Chapter 5: Security

Jyh-Cheng Chen and Tao Zhang

IP-Based Next-Generation Wireless Networks
Published by John Wiley & Sons, Inc.
January 2004

Outline

5.1 Introduction

5.2 Internet Security

5.3 Security in Wireless Networks

5.4 Security in IS-41

5.5 Security in GSM

5.6 Security in GPRS

5.7 Security in 3GPP

5.8 Security in 3GPP2

5.1 Introduction

5.1.1 Different Facets of Security

5.1.2 Security Attacks

5.1.3 Cryptography

5.1.4 Public-Key Infrastructure (PKI)

5.1.1 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

5.1.2 Security Attacks

- Passive attacks: eavesdrop the 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

5.1.3 Cryptography

5.1.3.1 Encryption

5.1.3.2 Message Authentication

5.1.3.1 Encryption

- Transforming of letters or characters without changing its information content
- Enciphering (encryption)
  - plaintext (cleartext) -> ciphertext
- Deciphering (decryption)
  - ciphertext -> plaintext (cleartext)
- Can be used to achieve the information confidentiality

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

Transposition Ciphering

- Rearrange the characters in the plaintext to produce the ciphertext
- Permutation

  i = 1, 2, 3, 4, 5, 6, 7 ->

  f(i) = 2, 4, 1, 6, 5, 3, 7
- m = IP-Based Next-Generation Wireless Networks

  f(m) = -IsPaBeNdt xe-nGaeretniioW ree lssNwektros

Substitution Ciphering

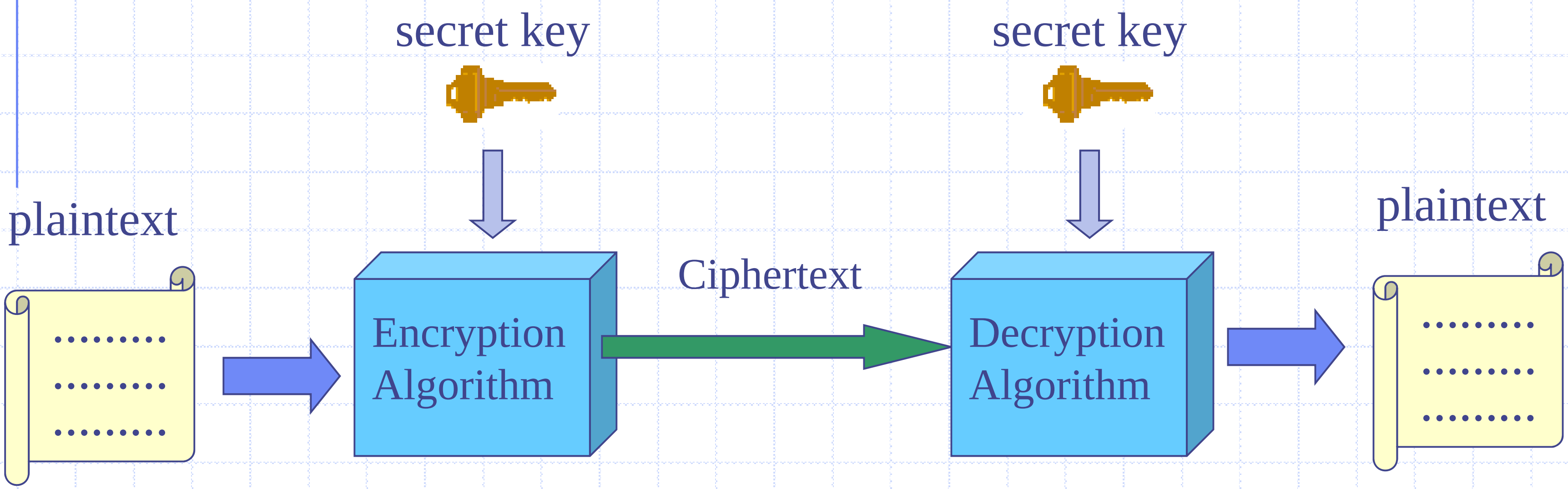
- Substitute characters in the plaintext with other characters to produce the ciphertext
- Caesar cipher: shift alphabet

  A B C D E F G H I J K L M N …

  D E F G H I J K L M N O P Q …
- m = THIS IS A PLAINTEXT

  g(m) = WKLV LV D SODLQWHAW

Fig. 5.1 Secret-key encryption and decryption



DES (Data Encryption Standard)

- Divide original message into blocks of 64 bits
- Each block is permuted
- Encrypt each block of plaintext using a 64-bit key
  - 1 bit in each byte is for parity check
    - Actual key length: 56 bits
  - 16 identical iteration that combines substitution and transposition ciphers
- Inverse original permutation
- Triple DES

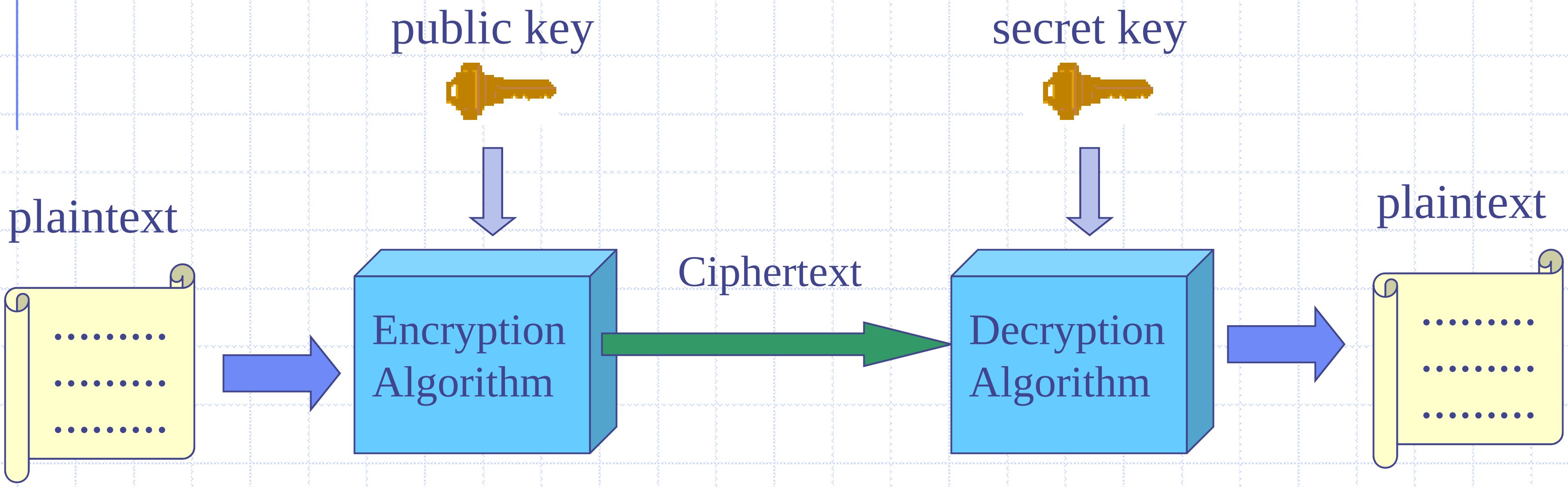
AES (Advanced Encryption Standard)

- By NIST (National Institute of Standards and Technology)
- AES-128
- AES-192
- AES-256

Public-Key Algorithm

- Public key
  - Publicly available to anyone
- Secret (private) key
  - Only users themselves know their own private keys.

Fig. 5.2 Public-key encryption and decryption



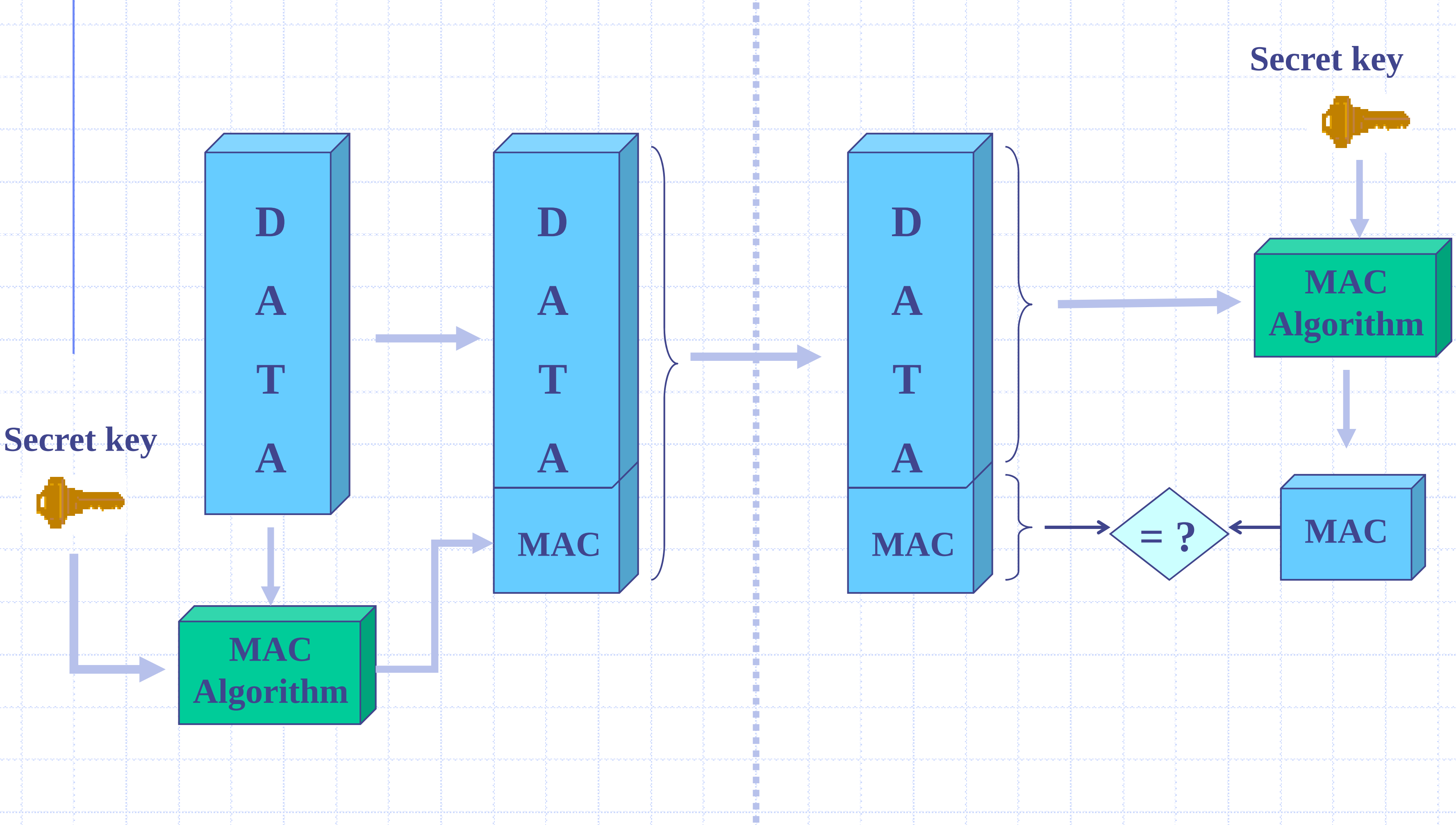
RSA

- It is extremely difficult to factor the product of two large prime numbers.
- A secret key can be generated by two selected large prime numbers.
- The product of the two large prime numbers will be used as the public key.
- Knowing the public key does not allow one to easily derive the associated private key.

5.1.3.2 Message Authentication

- A methodology to assure data integrity and to authenticate the data origin
- Message Authentication Code (MAC)
- 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.

Fig. 5.3 Message authentication code (MAC)



Hash Function

- Unkeyed hash: there is no secret key between the communicating parties
  - Message Digest 5 (MD5)
  - Secure Hash Algorithm (SHA-1)
- Keyed hash
  - HMAC

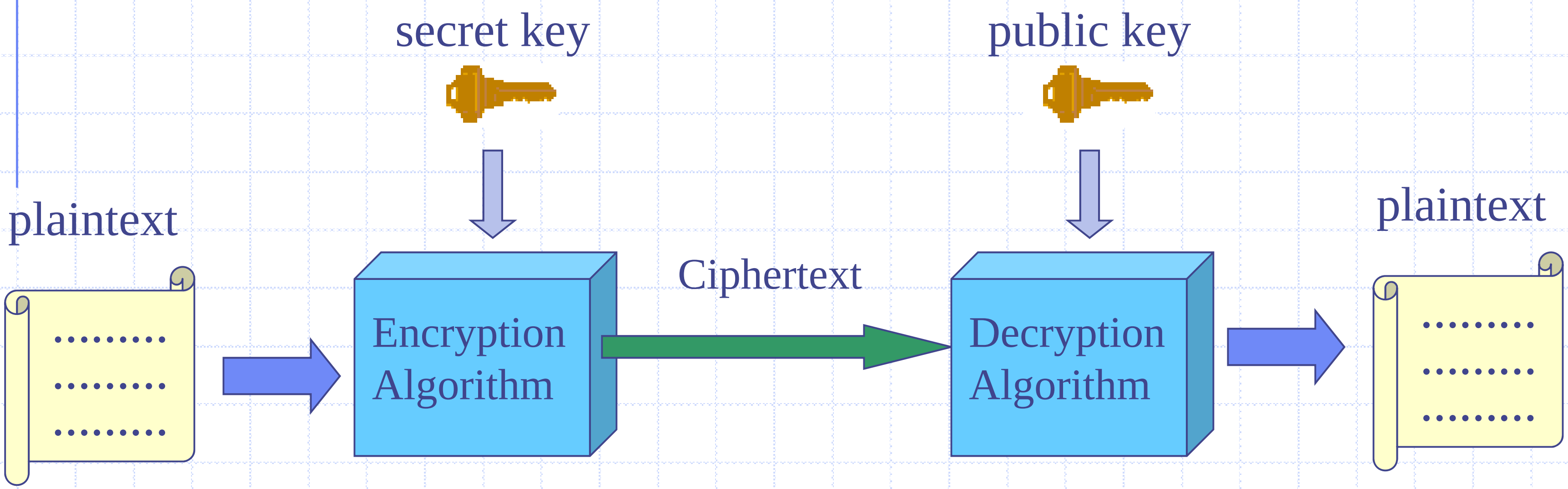
MD5 and SHA

- Message Digest 5 (MD5)
  - Produce an output of 128-bit *fingerprint* or *message digest*
  - The sender sends the original message and the message digest together to the destination.
  - The destination computes its own message digest from the received message.
  - Any change to the original message during transmission will result in a different message digest.
- Secure Hash Algorithm (SHA-1) generates a 160-bit message digest

Digital Signature

- Public-key algorithms can be used for integrity and message authentication as well.
- Digital Signature Standard (DSS)
  - Specify algorithms for computing digital signatures that can be used by a receiver to verify the identity of the signatory and the integrity of the data

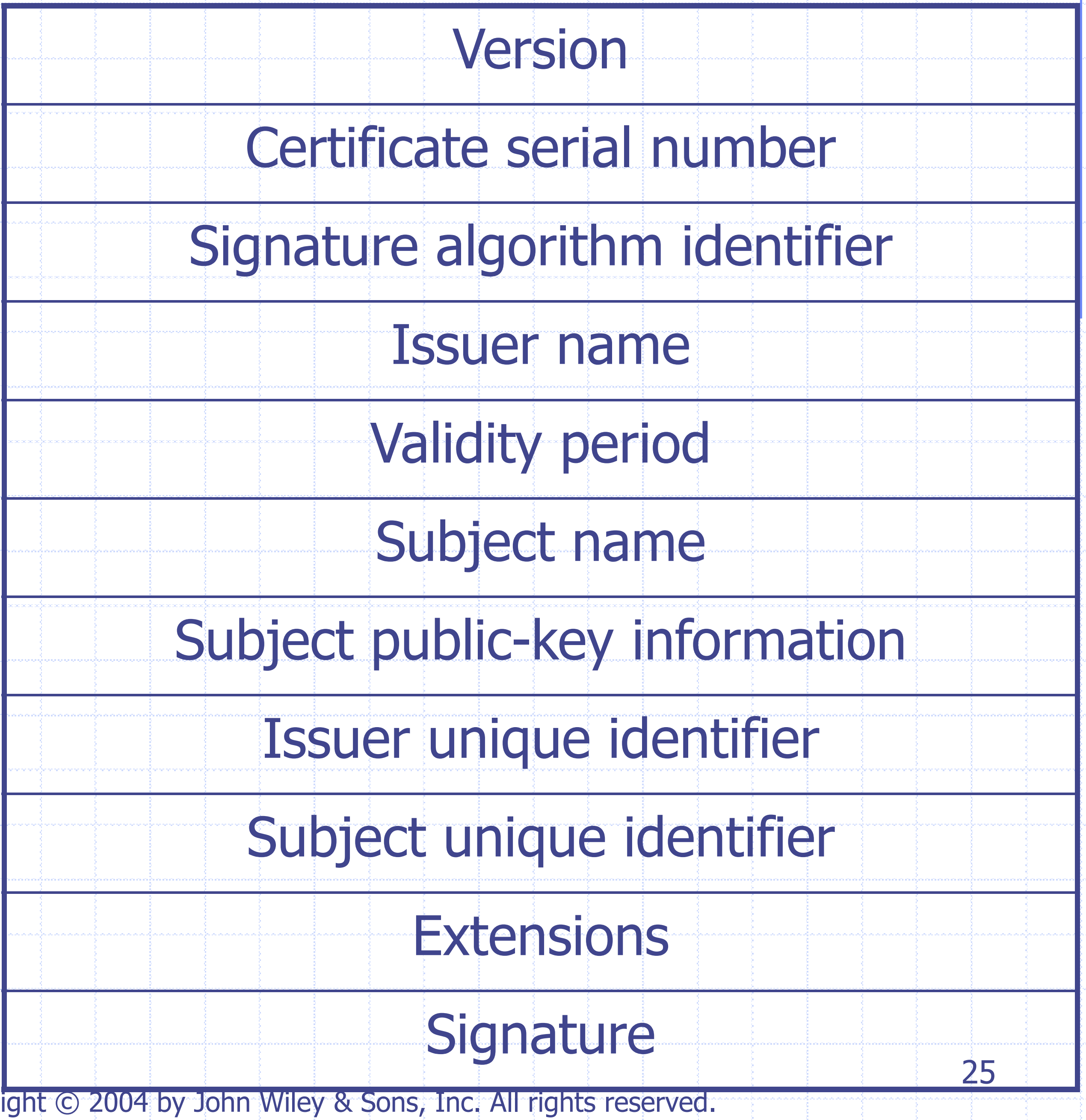
Fig. 5.4 Integrity and authentication by public-key



