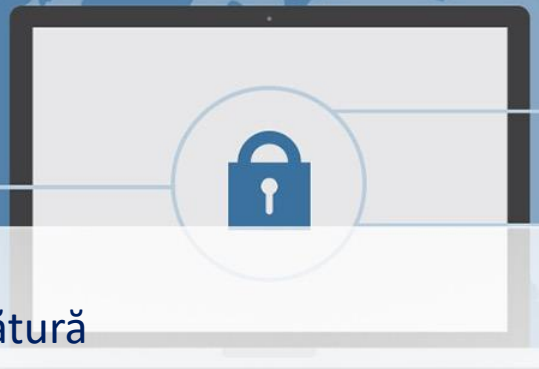
```
Content-Type: application/pkcs7-mime; smime-type=enveloped-
      data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V
```

Procesare certificate S/MIME

- Tipuri de certificate
  - (VeriSign oferă 3 clase de certificate cu cheie publică)

	Class 1	Class 2	Class 3
Summary of Confirmation of Identity	Automated unambiguous name and e-mail address search.	Same as Class 1, plus automated enrollment information check and automated address check.	Same as Class 1, plus personal presence and ID documents plus Class 2 automated ID check for individuals; business records (or filings) for organizations.
IA Private Key Protection	PCA: trustworthy hardware; CA: trustworthy software or trustworthy hardware.	PCA and CA: trustworthy hardware.	PCA and CA: trustworthy hardware.
Certificate Applicant and Subscriber Private Key Protection	Encryption software (PIN protected) recommended but not required.	Encryption software (PIN protected) required.	Encryption software (PIN protected) required; hardware token recommended but not required.
Applications Implemented or Contemplated by Users	Web-browsing and certain e-mail usage.	Individual and intra- and inter-company e-mail, online subscriptions, password replacement, and software validation.	E-banking, corp. database access, personal banking, membership-based online services, content integrity services, e-commerce server, software validation; authentication of LRAAs; and strong encryption for certain servers.

Servicii de securitate



- Sunt disponibile 3 tipuri de servicii
  - Confirmare de primire cu semnătură

    O confirmare de primire a mesajului poate fi solicitată prin intermediul obiectului de tip SignedData
  - Etichete de securitate

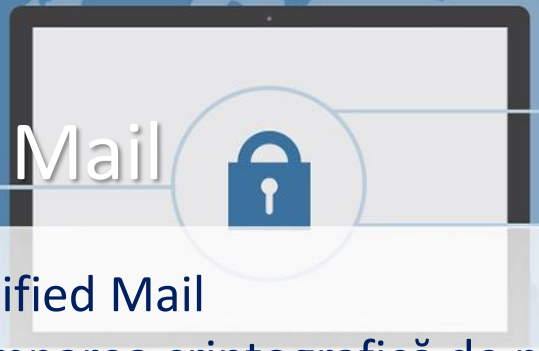
    Între atributele de autentificare ale unui obiect de tip SignedData poate fi inclusă și o etichetă de securitate,

    folosită pentru controlul accesului, prioritate(secret, confidențial)
  - Liste de discuții securizate

    Folosirea unui agent MLA (S/MIME Mail List Agent)

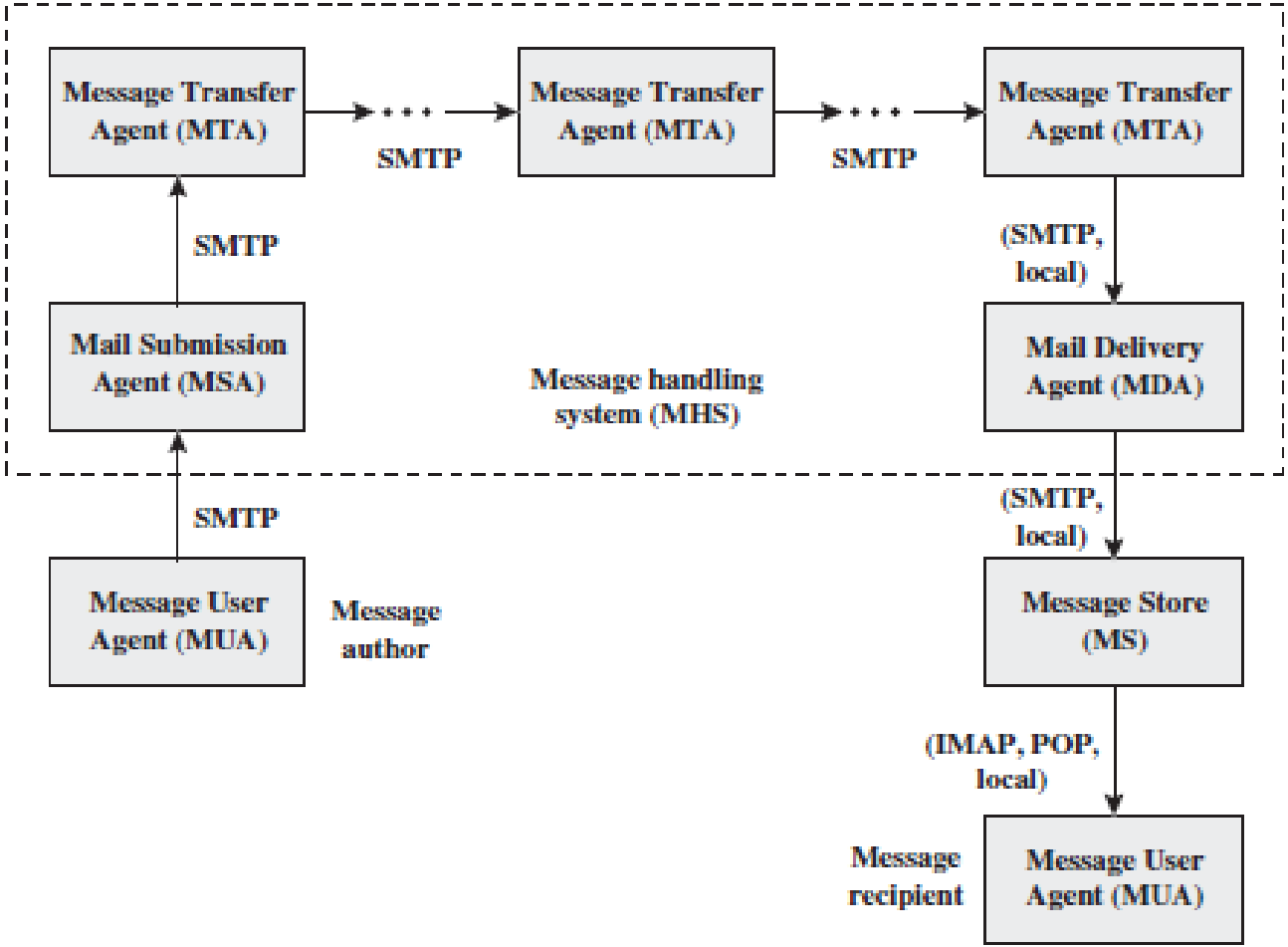
    Utilizatorul trimite mesaje către MLA, criptate de cu cheia publică MLA, iar MLA realizează criptarea către fiecare destinatar

