Seminar on Network Security and Related Research Issues

Dr. Haitham S Cruickshank
http://www.ee.surrey.ac.uk/Personal/H.Cruickshank/

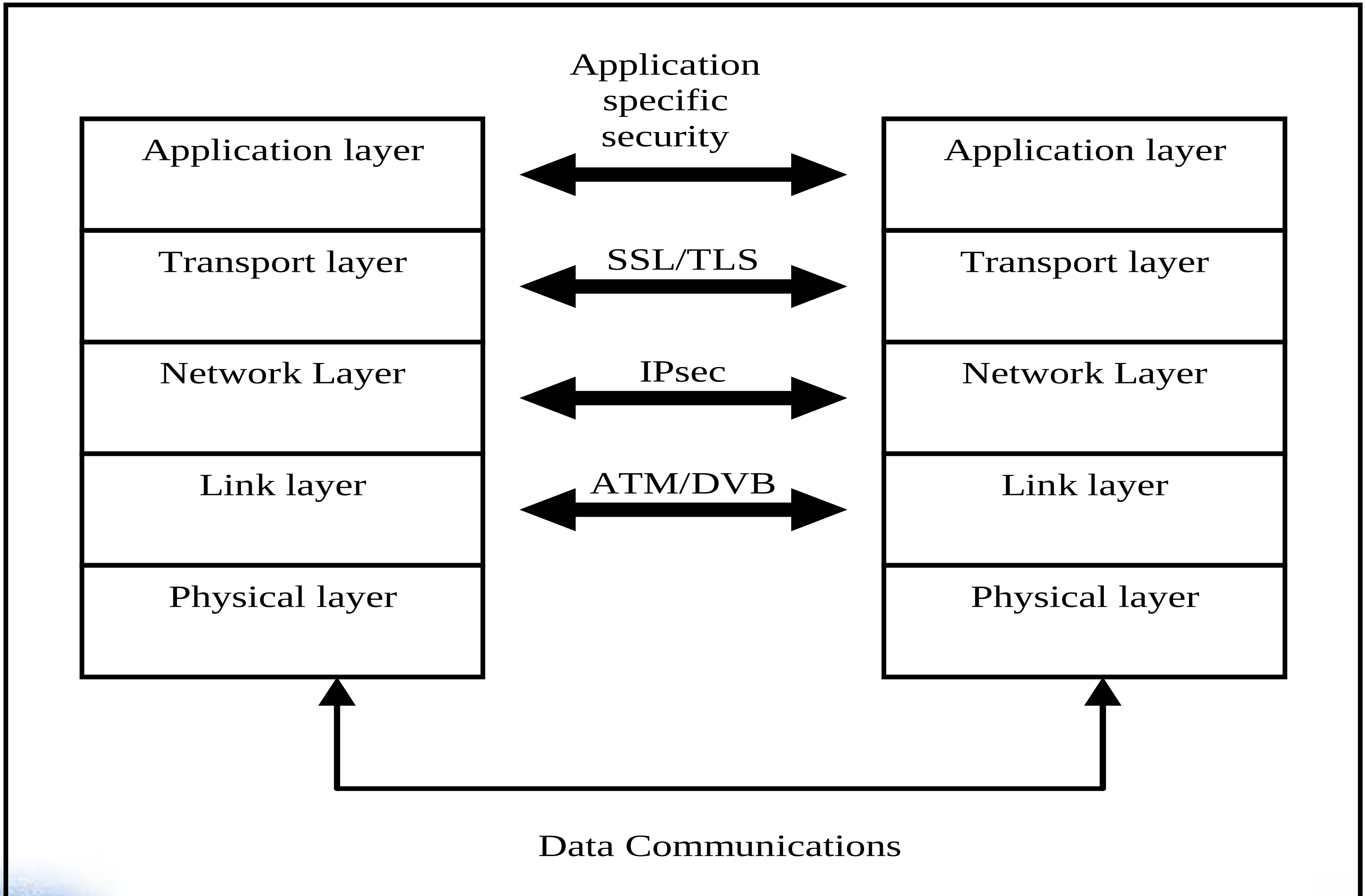
- Q: Why do everybody agree that network security is very important, but not many providers are welling to implement it?

- **Answer: Not understood very well and too complex to implement effectively**

Seminar outline

- Introduction to security basics
- Examples of security systems in communication network
- Overview to IPSec and secure multicast
- Impact of using IPSec on middle entities such as Performance Enhancing Proxies (PEPs)
- Security issues in challenged networks such as Delay Tolerant Networks (DTN)

Existing security technologies



Different facets of security

- Authentication: validate authentic identity.
- Authorization: access control.
- Integrity: protection from unauthorized change.
- Confidentiality or Privacy: keep information private such that only authorized users can understand it.
- Availability: outsider cannot block legitimate access.
- Non-repudiation: supply undeniable evidence to prove the message transmission and network access.

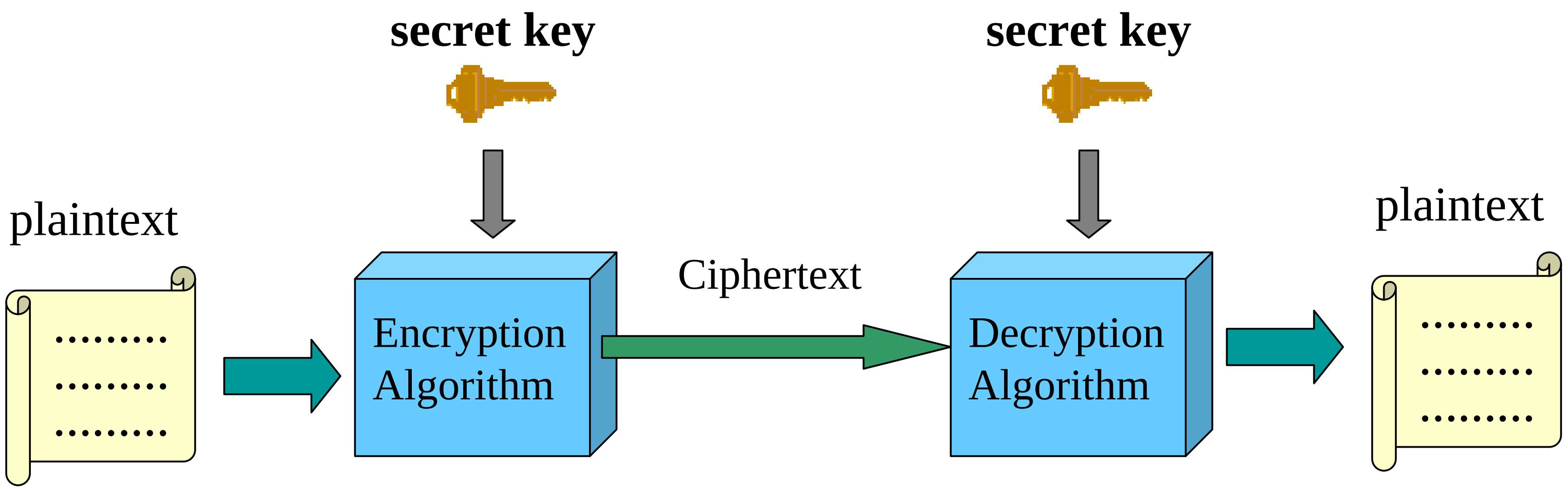
Security attacks

- Passive attacks: eavesdropping on transmission or monitor and analyze the network traffic.
- Active attacks: modification of information, interruption of information transmission and fabrication of messages:
  - Denial-of-service (DoS)
  - Masquerade
  - Man-in-the-middle
  - Replay

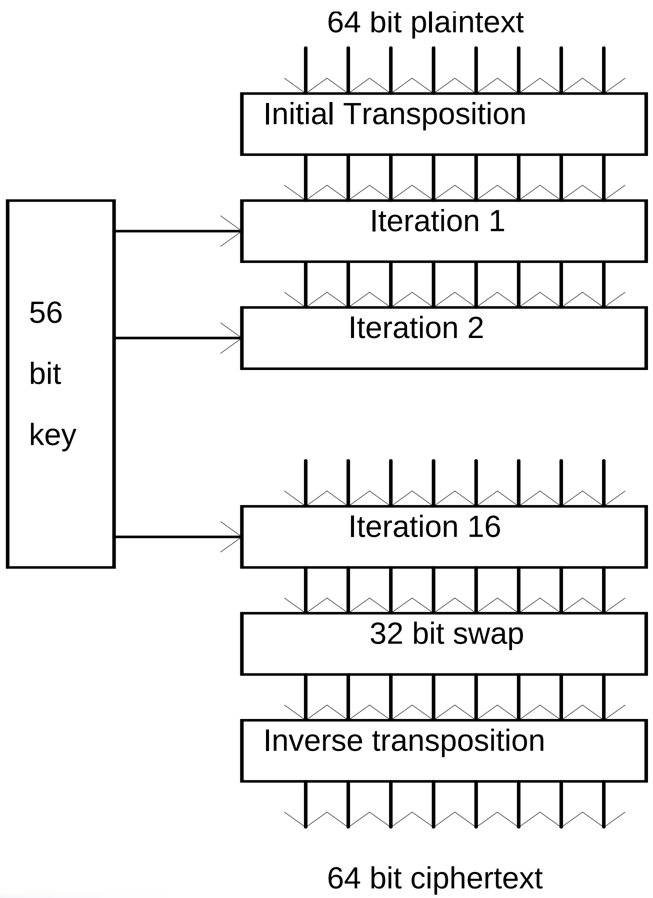
Security systems - two categories

- **Secret-key algorithm:**
  - Symmetric: same secret-key is used for both encryption and decryption
  - DES: Data Encryption Standard
  - AES: Advanced Encryption Standard
- **Public-key algorithm:**
  - Asymmetric: different keys are used for encryption and decryption
  - RSA (Rivest, Shamir and Adleman)

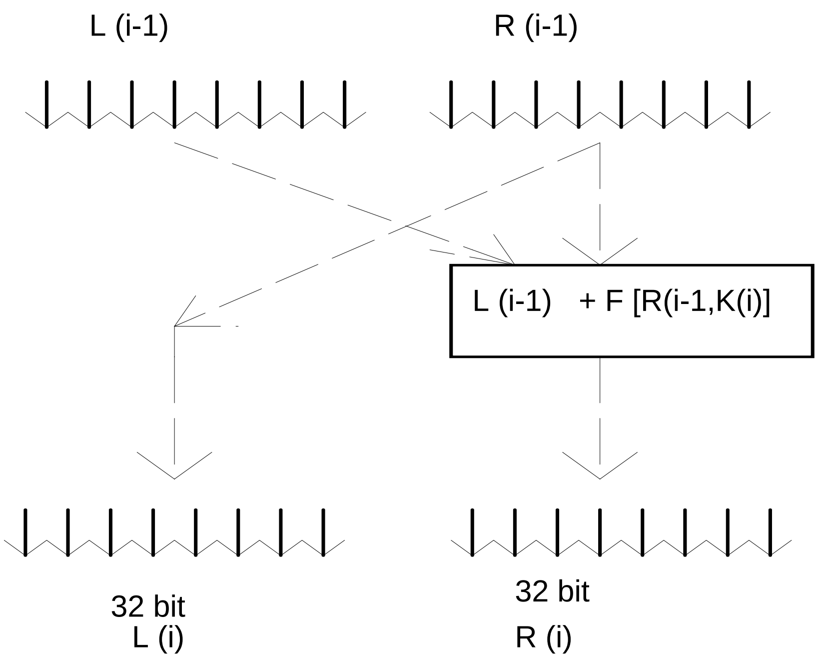
Secret-key system: encryption and decryption



Secret-key system example – Data Encryption Standard (DES)



(a)



(b)

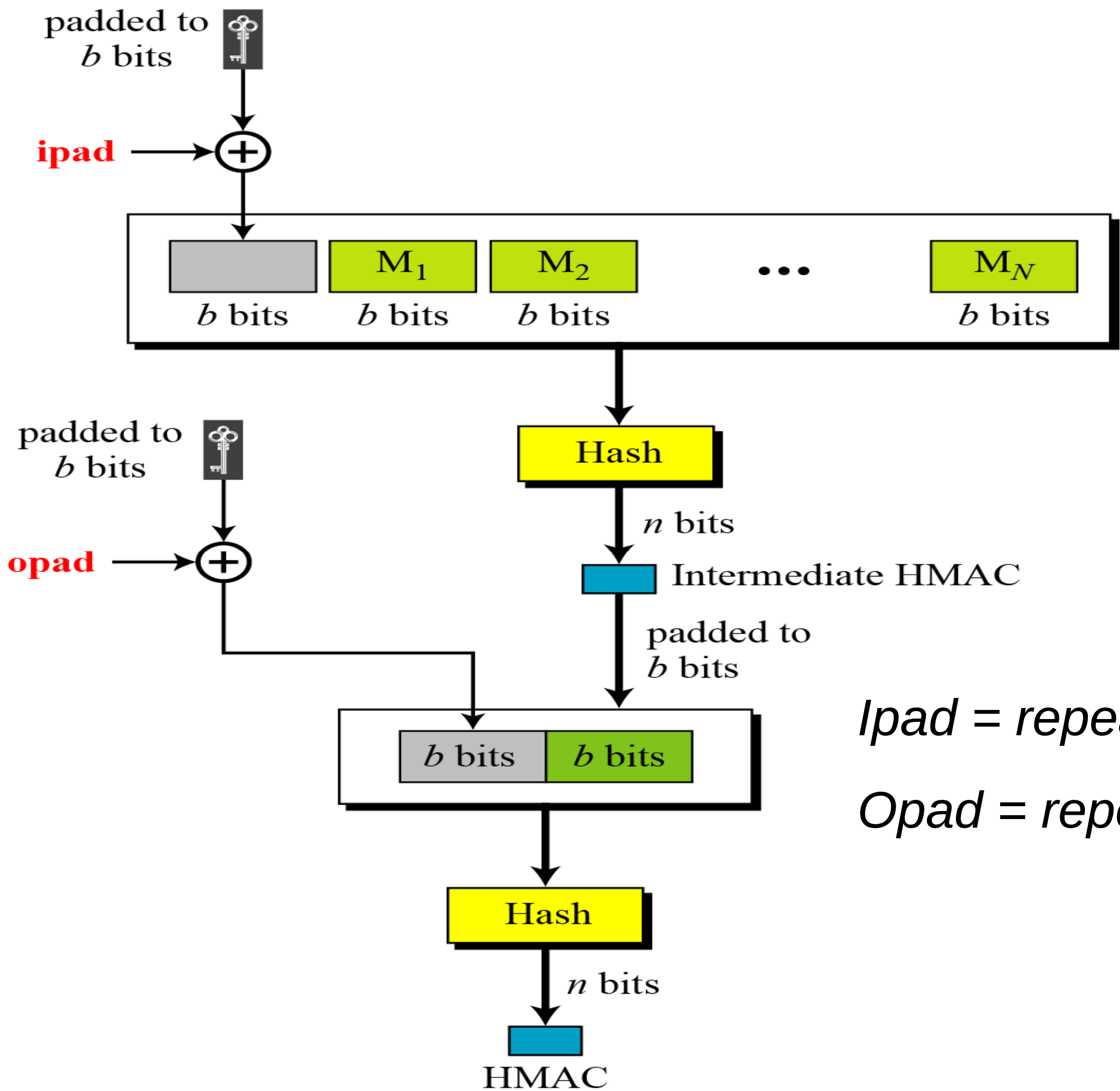
Other secret-key algorithms

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Message authentication

- A methodology to assure data integrity and to authenticate the data origin.
- One-way hash function:
  - A one-way hash function takes an arbitrarily long input message and produces a fixed-length, pseudorandom output called a hash
  - Knowing a hash, it is computationally difficult to find the message that produced that hash
  - It is almost impossible to find different messages that will generate the same hash
- Message Authentication Code (MAC).

Message authentication code (MAC)



Hashed MAC (HMAC)

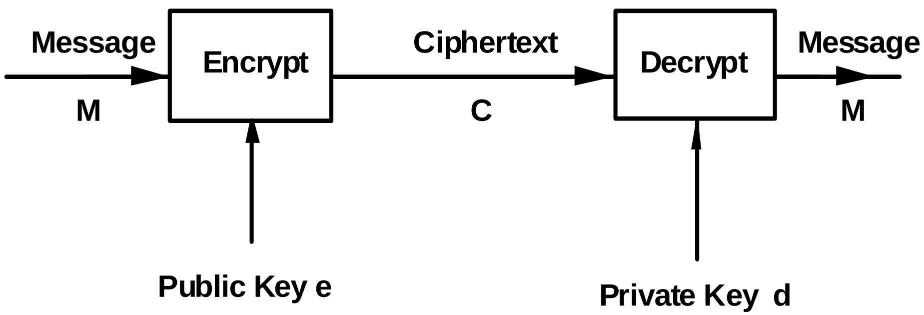
Ipad = repeated 36 in Hex

Opad = repeated 5c in Hex

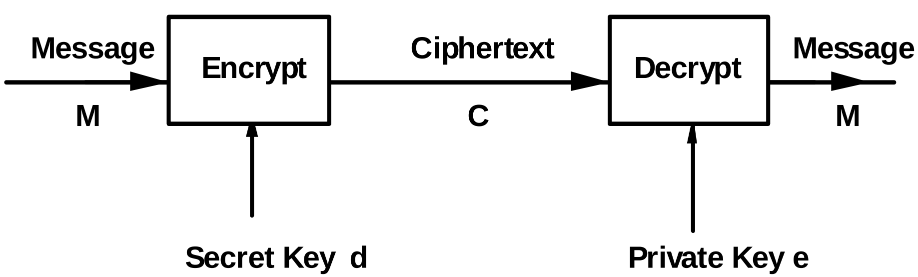
Public-key system

- Public key:
  - Publicly available to anyone
- Private key:
  - Only users themselves know their own private keys

Public-key system example – RSA (Rivest, Shamir and Adleman)



Public key system - Privacy



Public key system - Authentication

Two large prime numbers p and q are chosen 'at random' and multiplied together to form a modulus n

$$n = p.q$$

Since it is not possible to factorise large numbers - the modulus can be published without disclosing p and q.