5.1.4 Public-Key Infrastructure (PKI)

- How can we assure that a public key is not forged?
- PKI: establish digital identities that can be trusted
  - A trusted third party is known as a certification authority (CA).
  - One can present a public key to the CA in a secure manner.
  - The CA then issues a *digital certificate* or *public-key certificate (PKC)* that contains the user’s public key to the user.
  - The certificate is signed digitally by the CA.
- X.509 Certificate: standardized by the ITU

Fig. 5.5 Format of ITU X.509 certificate



Version

Certificate serial number

Signature algorithm identifier

Issuer name

Validity period

Subject name

Subject public-key information

Issuer unique identifier

Subject unique identifier

Extensions

Signature

5.2 Internet Security

5.2.1 IP Security (IPsec)

5.2.2 Authentication, Authorization, and Accounting (AAA)

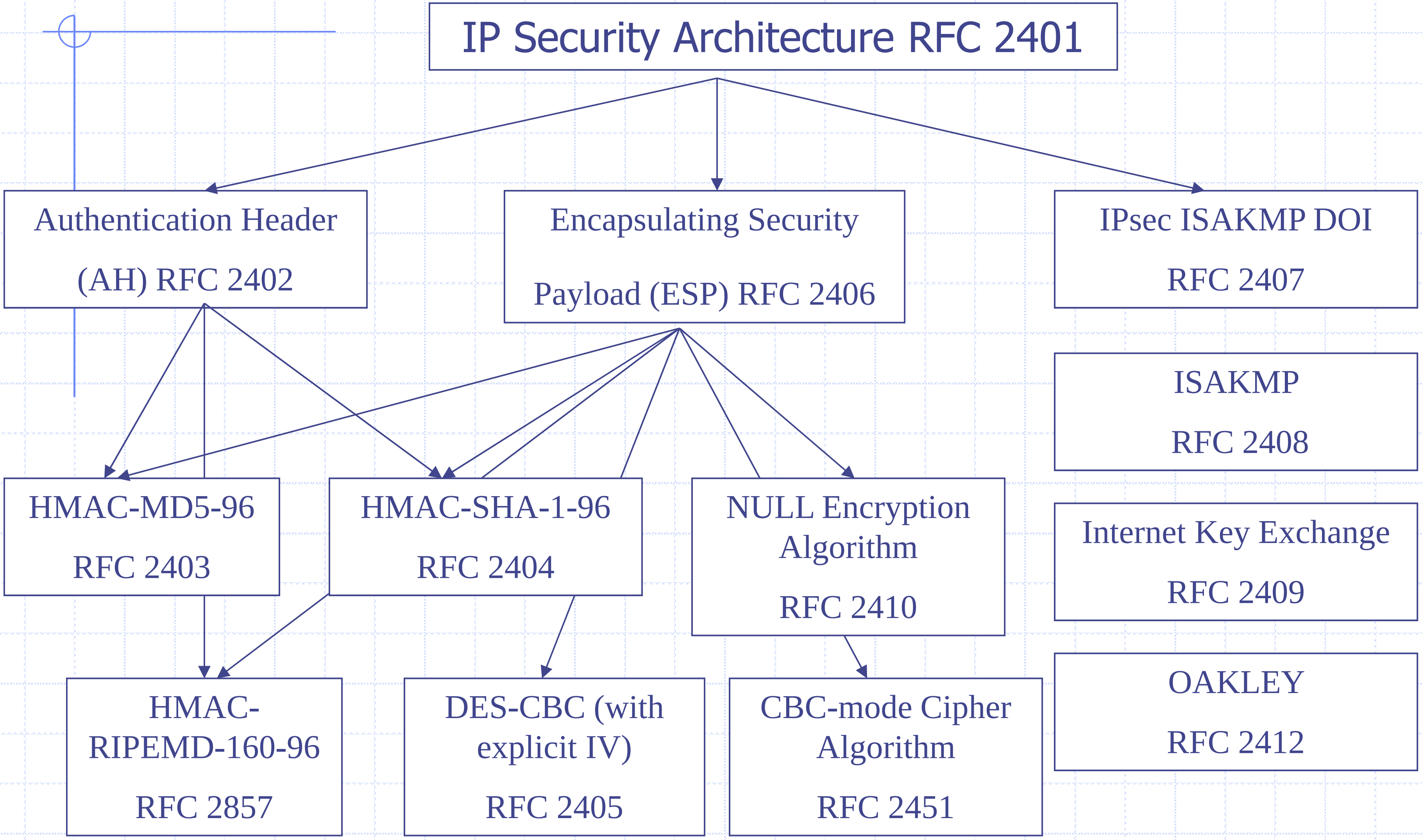
5.2.1 IP Security (IPsec)

5.2.1.1 Security Protocols
5.2.1.2 Authentication and Encryption Algorithms
5.2.1.3 Security Associations
5.2.1.4 Key Management
5.2.1.5 Implementation
5.2.1.6 Authentication Header (AH)
5.2.1.7 Encapsulating Security Payload (ESP)
5.2.1.8 Traffic Processing
5.2.1.9 IPsec Applications

IPsec

- IPsec is a suite of protocols for protecting IP datagrams and upper layer protocols
- Defined by IETF
  - Optional for IPv4
  - Mandatory for IPv6

Fig. 5.6 Family of IPsec protocols



IP Security Architecture RFC 2401

Authentication Header (AH) RFC 2402

Encapsulating Security Payload (ESP) RFC 2406

IPsec ISAKMP DOI RFC 2407

ISAKMP RFC 2408

HMAC-MD5-96 RFC 2403

HMAC-SHA-1-96 RFC 2404

NULL Encryption Algorithm RFC 2410

Internet Key Exchange RFC 2409

HMAC-RIPEMD-160-96 RFC 2857

DES-CBC (with explicit IV) RFC 2405

CBC-mode Cipher Algorithm RFC 2451

OAKLEY RFC 2412

5.2.1.1 Security Protocols

- AH (Authentication Header)
  - support data integrity and authentication of the IP packets
- ESP (Encapsulating Security Payload)
  - provides confidentiality services

Operation

- Transport
  - security is applied to higher-level protocols to protect the payload
- Tunnel
  - security is applied to the encapsulated IP packet to protect the entire packet

5.2.1.2 Authentication and Encryption Algorithms

- IPsec specifies various options for cryptography algorithm.
  - HMAC-MD5-96, HMAC-SHA-1-96, NULL encryption algorithm, HMAC-RIPEMD-160-96, DES-CBC, and CBC-Mode cipher algorithms, and others
- To be compliant with ESP
  - DES-CBC, HMAC-MD5-96, HMAC-SHA-1-96, NULL encryption algorithm, and NULL authentication algorithm must be implemented
  - Encryption algorithm and authentication algorithm cannot be both NULL.
- To be compliant with AH
  - HMAC-MD5-96 and HMAC-SHA-1-96 are mandatory

5.2.1.3 Security Associations

- A set of information maintained by the two nodes that defines:
  - Which security services will be supported
  - How these security services will be provided
  - For example, it identifies:
    - Security mechanisms (e.g., cryptography algorithms, key management mechanisms) will be used to support the security services
    - Parameter values (e.g., security keys) needed by the security mechanisms
    - How long these parameter values (e.g., the keys) will be valid

Security Association Database (SAD)

- Because the information maintained in a SA generally is too big to fit into IP header, the SAs are maintained in SAD.
- Each SA is identified uniquely by a triplet:
  - Security protocol identifier: AH or ESP
  - Destination IP address: the IP address of the other node with which the SA is established
  - Security Parameter Index (SPI): a 32-bit value that uniquely identifies one SA among different SAs terminating at the same destination

Security Policy Database (SPD)

- SA enforces *Security Policies* that define how communicating parties will communicate by IPsec.
- Security policies are stored on Security Policy Database (SPD), which specifies the policies that determine the disposition of all inbound or outbound, IPsec or non-IPsec IP traffic.
- Each packet is either applied IPsec, be allowed to bypass IPsec, or discarded.

5.2.1.4 Key Management

- Both manual and automated SA and key management are mandated in IPsec.
- Diffie-Hellman (DH) algorithm is adopted by most automated key management protocols.
- OAKLEY
- SKEME
- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE): the default automated key management protocol selected for use with IPsec

Diffie-Hellman (DH) Algorithm

- First agree on a large prime number p and a number α such that α is primitive mod p

1. Tao chooses a random secret x and calculates A as follows

   $A = \alpha^{x} \mod p$

   Tao then sends A to Jyh-Cheng
2. Jyh-Cheng chooses a random secret y and calculates B as follows

   $B= \alpha^{y} \mod p$

   Jyh-Cheng then sends B to Tao
3. Tao calculates $K = B^{x} \mod p$
4. Jyh-Cheng calculates $K' = A^{y} \mod p$

- $K = K' = \alpha^{xy} \mod p$
- It is computationally difficult to calculate the discrete logarithm to get x and y

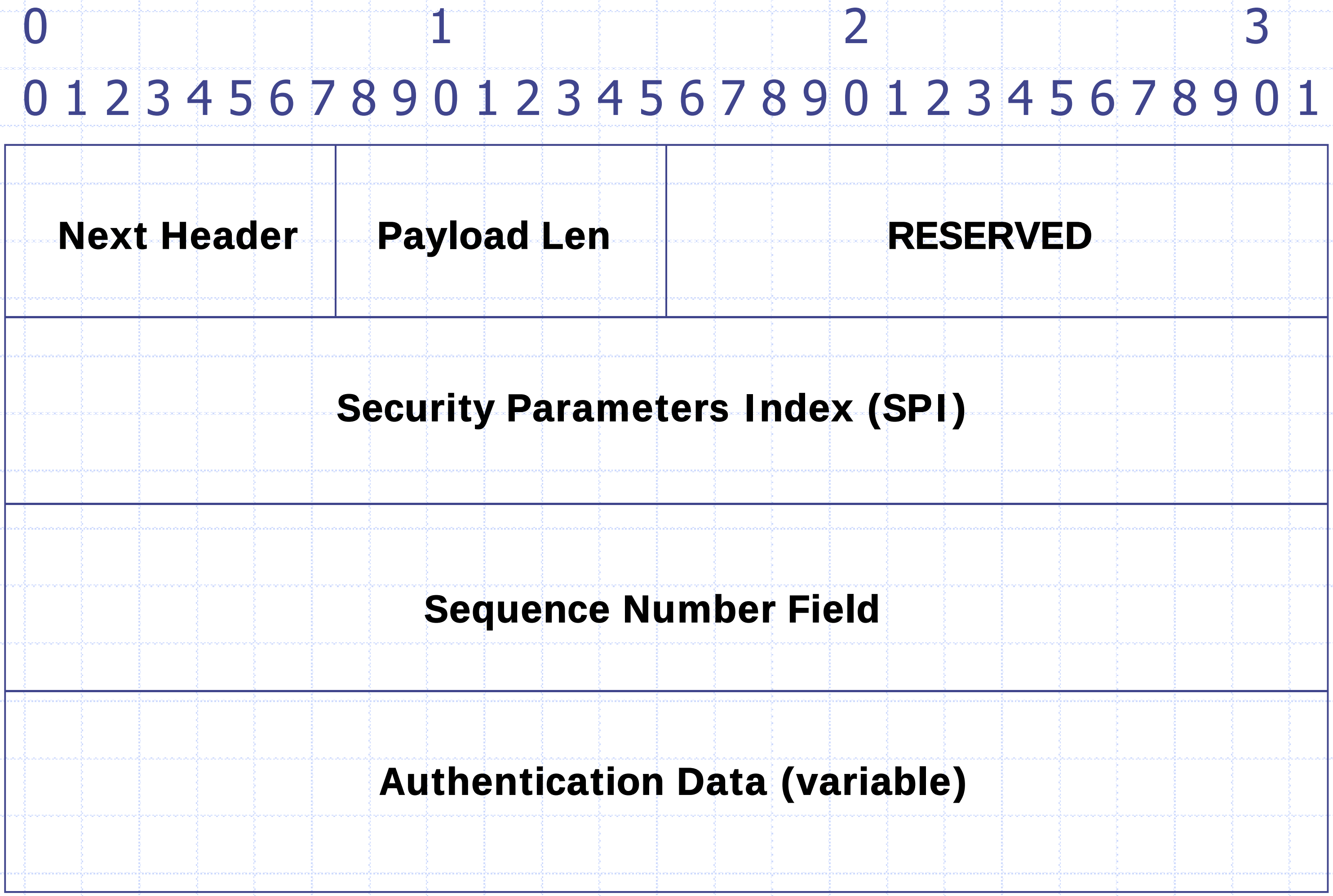
5.2.1.5 Implementation

- IP stack integration
  - IPsec could be integrated into the network layer of the protocol to provide security services.
- Bump-in-the-stack (BITS)
  - IPsec is inserted as a thin layer between IP layer and link layer.
- Bump-in-the-wire (BITW)
  - This implementation assumes that IPsec is running on a separate device attached to the physical interface of a host or router.

5.2.1.6 Authentication Header (AH)

- Provide data integrity and authentication of data origin
- Also optionally provides replay detection
- May be applied alone or in combination with the ESP to provide confidentiality service

Fig. 5.7 Header format of AH



0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Next Header	**Payload Len**	**RESERVED**
Security Parameters Index (SPI)		
Sequence Number Field		
Authentication Data (variable)		

Security Parameter Index (SPI)

- A 32-bit value that uniquely identifies one SA among different SAs terminating at the same destination

Sequence Number

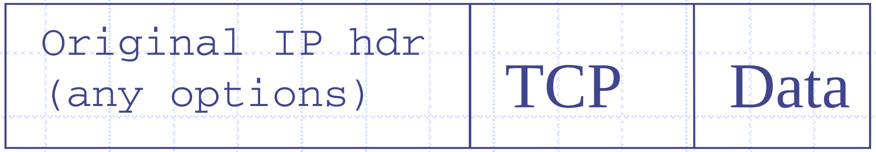
- 32-bit
- Incremented by 1 for each packet sent in order to protect against replay attacks

Authentication Data

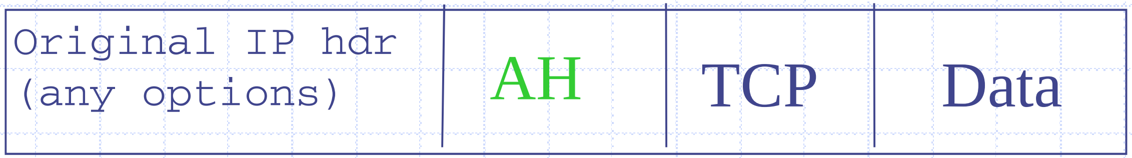
- Integrity Check Value (ICV)
  - Produced by MAC (Message Authentication Checksum) by an algorithm specified by the SA
    - Secret key between two parties
    - HMAC: produced by a *hash* function
  - Variable length but must be an integral number of 32-bit words
  - Computed over
    - immutable IP header fields
    - AH header
    - upper-level protocol data (assumed to be immutable)

Fig. 5.8 AH in IPv4 in transport mode

IPv4 – BEFORE APPLYING AH



IPv4 – AFTER APPLYING AH



```
|<-----------authenticated ----------->|
      except for mutable fields
```

Fig. 5.9 AH in IPv6 in transport mode

IPv6 – BEFORE APPLYING AH

Original IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING AH

Original IP hdr	hop-by-hop, dest*, routing, fragment.	AH	**Dest** **opt***	TCP	Data

|<--------- authenticated except for mutable fields -------------->|

* = if present, could be before AH, after AH, or both

Fig. 5.10 AH in tunnel mode

IPv4 – BEFORE APPLYING AH

New IP hdr (any options)	Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING AH

New IP hdr (any options)	AH	Original IP hdr (any options)	TCP	Data

|<--------------authenticated except for mutable fields in the new IP header--------------->|

IPv6 – BEFORE APPLYING AH

New IP hdr	ext hdrs if present	orig IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING AH

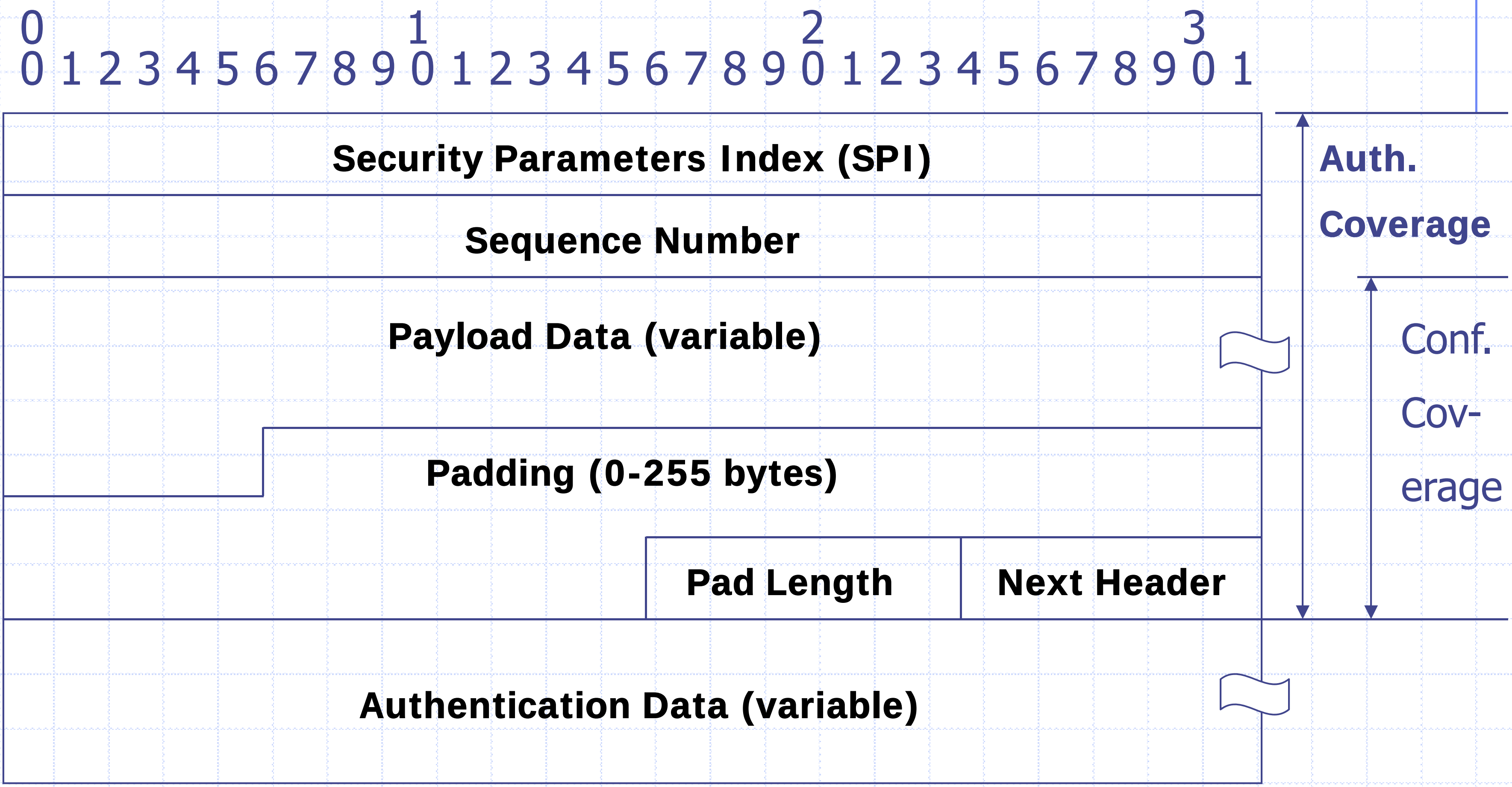
New IP hdr	ext hdrs if present	AH	orig IP hdr	ext hdrs if present	TCP	Data

|<------- authenticated except for mutable fields in the new IP header------->|

5.2.1.7 Encapsulating Security Payload (ESP)

- Provide confidentiality (encryption) and authentication
  - the authentication service includes data integrity and data origin authentication
- Also support replay detection
- Does not protect IP header unless it is encapsulated in the tunnel mode
- Either confidentiality or authentication must be selected