DKIM - DomainKeys Identified Mail

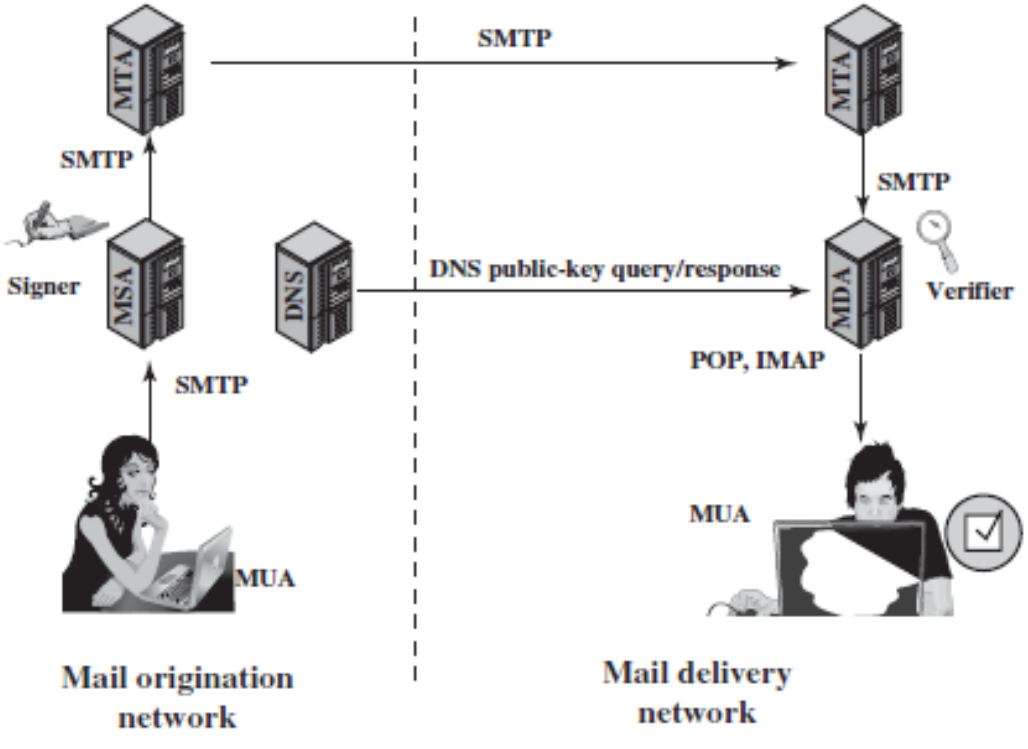


- DKIM - DomainKeys Identified Mail
  - Specificații pentru semnarea criptografică de mesaje email
  - Permite identificarea domeniului folosit în adresele email
  - Destinatarul poate verifica semnătura
    prin interogare directă a domeniul,
    primind cheia publică a domeniului,
    se confirma astfel ca mesajul a fost trimis criptat cu cheia privata a domeniului respectiv
  - RFC 4871: *DomainKeys Identified Mail (DKIM) Signatures*
  - Adoptat la scară largă (Gmail, Yahoo …)

Arhitectura poștă electronică

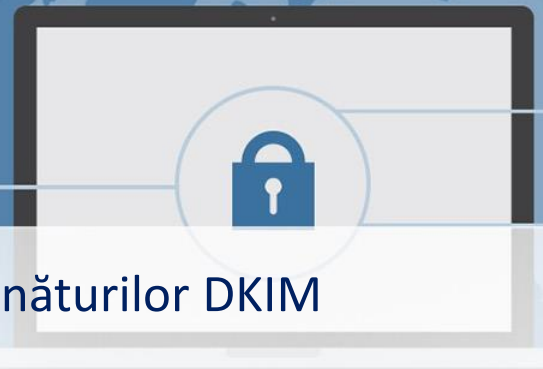


Integrare DKIM



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Semnătura DKIM



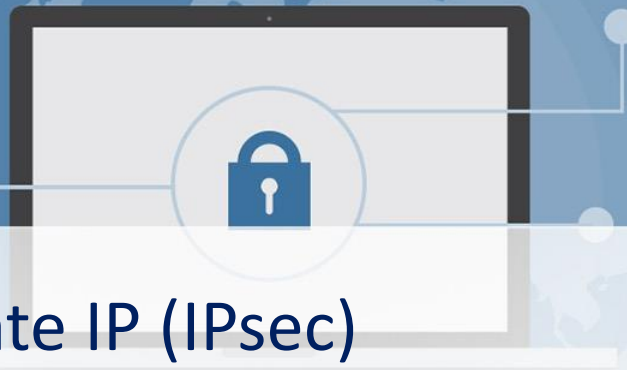
- Elementele specifice semnăturilor DKIM
  - **v** – versiunea DKIM
  - **a** – algoritmul utilizat pentru generarea semnăturii (rsa-sha1 sau rsa-sha256)
  - **c** – tipul de reprezentare canonică
  - **d** – numele de domeniu ce identifică organizația Signing Domain IDentifier (SDID)
  - **s** – selector de cheie (nume asociat unei chei)
  - **h** – lista de câmpuri din antet asociate cu algoritmul criptografic
  - **bh** – hash al conținutului mesajului
  - **b** – semnătura în format base64

Exemplu DKIM

- Semnătură DKIM, inclusă ca intrare suplimentară în antet

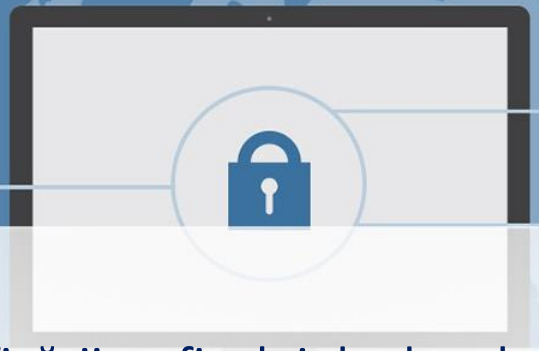
```
Dkim-Signature:     v=1; a=rsa-sha256; c=relaxed/relaxed;
                    d=gmail.com; s=gamma; h=domainkey-signa-
                    ture:mime-version:received:date:message-
                    id:subject :from:to:content-type:con-
                    tent-transfer-encoding;
                    bh=5mZvQDyCRuyLb1Y28K4zgS2MPOemFToDBgvbJ
                    7GO90s=;
                    b=PcUvPSDygb4ya5Dyj1rbZGp/VyRiScuaz7TTG
                    J5qW5s1M+klzv6kcfYdGDHzEVJW+Z
                    FetuPfF1ETOVhELtwH0zjSccOyPkEibl0f6gILO
                    bm3DDRm3Ys1/FVrbhVO1A+/jH9Aei
                    uIIw/5iFnRbSH6qPDVv/beDQqAWQfA/wF7O5k=
```

Securitatea IP



- Elemente de securitate IP (IPsec)
- Politici de securitate IP
- Încapsularea datelor
- Soluții de securitate combinate
- Internet Key Exchange
- Soluții criptografice