A pair of keys, e = encryption key, d = decryption key, are found by solving the following equation

$$e.d \bmod (p-1)(q-1) = 1$$

A message M may then be enciphered with the encryption key e by raising M to the power e modulo n

$$\text{Ciphertext } C = M^e \bmod n$$

This message may be recovered by raising the cipher text C to the power d modulo n

$$M = C^d \bmod n$$

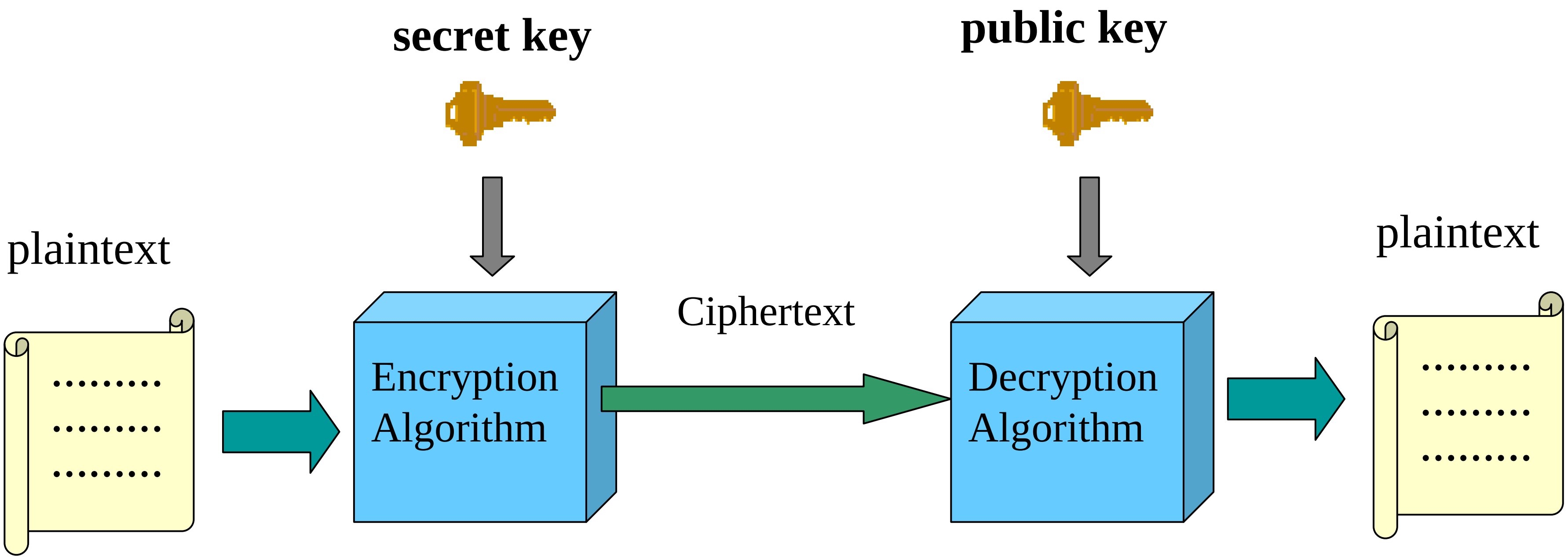
<u>Simple example</u>
Choose p = 3, q = 11, then n = 33
now (p-1)(q-1) = 20
so e.d mod 20 = 1
choose d = 7 then e = 3

if M = 5 (the message)

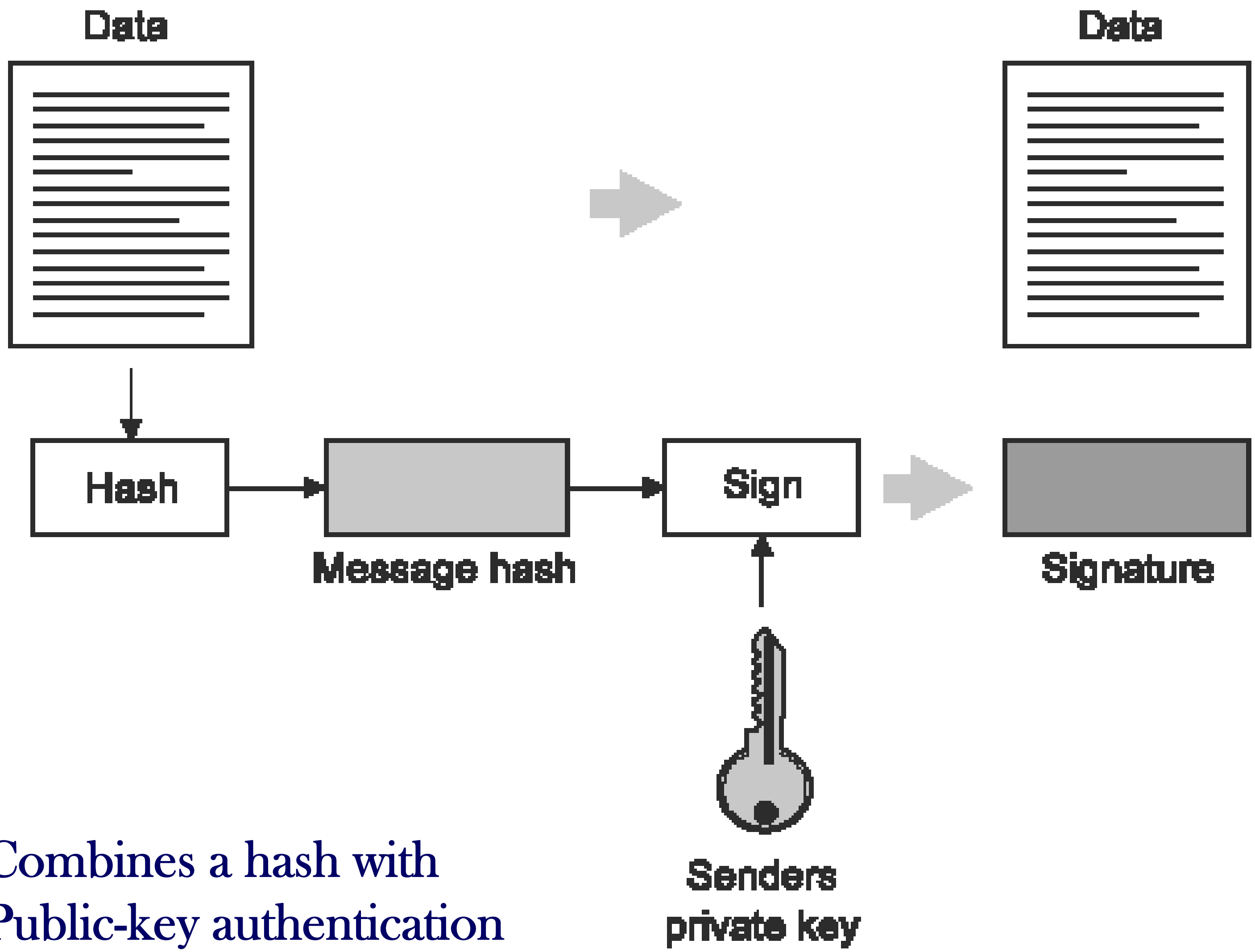
$C = 5^3 \bmod 33 = 26$, *Encryption*

$M = 26^7 \bmod 33 = 5$ *Decryption*

Integrity and authentication by public-key



Digital signature concept



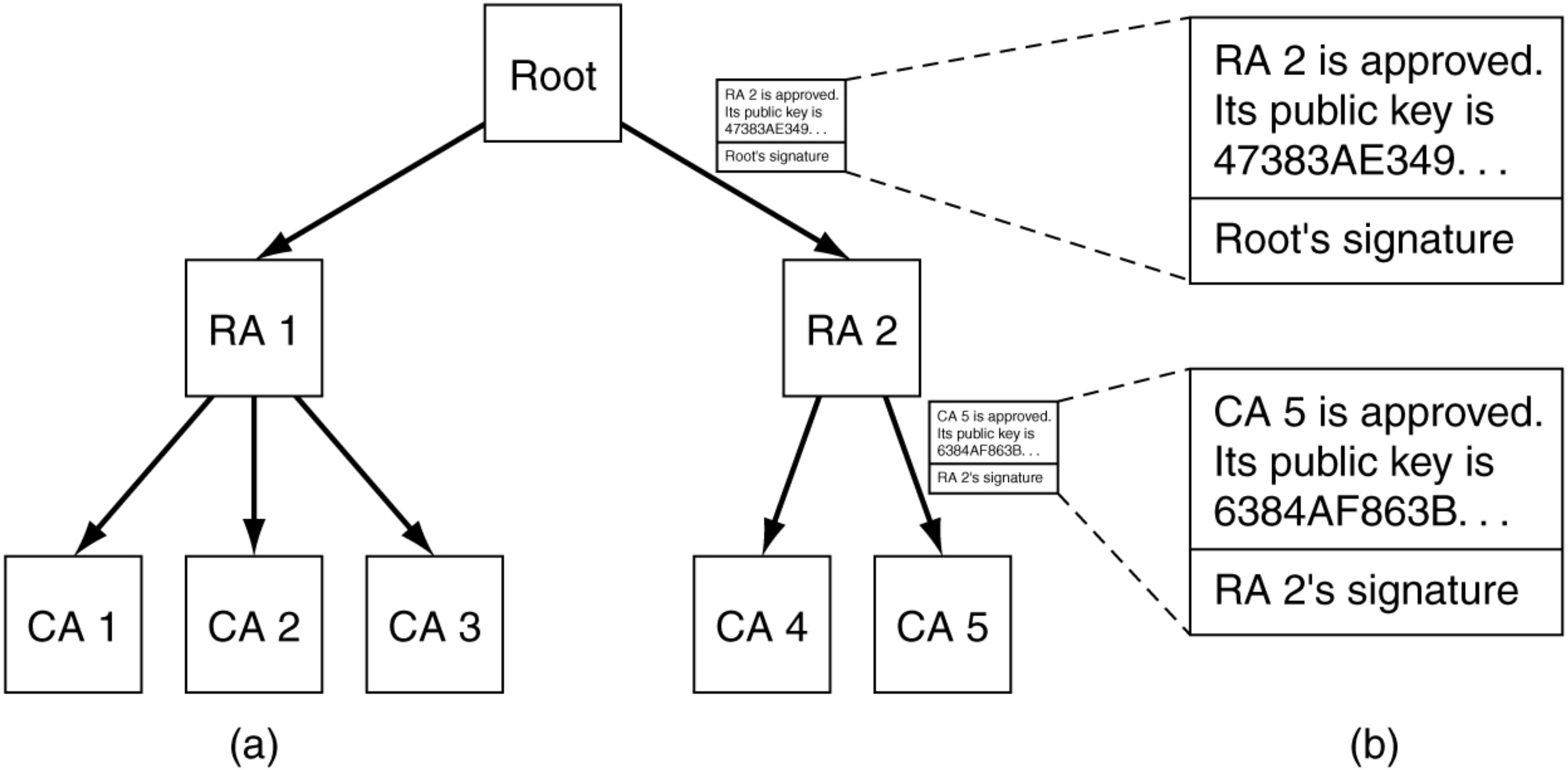
- Combines a hash with Public-key authentication

Digital certificates

- *Certificates bind a public key to a named entity*
- *Relies on the trust of the certificate authority*
- *A possible certificate and its signed hash, may look like this:*

I hereby certify that the public key 19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A belongs to Robert John Smith 12345 University Avenue Berkeley, CA 94702 Birthday: July 4, 1958 Email: bob@superdupernet.com
SHA-1 hash of the above certificate signed with the CA's private key

Public-Key Infrastructures (PKI)



RA: Regional Authority

CA: Certification Authority

Diffie-Hellman key exchange protocol - 1

- Diffie-Hellman key exchange protocol allows senders and recipients such as Alice and Bob to exchange a shared secret-key.
- Alice and Bob have to agree on two large prime numbers: n and g where (n - 1) / 2 is prime as well. These numbers can be public, so either of them can pick n and g and tell the other openly.
- Now Alice picks a large number (say 512-bits) x and keep it secret. Similarly, Bob picks a large prime number y.
- Alice initiates the key exchange protocol by sending message M1:
  - M1 = (n, g, $g^x \bmod n$)

Diffie-Hellman key exchange protocol - 2

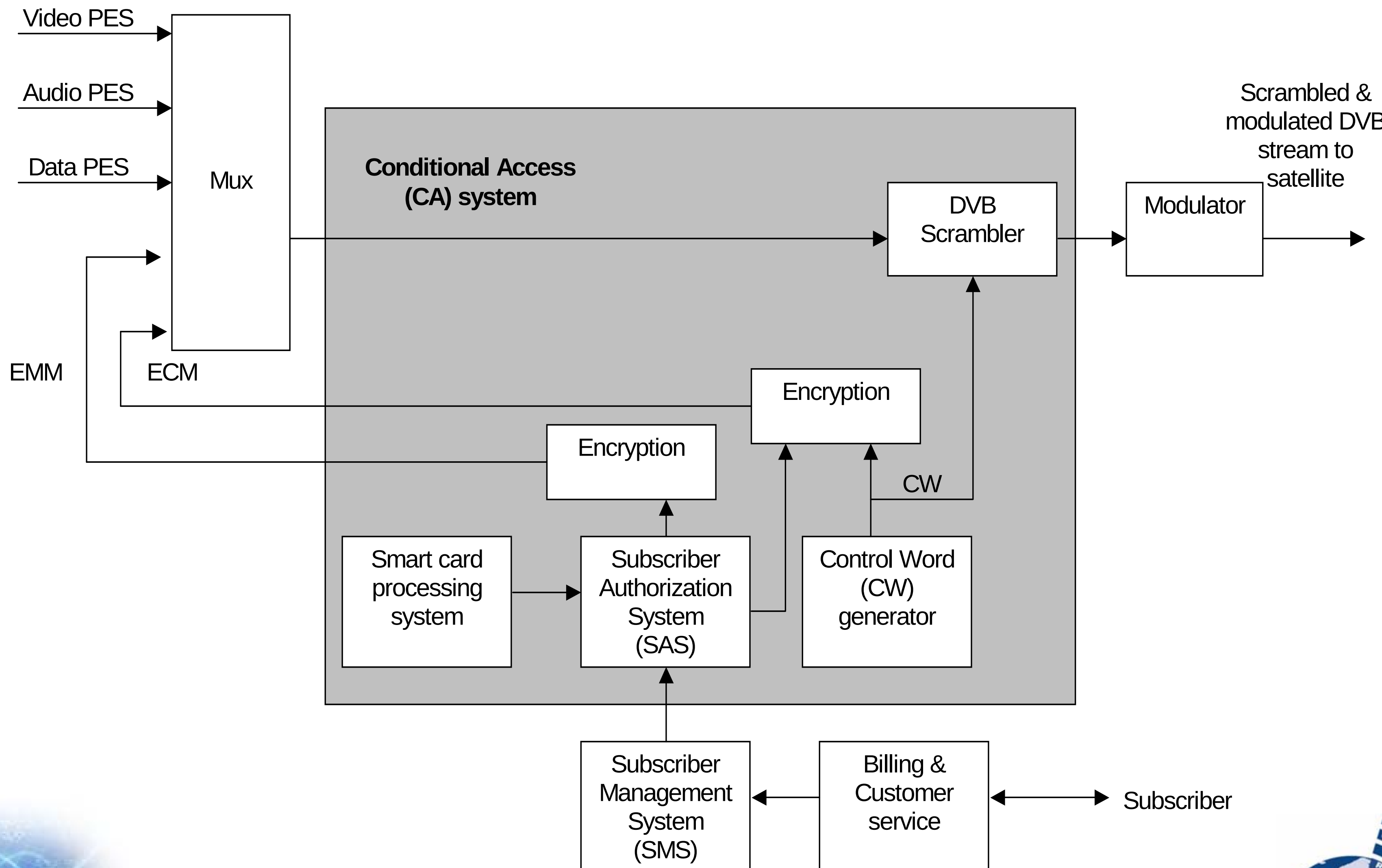
- Bob responds by sending message M2:
  - $M2 = (g^y \bmod n)$
- Now Alice can calculate the shared secret-key K:
  - $k = (g^y \bmod n)^x \bmod n = g^{yx} \bmod n = g^{xy} \bmod n$
- Also Bob can calculate the same secret-key k:
  - $k = (g^x \bmod n)^y \bmod n = g^{xy} \bmod n$
- The main weakness of Diffie-Hellman protocol is that neither Alice nor Bob can authenticate the origin of messages M2 and M1 respectively. One solution is to add Alice's digital signature to message M1 and Bob's digital signature to M2.

Examples of Security Systems in Communication Network

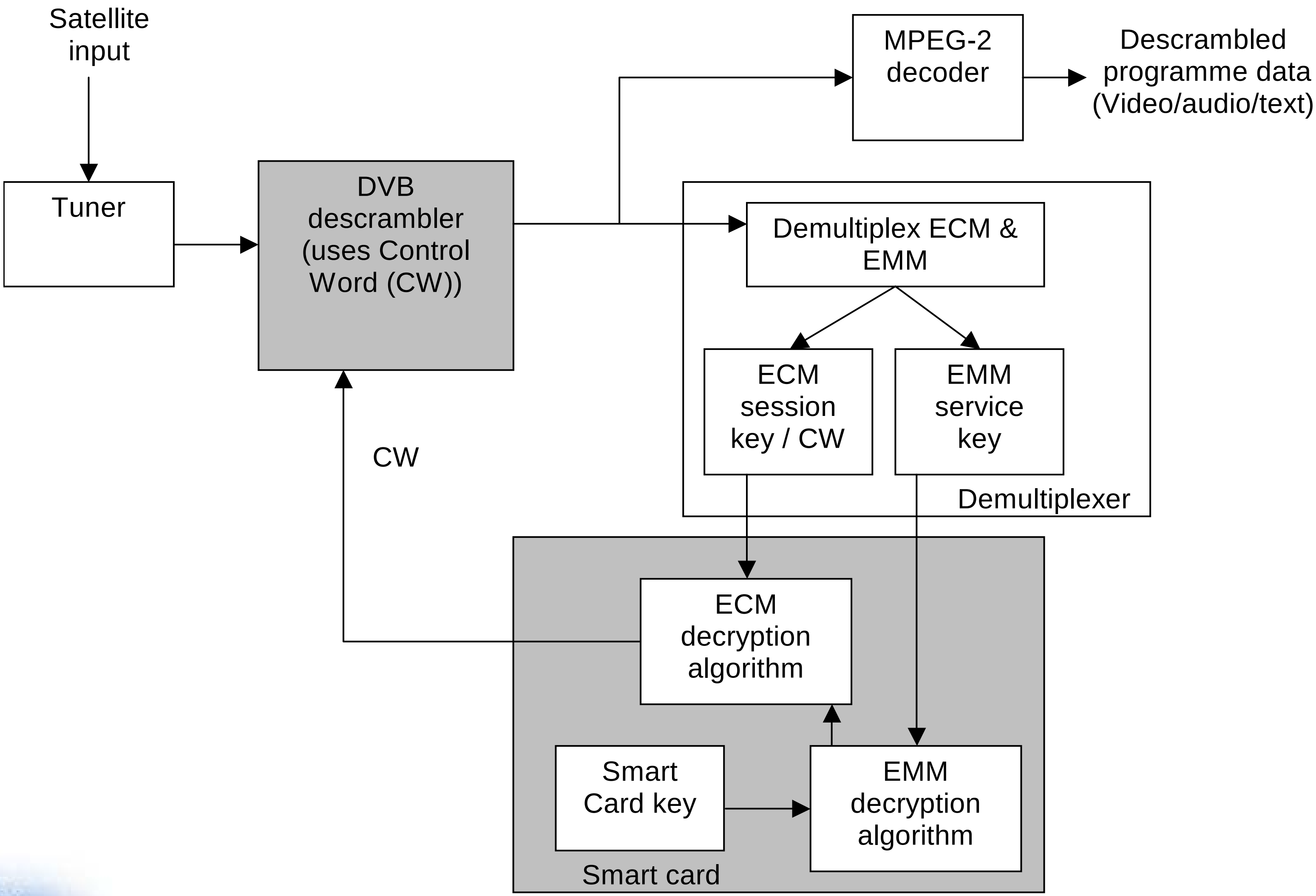
Digital Video Broadcasting (DVB) - introduction to conditional access

- The scrambling/descrambling function aims to make the service incomprehensible to unauthorised users:
  - Descrambling can be achieved by any receiver having an appropriate descrambler and holding a secret Control Word (CW).
- The CW is encrypted with a service key and sent inside a dedicated message (DVB tables) called Entitlement Control Messages (ECMs).
- The service key is encrypted with the smart card key and sent inside a dedicated message called Entitlement Management Messages (EMMs).