Fig. 5.11 ESP packet format



0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Security Parameters Index (SPI)

Sequence Number

Payload Data (variable)

Padding (0-255 bytes)

Pad Length

Next Header

Authentication Data (variable)

Auth. Coverage

Conf. Cov- erage

ESP Header

- SPI
- Sequence Number

ESP Trailer

- Padding
- Pad Length
  - indicate the number of pad bytes immediately preceding it
- Next Header
  - an 8-bit field that identifies the type of data contained in the *Payload Data* field

Padding

- Some encryption algorithms require the plaintext to be a multiple of some number of bytes
- *Pad Length* and *Next Header* fields must be right aligned within a 4-byte word
- May be used to conceal the actual length of the payload

Authentication Data

- A variable-length field containing an Integrity Check Value (ICV)

Fig. 5.12 ESP in IPv4 in transport mode

IPv4 – BEFORE APPLYING ESP

Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING ESP

Original IP hdr (any options)	ESP header	TCP	Data	ESP Trailer	ESP Auth

```
      |<---encrypted-->|
|<---authenticated---->|
```

Fig. 5.13 ESP in IPv6 in transport mode

IPv6 – BEFORE APPLYING ESP

Original IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING ESP

Orig IP hdr	hop-by-hop, dest*, routing, fragment.	ESP	**Dest Opt***	TCP	Data	ESP Trailer	ESP Auth

```
    |<----encrypted--->|
|<---authenticated---->|
```

* = if present, could be before ESP, after ESP, or both

Fig. 5.14 ESP in tunnel mode

IPv4 – BEFORE APPLYING ESP

New IP hdr (any options)	Original IP hdr (any options)	TCP	Data

IPv4 – AFTER APPLYING ESP

New IP hdr (any options)	ESP header	Original IP hdr (any options)	TCP	Data	ESP Trailer	ESP Auth

|<------------------- encrypted ------------------->|

|<--------- authenticated except for mutable fields -------->|

IPv6 – BEFORE APPLYING ESP

New IP hdr	ext hdrs if present	Orig IP hdr	ext hdrs if present	TCP	Data

IPv6 – AFTER APPLYING ESP

New IP hdr	New ext hdrs	ESP header	Orig IP hdr	Orig ext hdrs	TCP	Data	ESP Trailer	ESP Auth

|<------------------- encrypted ------------------->|

|<----- authenticated except for mutable fields ------->|

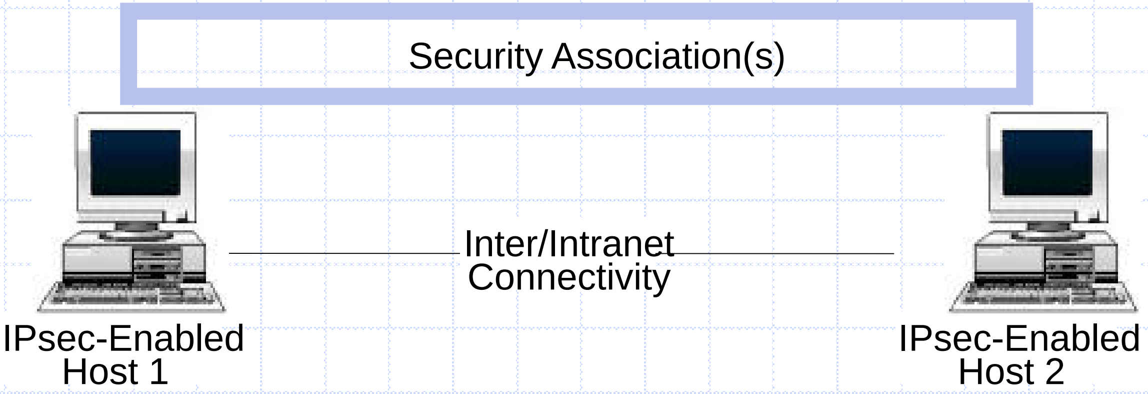
5.2.1.8 Traffic Processing

- When a node wants to send a packet to another node, this outbound packet will be compared against the SPD to determine what processing is required for the packet.
- If IPsec processing is required, the packet is mapped into an existing SA or SA bundle in the SAD.
- If there is no SA that is currently available, a new SA or SA bundle is created for the packet.
  - To create a new SA or SA bundle, the communicating nodes may need to use IKE to establish IKE SA (SA bundle) first.
  - After the IKE SA is authenticated, IPsec SA is created under the protection of IKE SA.
- Once IPsec SA is established, either AH or ESP (or both) can be used in either transport mode or tunnel mode to protect the packets.

5.2.1.9 IPsec Applications

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

Fig. 5.15 End-to-end security



Security Association(s)

Inter/Intranet Connectivity

IPsec-Enabled Host 1

IPsec-Enabled Host 2

Modes of operation:

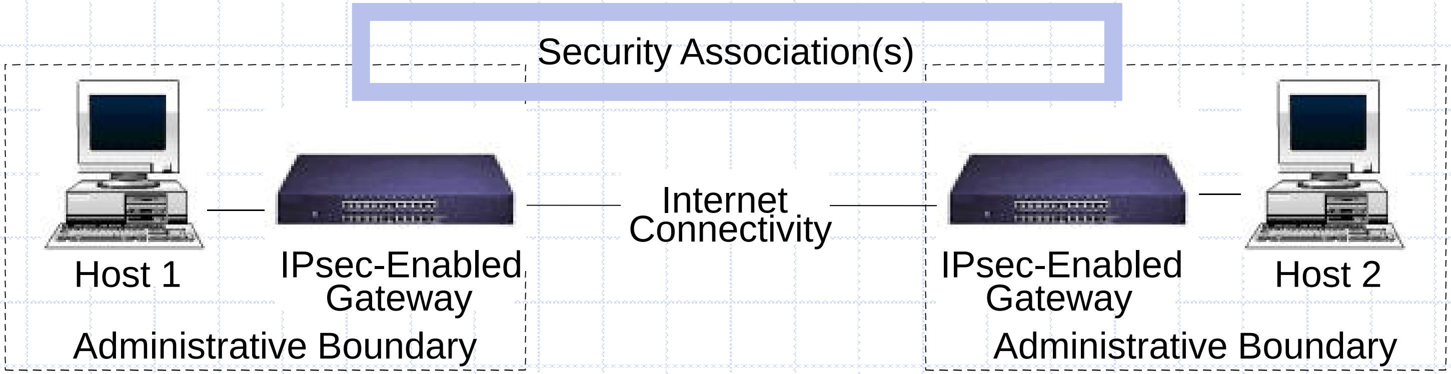
Transport

1	IP1	AH	upper	
2	IP1	ESP	upper	
3	IP1	AH	ESP	upper

Tunnel

1	IP2	AH	IP1	upper
2	IP2	ESP	IP1	upper

Fig. 5.16 VPN (virtual private network) with IPsec



Modes of Operation:

Tunnel

1	IP2	AH	IP1	upper
2	IP2	ESP	IP1	upper

Fig. 5.17 End-to-end with VPN security

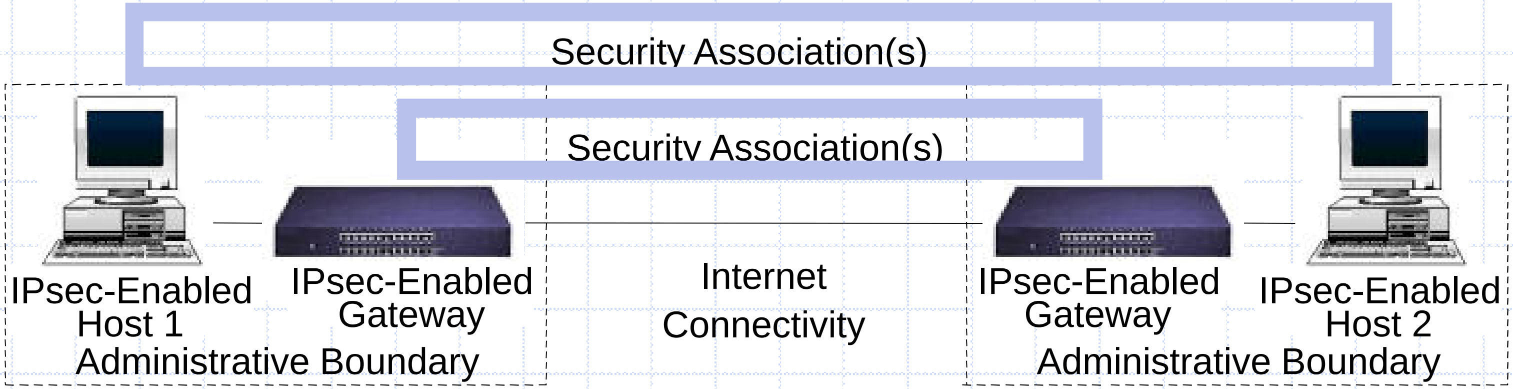
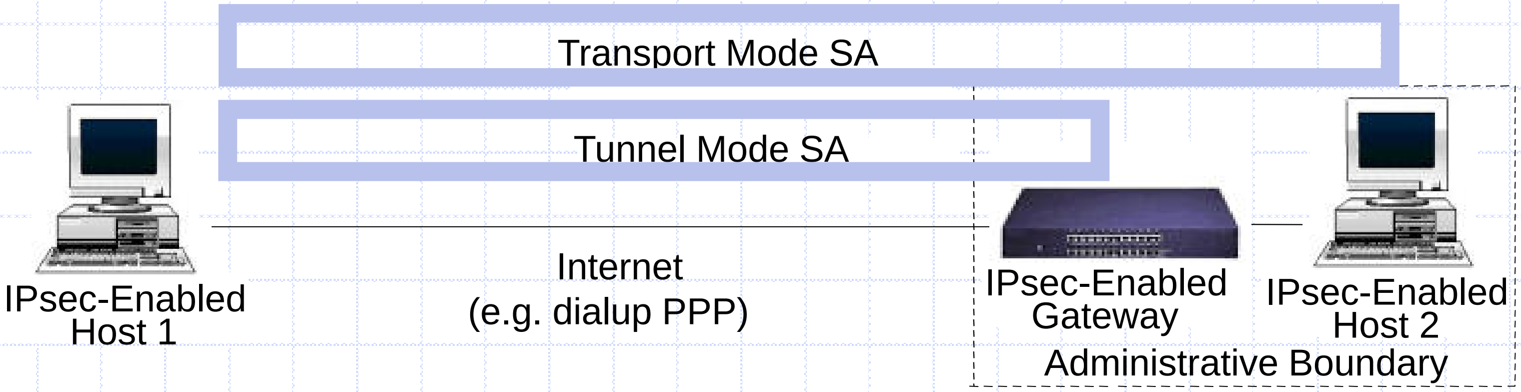


Fig. 5.18 Secured remote access



5.2.2 Authentication, Authorization, and Accounting (AAA)

5.2.2.1 Diameter

5.2.2.2 Diameter with Mobile IPv4 Application

AAA

- Remote Authentication Dial In User Service (RADIUS)
- SNMP
- COPS
- Diameter

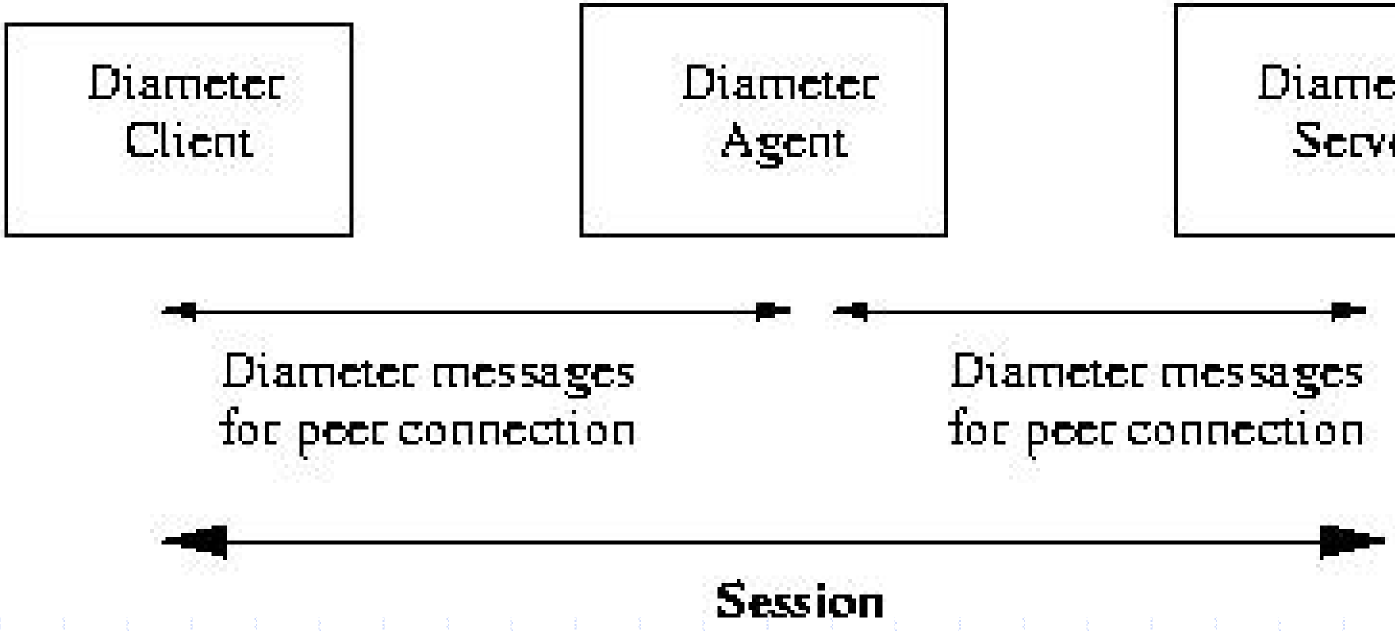
5.2.2.1 Diameter

- Provide a base protocol to support AAA
- Typically not used alone unless used only for accounting
- Peer-to-peer protocol
  - A peer could be a client, agent, or server
- A agent could be a relay, proxy, redirect, or translation agent

Attribute Value Pair (AVP)

- Messages exchanged between peers
- Contain a header and a protocol-specific data
- New Diameter applications can reuse existing AVPs and/or create new AVPs

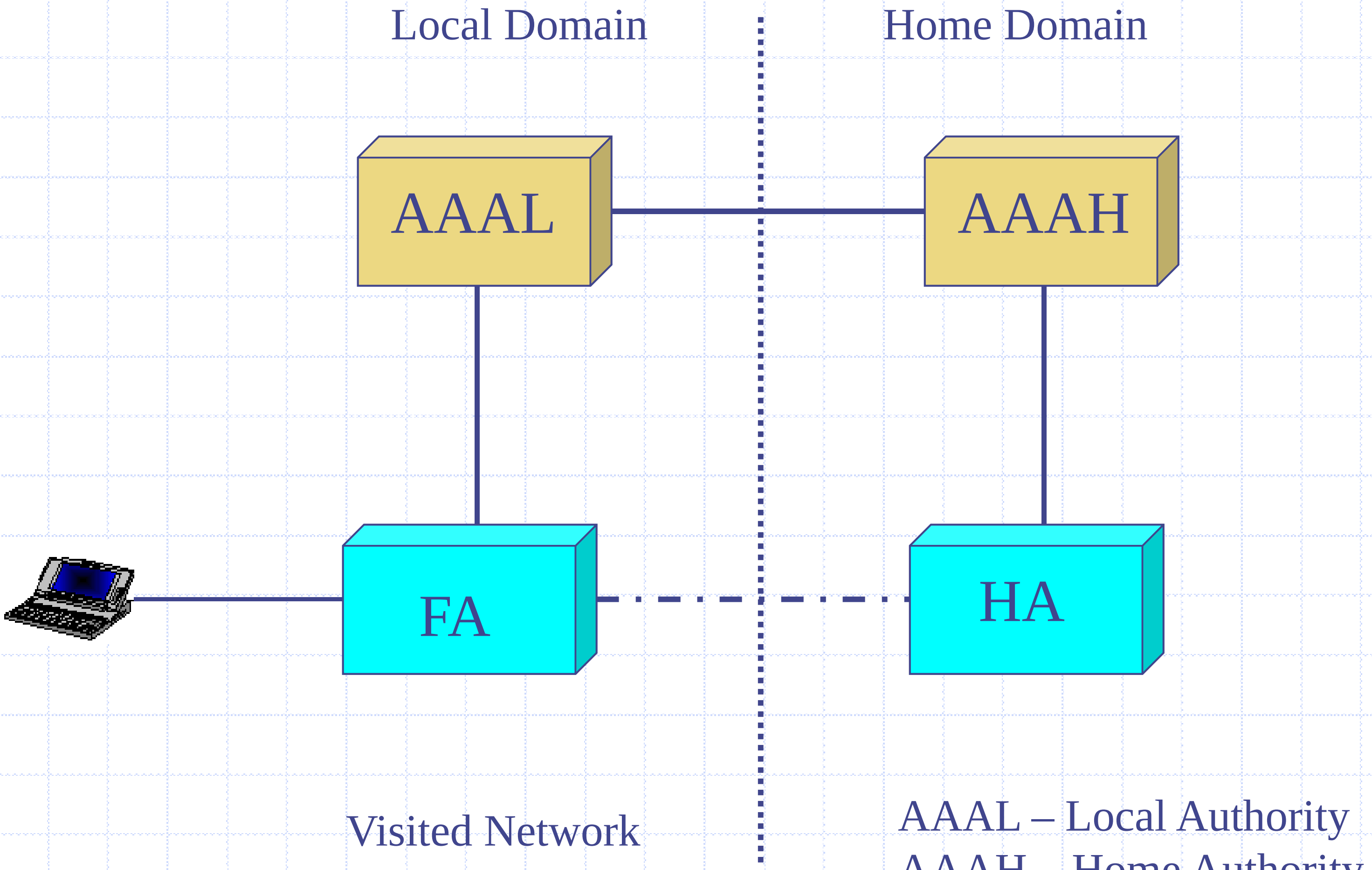
Fig. 5.19 Typical flows in Diameter


Diameter Client
Diameter Agent
Diameter Server
Diameter messages for peer connection
Diameter messages for peer connection
Session