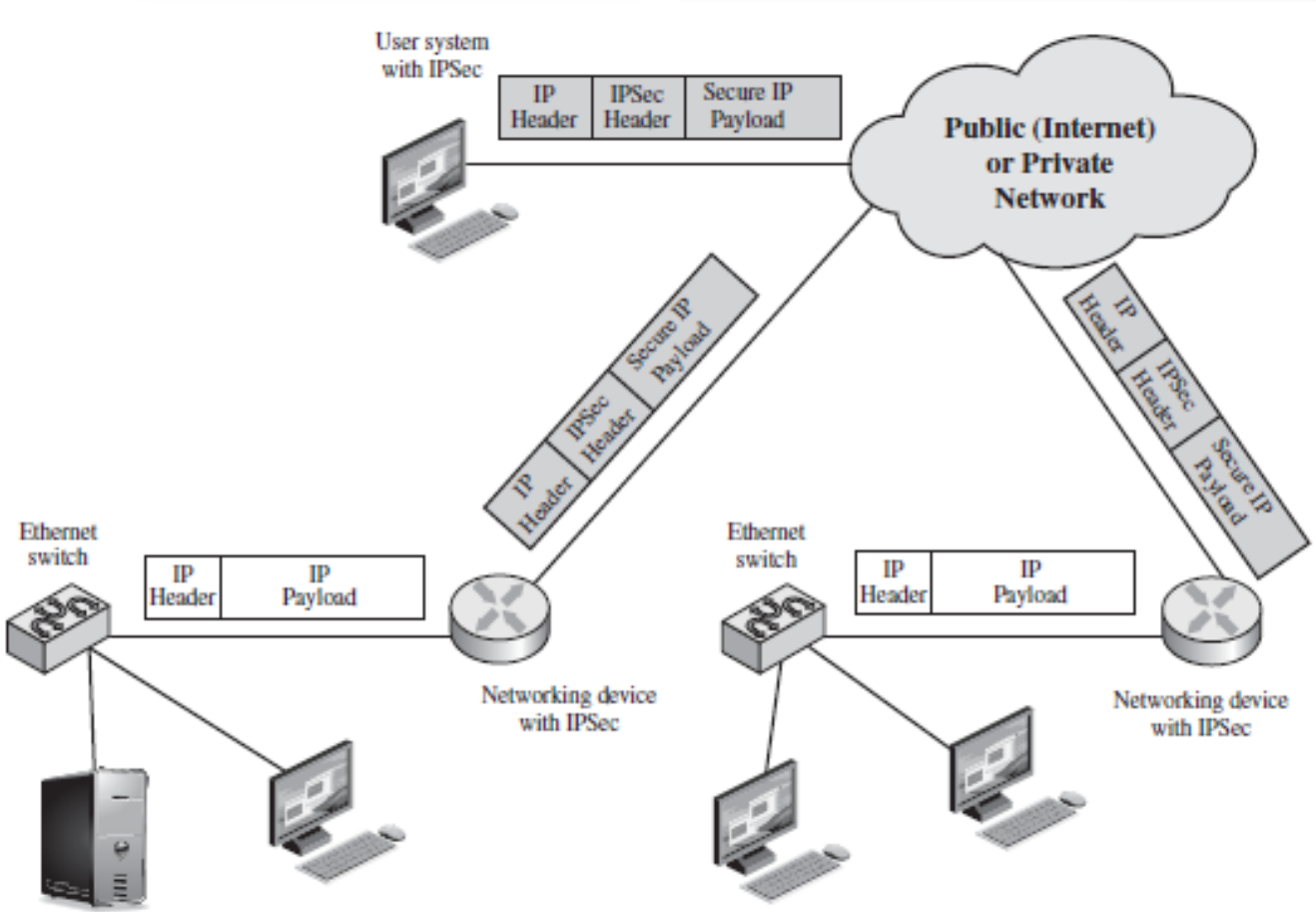
Securitatea IP (IPsec)



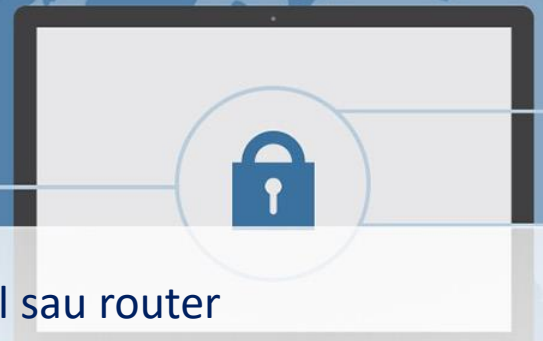
Elemente vizate:

- Posibilitatea criptării și/sau autentificării traficului de date la nivel IP
- Toate aplicațiile (login, client/server, email, ftp, web etc.) sunt securizate
- Domenii de aplicabilitate ale IPSec
  - Securizarea conectivității diferitelor sucursale prin intermediul Internet
  - Acces le distanță securizat prin Internet
  - Stabilirea de conexiuni extranet/intranet cu parteneri
  - Creșterea nivelului de securitate pentru aplicații de comerț electronic

Scenariu IPSec



Beneficii IPsec



- Poate fi implementat la nivel de firewall sau router
  - Oferă nivel ridicat de securitate, care poate aplicat întregului domeniu
  - Sistemele firewall pot permite în rețea doar trafic securizat
  - Este transparent pentru aplicații (sub protocoalele de transport UDP și TCP)
  - Nu sunt necesare modificări ale aplicațiilor (chiar dacă IPSec este implementat la nivel utilizator, aplicațiile de nivel superior nu sunt afectate)
  - Poate fi transparent utilizatorilor (nu necesită proceduri de instruire pentru utilizatori, producerea elementelor de securizare ale utilizatorilor și distrugerea acestor elemente la părăsirea domeniului se realizează automat)
  - Poate fi folosit pentru securizarea individuală a utilizatorilor
  - Protocoalele de dirijare a pachetelor se pot baza pe IPSec

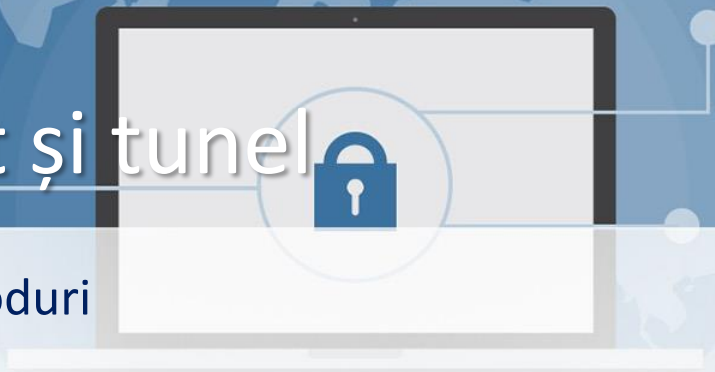
Servicii IPSec

- Protocoale folosite pentru securizare IP
  - Un protocol de autentificare identificat prin antetul protocolului,

    AH - Authentication Header
  - Un protocol combinat de criptare/autentificare identificat prin formatul de pachet specific protocolului

    ESP - Encapsulating Security Payload
- Servicii oferite
  - Controlul accesului
  - Integritatea comunicațiilor neorientate pe conexiune
  - Autentificarea originii datelor
  - Respingerea pachetelor
  - Confidențialitate (criptare)

Modurile transport și tunel



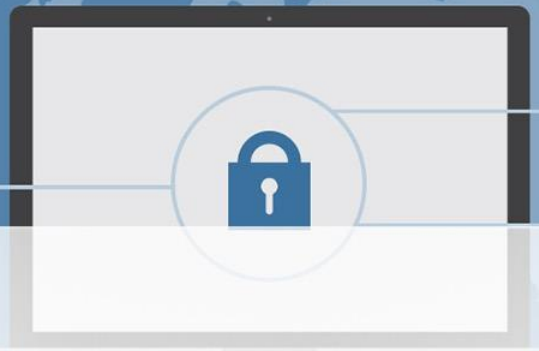
- AH și ESP pot fi utilizate în 2 moduri
  - Transport
    - Oferă protecție, în principal, pentru protocoalele de nivel superior (încapsulează pachetele IP)
    - ESP criptează și opțional autentifică datele IP (payload) dar nu și antetul IP (header)
    - AH autentifică datele IP și porțiuni selectate ale antetului IP
  - Tunel
    - Oferă protecție întregului pachet IP
    - După adăugarea câmpurilor AH și ESP, întregul pachet inclusiv cu tot cu câmpuri de securitate este preluat ca și date IP ale unui pachet IP exterior (acesta având propriul antet IP)