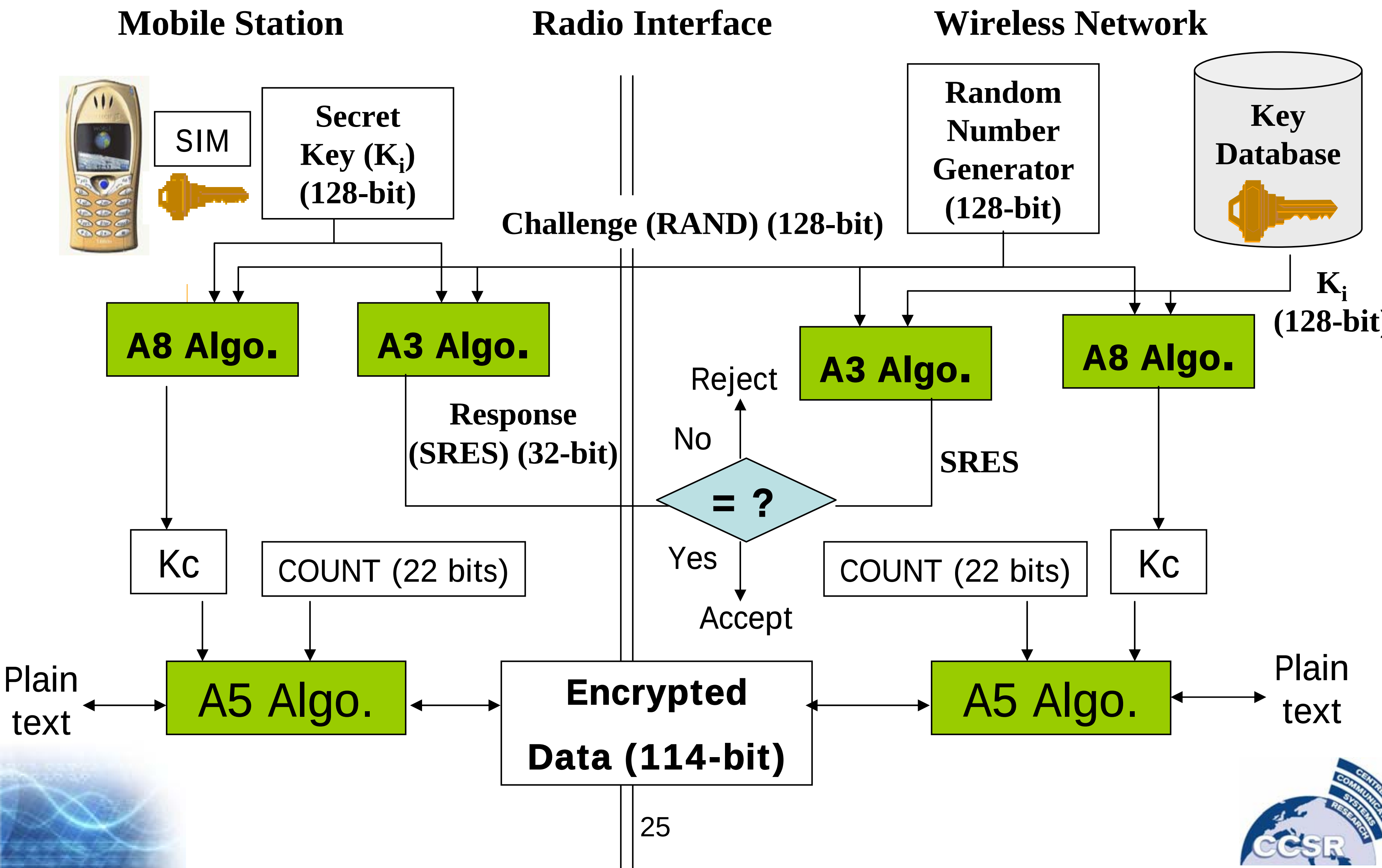
DVB conditional access - encryption



DVB conditional access - descrambling

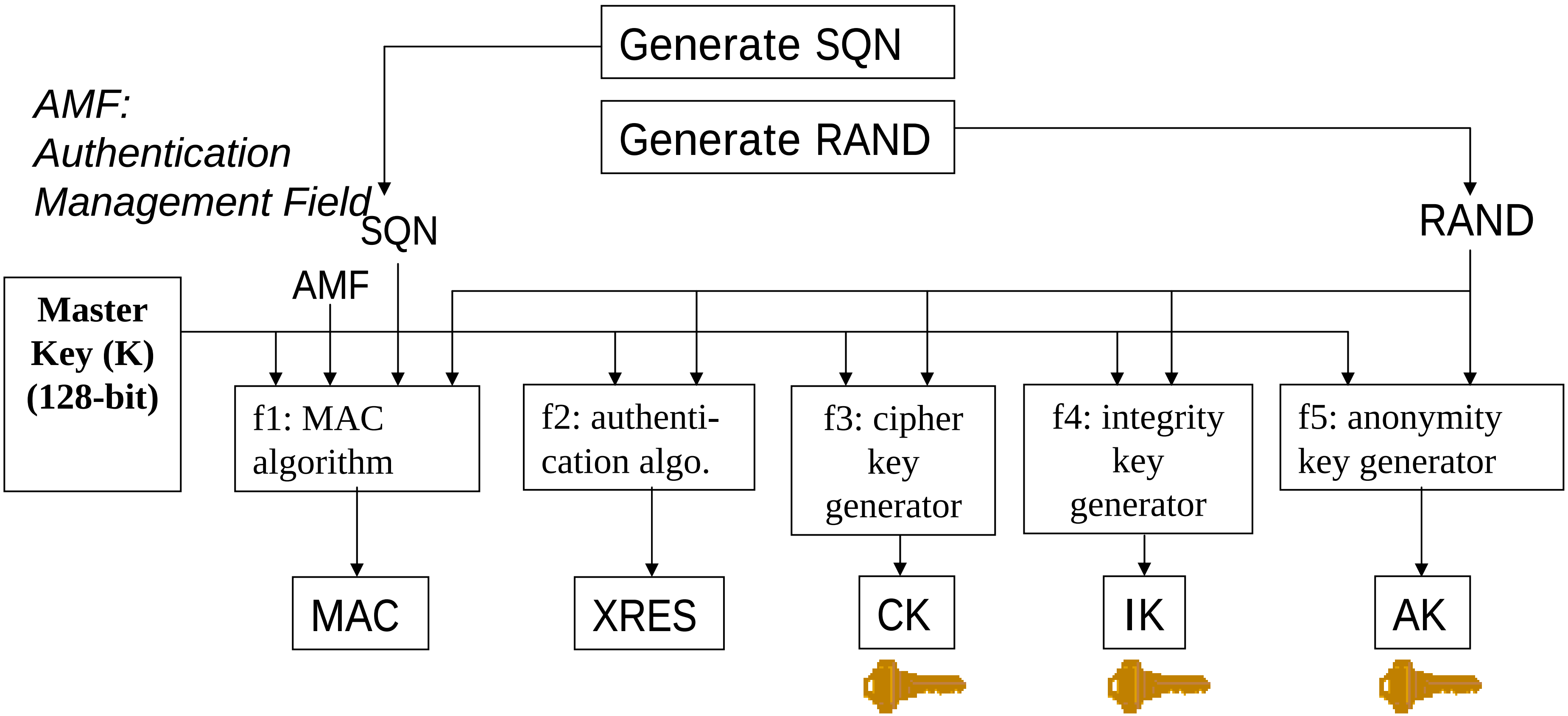


Mobile networks - GSM security system



Mobile networks - 3G: authentication vector

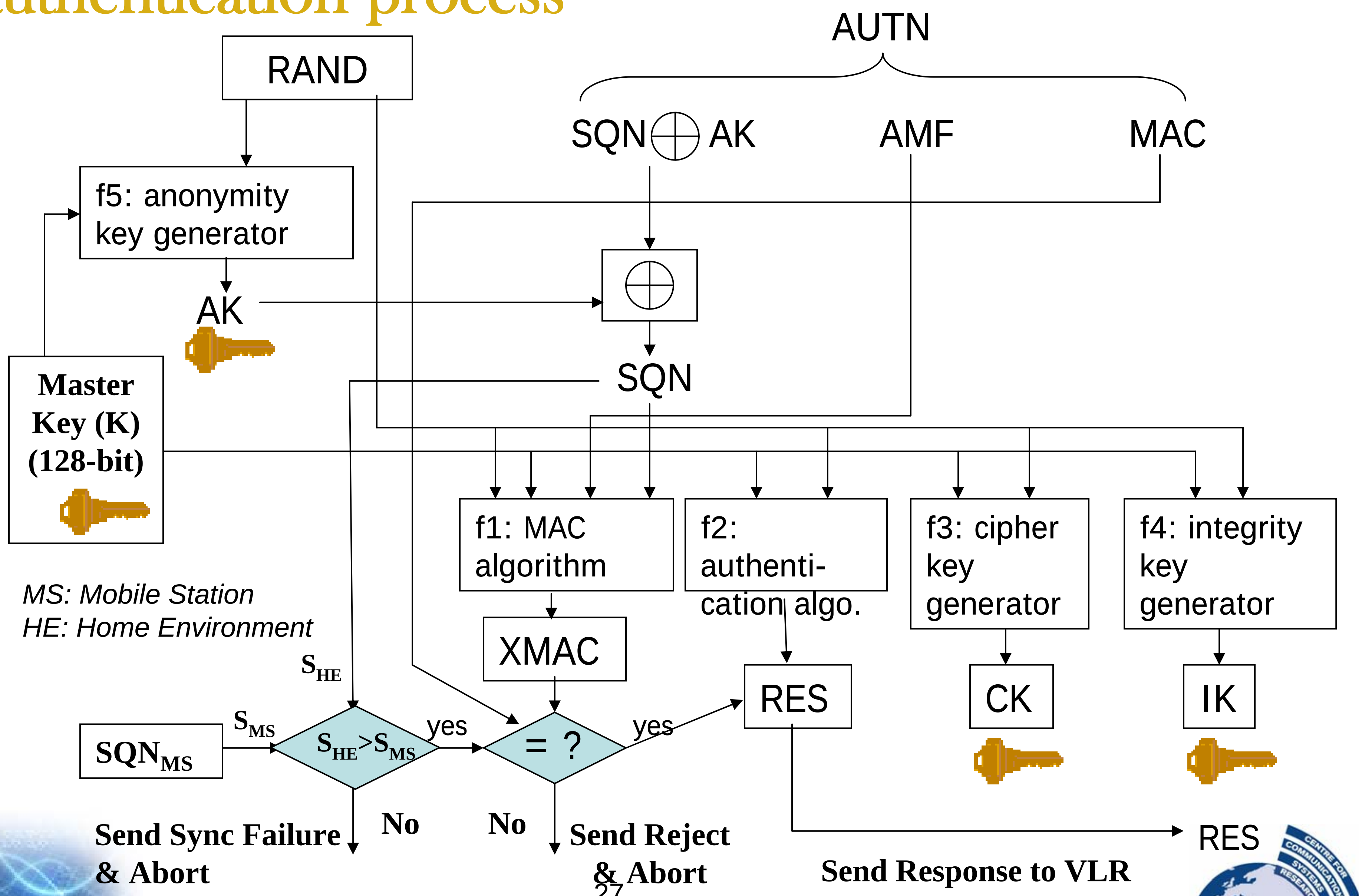
AMF: Authentication Management Field



AUTN := SQN $\oplus$ AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

Mobile networks - 3G: authentication process

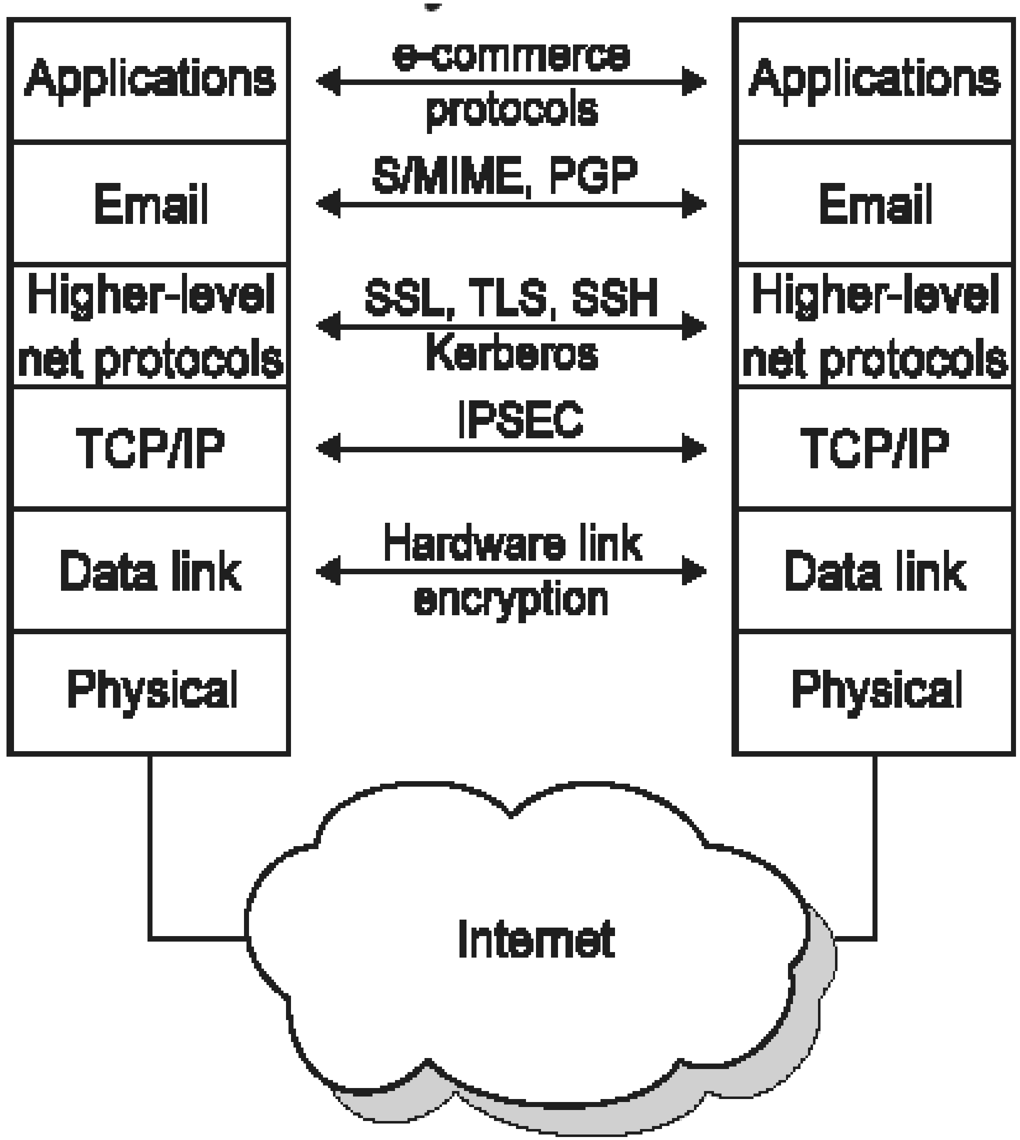


Network layer security (IPSec)

Internet security - introduction

- **Internet security is difficult because:**
  - the internet spans a very wide area across political and organisational boundaries
  - it involves how and when communicating parties (such as users, computer, services and network) can trust each other, as well as understanding the network hardware and protocols
- **Mechanics for Internet security:**
  - access control using firewalls
  - IPSec
  - Application layer security

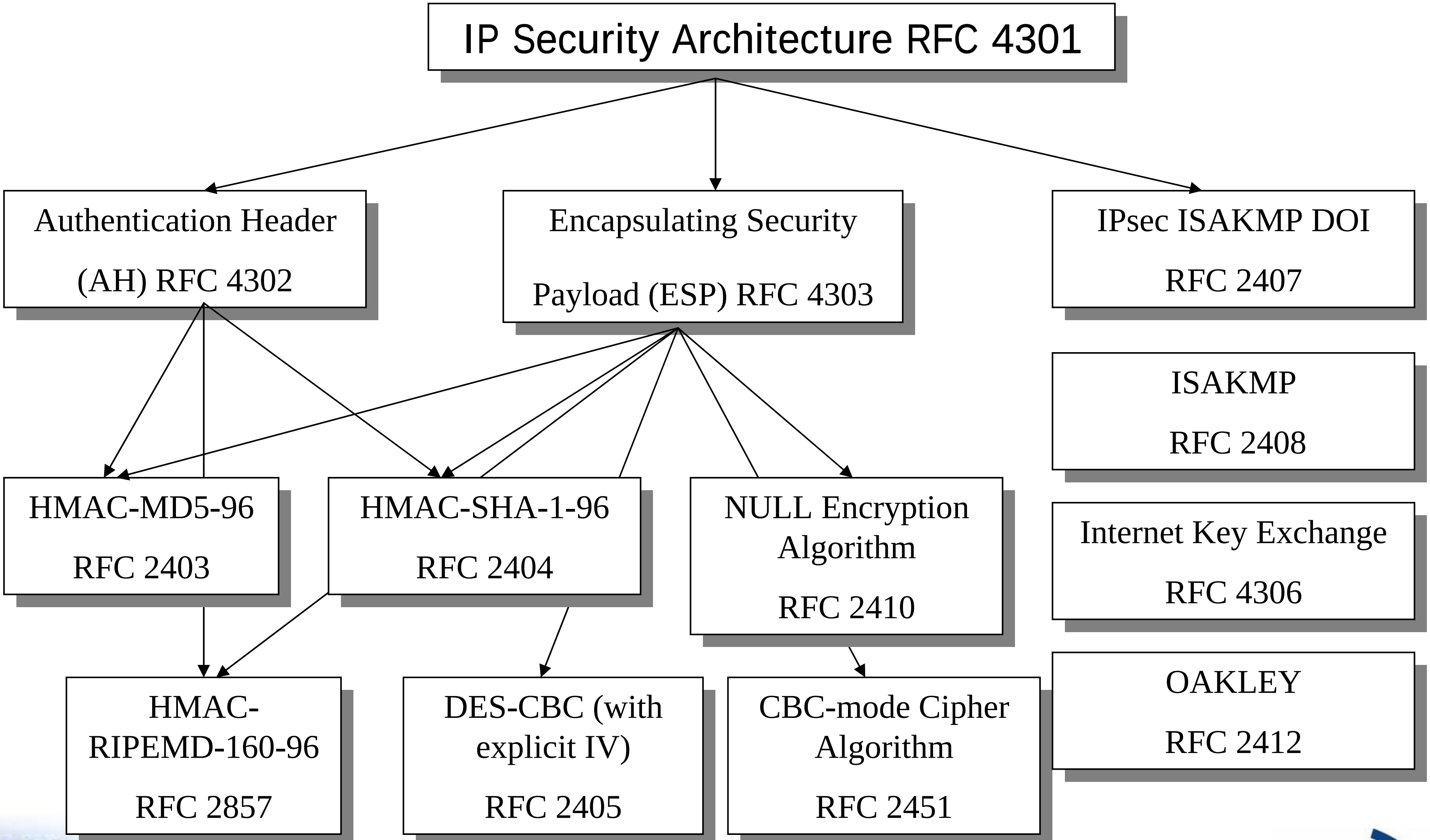
Internet security protocol layers



IPSec overview

- IPSec provides a set of security services for traffic at the IP layer, in IPv4 and IPv6, through the use of IP Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols.
- Important IPsec databases:
  - Security Policy Database (SPD): Defined the protection offered by IPsec: PROTECTed using IPsec security services, DISCARDed, or allowed to BYPASS
  - Security Association Database (SAD): Which encryption and integrity keys are associated with each IP packet
- Two modes of operations:
  - Transport mode: End-to-end principle is observed
  - Tunnel mode