5.2.2.2 Diameter with Mobile IPv4 Application

- Allow Diameter to be used to authenticate, authorize and collect accounting information for Mobile IPv4 services

Fig. 5.20 Mobile IP with AAA



AAAL – Local Authority
AAAH – Home Authority

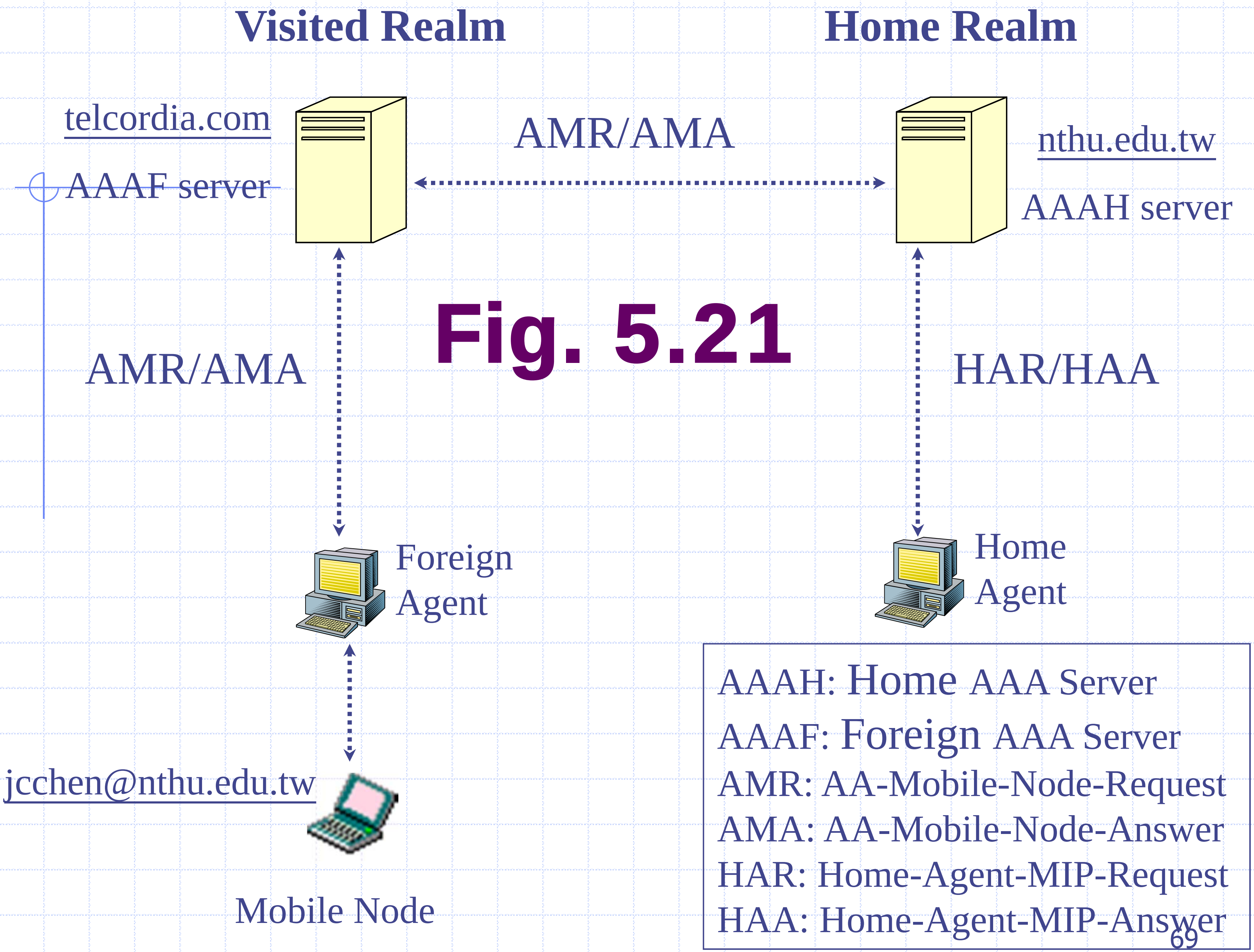
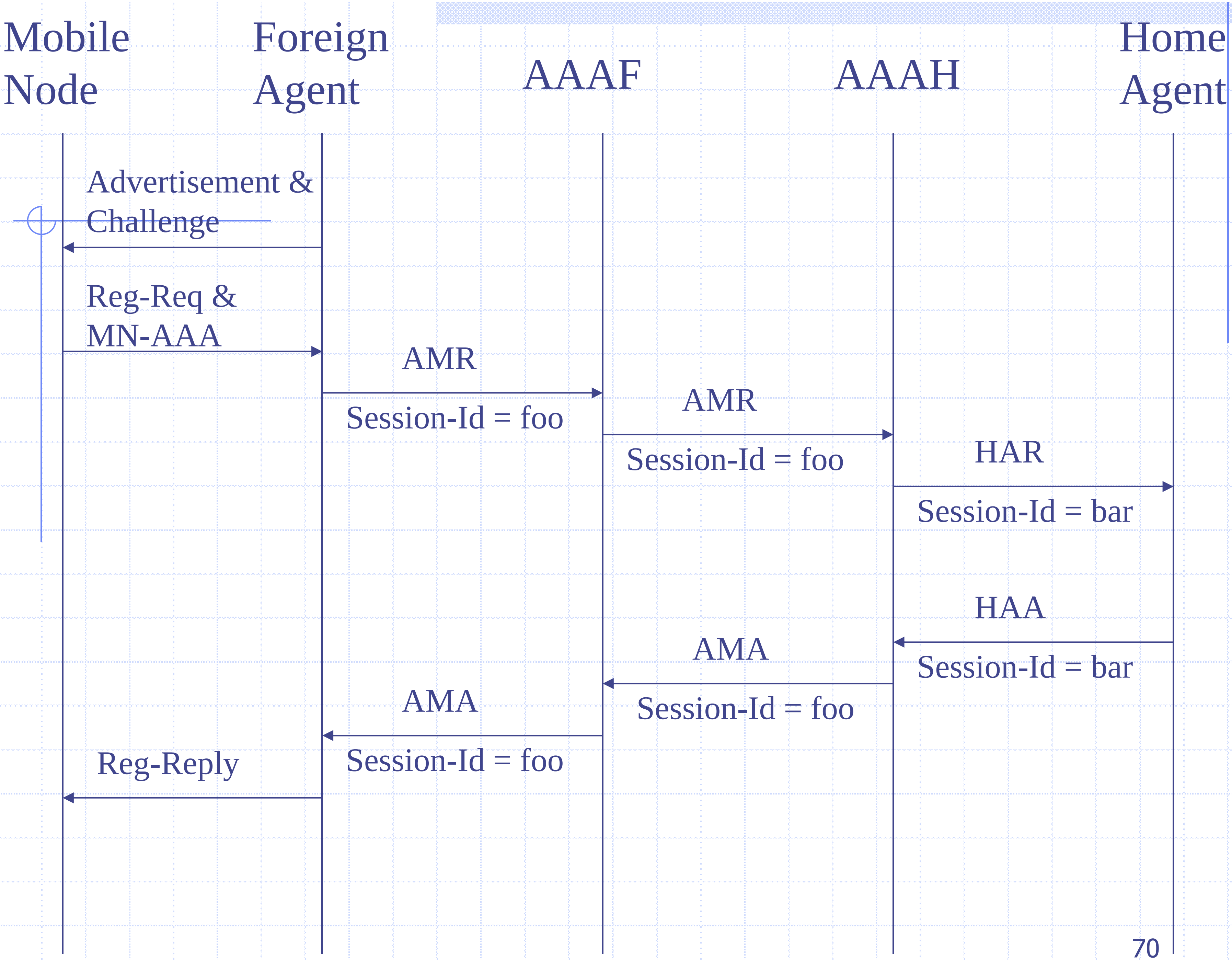


Fig. 5.21

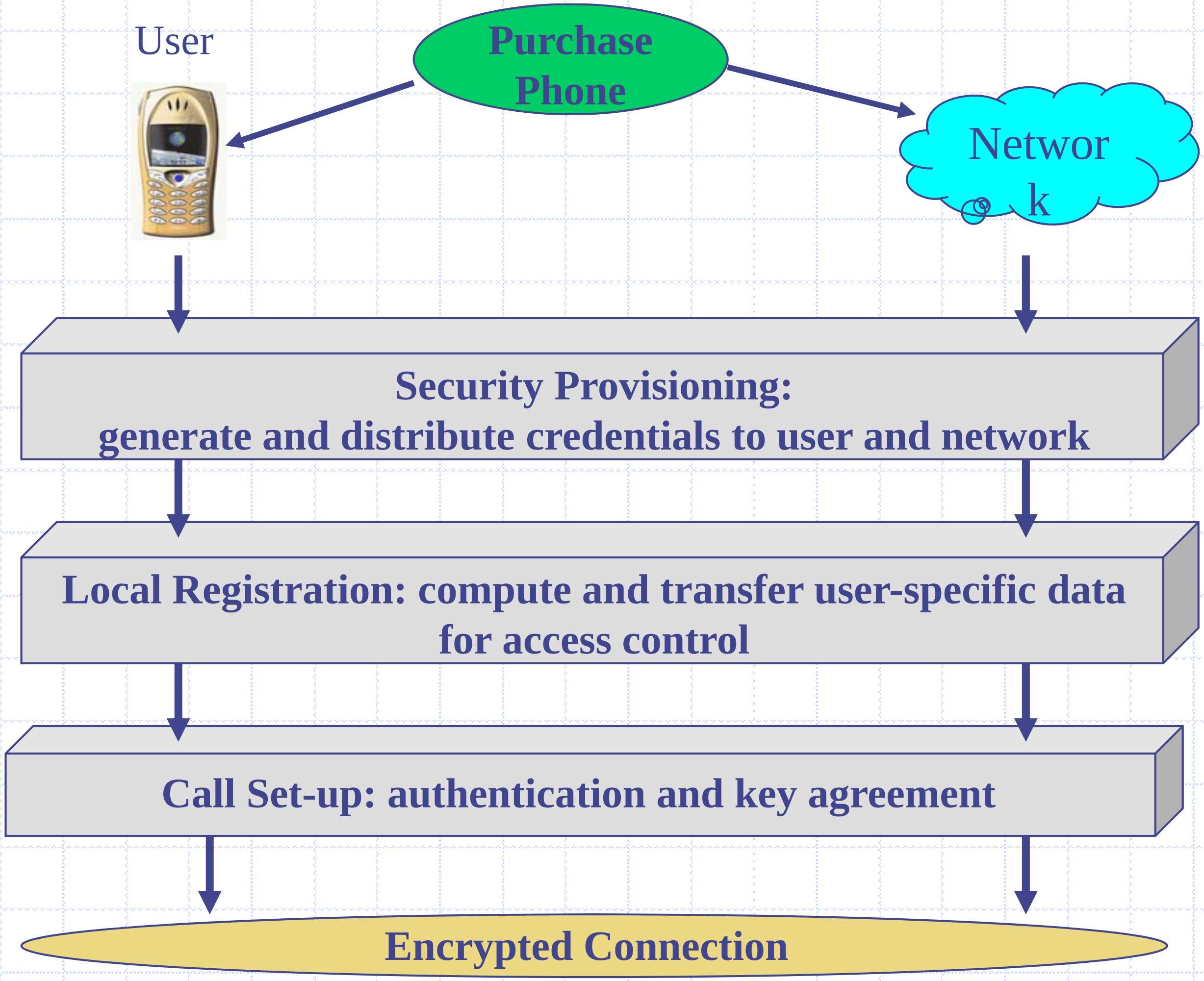
AAAH: Home AAA Server
AAAF: Foreign AAA Server
AMR: AA-Mobile-Node-Request
AMA: AA-Mobile-Node-Answer
HAR: Home-Agent-MIP-Request
HAA: Home-Agent-MIP-Answer


Mobile Node
Foreign Agent
AAAF
AAAH
Home Agent
Advertisement & Challenge
Reg-Req & MN-AAA
AMR
Session-Id = foo
AMR
Session-Id = foo
HAR
Session-Id = bar
HAA
Session-Id = bar
AMA
Session-Id = foo
AMA
Session-Id = foo
Reg-Reply

5.3 Security in Wireless Networks

- Security provisioning
- Local registration
- Authentication and key agreement (AKA)

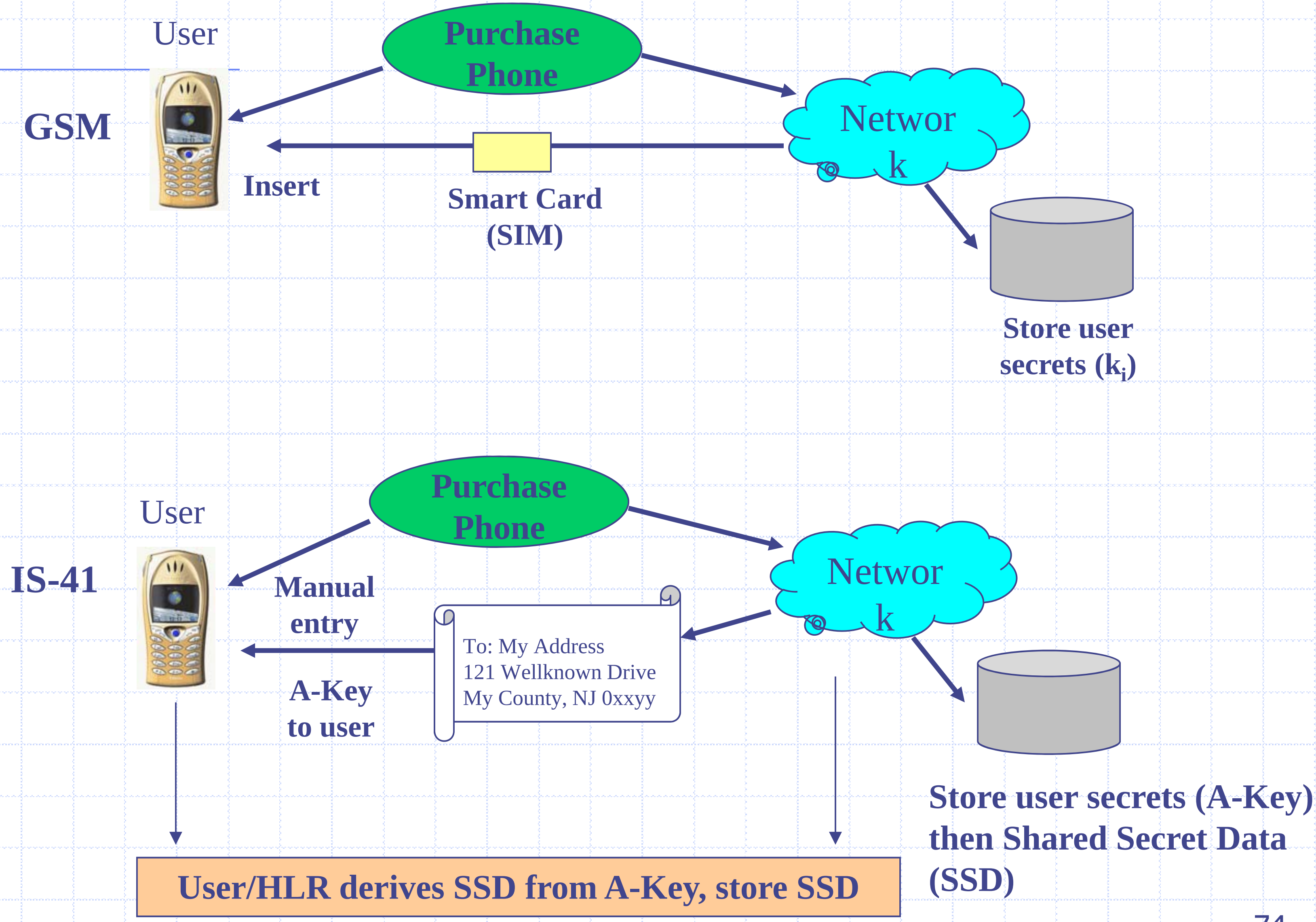
Fig. 5.23 Generic security model in cellular systems


User
Purchase Phone
Networ k
Security Provisioning: generate and distribute credentials to user and network
Local Registration: compute and transfer user-specific data for access control
Call Set-up: authentication and key agreement
Encrypted Connection

Security Provisioning

- In GSM
  - A secret key called K_i shared between the network operator and the user
- In IS-41
  - A secret key called *Authentication Key (A-key)* shared by the user and the network provider