Funcțiile IPSec

- Funcțiile specifice IPSec, in cele 2 moduri, tunel și transport

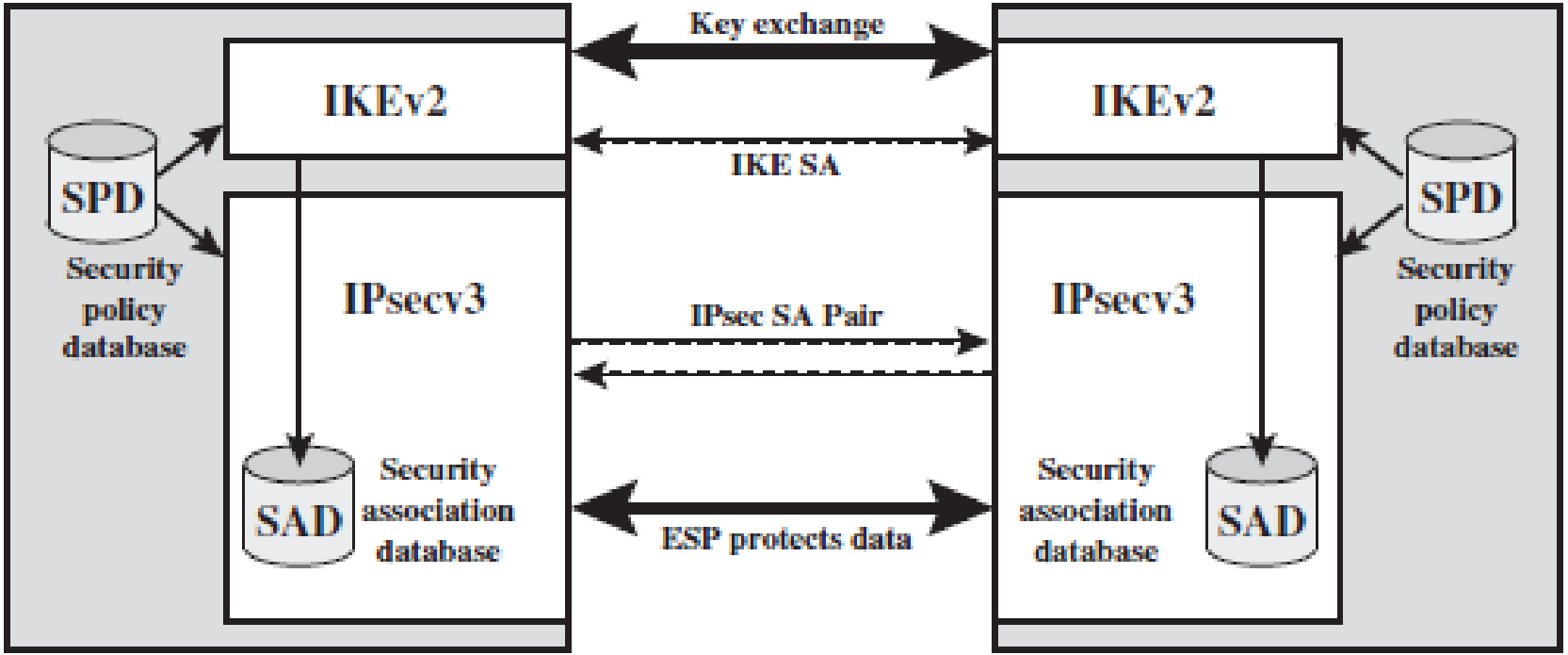
	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

Politici IPSec

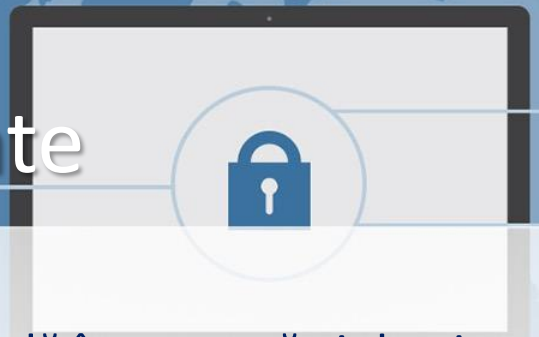


- Concept fundamental IPSec
  - aplicarea politicilor de securitate fiecărui pachet IP
- Politica de securitate este determinată de 2 resurse
  - Baza de date cu asocieri de securitate (SA)
    (Security Association Database - SAD)
  - Baza de date cu politici de securitate
    (Security Policy Database - SPD).

Arhitectura IPSec

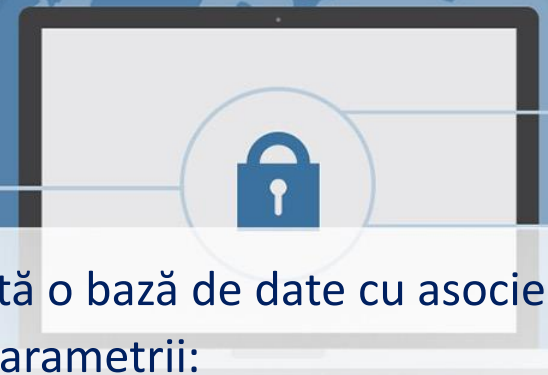


Asocierile de securitate



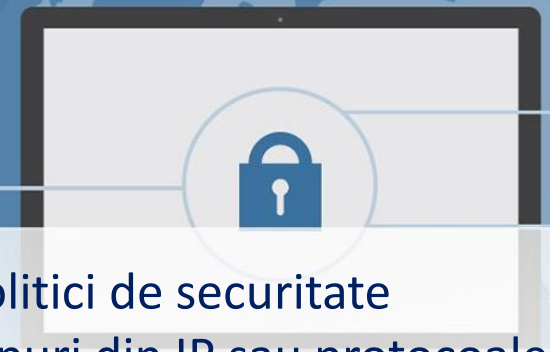
- Asocierile de securitate (SA)
  - Legătură logică unidirecțională între sursă și destinație
  - Permite servicii de securitate la nivelul traficului efectuat
  - Pentru un schimb securizat de mesaje bidirecțional sunt necesare două asocieri
- O asociere de securitate este identificată prin 3 elemente
  - Indexul parametrilor de securitate - număr (32biți) pentru selectarea asocierilor de securitate
  - Adresa IP destinație - destinația finală a asocierii de securitate
  - Identificatorul protocolului de securitate - identificare folosirii protocolului AH sau ESP

Baza de date cu asocieri de securitate (SAD)



- În orice implementare IPSec există o bază de date cu asocieri de securitate
- O asociere de securitate având parametrii:
  - Indexul parametrului de securitate
  - Contor de număr de secvență
  - Indicator depășire contor de secvență
  - Fereastră anti-replay
  - Informație AH
  - Informație ESP
  - Timpul de viață al asocierii de securitate
  - Modul IPSec (tunel, transport sau *wildcard*)
  - MTU (Maximum Transmission Unit) – dimensiune pachet