Family of IPSec protocols



IPSec: Authentication Header (AH)

Transport mode:

IPv4

Original IP header	AH	TCP	Data

coverage of authentication (except for mutable fields)

IPv6:

Original IP header	Hop-by-hop extensions	AH	End-to-end extensions	TCP	Data

coverage of authentication (except for mutable fields)

Tunnel mode:

IPv4 and IPv6:

Encapsulating IP header	AH	Original + ext IP header fields	TCP	Data

coverage of authentication (except for mutable fields)

IPSec: Encapsulated Security Payload (ESP)

Transport mode:

IPv4

	ESP header		ESP payload		ESP trailer	
Original IP header	SPI	Seq Nr.	TCP	Data	Padding	Auth Data

coverage of confidentiality

coverage of authentication

IPv6:

		ESP header		ESP payload			ESP trailer	
Original IP header	Hop-by-hop extensions	SPI	Seq Nr.	End-to-end extensions	TCP	Data	Padding	Auth Data

coverage of confidentiality

coverage of authentication

Tunnel mode:

IPv4 and IPv6:

		ESP header		Original IP datagram			ESP trailer	
New IP header	New extensions	SPI	Seq Nr.	Original IP header	TCP	Data	Padding	Auth Data

coverage of confidentiality

coverage of authentication

IPSec applications

- End-to-end security
- VPN (virtual private network) with IPsec (Satellite example)
- End-to-end with VPN security
- Secured remote access

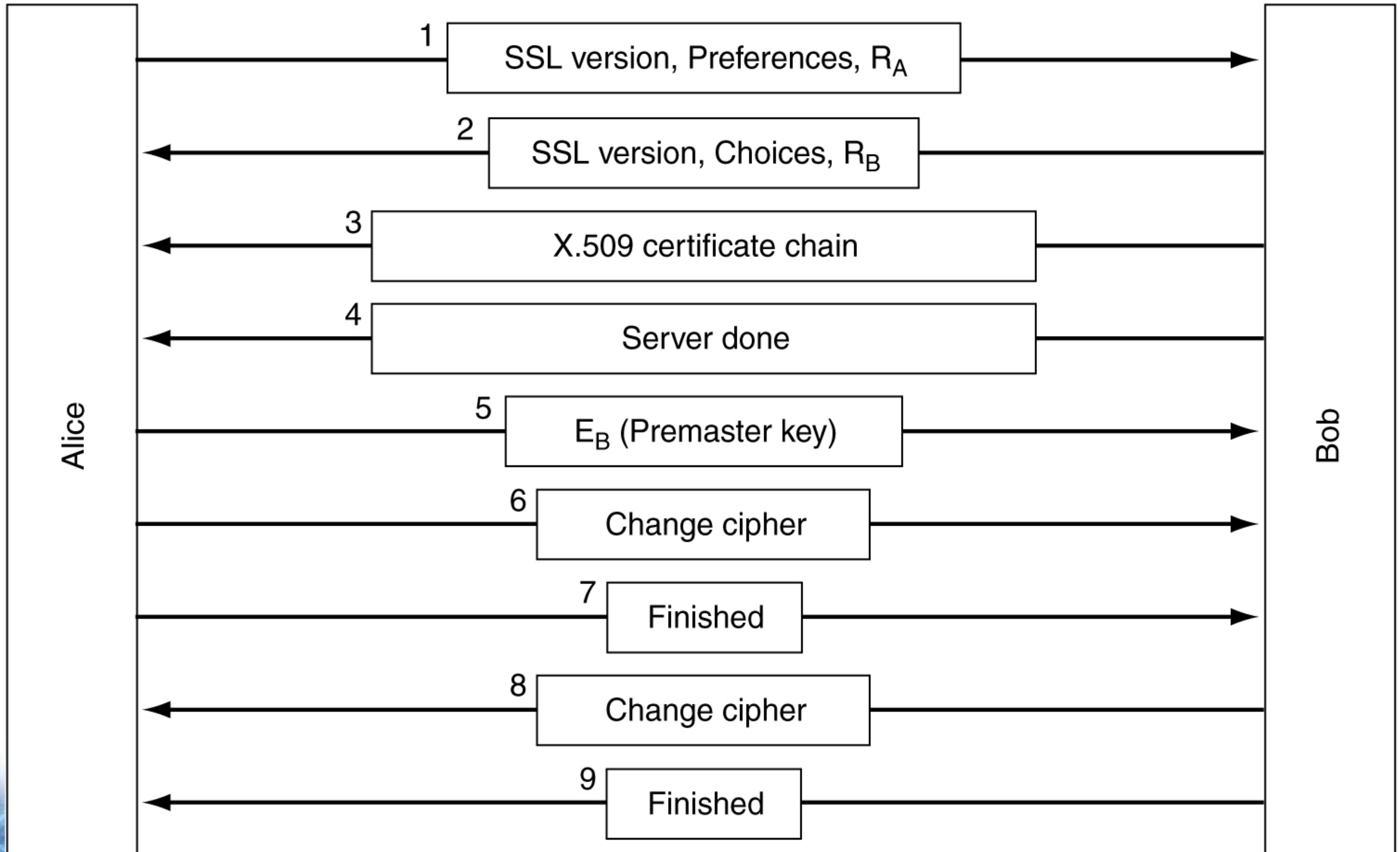
Limitations of IPSec - problems with middle entities

- IPSec in transport mode encrypts all data above IP layer. IPSec in tunnel mode encrypts all data including the original IP layer. However it conflicts with:
  - Satellite bandwidth acceleration: Performance Enhancing proxies (PEPs) need to inspect TCP and HTTP header.
  - Traffic Analysis: Service provider might require monitoring of their network traffic for management and QoS purposes.
  - Traffic Engineering: Flow classification is essential in supporting a variety of classes of service and QoS.

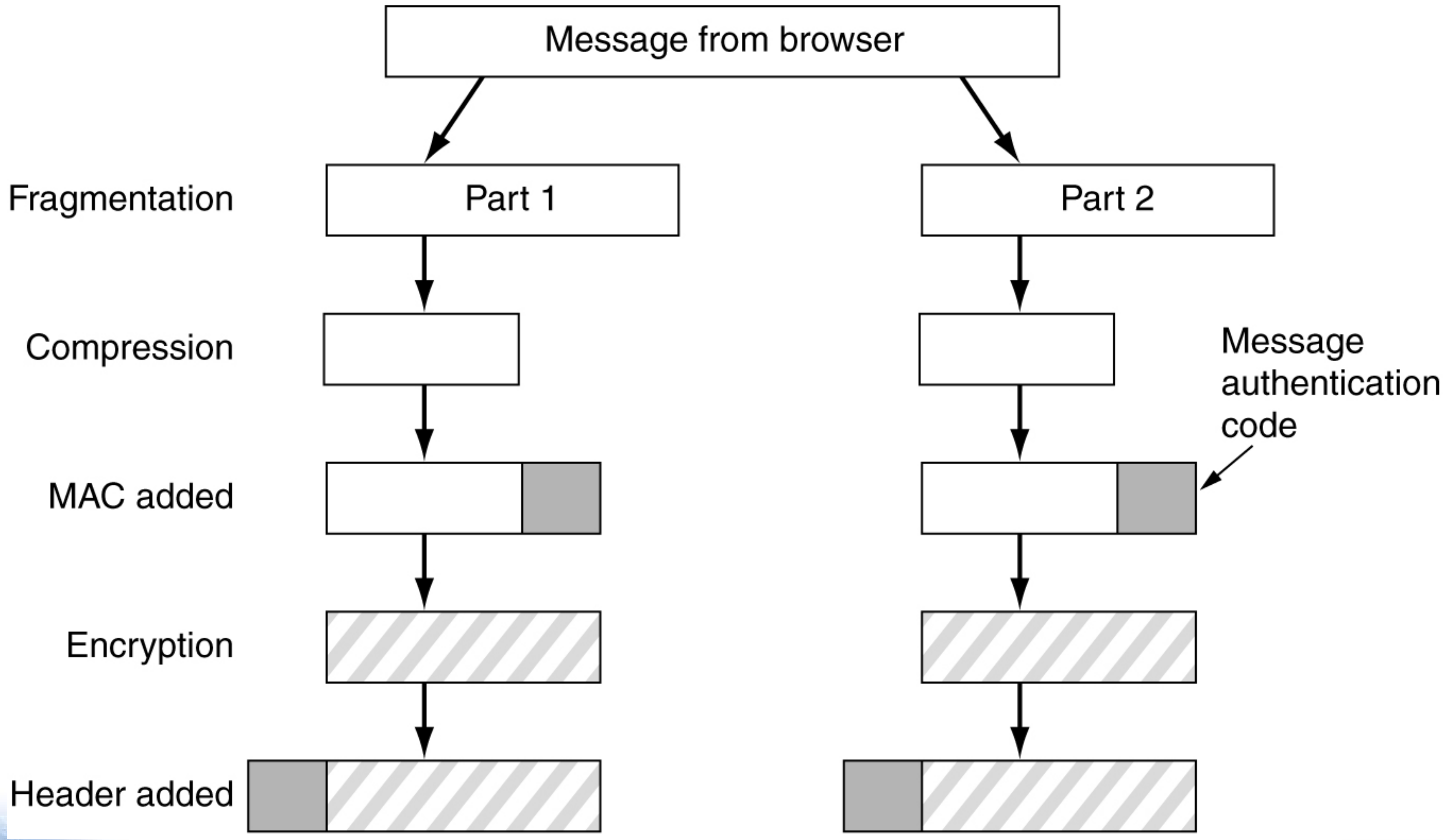
Secure Sockets Layer (SSL)

Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

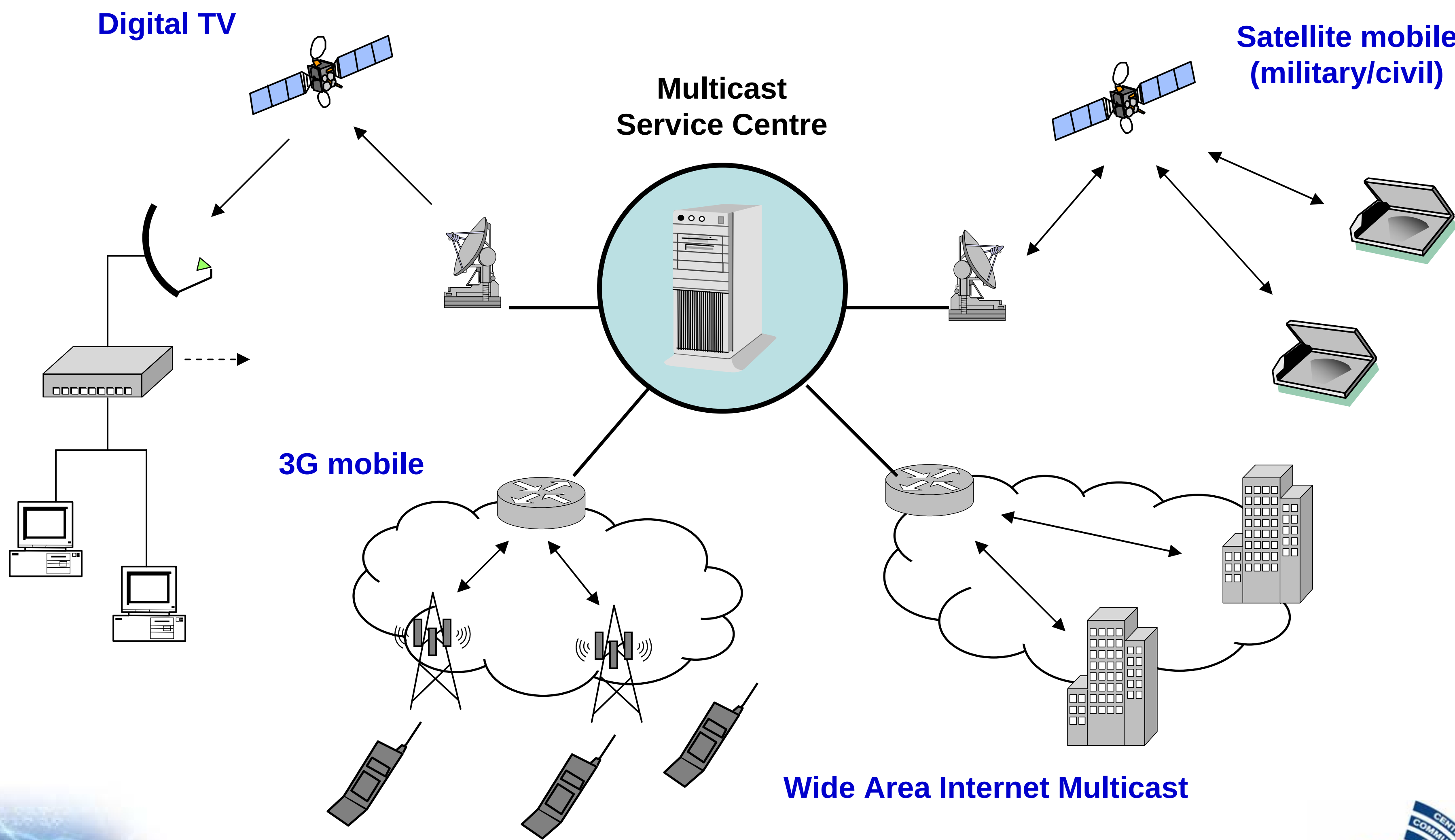
SSL - Connection establishment



SSL – Data transmission



Example multicast applications

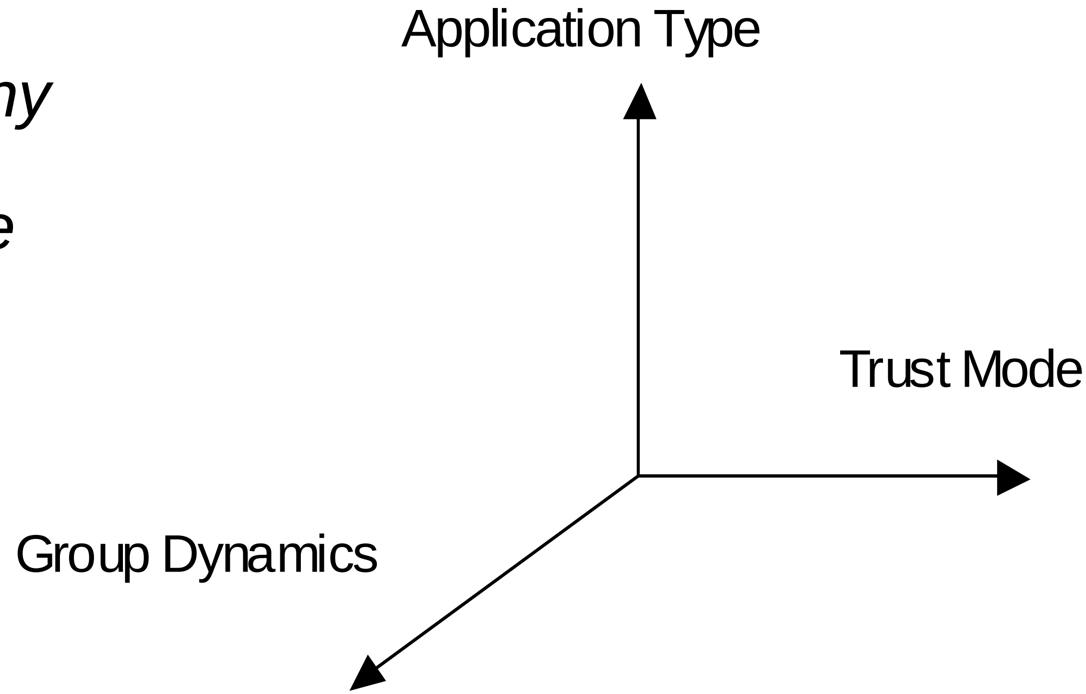


Secure group communications

- The IPSEC standards and its related technologies, are aimed mainly at unicast transmissions between one sender and one receiver:
  - Securing multicast is a difficult issue because it involves group communications
- MSEC is an IETF Working Group focusing on standardizing building blocks and protocols for secure group communications and multicast.
- In addition, there is a Research Group called GSEC which is an IRTF (Internet Research Task Force) group formed to discuss research issues related to multicast security.