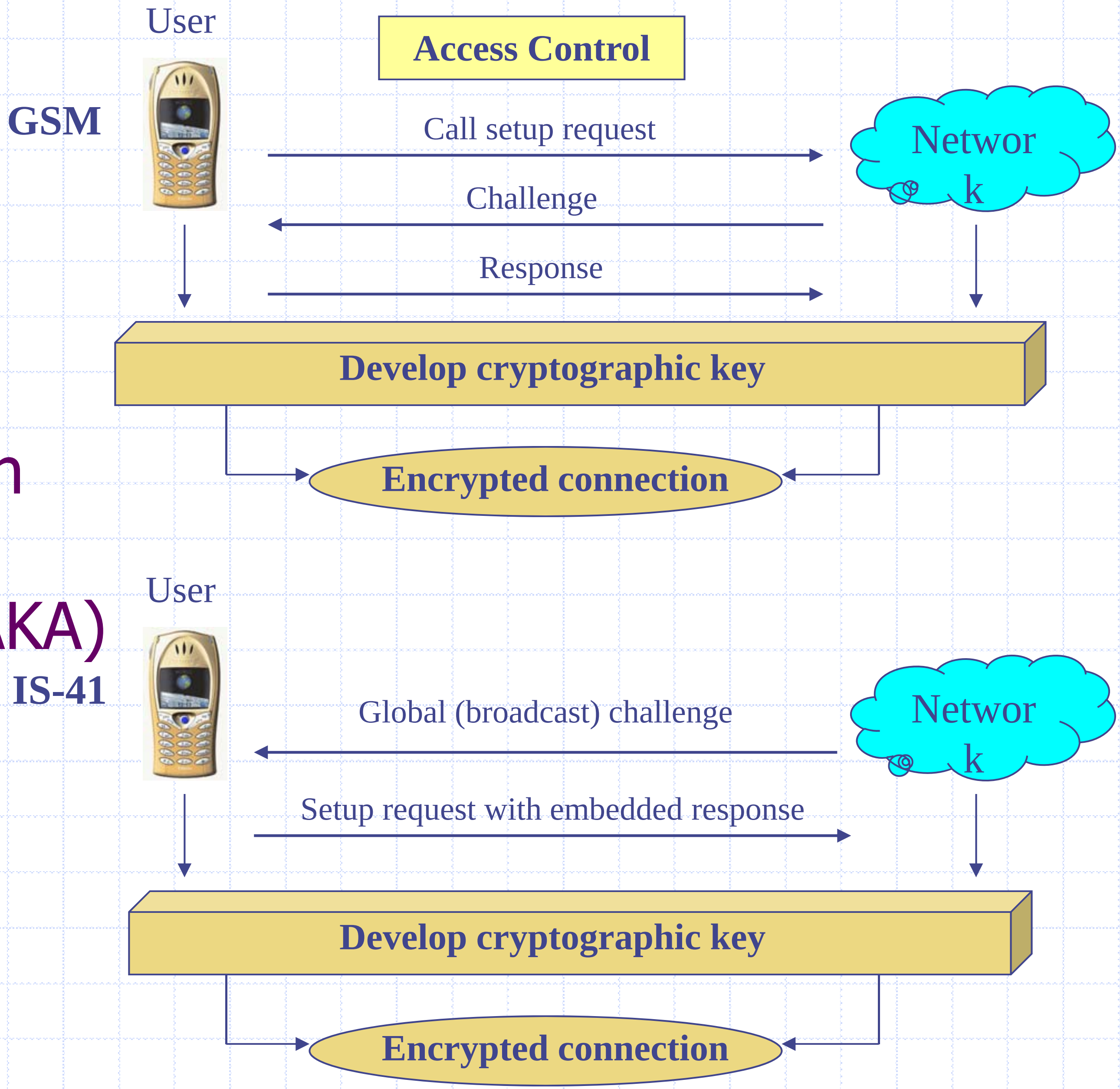
Fig. 5.24 Key generation and distribution



Authentication and Key Agreement (AKA)

- For GSM
  - Once the network receives a request for call setup, it challenges the user and expects a correct response from the user.
- For IS-41
  - Similar to GSM
  - IS-41 uses a global challenge that is broadcast periodically by the network

Fig. 5.25 Authentication and key agreement (AKA)



5.4 Security in IS-41

5.4.1 Secret Keys

5.4.2 Authentication

5.4.3 Privacy

IS-41 Security

- Independent of the air interface
- Subscribers don’t involve in the process
- Authentication Center (AC) is the primary functional entity
- Based on CAVE (Cellular Authentication and Voice Encryption) algorithm

Events for Authentication

- Registration
- Call origination
- Call termination

5.4.1 Secret Keys

- Authentication Key (A-key)
- Shared Secret Data (SSD)

Authentication Key (A-key)

- 64-bit *permanent* secret number used by MS and AC
- Installing A-key in the MS is not standardized
  - Program A-key manually: TIA/EIA TSB50
  - Over-the-air A-key programming: IS-725
- A-key is never transmitted over the air or passed between systems

Shared Secret Data (SSD)

- A 128-bit temporary secret key calculated in both MS and AC
- Can be shared with the serving system (VLR, etc.)
- Two parts
  - SSD-A: for authentication
  - SSD-B: for confidentiality

Generation of SSD

- Using CAVE algorithm
- Generate SSD random number (RANDSSD)
- Propagate to HLR/AC
  - Retrieve ESN (Electronic Serial Number) and MIN (Mobile ID)
- Propagate to the MS
- Generate SSD based on A-key, ESN, and RANDSSD
  - both MS and network

Fig. 5.26 Generation of shared secret data (SSD)

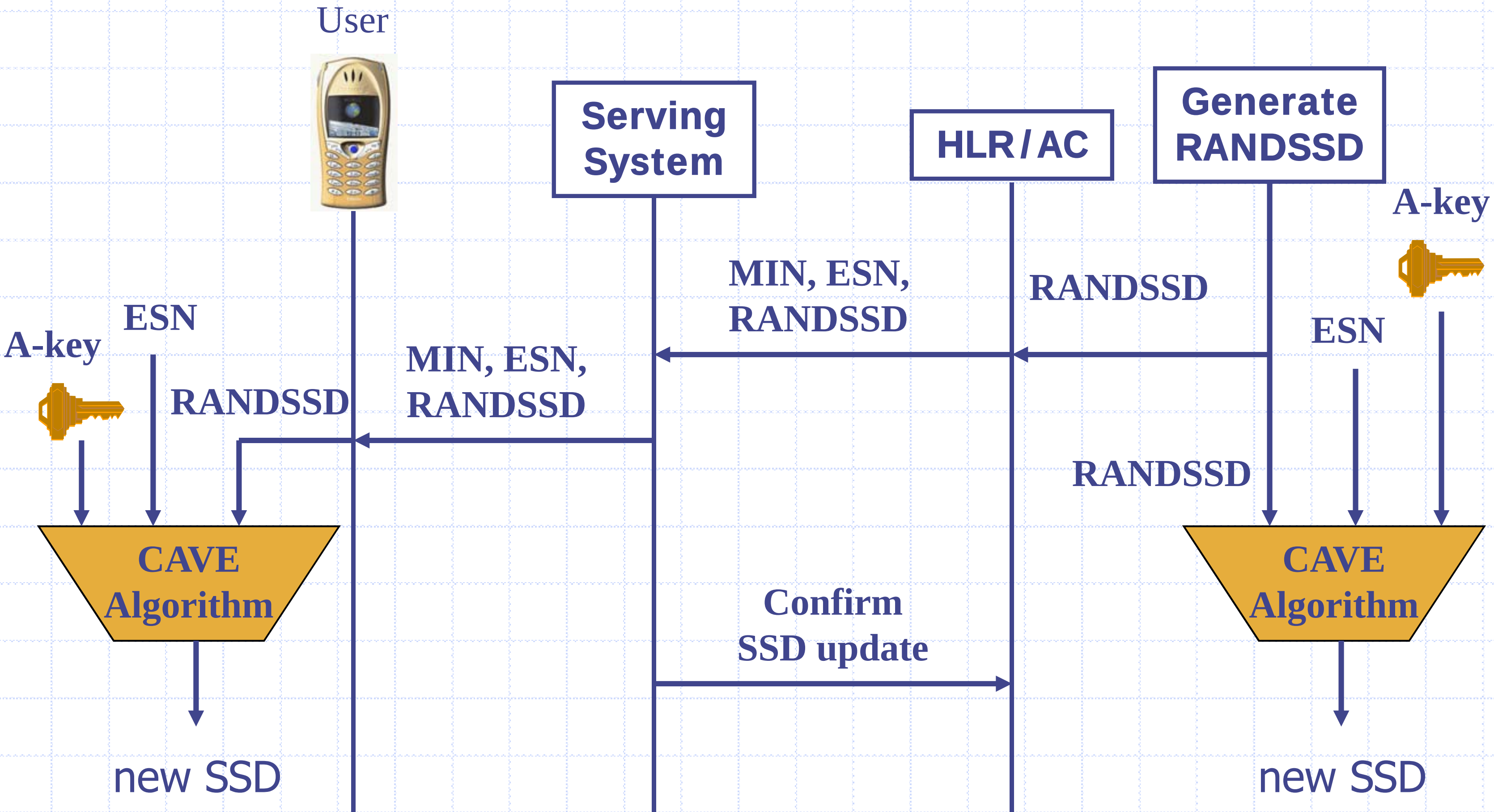
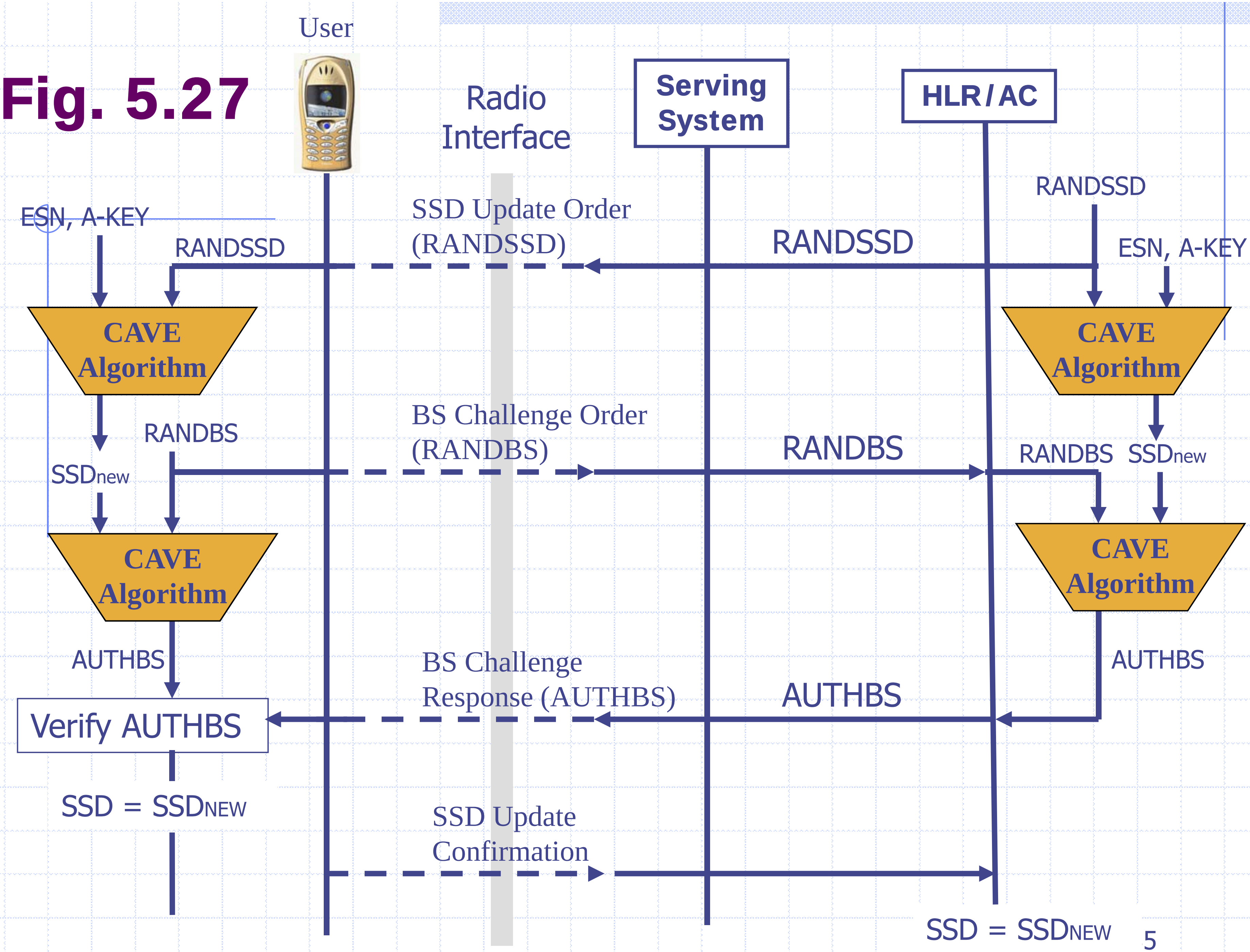


Fig. 5.27


User
Radio Interface
Serving System
HLR / AC
ESN, A-KEY
RANDSSD
SSD Update Order (RANDSSD)
RANDSSD
RANDSSD
ESN, A-KEY
CAVE Algorithm
CAVE Algorithm
RANDBS
SSDnew
BS Challenge Order (RANDBS)
RANDBS
RANDBS
SSDnew
CAVE Algorithm
CAVE Algorithm
AUTHBS
BS Challenge Response (AUTHBS)
AUTHBS
AUTHBS
Verify AUTHBS
SSD = SSDNEW
SSD Update Confirmation
SSD = SSDNEW

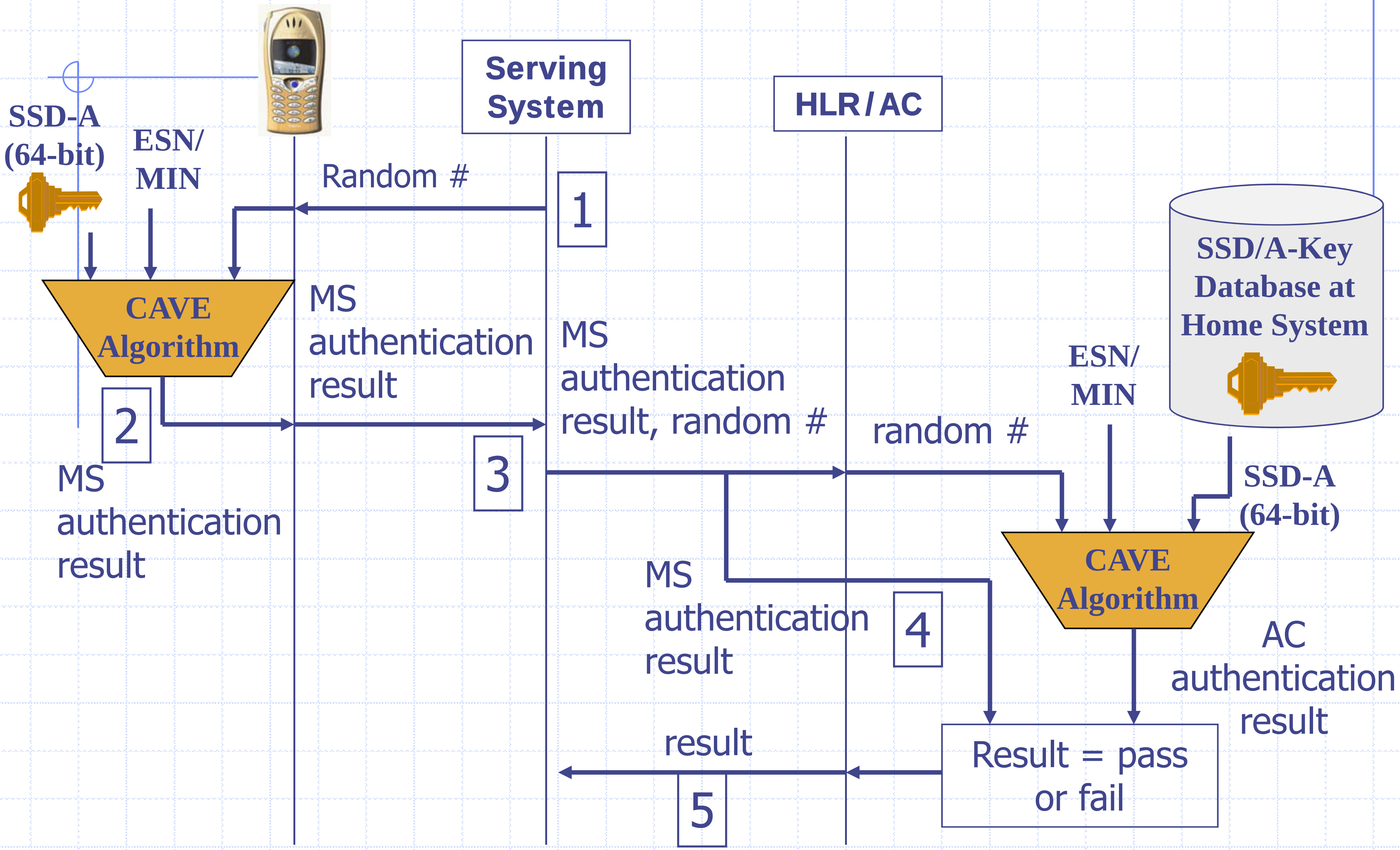
5.4.2 Authentication

- Global challenge
- Unique challenge

Global Challenge

- Serving system presents a challenge to all MSs using a particular radio control channel
  - Broadcast and update periodically
- AC verifies the response from an MS