Baza de date cu politici de securitate (SPD)



- Intrările din Baza de date cu politici de securitate
  - Definite prin selectori (câmpuri din IP sau protocoale de nivel superior)
  - Filtrarea traficului pentru a realiza maparea cu o anumită asociere de securitate
- Selectori
  - Adresa IP destinație
  - Adresa IP locală
  - Protocolul de la nivelul următor (câmpul *Protocol* pentru IPv4, câmpul *Next Header* la IPv6)
  - Nume (identificator al utilizatorului din sistemul de operare)
  - Adresele de port local și la distanță

Exemplu

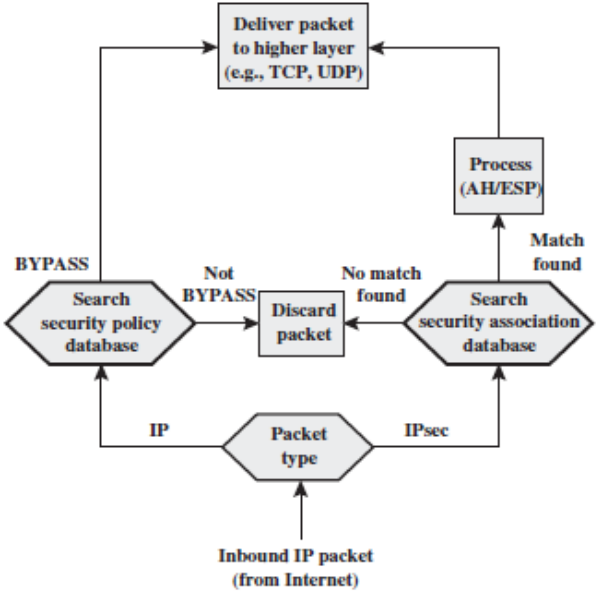
- Baza de date cu politici de securitate