Factors affecting secure multicast

- *Applications: One-to-many and many-to-Many*
- *Group dynamics: Size and behaviour*
- *Trust model: Security policies and key management*



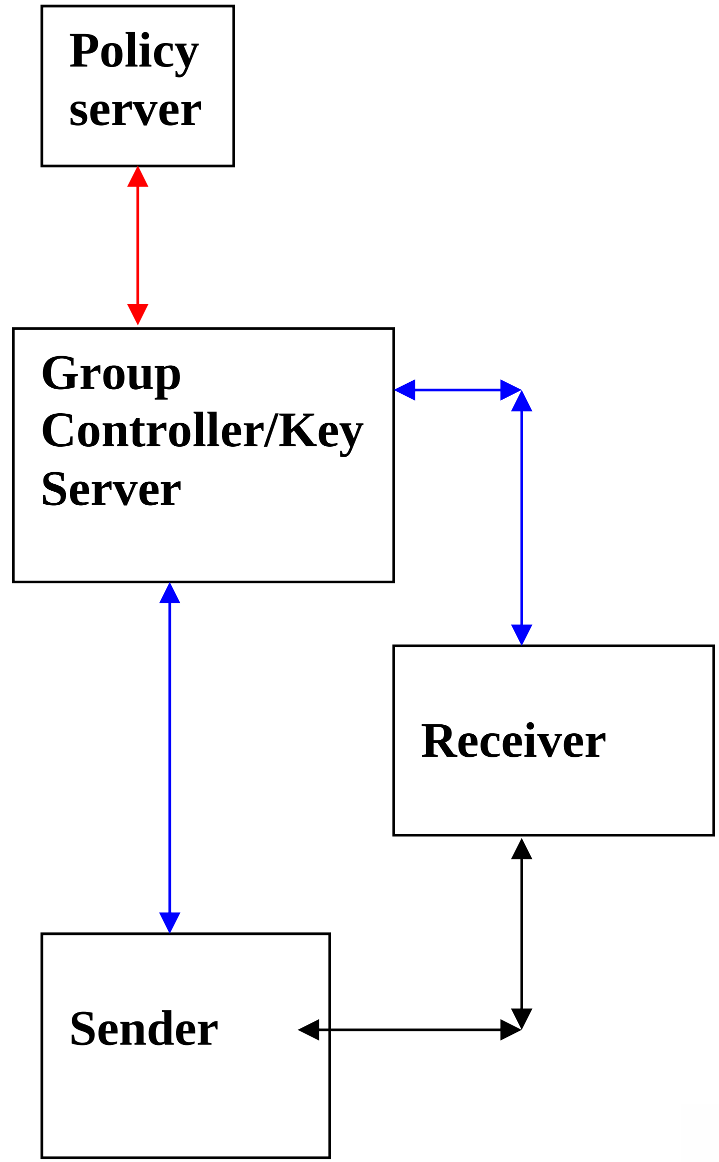
- *Critical issues:*
  - ✓*Secure group management*
  - ✓*Key distribution for large groups*

Secure Multicast architecture - Centralised

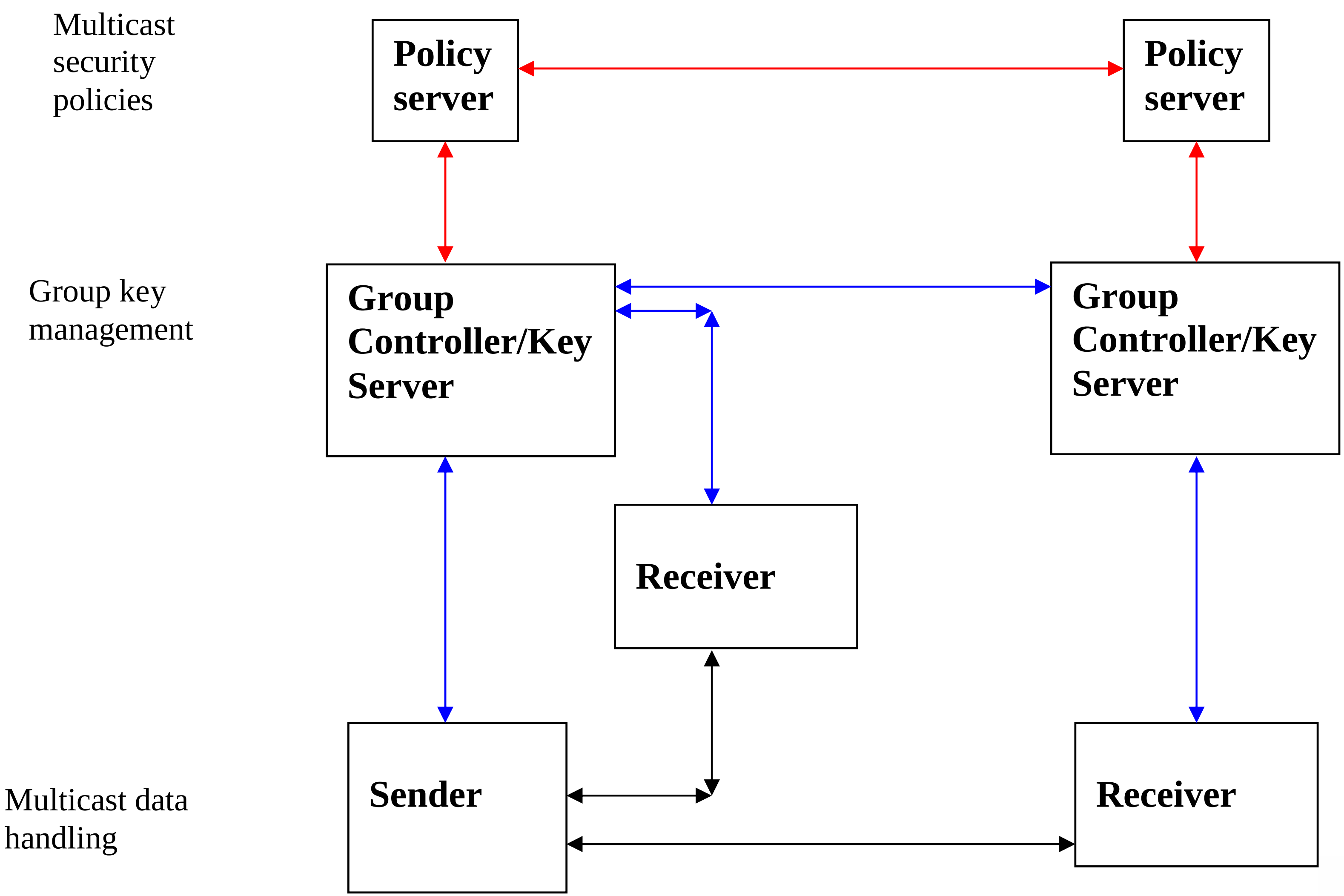
Multicast security policies

Group key management

Multicast data handling



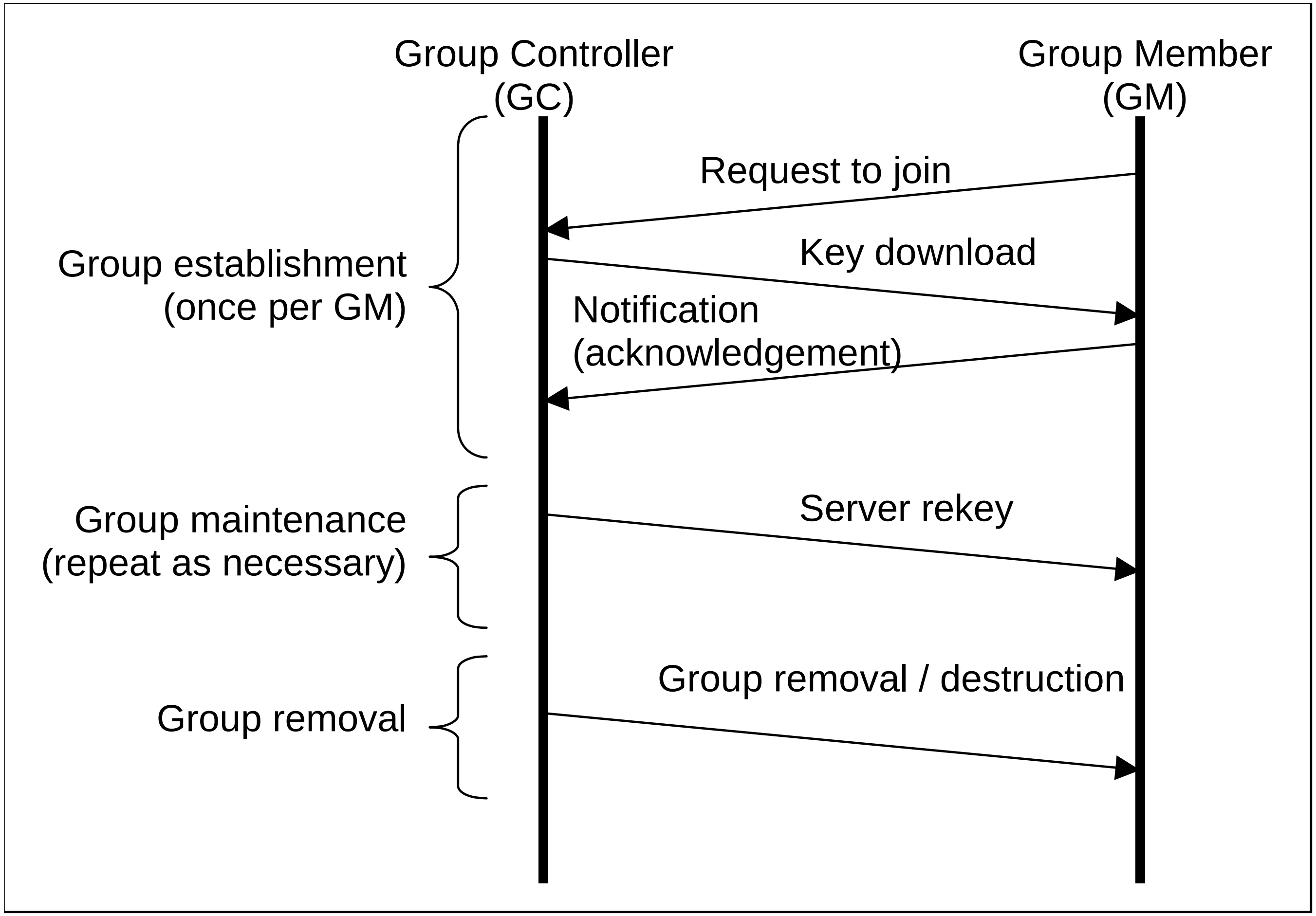
Secure Multicast architecture - Distributed



Group key management protocols

- **Group Secure Association Key Management Protocol (GSAKMP):**
  - It includes mechanisms for group policy dissemination, group key dissemination, and group rekey operation
- **Multimedia Internet KEYing (MIKEY):**
  - The MIKEY protocol is used for peer-to-peer, simple one-to-many, and small-size (interactive) groups, and is intended for use in real-time applications. One of the main multimedia scenarios is the conversational multimedia scenario, where users may interact and communicate in real-time
- **Group Domain of Interpretation (GDOI):**
  - GDOI (RFC 3547) is an ISAKMP Domain of Interpretation (DOI) for group key management to support secure group communications. It proposes new exchanges according to the ISAKMP and IKE standard

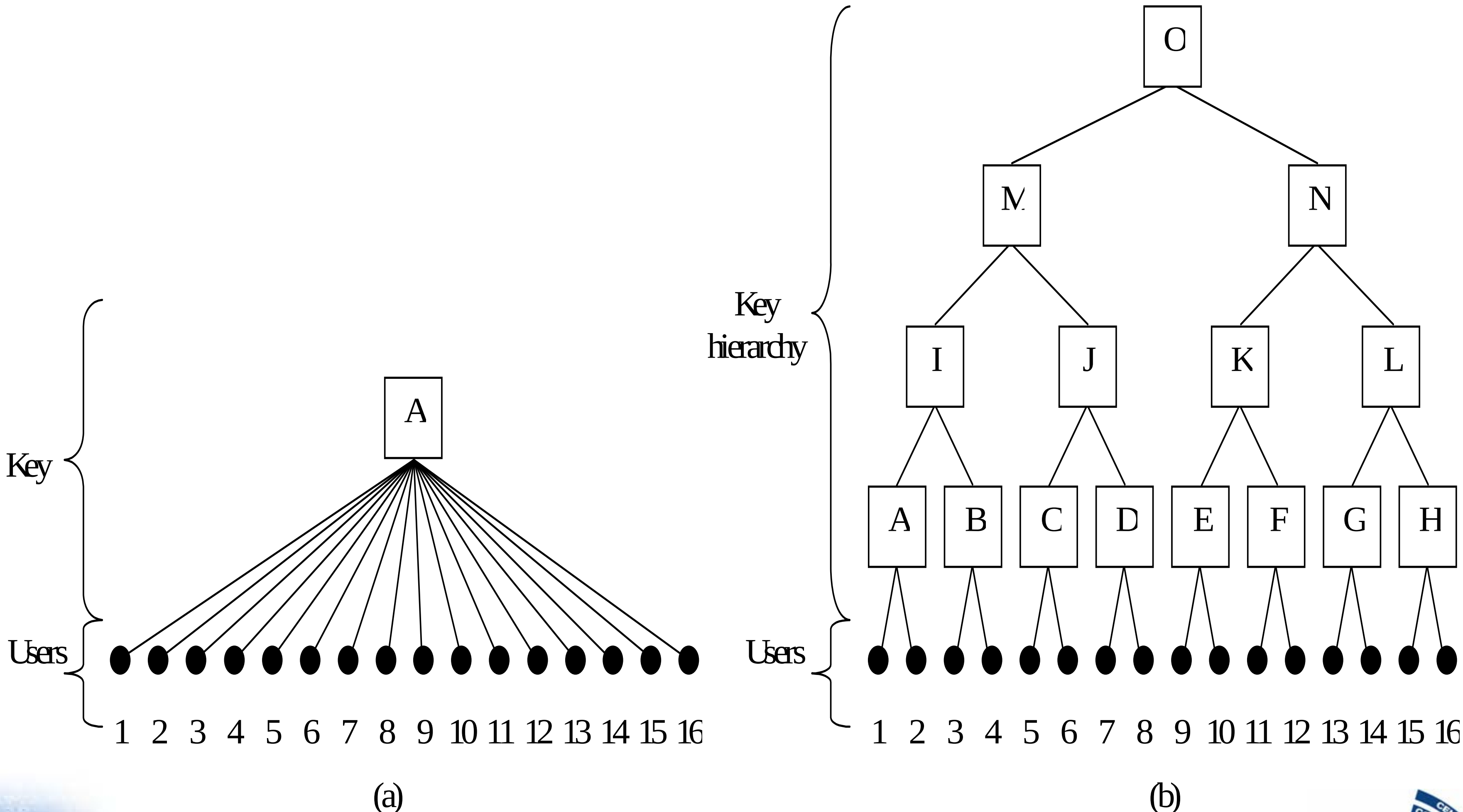
GSAKMP message sequence



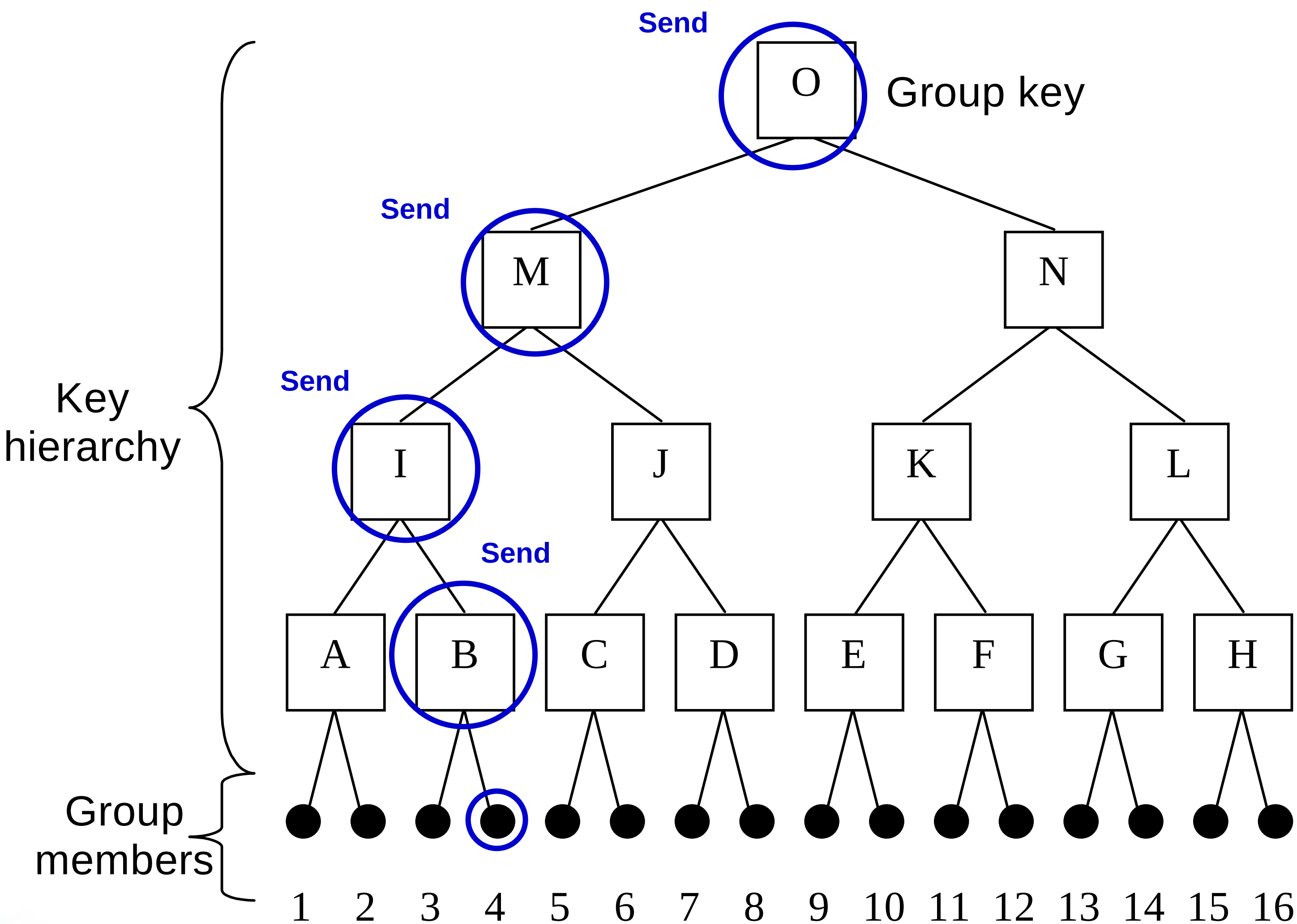
Key distribution: Logical Key Hierarchy (LKH) - 1

- RFC 2627 defines the Logical key hierarchy (LKH) as a mechanism for improving the scalability of multicast key management.
- LKH provides the following two features:
  - Secure removal of a compromised user from the multicast group.
  - Key transmission efficiency.