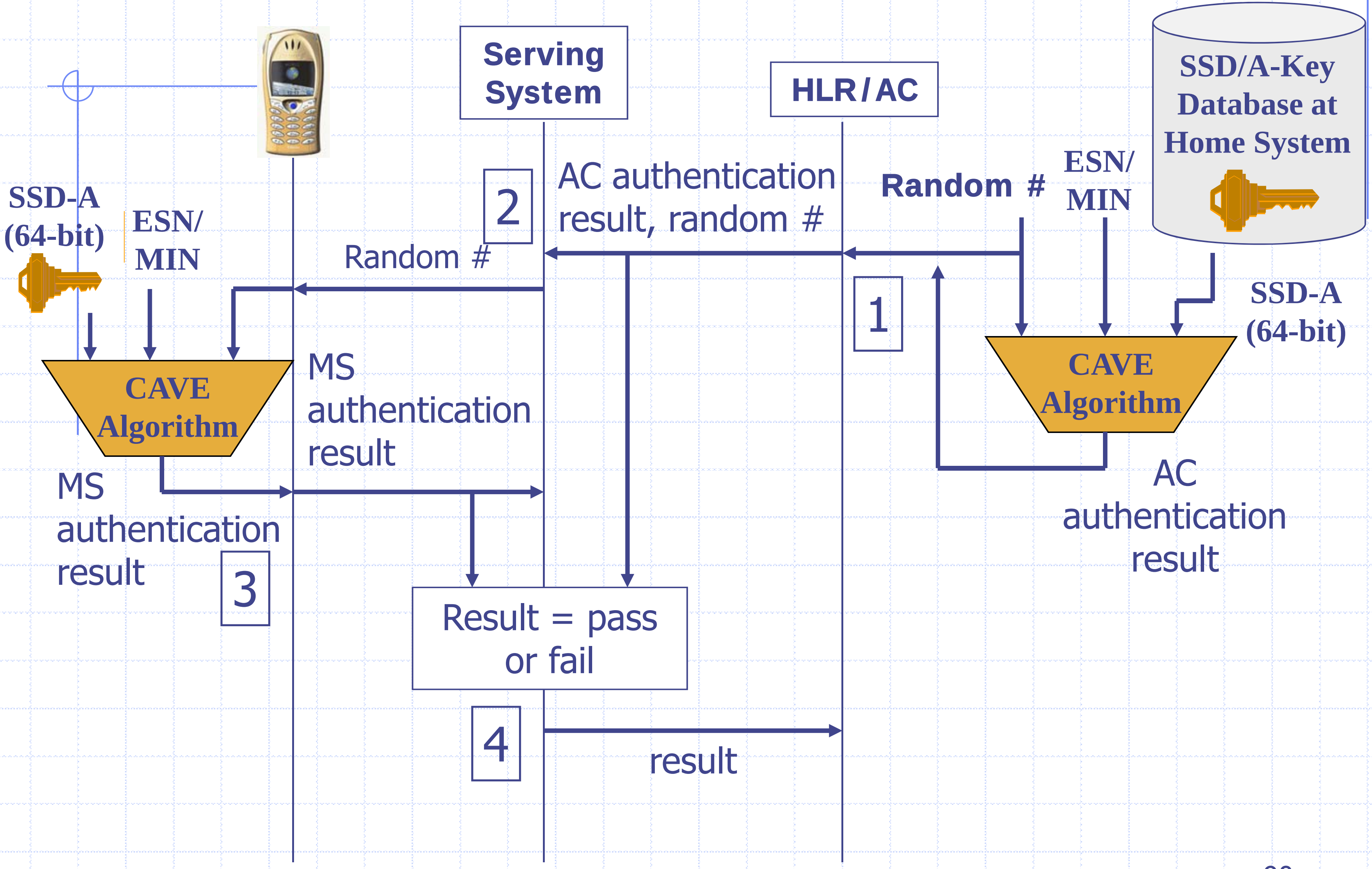
Fig. 5.28 Global challenge in CAVE algorithm



Unique Challenge

- AC directs the serving system to issue a challenge to a single MS which either is requesting service or is already engaged in a call
- MS and AC pass the calculation to the serving system
- The serving system verifies the authentication response

Fig. 5.29 Unique challenge in CAVE algorithm



5.4.3 Privacy

- Voice Privacy (VP)
  - VPMASK: generated using CAVE and SSD-B
- Signaling Message Encryption (SME)
  - Only certain fields of signaling messages are encrypted
  - SMEKEY: generated using CAVE and SSD-B
  - Cellular Message Encryption Algorithm (CMEA)
- Between MS and BS only

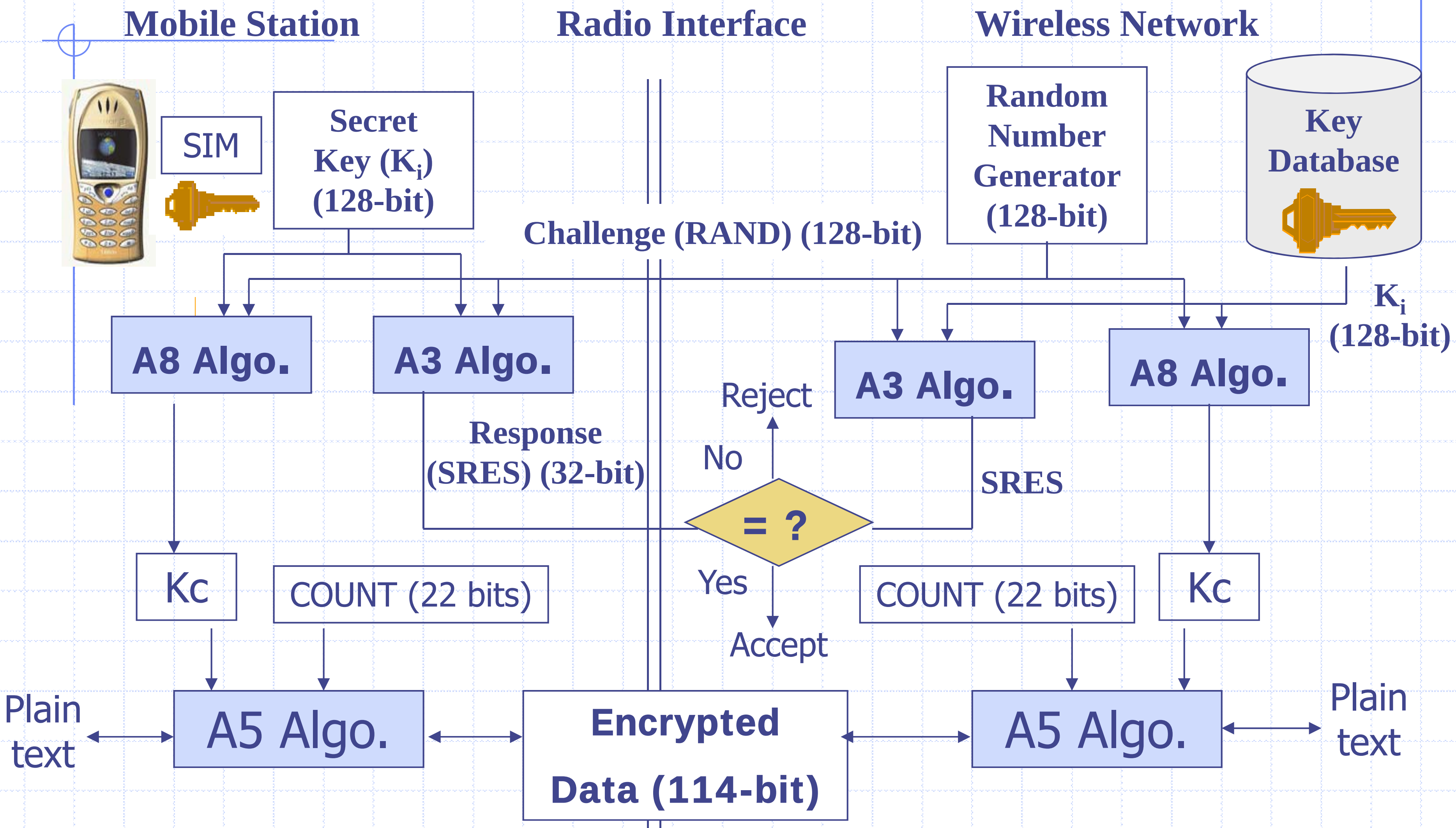
Weakness

- A 64-bit key may not be long enough
- Single cryptographic algorithm for authentication and privacy
- Does not provide for authentication of the network
- Critical key provisioning step required to get A-key to MS and AC
- Use of SSD and its periodic updating introduces complexity into the authentication process

5.5 Security in GSM

- Three algorithms
  - A3: authentication
  - A5: stream cipher algorithm
  - A8: cipher key generation

Fig. 5.30 GSM algorithms



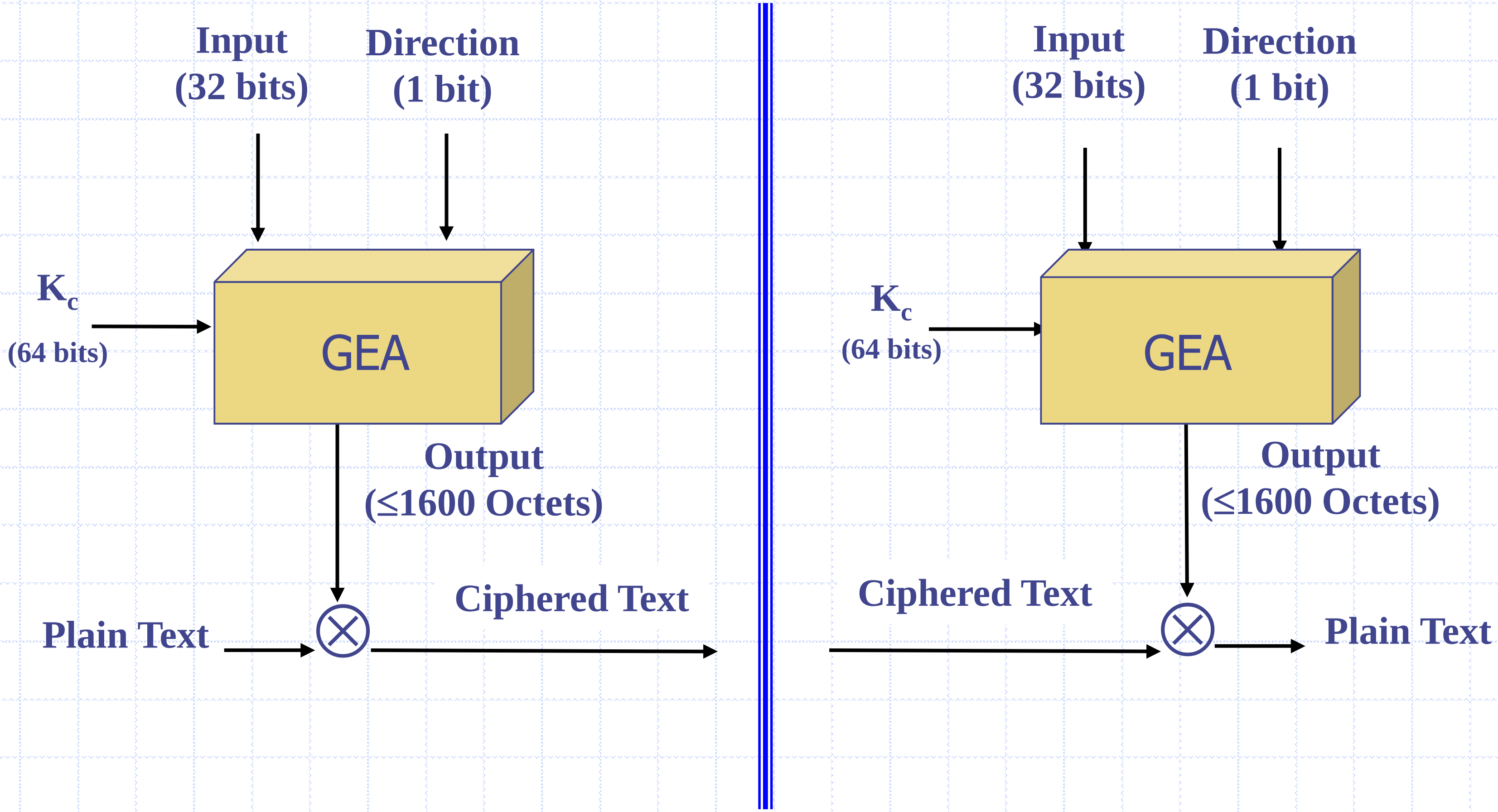
Weakness

- Does not provide for authentication of the network
- The home system trusts the visited system to handle cryptographic keying material, and to authenticate the MS
- Assume that the intersystem signaling links are secure
- A 64-bit key (Kc) may not long enough
- Lack of end-to-end encryption
- A number of attacks on the A5 algorithm have been reported

5.6 Security in GPRS

- Authentication: GSM authentication
- Confidentiality: GPRS Encryption Algorithm (GEA)
  - restricted to MS-SGSN encryption
  - installed in the MS and SGSN
  - ciphering for uplink and downlink are generated from different inputs

Fig. 5.31 GPRS encryption algorithm (GEA)



5.7 Security in 3GPP

5.7.1 Security Principles

5.7.2 Security Architecture

5.7.3 Network Access Security

5.7.4 Network Domain Security

5.7.5 Summary

5.7.1 Security Principles

- 3G security will build on the security of second generation systems. Security elements within GSM and other second generation systems that have proved to be **needed** and **robust** shall be adopted for 3G security.
- 3G security will improve on the security of second generation systems - 3G security will address and correct real and perceived weaknesses in second generation systems.
- 3G security will offer new security features and will secure new services offered by 3G.

Definitions

- **Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.
- **Data integrity:** The property that data has not been altered in an unauthorised manner.
- **Data origin authentication:** The corroboration that the source of data received is as claimed.
- **Entity authentication:** The provision of assurance of the claimed identity of an entity.
- **Key freshness:** A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

Definitions (Cont.)

- **GSM Entity authentication and key agreement:** The entity Authentication and Key Agreement procedure to provide authentication of a SIM to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20.
- **User**: Within the context of this specification a user is either a UMTS subscriber or a GSM Subscriber or a physical person as defined in TR 21.905.
- **UMTS subscriber**: a Mobile Equipment with a UICC inserted and activated USIM-application.
- **GSM subscriber**: a Mobile Equipment with a SIM inserted or a Mobile Equipment with a UICC inserted and activated SIM-application.

Definitions (Cont.)

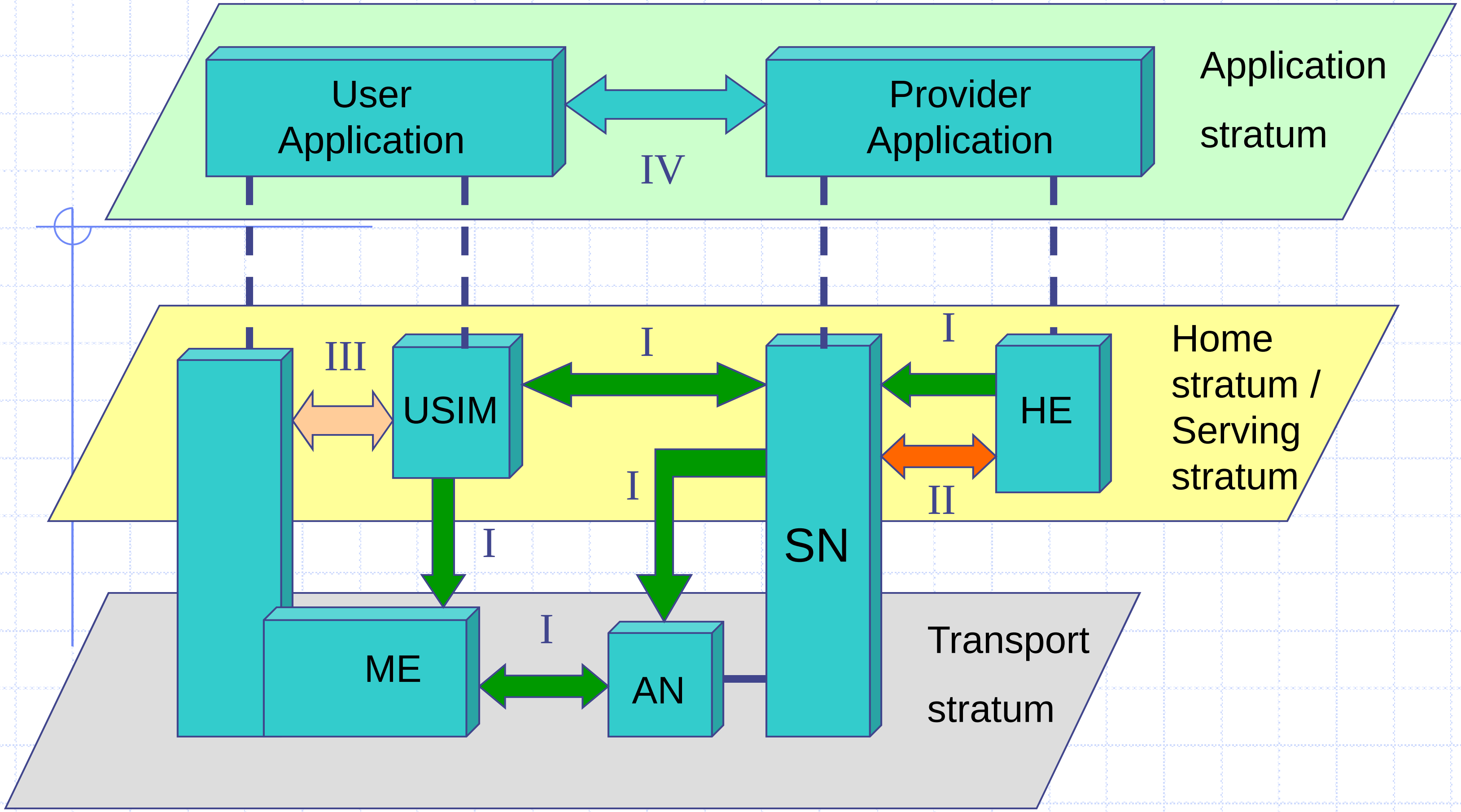
- **UMTS security context:** a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. One is still in a UMTS security context, if the keys CK/IK are converted into Kc to work with a GSM BSS.
- **GSM security context:** a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.
- **Quintet, UMTS authentication vector:** temporary authentication and key agreement data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Definitions (Cont.)

- **Authentication vector:** either a quintet or a triplet.
- **Temporary authentication data:** either UMTS or GSM security context data or UMTS or GSM authentication vectors.
- **R98-:** Refers to a network node or ME that conforms to R97 or R98 specifications.
- **R99+:** Refers to a network node or ME that conforms to R99 or later specifications.
- **R99+ ME capable of UMTS AKA**: either a R99+ UMTS only ME, a R99+ GSM/UMTS ME, or a R99+ GSM only ME that does support USIM-ME interface.
- **R99+ ME not capable of UMTS AKA**: a R99+ GSM only ME that does not support USIM-ME interface.

5.7.2 Security Architecture

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations;
- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages;
- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.



HE: Home environment

SN: Serving Network

AN: Access Network

ME: Mobile Equipment

USIM: Universal Subscriber Identification Module

Fig. 5.32 3GPP security architecture

Visibility

- Indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up.
- Indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G -> 2G).