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

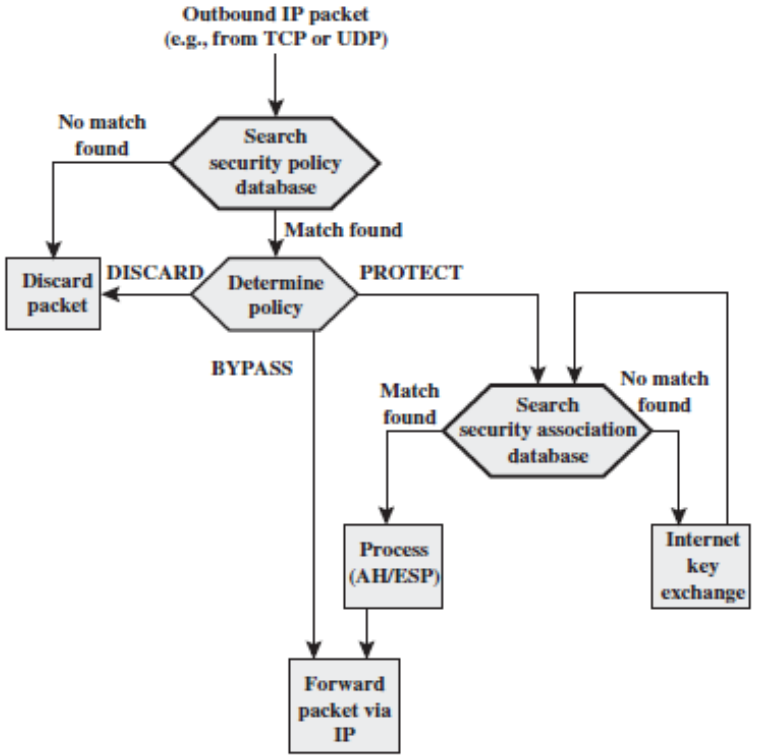
Procesarea traficului IP

- IPSec este aplicat asupra traficului pachet cu pachet,

la intrare



la ieșire

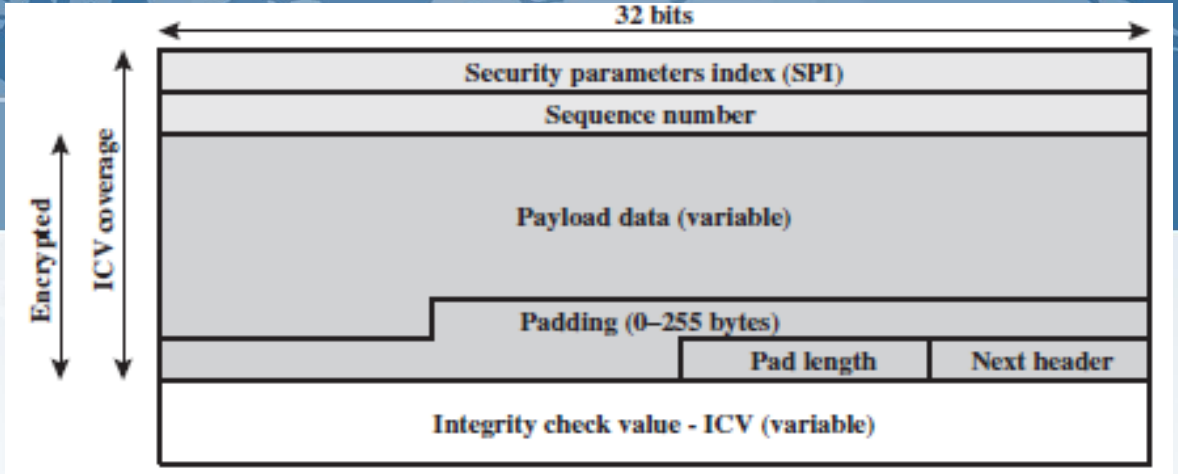


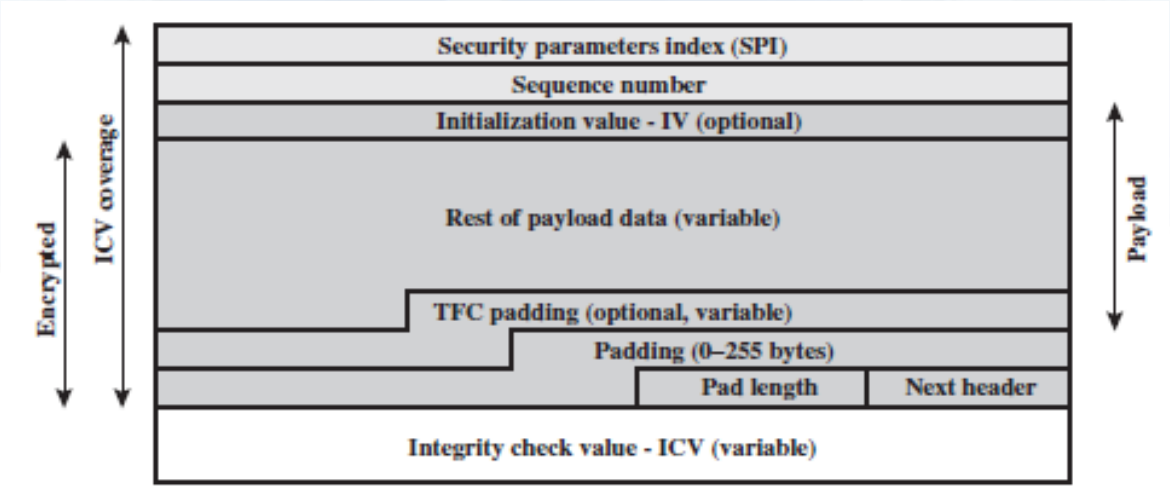
ESP

- Encapsulating Security Payload

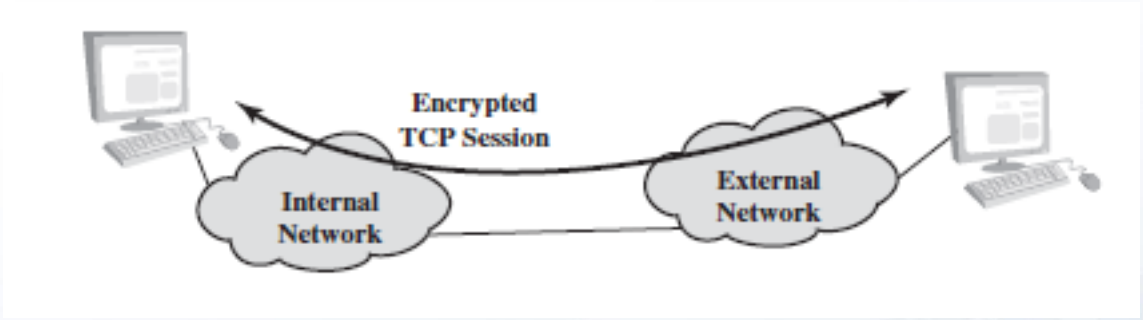
- Format pachete (sus)

- Format date (jos)