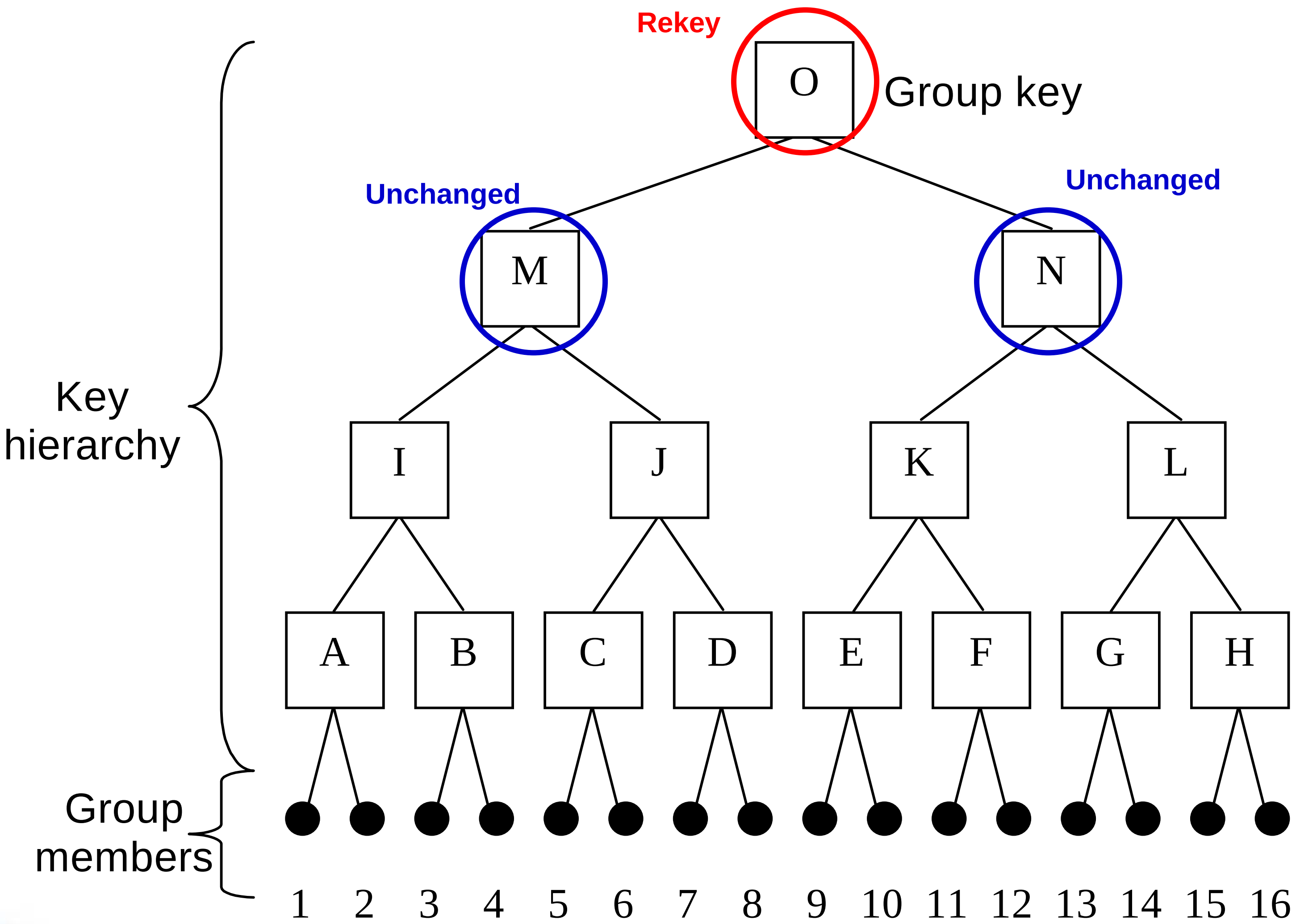
Key distribution:
Logical Key Hierarchy (LKH) - 2



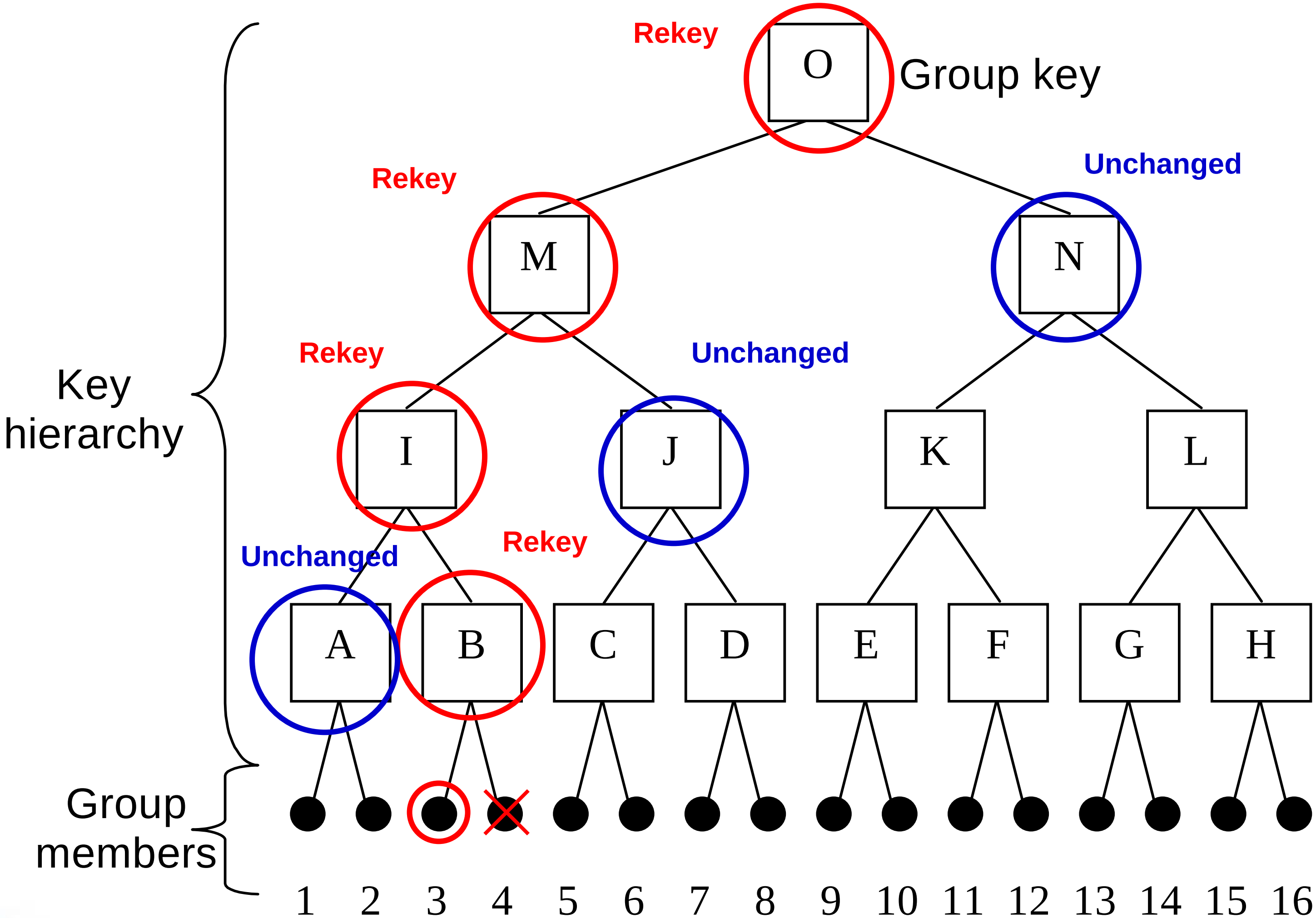
LKH – Tree (user 4 joins)



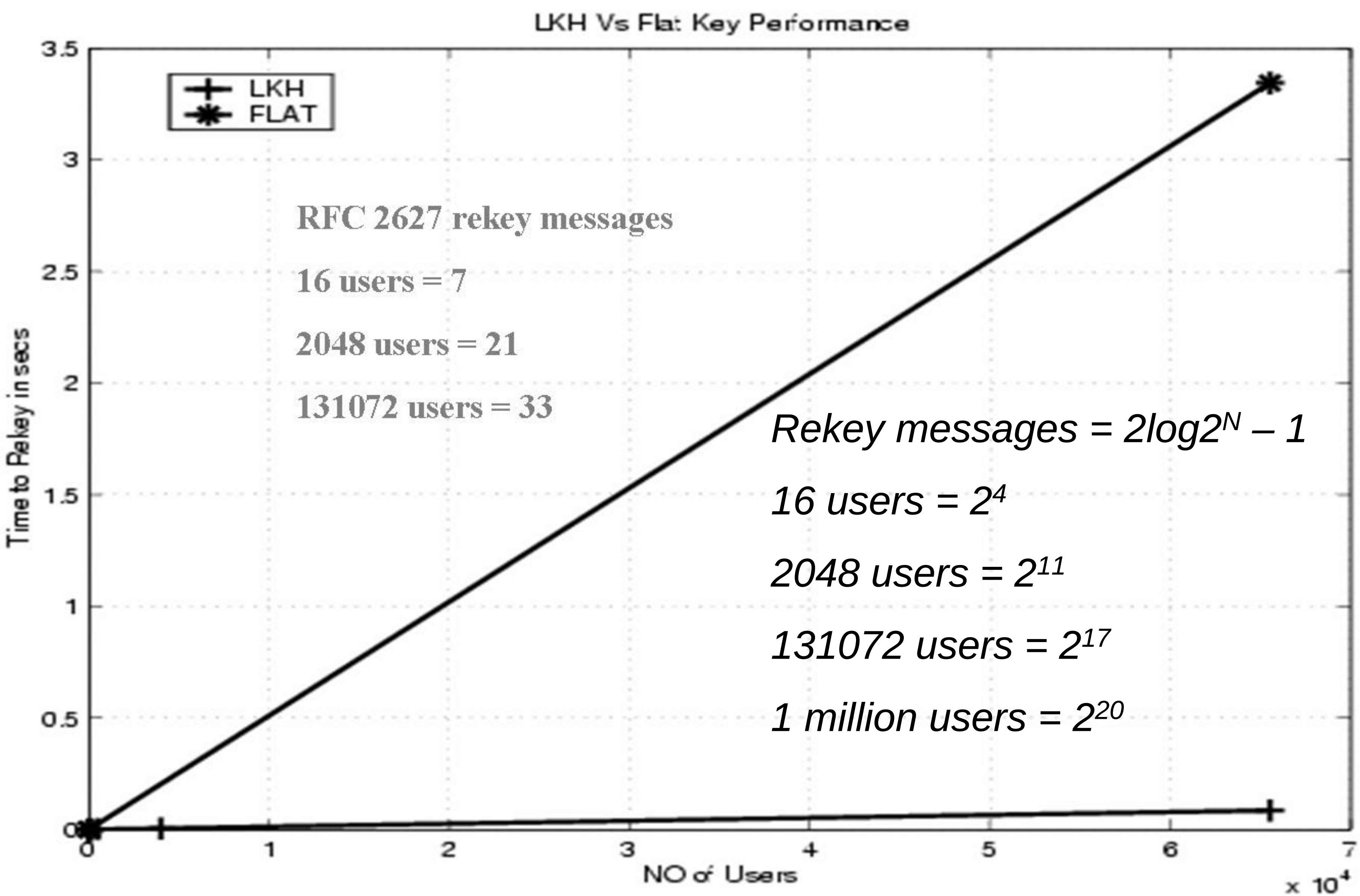
LKH – Tree (group rekey)



LKH – Tree (removal of member 4)



Screen capture for LKH

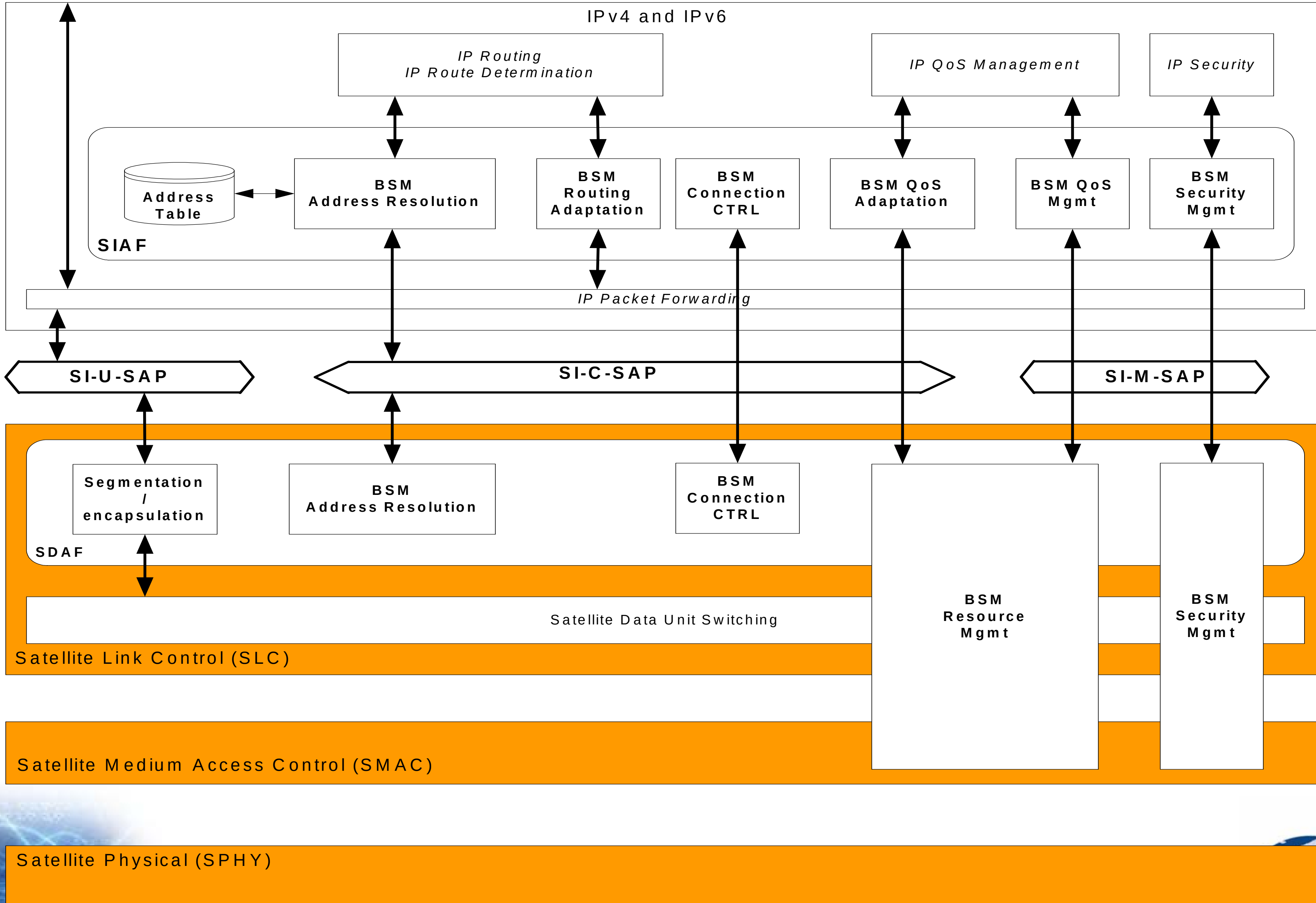


Performance Enhancing proxies (PEPs)

ETSI - BSM Architecture

- The Broadband Satellite Multimedia (BSM) architecture divides the protocol stack into 2 parts:
  - Satellite Independent (SI) upper layers
  - Satellite Dependent (SD) lower layers
- The upper layers contain a set of common IP interworking functions:
  - Define Satellite Independent Adaptation Functions (SIAF)
  - Common ways of handling Quality of Service (QoS); Addressing; Multicast and Security etc.
- Satellite Independent Service Access Point (SI-SAP) defined as a common interface between the upper and lower layers.
- The lower layers contain the satellite specific functions:
  - The lower layers are closely tied to the payload capability of the satellite

BSM Protocol Stack



Performance Enhancing Proxies (PEPs) types and layering

- Transport Layer PEPs (T-PEP): T-PEPs interact with TCP. Such an implementation is sometimes called TCP Performance Enhancing Proxy (TCP PEP). The term TCP spoofing is sometimes used synonymously for TCP PEP functionality.
- Application layer PEPs (A-PEP): Application layer PEPs operate above the transport layer. An example of application layer proxy is a Web cache. A-PEPs can be implemented to improve the HTTP performance over wireless links.

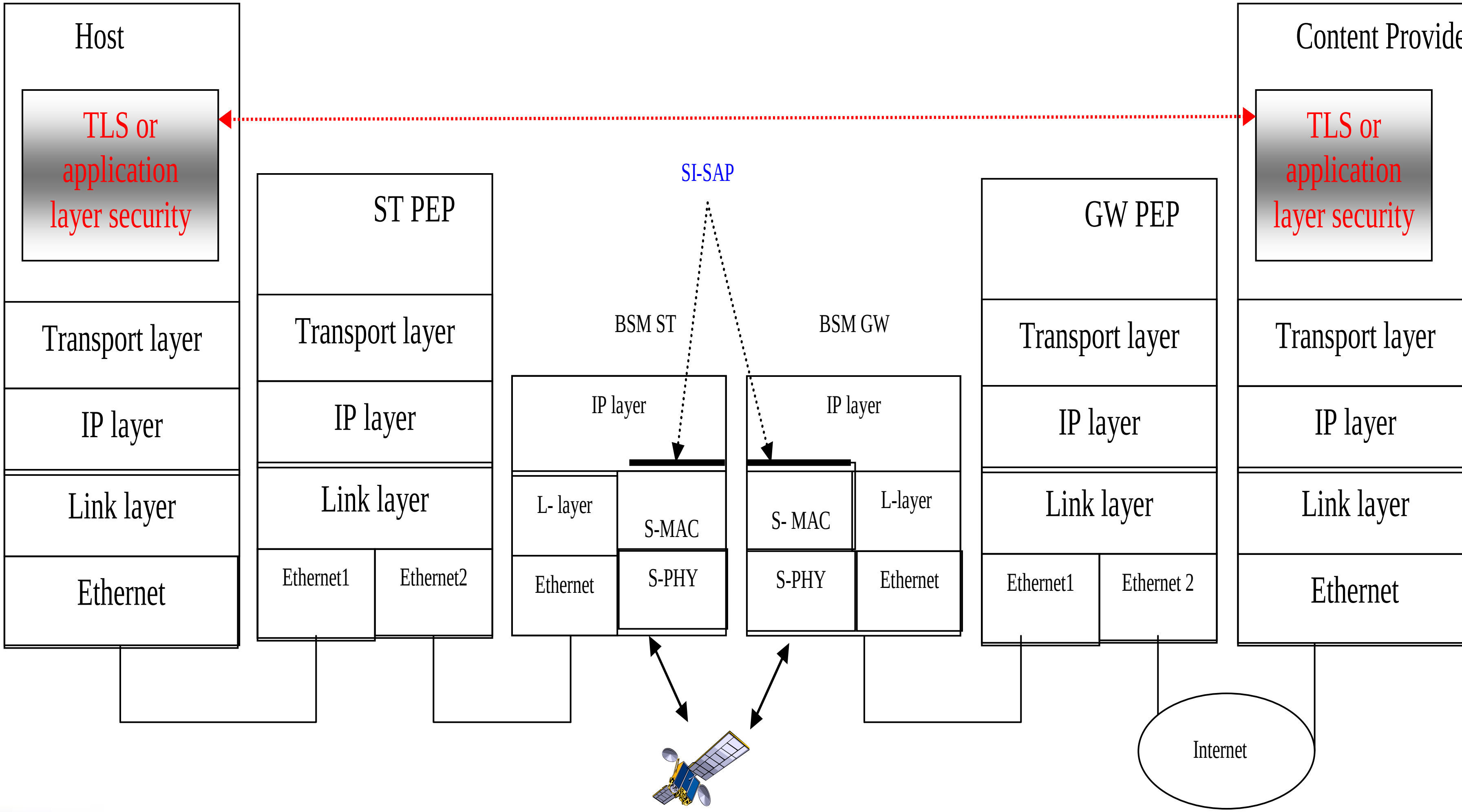
T-PEP and A-PEP mechanisms

- TCP ACK Spacing: In environments where ACKs tend to bunch together, ACK spacing is used to smooth out the flow of TCP acknowledgments traversing a link.
- Local TCP Acknowledgements: In some PEP implementations, TCP data segments received by the PEP are locally acknowledged by the PEP.
- Local TCP Retransmissions: A TCP PEP may locally retransmit data segments lost on the path between the TCP PEP and the receiving end system.
- Browser Cache Leveraging: Caching some web pages not residing in browser cache, improving efficiency.
- HTTP pre-fetching: Intercepting requested Web pages, identifying Web objects referred to by the Web pages, downloading these objects in anticipation of the next user requests.