Configurability

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

5.7.3 Network Access Security

5.7.3.1 Authentication and Key Agreement (AKA)

5.7.3.2 UMTS Encryption Algorithm (UEA)

5.7.3.3 UMTS Integrity Algorithm (UIA)

5.7.3.1 Authentication and Key Agreement (AKA)

- Main purpose
  - Mutual authentication
  - Establish a new pair of cipher and integrity keys
- Secret key K: shared between and available only to the USIM and the AuC in the user's HE
- SQN_{HE}: an individual counter for each user kept in HE
- SQN_{MS}: the highest sequence number the USIM has accepted
- Achieve maximum compatibility with the current GSM security architecture

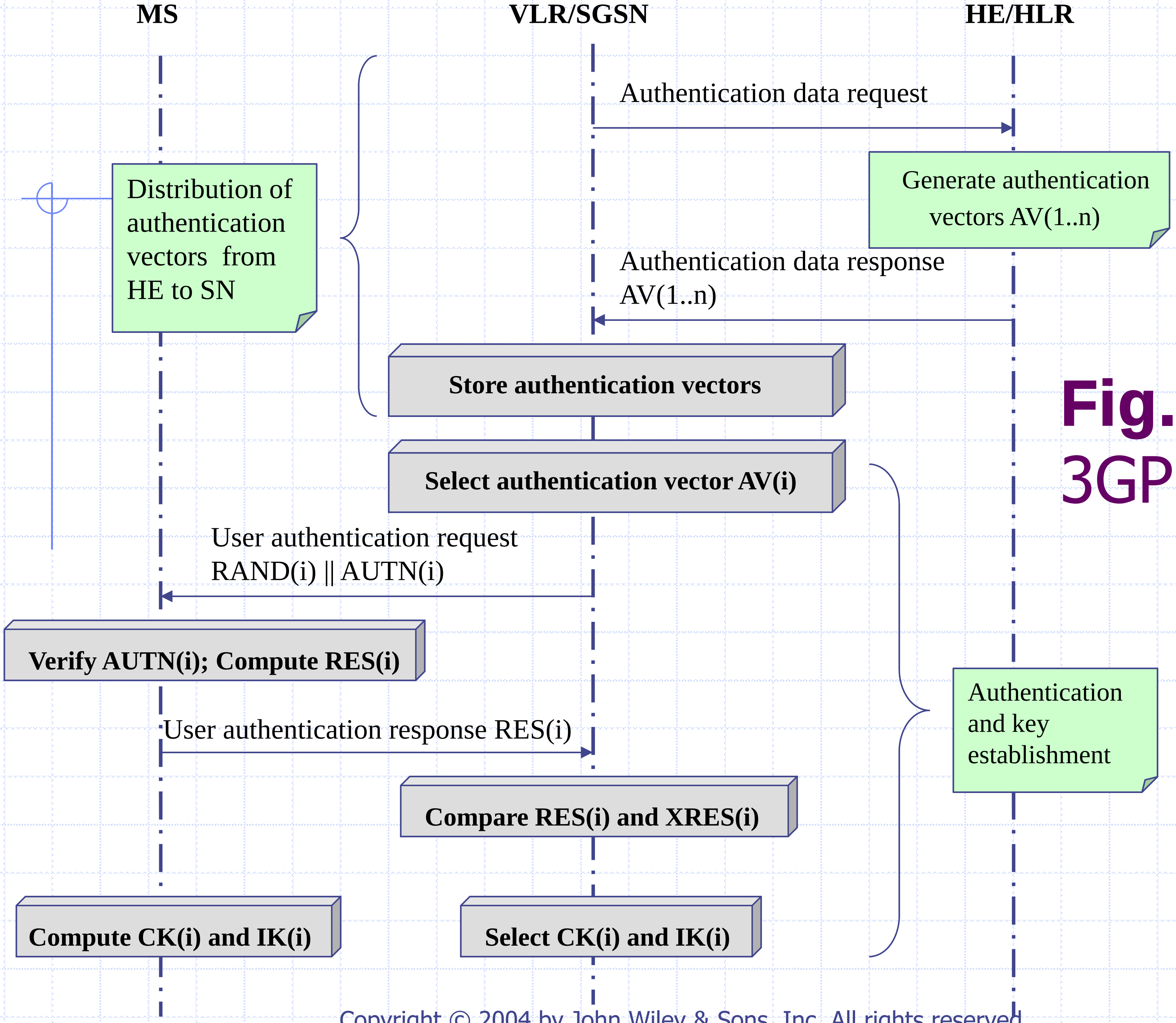
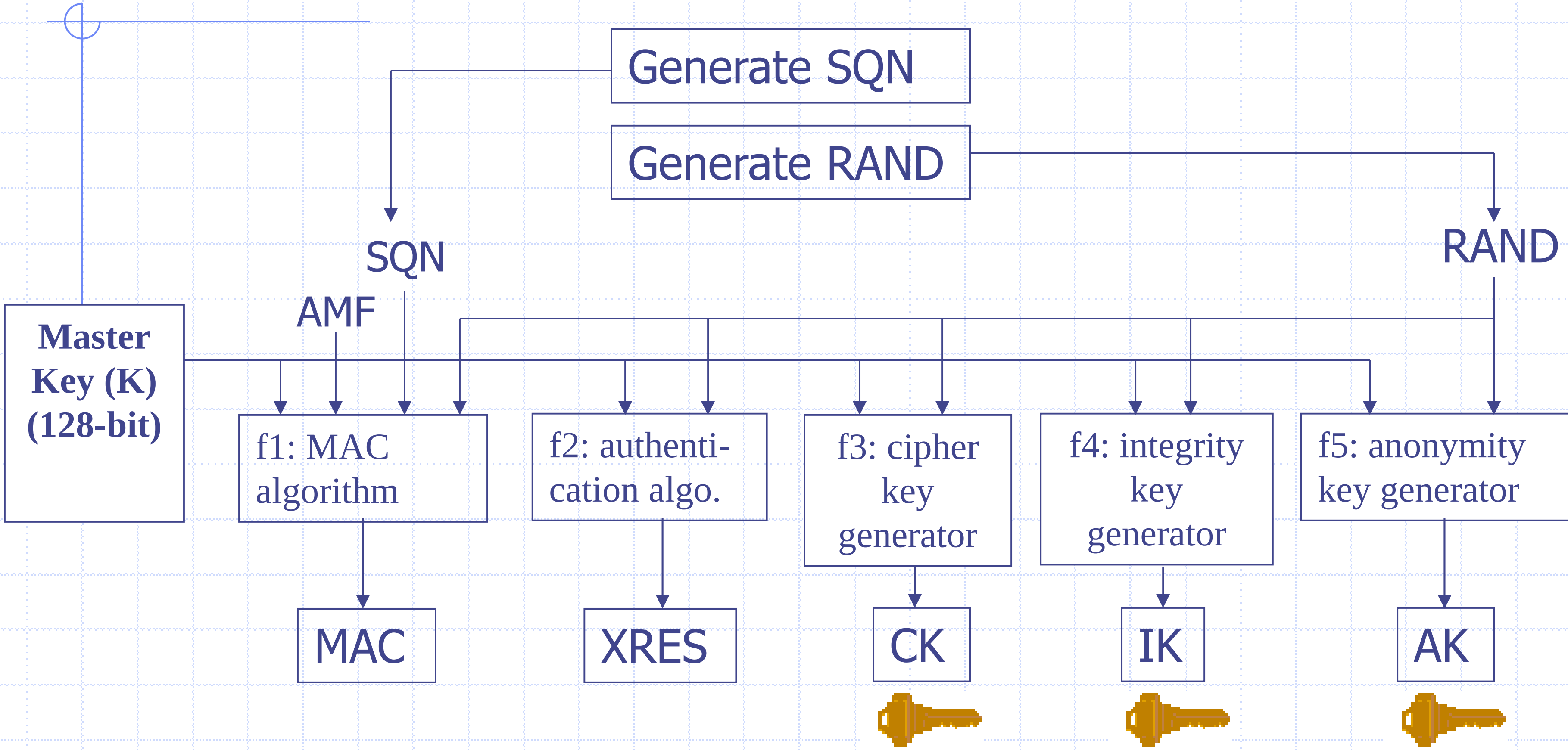

MS
VLR/SGSN
HE/HLR
Authentication data request
Generate authentication vectors AV(1..n)
Distribution of authentication vectors from HE to SN
Authentication data response AV(1..n)
Store authentication vectors
Select authentication vector AV(i)
User authentication request RAND(i) || AUTN(i)
Verify AUTN(i); Compute RES(i)
User authentication response RES(i)
Authentication and key establishment
Compare RES(i) and XRES(i)
Compute CK(i) and IK(i)
Select CK(i) and IK(i)

Fig. 5.33 3GPP AKA

Authentication Vector (AV)

- Ordered based on sequence number
- Consists of the following components
  - a random number RAND
  - an expected response XRES
  - a cipher key CK
  - an integrity key IK
  - an authentication token AUTN
- Each authentication vector is good for one AKA between the VLR/SGSN and the USIM

Fig. 5.34 Generation of authentication vectors



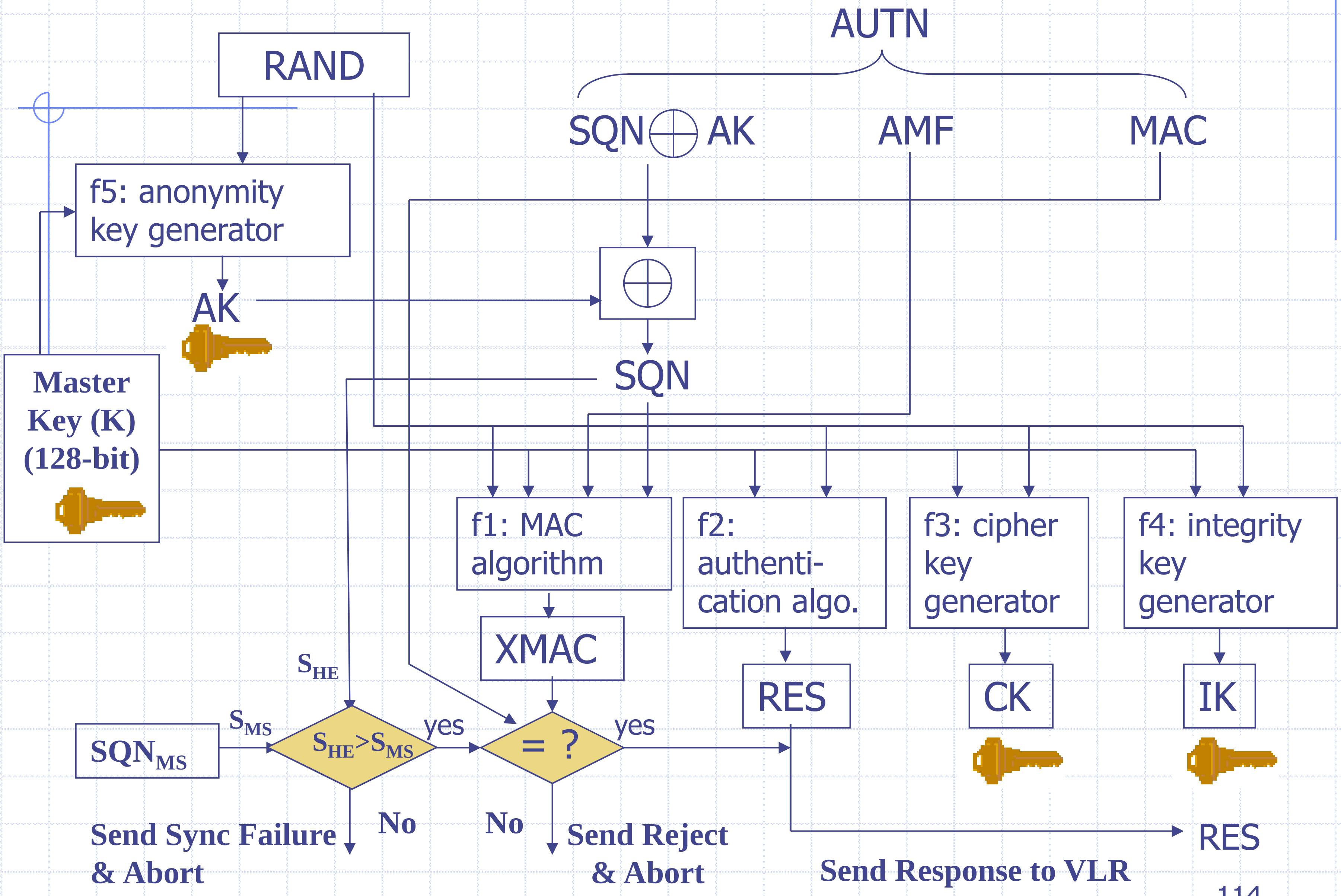
AUTN := SQN ⊕ AK || AMF || MAC

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

Anonymity Key (AK)

- AK is used to conceal the sequence number (SQN)
  - SQN may expose the identity and location of the user
- f5 $\equiv$ 0, i.e. AK = 0 if no concealment is needed

Fig. 5.35 Authentication process in USIM



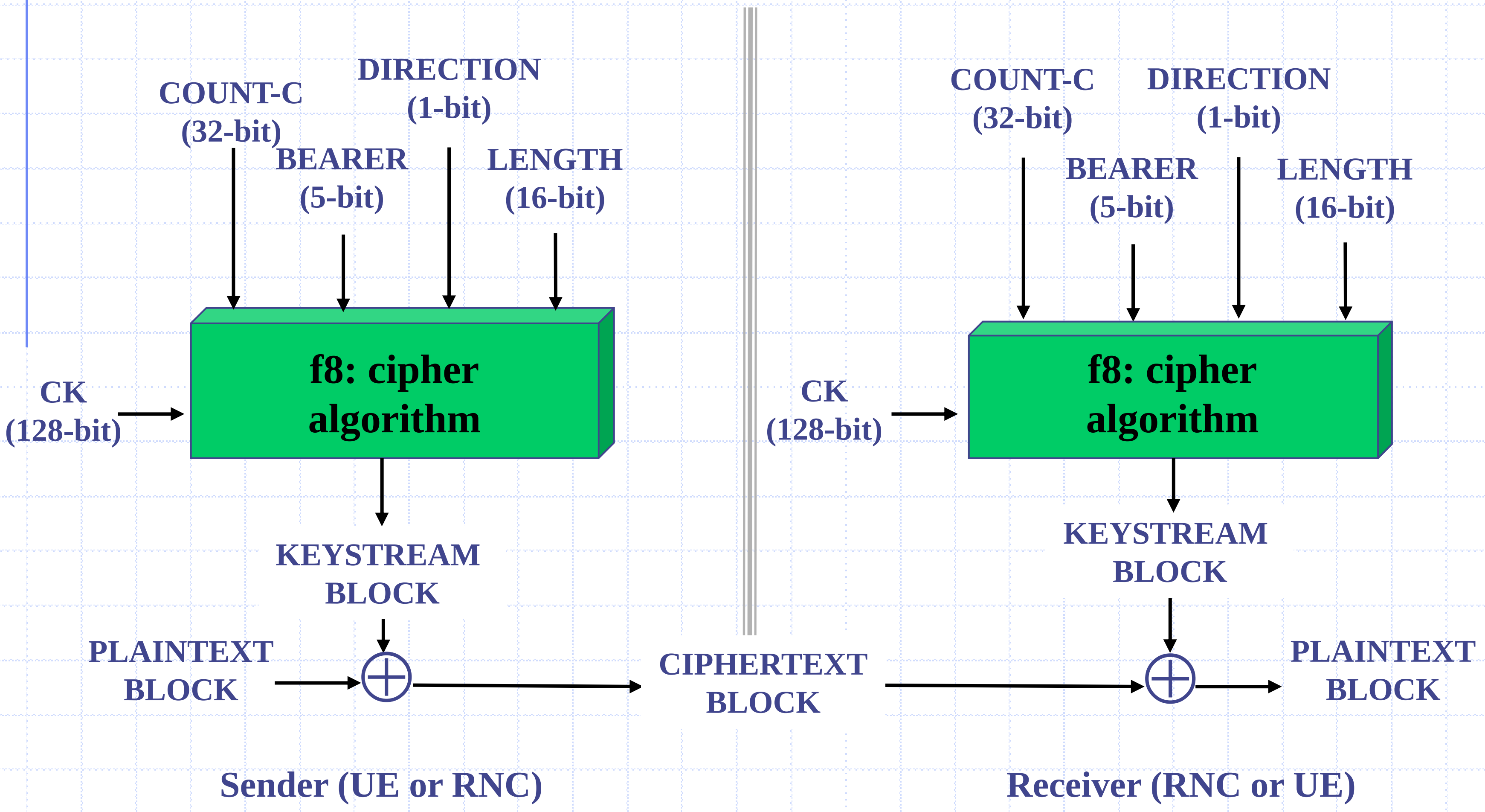
Key Length

- K: 128 bits
- RAND: 128 bits
- SQN: 48 bits
- AK: 48 bits
- AMF: 16 bits
- MAC: 64 bits
- CK: 128 bits
- IK: 128 bits
- RES: 32-128 bits

5.7.3.2 UMTS Encryption Algorithm (UEA)

- Access Link Data Confidentiality
- For data and some signaling traffic
- Applied on dedicated channels between ME and RNC

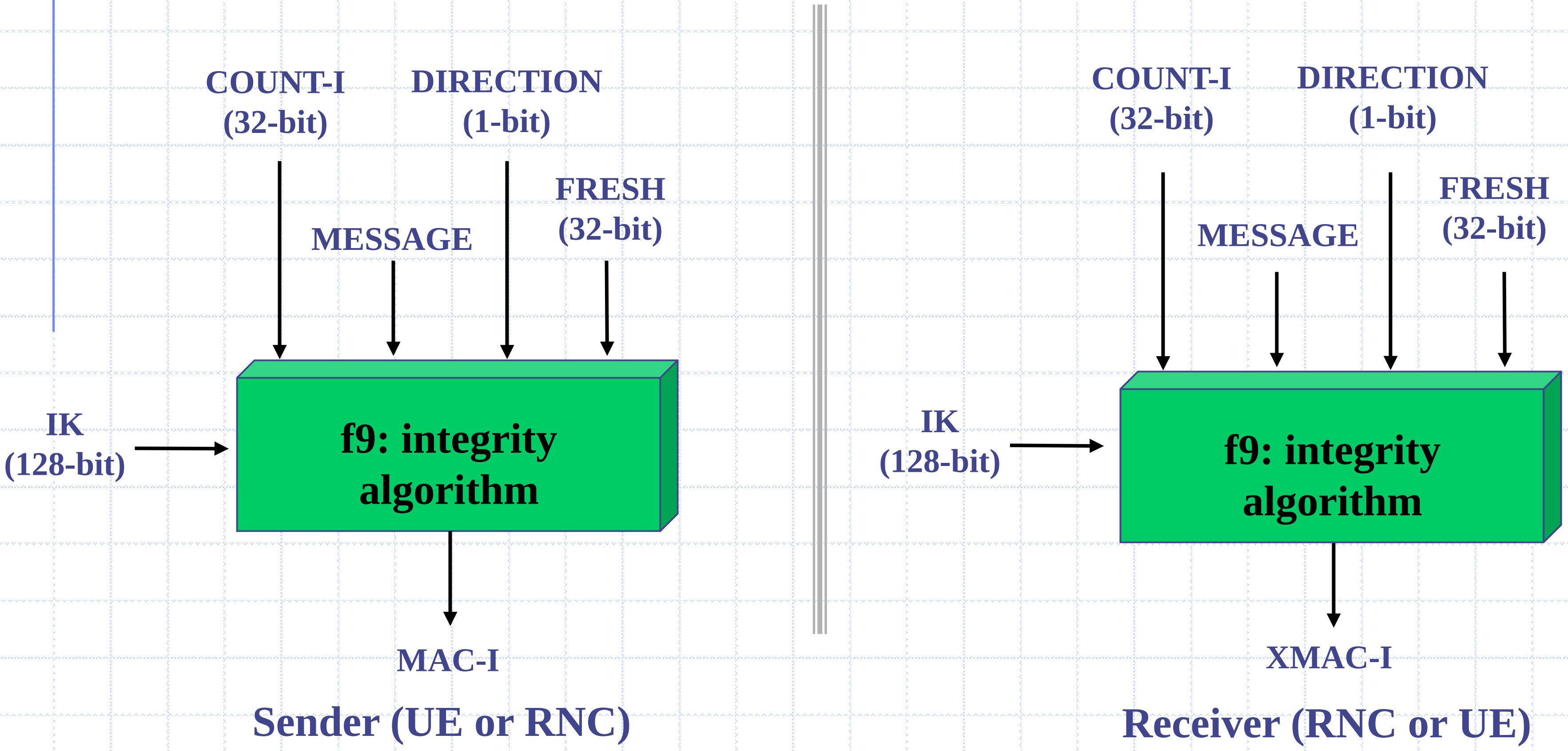
Fig. 5.36 UMTS encryption algorithm (UEA)



5.7.3.3 UMTS Integrity Algorithm (UIA)

- Access Link Data Integrity
- Shall be implemented in the ME and in the RNC
- Most control signaling messages between ME and RNC are integrity protected
- Integrity protection should be applied at the RRC layer

Fig. 5.37 UMTS integrity algorithm (UIA)



COUNT-I (32-bit)

DIRECTION (1-bit)

MESSAGE

FRESH (32-bit)

IK (128-bit)

f9: integrity algorithm

MAC-I

Sender (UE or RNC)

COUNT-I (32-bit)

DIRECTION (1-bit)

MESSAGE

FRESH (32-bit)

IK (128-bit)

f9: integrity algorithm

XMAC-I

Receiver (RNC or UE)

FRESH

- At connection set-up the RNC generates a random value FRESH and sends it to the user.
- The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection.
- This mechanism protects the network against replay of signalling messages by the user.