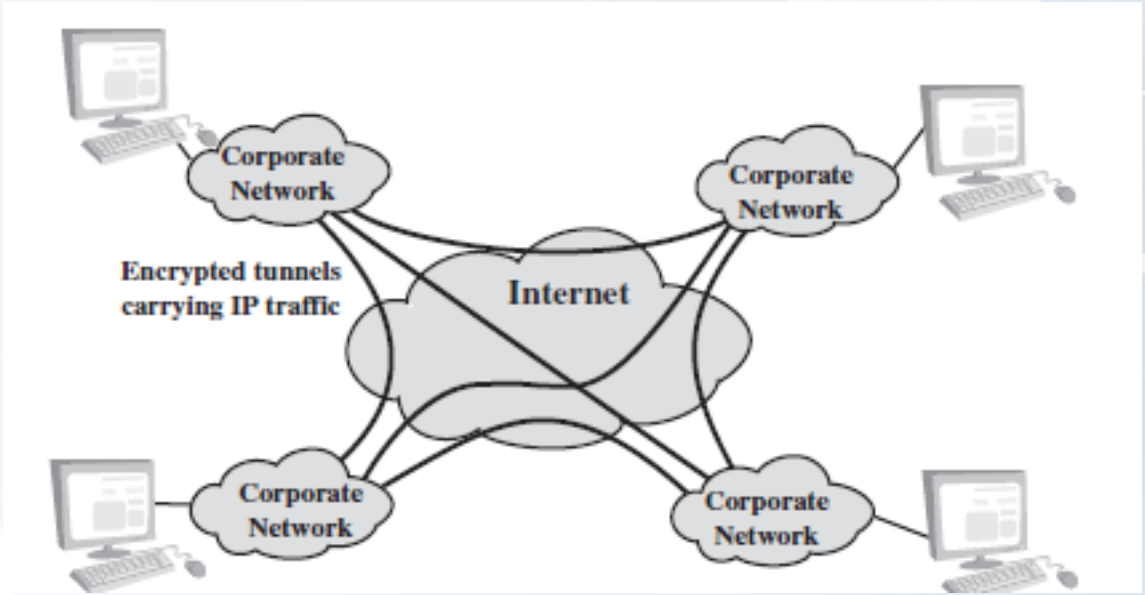




Securizare transport vs. tunel



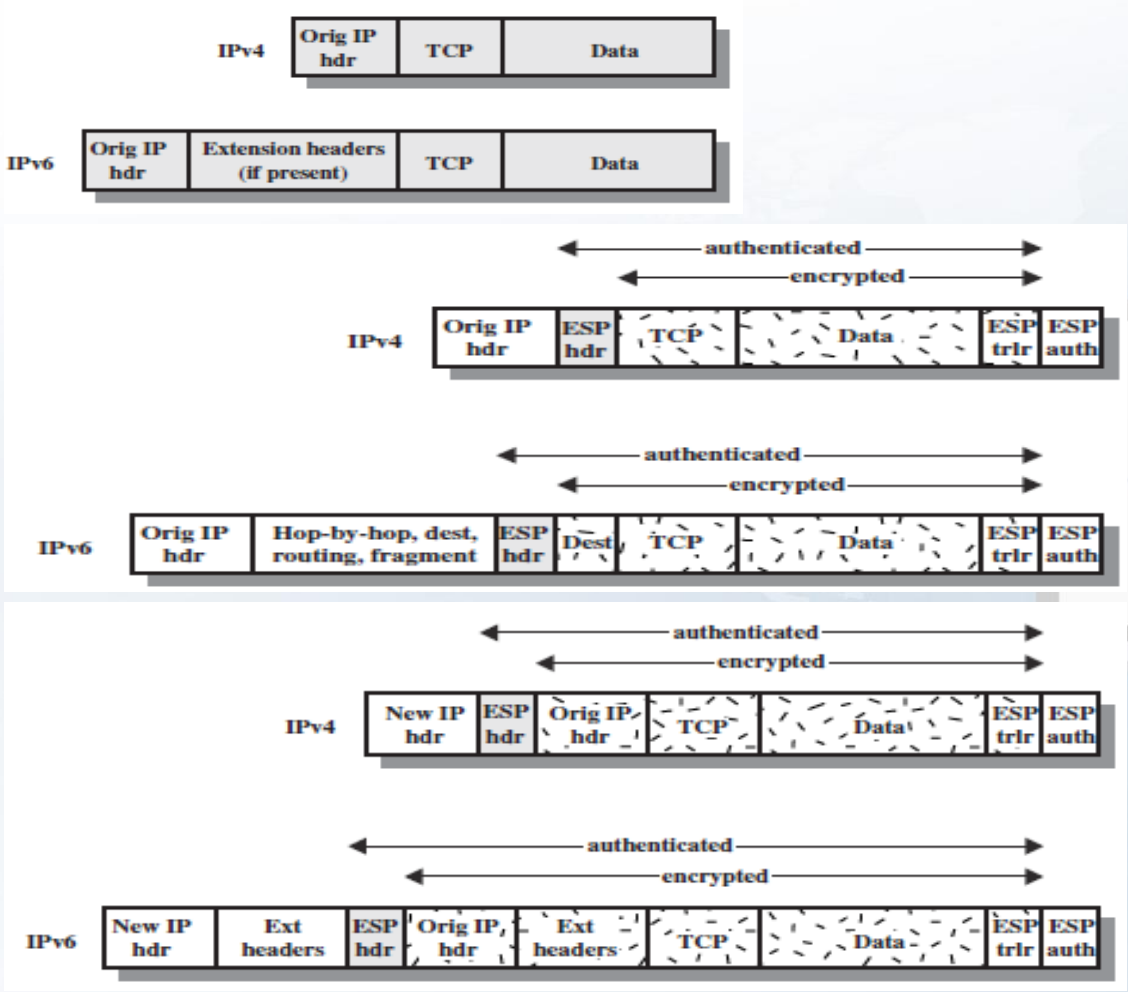
- Securizare în mod transport



- VPN în mod tunel

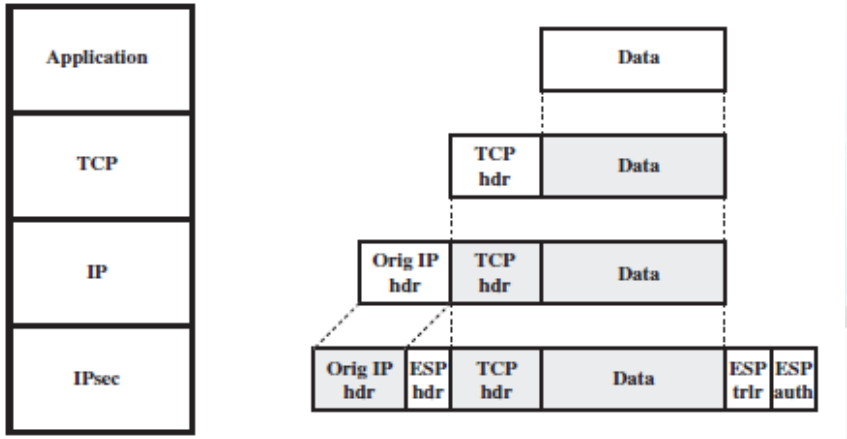
Autentificare și criptare ESP

- Fără ESP
- Mod transport
- Mod tunel

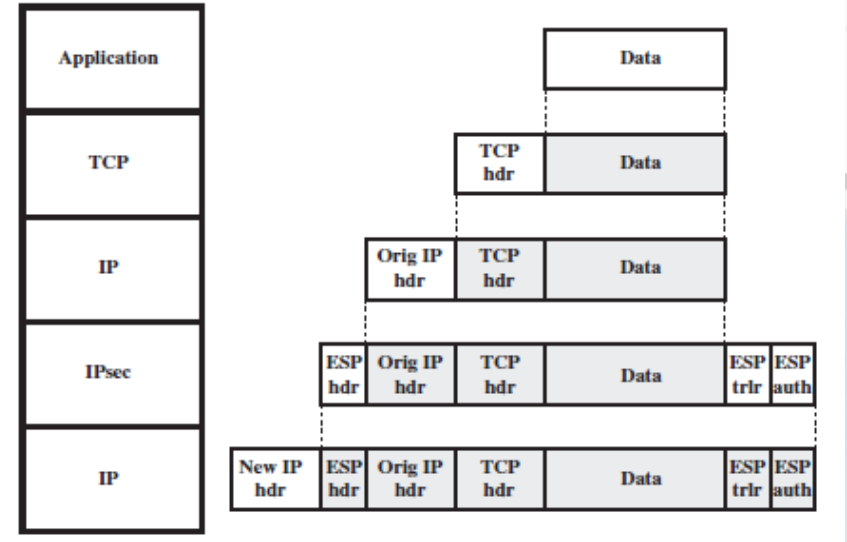


Încapsulare ESP

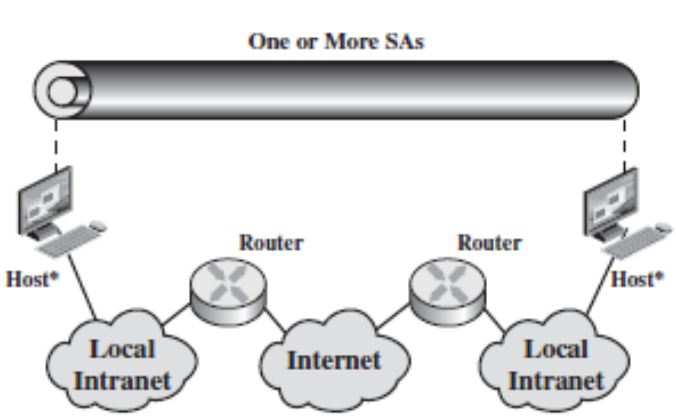
- Mod transport

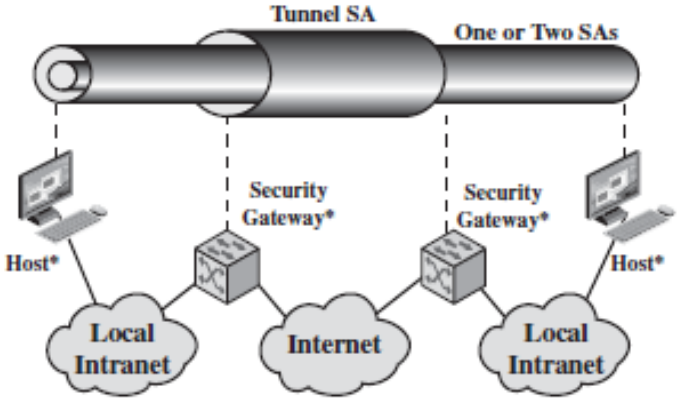


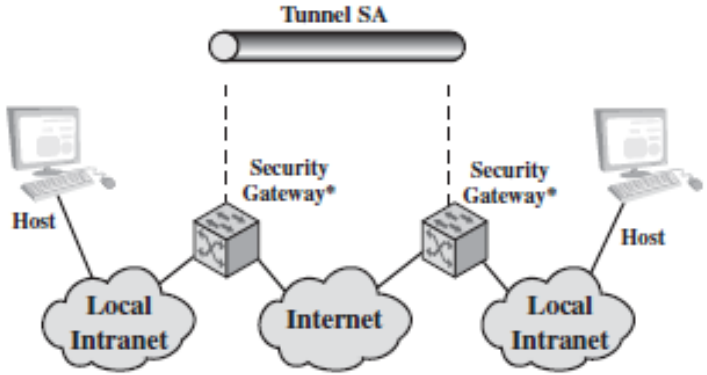
- Mod tunel

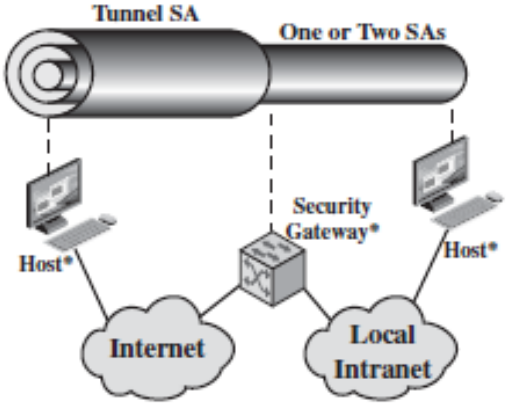


Soluții de securitate

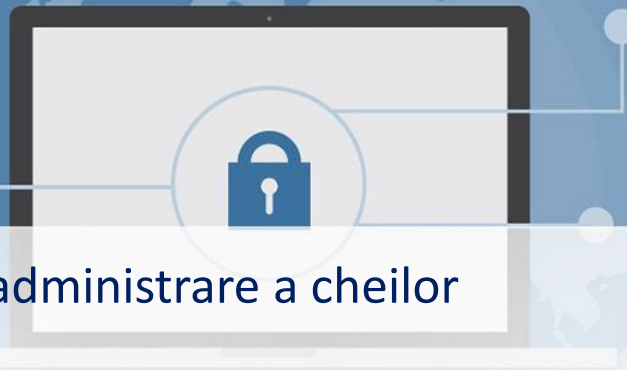








IKE - Internet Key Exchange



Arhitectura IPsec permite 2 moduri de administrare a cheilor

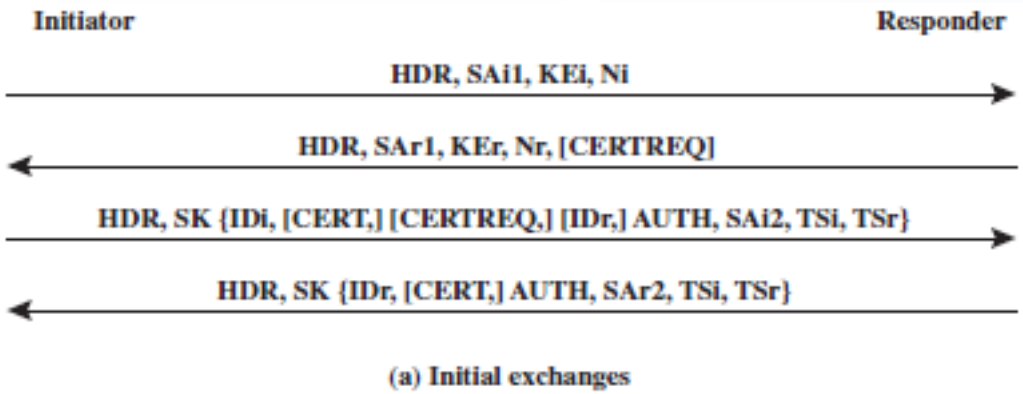
- Manual (realizată de administrator)
- Automat (protocol ce răspunde la solicitări)
  - ISAKMP/Oakley protocolul implicit, are 2 componente
    - **Oakley Key Determination Protocol**

      Protocolul pentru schimbul cheilor

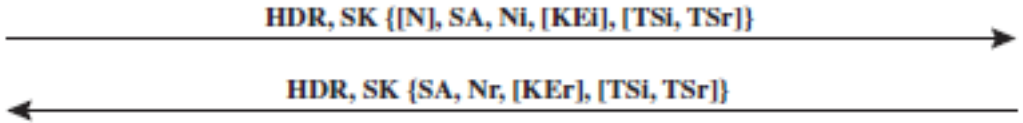
      (algoritm criptografic Diffie-Hellman)
    - **Internet Security Association and Key Management Protocol (ISAKMP)**

      Cadrul de lucru pentru susținerea protocolarelor de comunicație, formatul mesajelor, negocierea atributelor de securitate