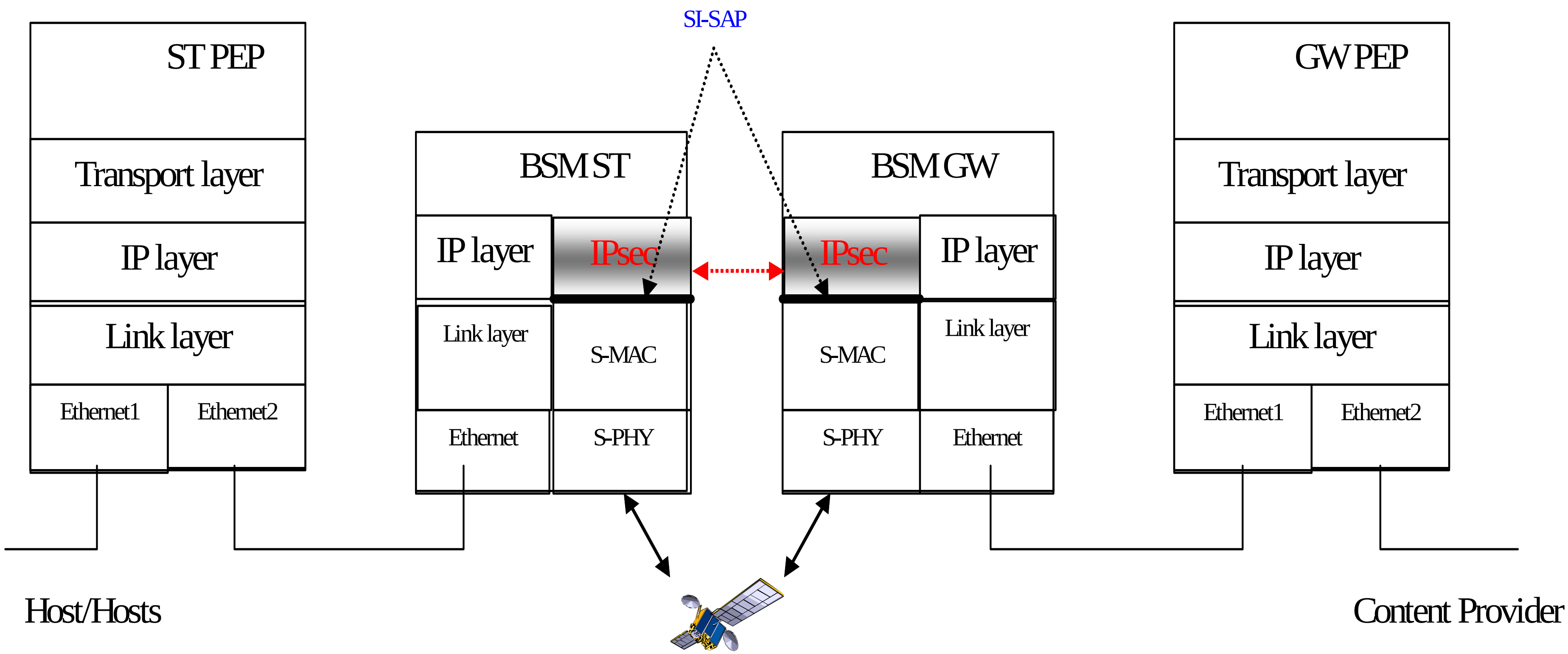
Security issues in PEPs

- ❖ Security can be applied in application, transport (SSL), IP (IPSec) or link layers:
  – However security must allow T-PEP access to the transport protocol headers and A-PEPs access to application layer contents (e.g web pages)
- ❖ This implies that IPSec and SSL can be applied in limited cases.
- ❖ Satellite link layer security can be applied transparently to T-PEPs and A-PEPs.

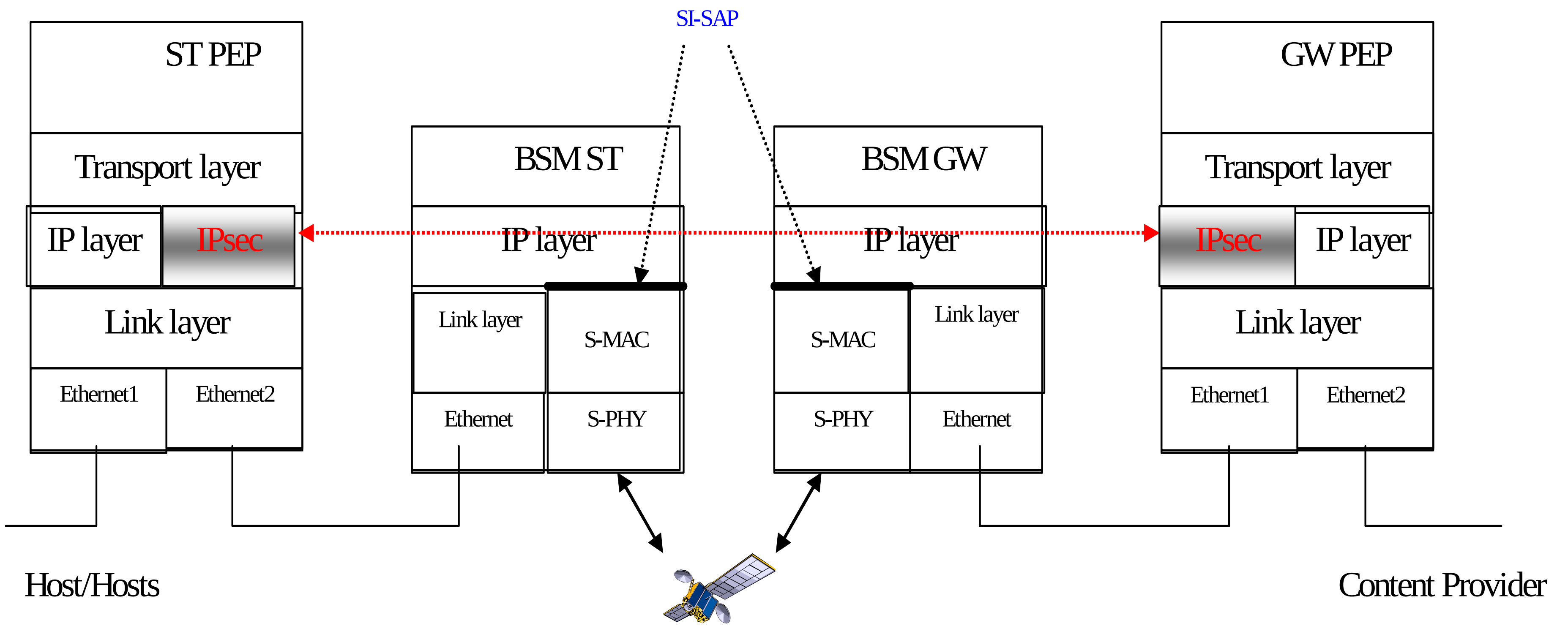
Successful T-PEP (not A-PEP) with end-to-end SSL



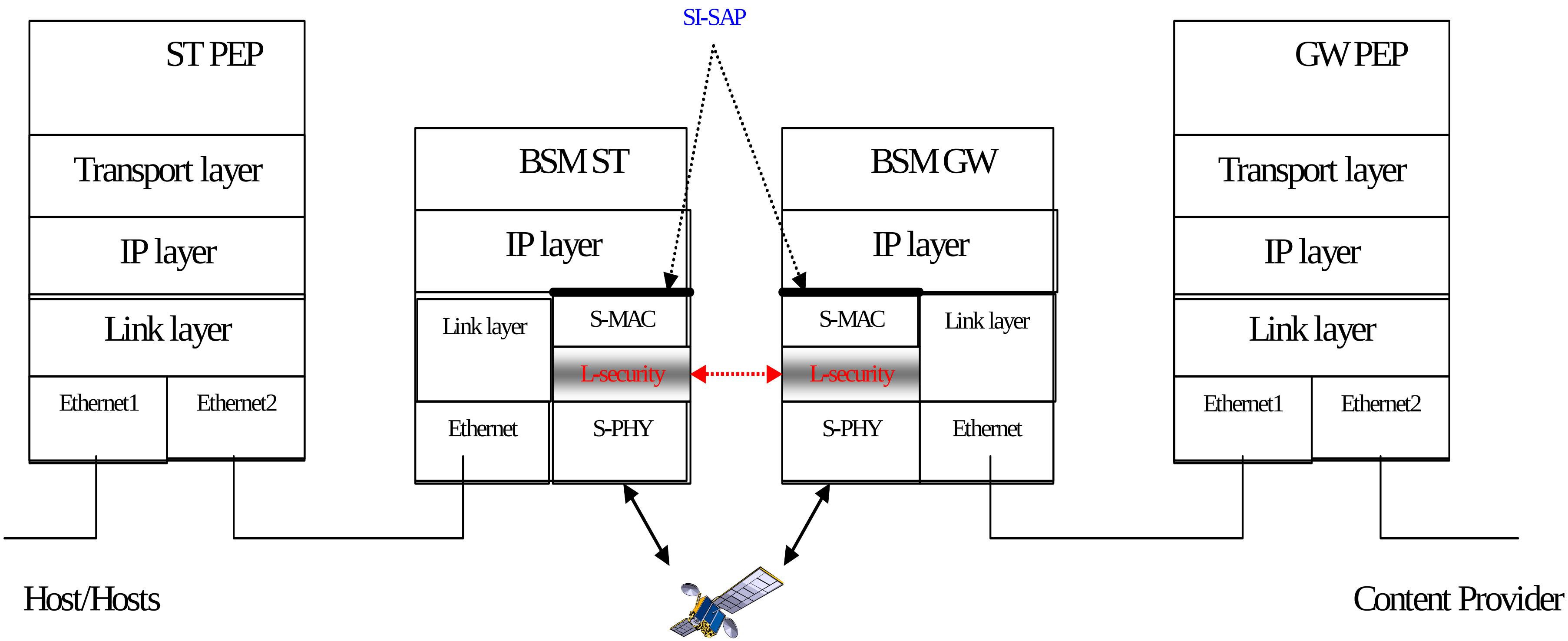
Successful T-PEP and A-PEP with IPSec - 1



Successful T-PEP and A-PEP with IPSec - 2



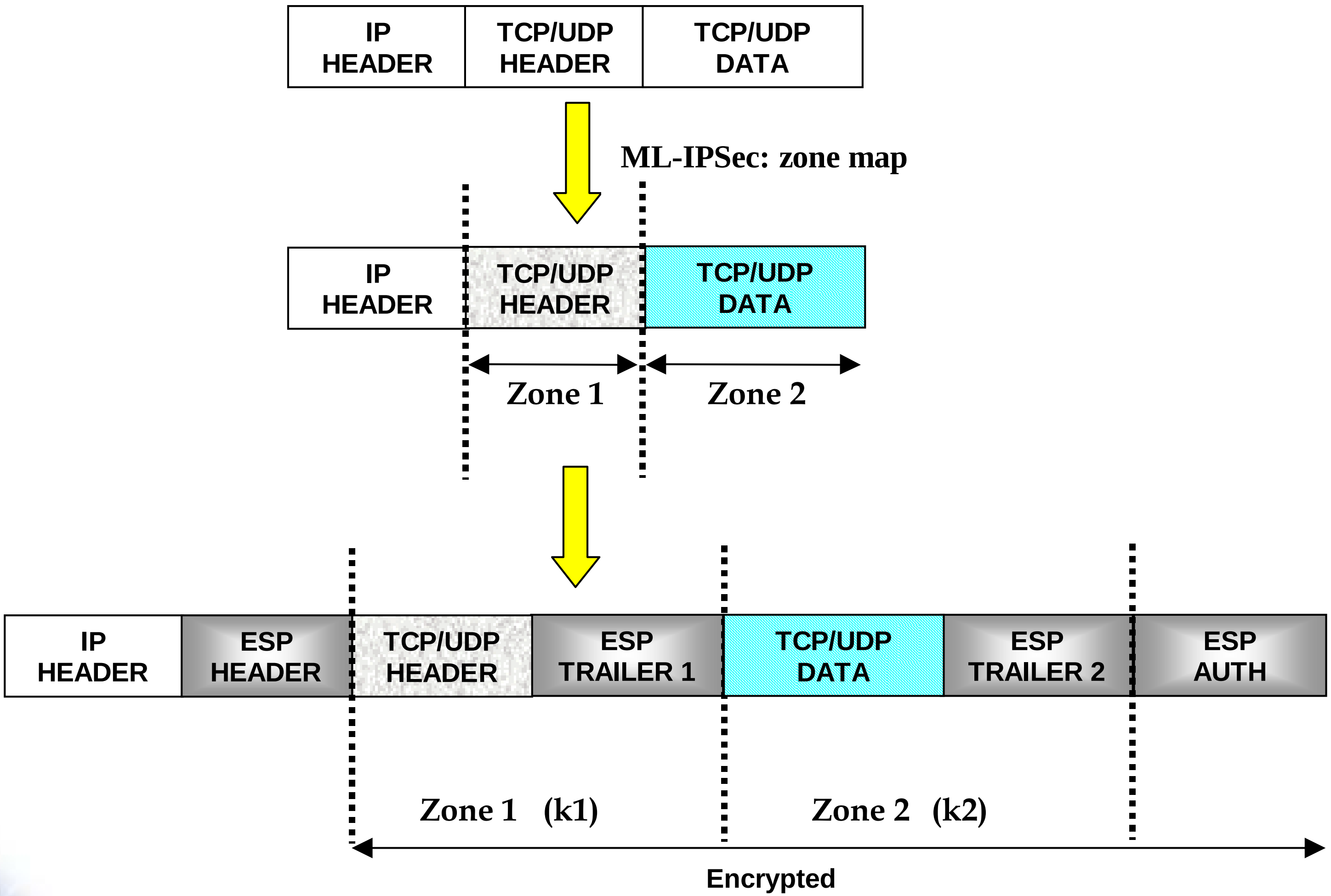
Successful PEPs with link layer security



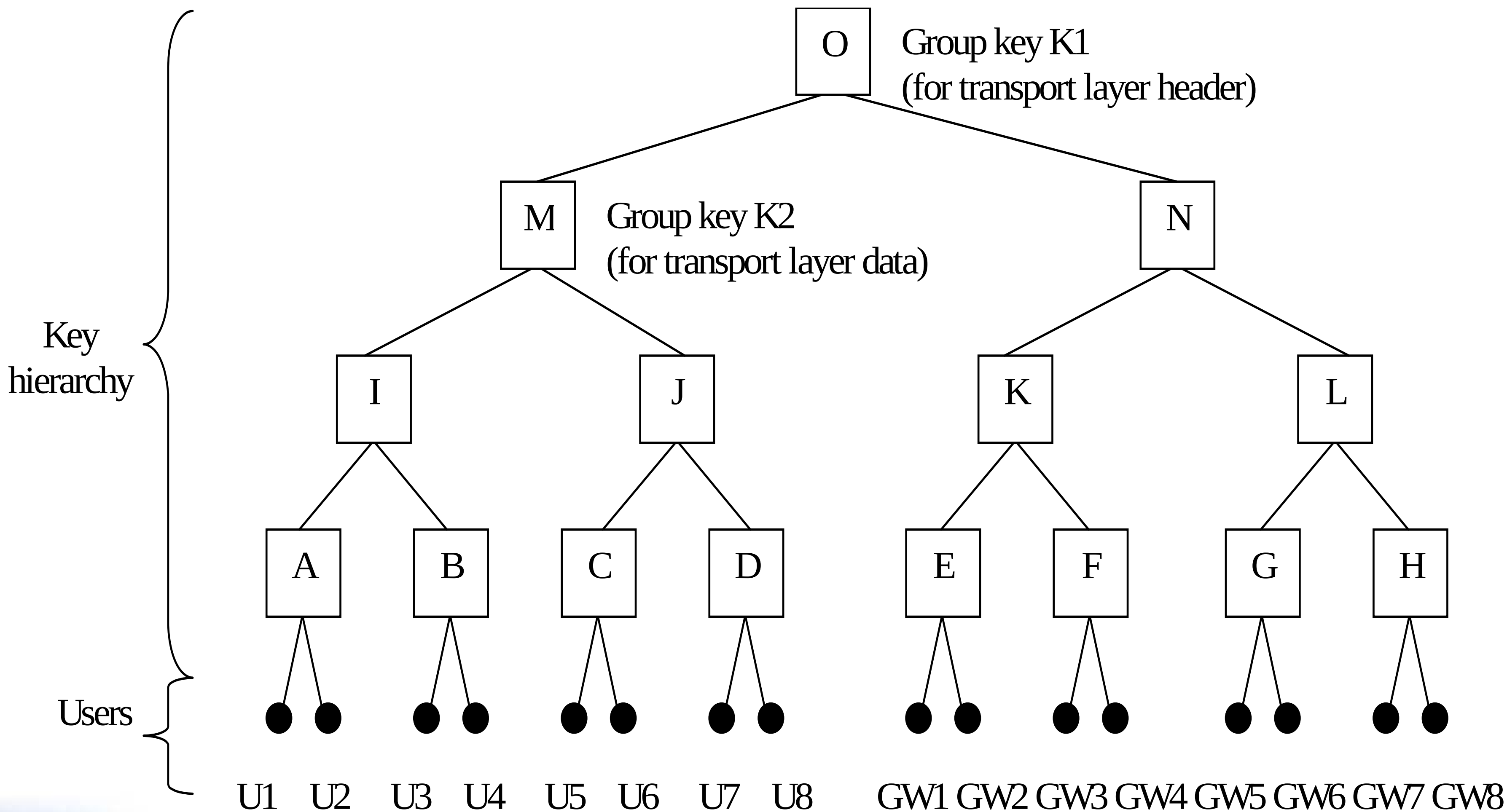
Limitations of IPSec - problems with middle entities - revisited

- IPSec in transport mode encrypts all data above IP layer. IPSec in tunnel mode encrypts all data including the original IP layer. However it conflicts with:
  - Satellite bandwidth acceleration: Performance Enhancing proxies (PEPs) need to inspect TCP and HTTP header.
  - Traffic Analysis: Service provider might require monitoring of their network traffic for management and QoS purposes.
  - Traffic Engineering: Flow classification is essential in supporting a variety of classes of service and QoS.
- A solution Multi Layer IPSec (ML-IPSec): divides the IP datagram into several zones and apply different protection schemes to each zone.