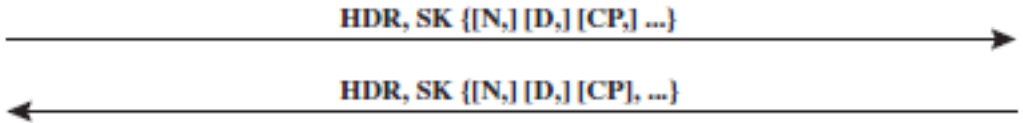
Specificații IKEv2



(a) Initial exchanges



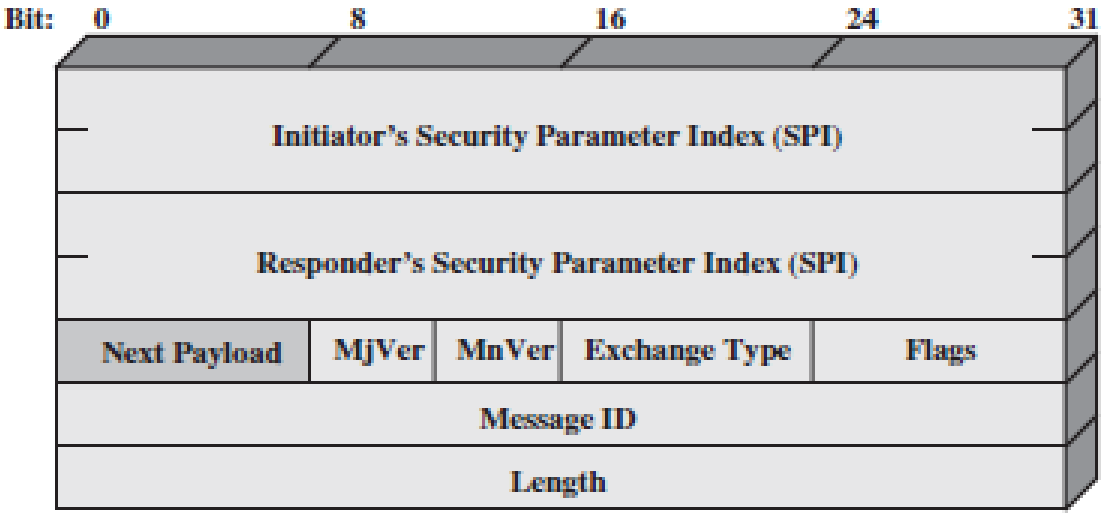
(b) `CREATE_CHILD_SA` exchange



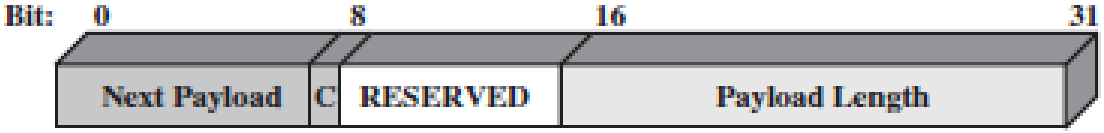
(c) Informational exchange

HDR = IKE header
SAx1 = offered and chosen algorithms, DH group
KEx = Diffie-Hellman public key
Nx= nonces
CERTREQ = Certificate request
IDx = identity
CERT = certificate
SK {...} = MAC and encrypt
AUTH = Authentication
SAx2 = algorithms, parameters for IPsec SA
TSx = traffic selectors for IPsec SA
N = Notify
D = Delete
CP = Configuration

Format antet IKE



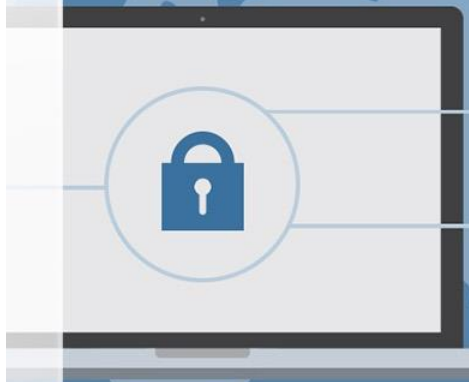
(a) IKE header



(b) Generic Payload header

Tipuri de date IKE

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message



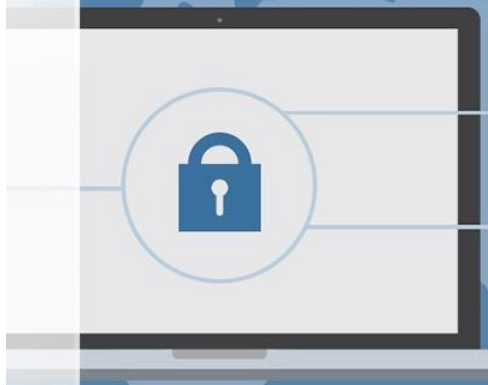
Suita criptografică IPsec

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

(a) Virtual private networks (RFC 4308)

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/ Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP

(b) NSA Suite B (RFC 4869)



CNSA

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

- Commercial National Security Algorithm Suite (CNSA) - RFC 8423
- Tranzitia la algoritmi cu rezistență cuantică