Multi Layer IPSec (ML-IPSec) - design



Interworking between ML-IPSEC and LKH



Delay/Disruption Tolerant Networks (DTN) - security

Delay/Disruption Tolerant Networking (DTN - Introduction

UNIVERSITY OF SURREY

- DTN is an overlay network architecture which runs on top of heterogeneous networks.
- It provides good services in high delay/disruption environments. It originated within the Inter Planetary research community.
- It has three main components:

DTN Node
Application
Bundle
Transport **A**
Network **A**
Link **A**
Physical **A**

DTN Router	
Application (Optional)	
Bundle	
Transport **A**	Transport **A**
Network **A**	Network **A**
Link **A**	Link **A**
Physical **A**	Physical **A**

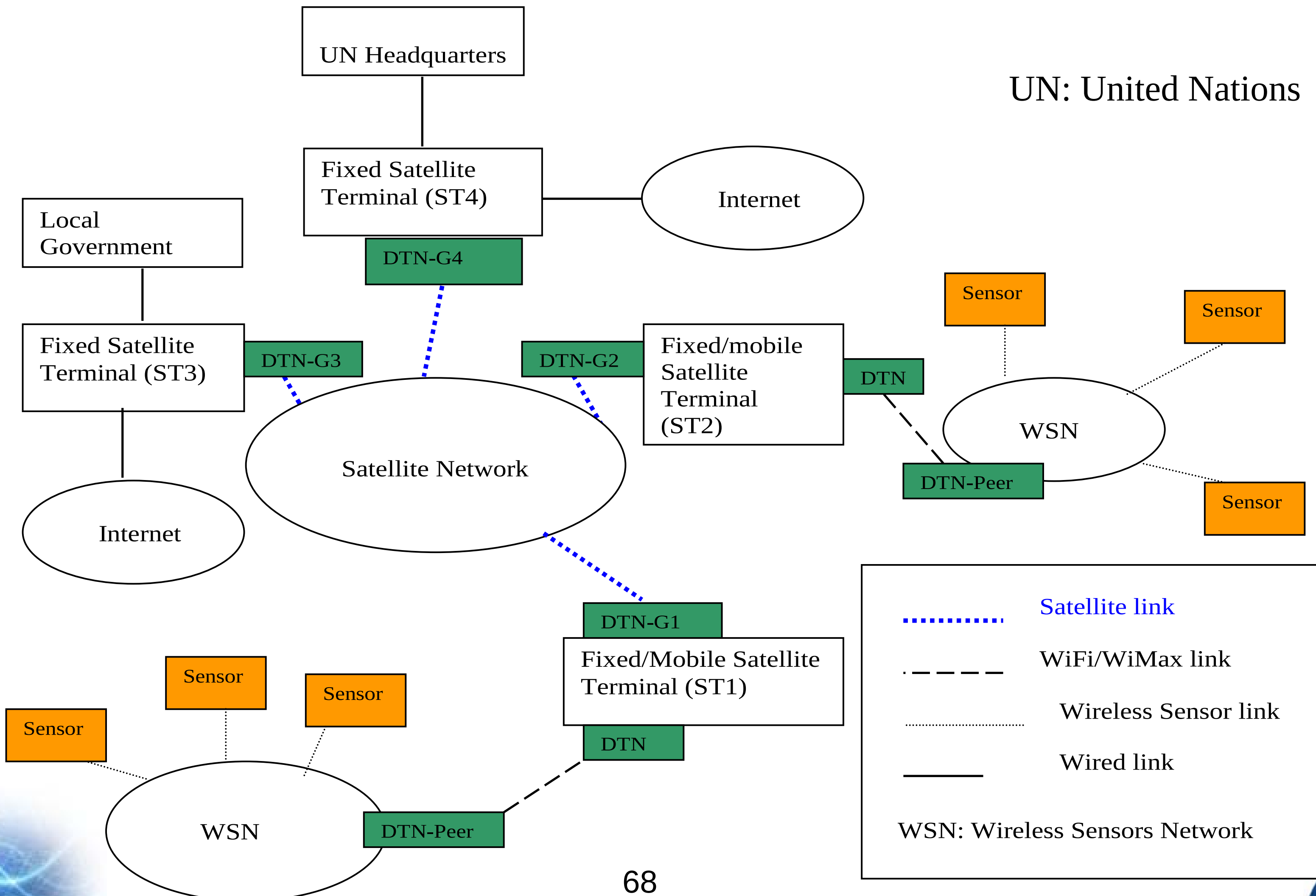
DTN Gateway	
Application (Optional)	
Bundle	
Transport **A**	Transport **B**
Network **A**	Network **B**
Link **A**	Link **B**
Physical **A**	Physical **B**

CCSR CENTRE FOR COMMUNICATION SYSTEMS RESEARCH

67

Example DTN scenario: UN monitoring in disaster and conflict areas

UN: United Nations



DTN security issues

- Current security protocols such as IPSec and TLS (or SSL) do not perform well in high delay/disruption conditions because of the following assumptions:
  - end-to-end connectivity is always present
  - low link delays
  - low error rate on link channels

DTN Security Architecture

- DTN security architecture provides hop-by-hop authentication and end-to-endish authentication, integrity, and confidentiality.
- It has several blocks (headers) to provide these security services.
  - Bundle Authentication Block (BAB): hop-by-hop authentication & integrity
  - Payload Integrity Block (PIB): end-to-endish authentication and integrity
  - Payload Confidentiality Block (PCB): end-to-endish confidentiality

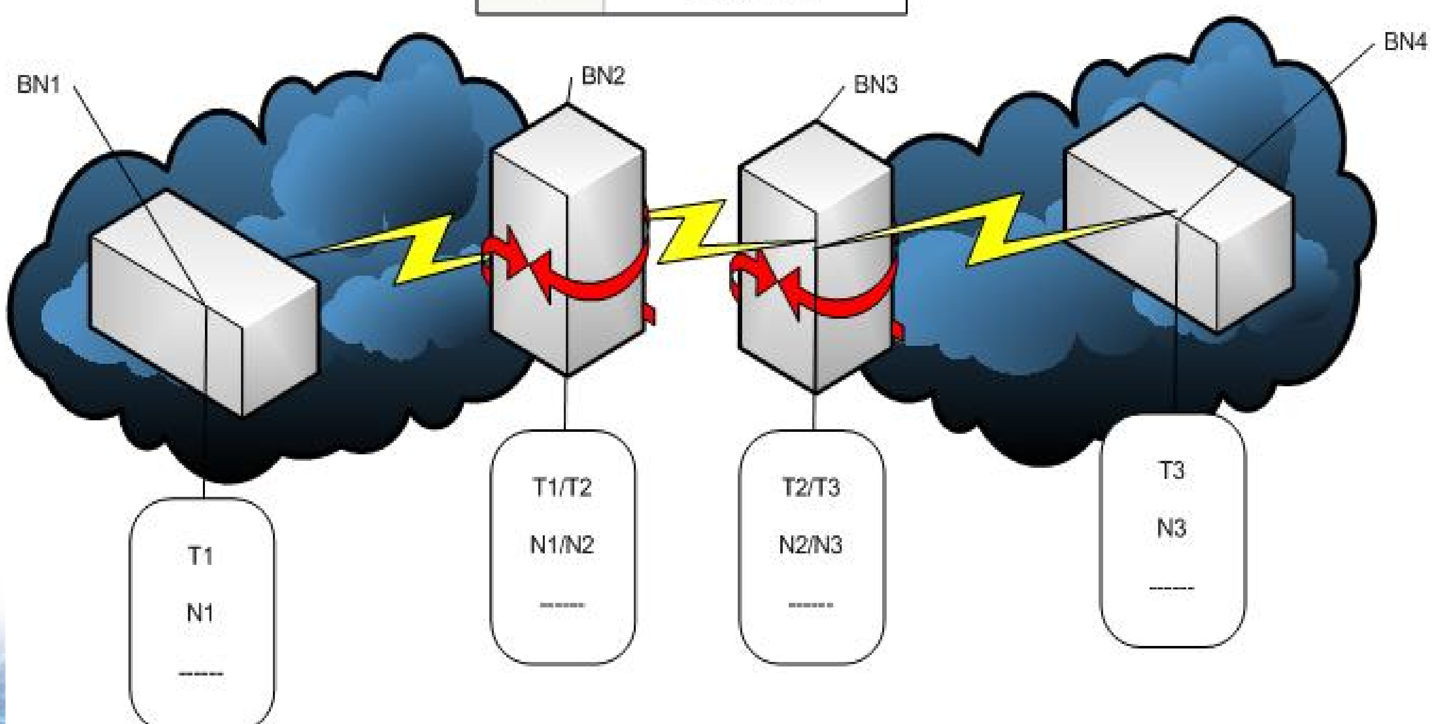
70

Internetworking of heterogeneous networks using DTN Gateways

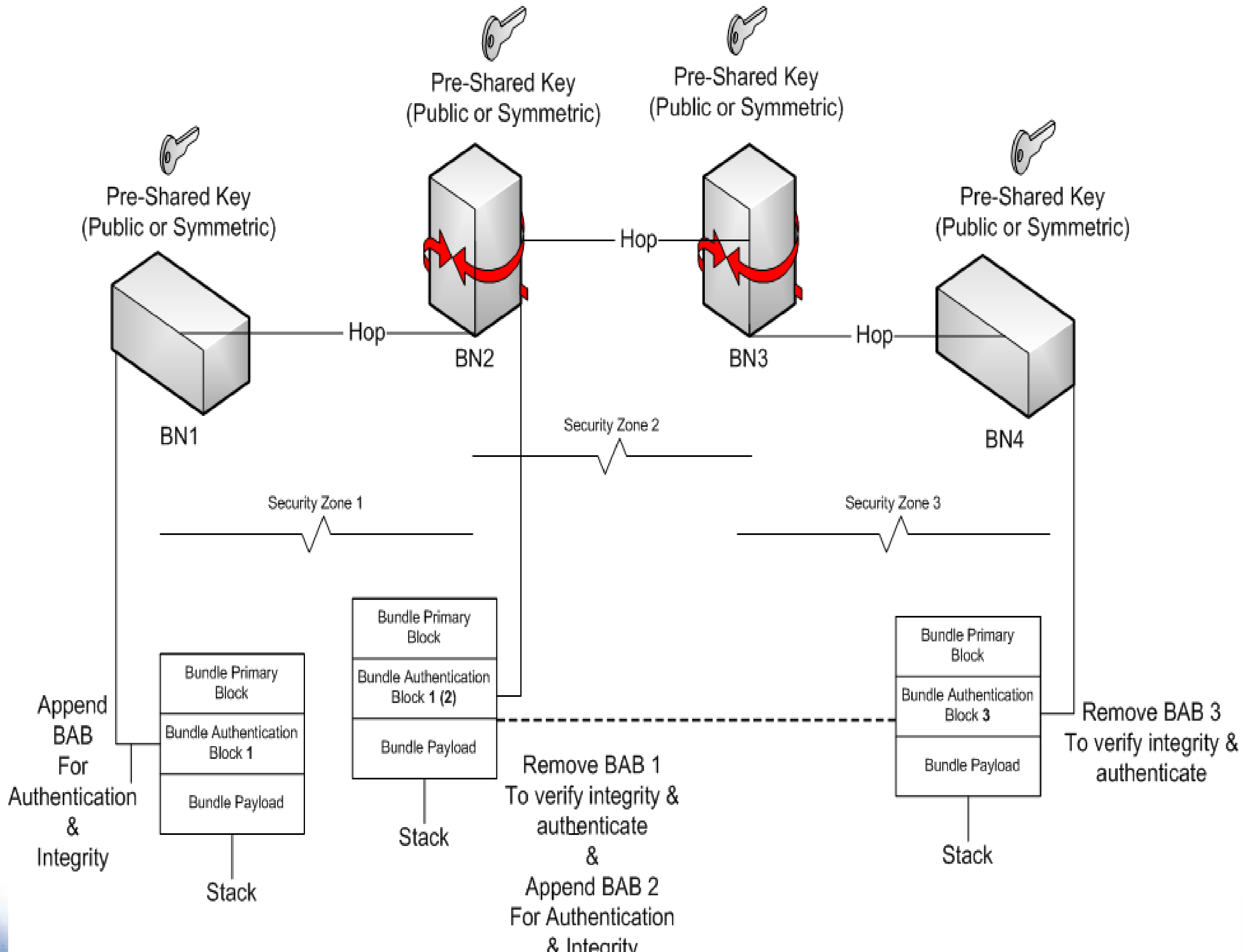
DTN Network	
Network Description	
Symbol	Description
	Network (e.g. Internet)
	DTN Gateway
	Bundle Node (BN)
	Comm-link

T = Transport Layer

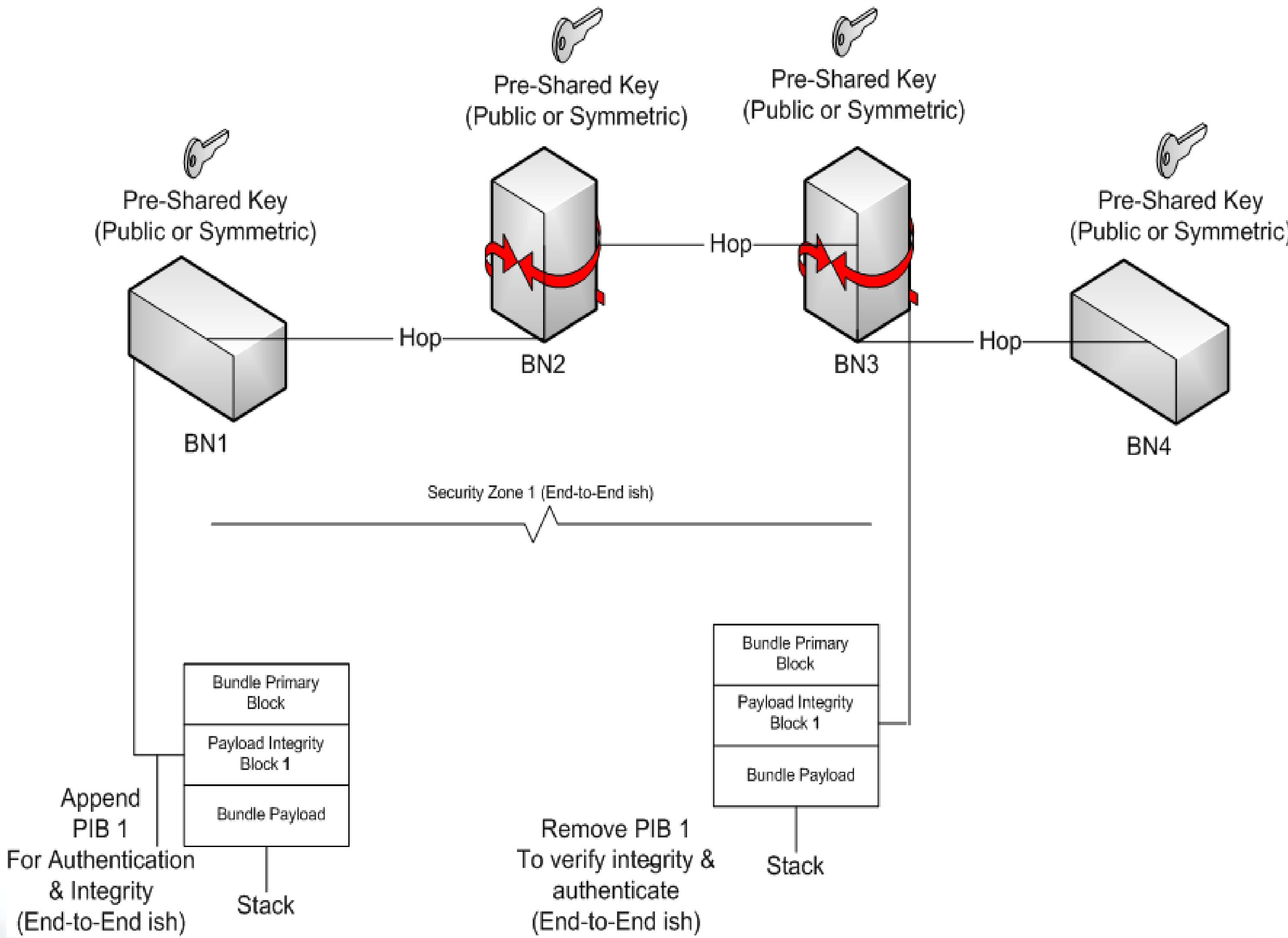
N = Network Layer



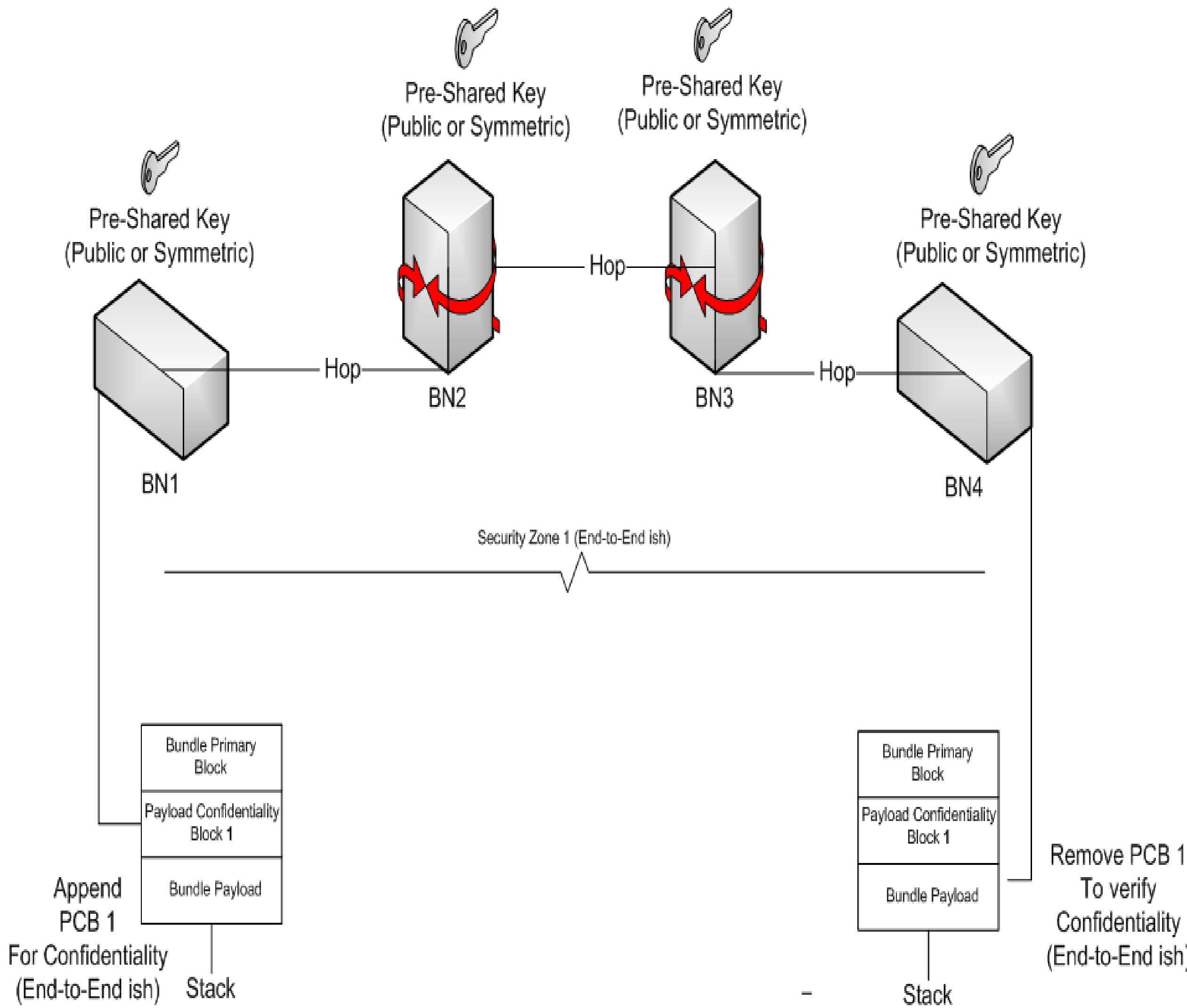
DTN security : Hop-by-Hop authentication



DTN security : End-to-End authentication and integrity



DTN security : End-to-End confidentiality



Open research issues in DTN security

- Lightweight key management
- Lightweight AAA-like architecture for authentication/authorisation
- Resilience to Denial of Service (DoS) attacks
- Providing anonymity to end users for some services/applications

Summary - security layers comparison

	Link layer	Network layer	Transport layer	Application layer
Major advantages	Complete control of the link security	IPSec is the best solution for Internet security	Widely used for securing TCP connections	Can satisfy applications requirement very well
Major disadvantages	Only the one link hop is secure	IPSec works only for IP networks	No security for UDP and multicast	No transparency, where applications need modification to fit security

Summary - security services at various protocol layers

	Link layer	IP Network layer	Transport layer	Application layer
Terminal authentication	*Yes*	*Yes (IP address)*	*No*	*No*
Host authentication	*No*	*Yes (IP address)*	*No*	*No*
User authentication	*No*	*No*	*Yes*	*Yes*
Link privacy	*Yes*	*Yes (IPSec IP tunnel)*	*No*	*No*
End to end privacy	*No*	*Yes*	*Yes*	*Yes*
Link data integrity	*Yes*	*Yes (IPSec IP tunnel)*	*No*	*No*
End to end data integrity	*No*	*Yes*	*Yes*	*Yes*