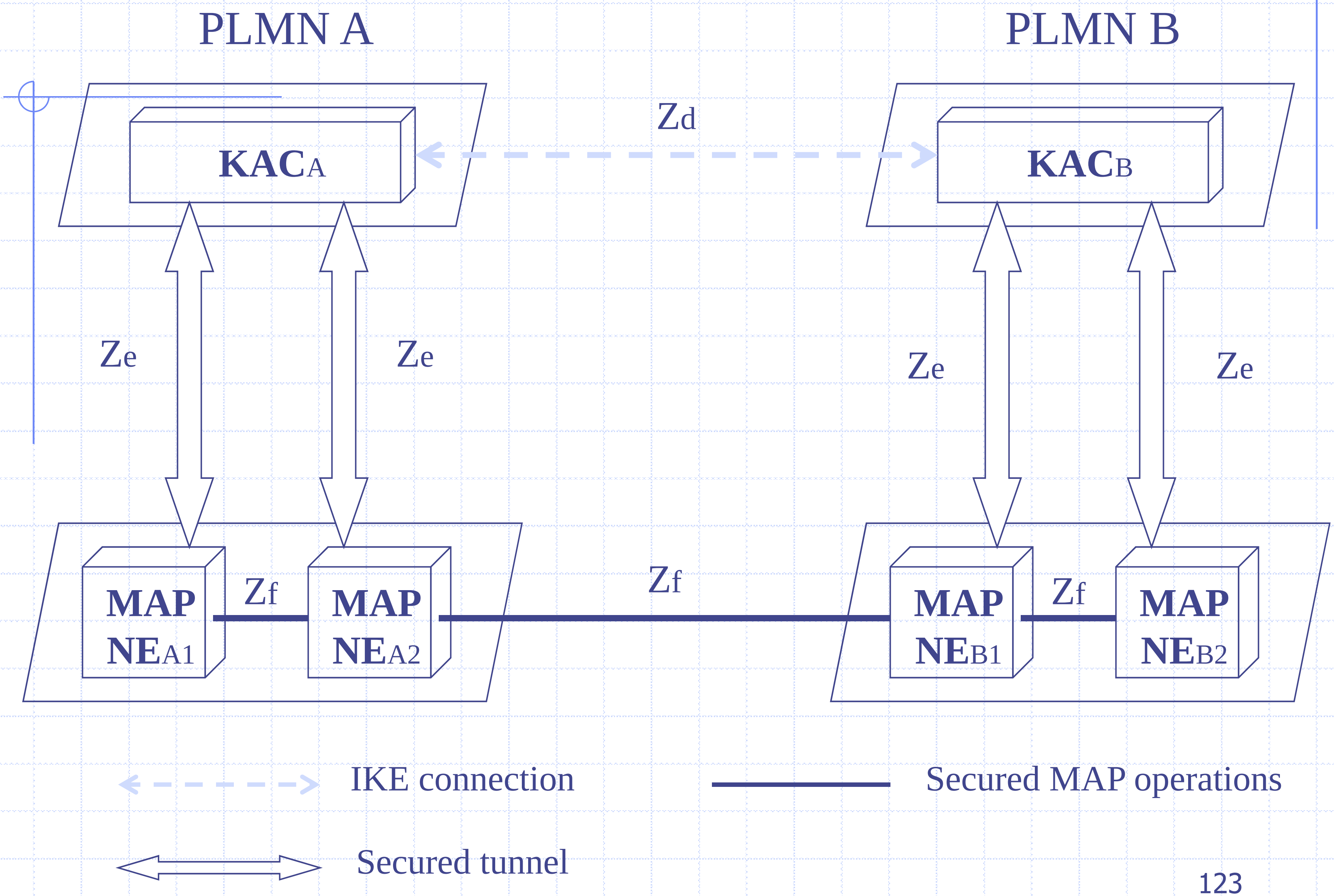
5.7.4 Network Domain Security

- IP network layer security
  - IPsec
- MAP application layer security
  - MAPsec

5.7.4.1 MAP Security (MAPsec)

- Protect the core network SS7 signalling protocols
- Confidentiality, integrity, authentication and anti-replay protection have been identified as necessary

Fig. 5.38 MAPsec architecture



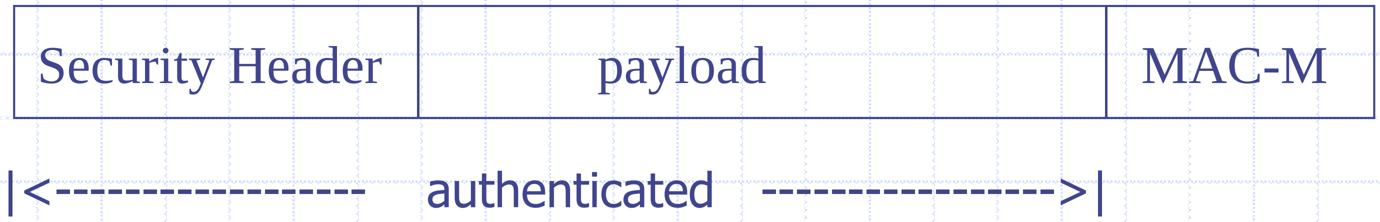
Protection Modes

- Protection Mode 0: no protection
- Protection Mode 1: integrity, authenticity
- Protection Mode 2: confidentiality, integrity, and authenticity

Message Format

- Protection Mode 0:
  - *Security header = SPI || Original component Id*
- Protection Mode 1 and 2:
  - *Security header = SPI || Original component Id || TVP || NE-Id || Prop*

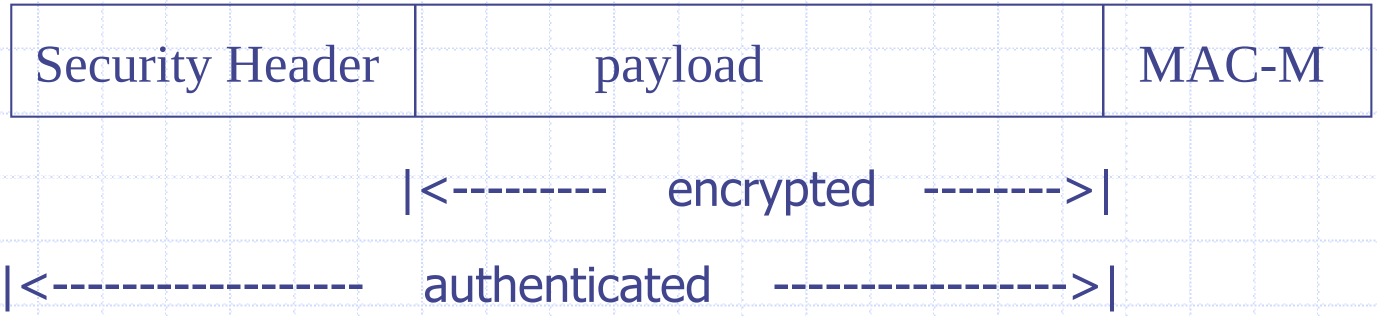
Fig. 5.39 Protection mode 1 in MAPsec



Security Header	payload	MAC-M

|<------------------ authenticated ----------------->|

Fig. 5.40 Protection mode 2 in MAPsec



Security Header	payload	MAC-M

|<--------- encrypted -------->|

|<----------------- authenticated ---------------->|

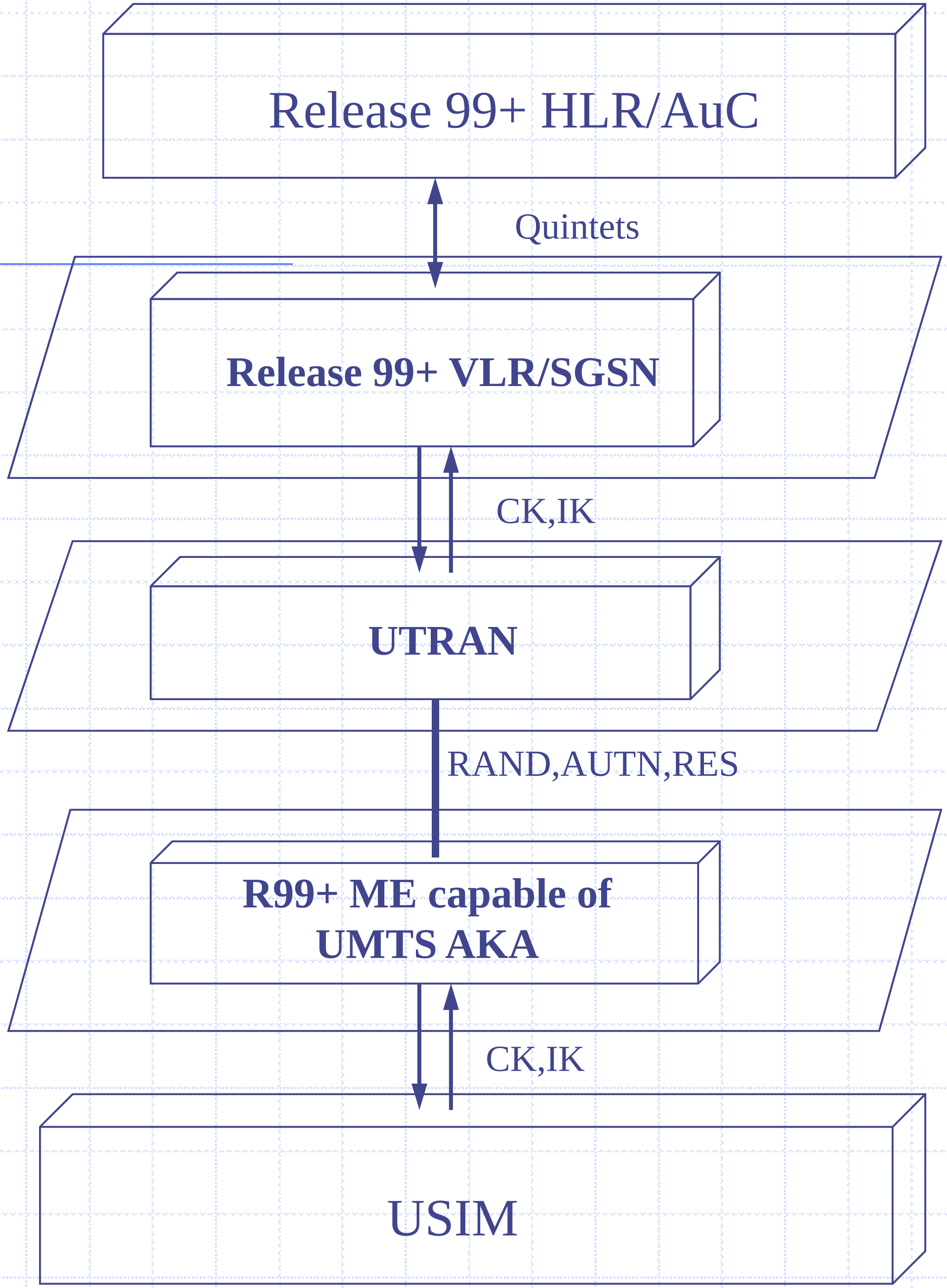
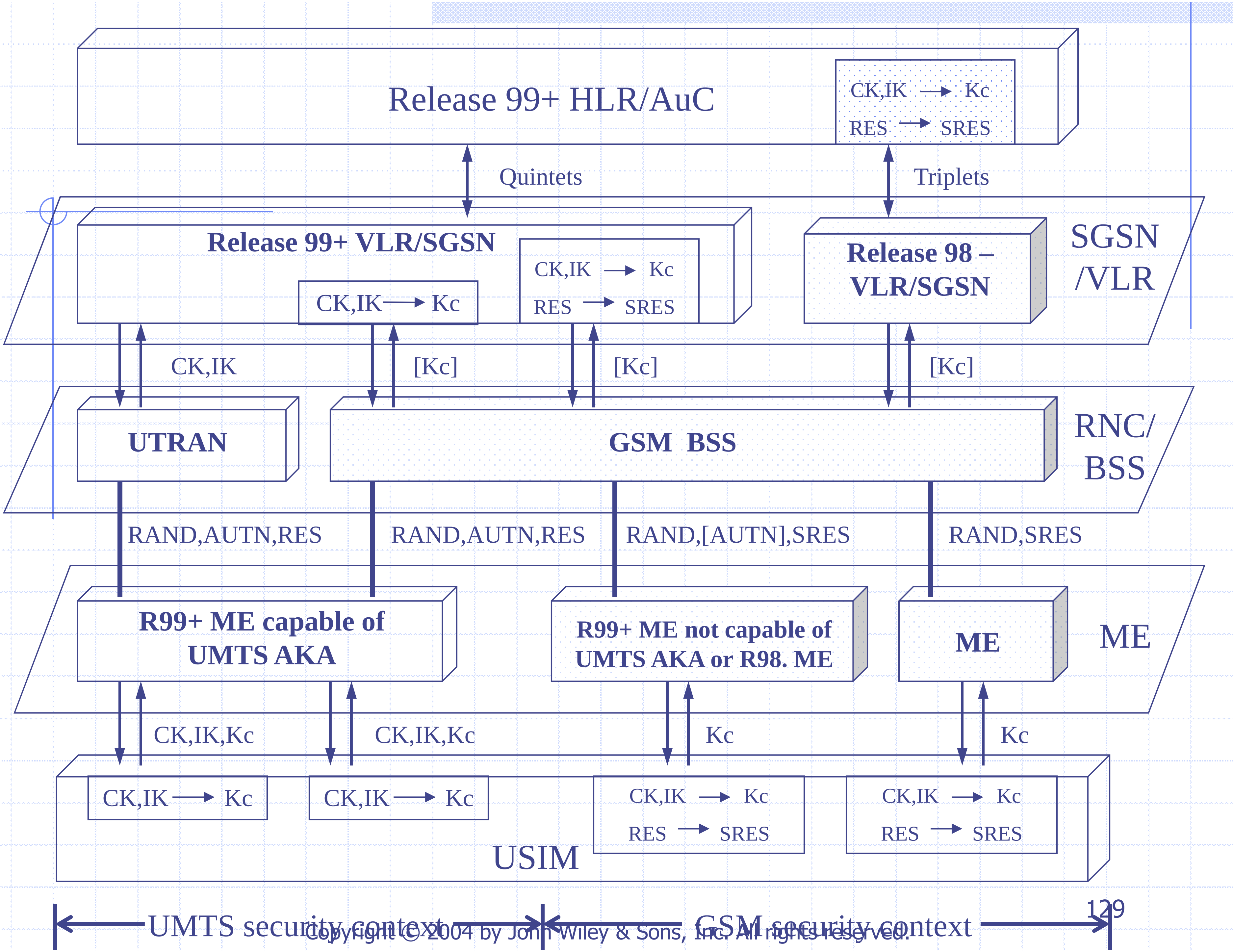


Fig. 5.41 3GPP network access security


Release 99+ HLR/AuC
CK,IK → Kc
RES → SRES
Quintets
Triplets
SGSN /VLR
Release 99+ VLR/SGSN
CK,IK → Kc
CK,IK → Kc
RES → SRES
Release 98 – VLR/SGSN
CK,IK
[Kc]
[Kc]
[Kc]
RNC/ BSS
UTRAN
GSM BSS
RAND,AUTN,RES
RAND,AUTN,RES
RAND,[AUTN],SRES
RAND,SRES
ME
R99+ ME capable of UMTS AKA
R99+ ME not capable of UMTS AKA or R98. ME
ME
CK,IK,Kc
CK,IK,Kc
Kc
Kc
CK,IK → Kc
CK,IK → Kc
CK,IK → Kc
RES → SRES
CK,IK → Kc
RES → SRES
USIM
UMTS security context
GSM security context

Security in IMS

- SIP is chosen as the signaling protocol for creating and terminating Multimedia sessions
- IMS security deals with
  - How the SIP signaling is protected between the subscriber and the IMS
  - How the subscriber is authenticated
  - How the subscriber authenticates the IMS

Lawful Interception

- The lawful interception provides means for an authorized person to access sensitive information and monitor other users.
- It however should be compliance with the national or regional laws and technical regulations.

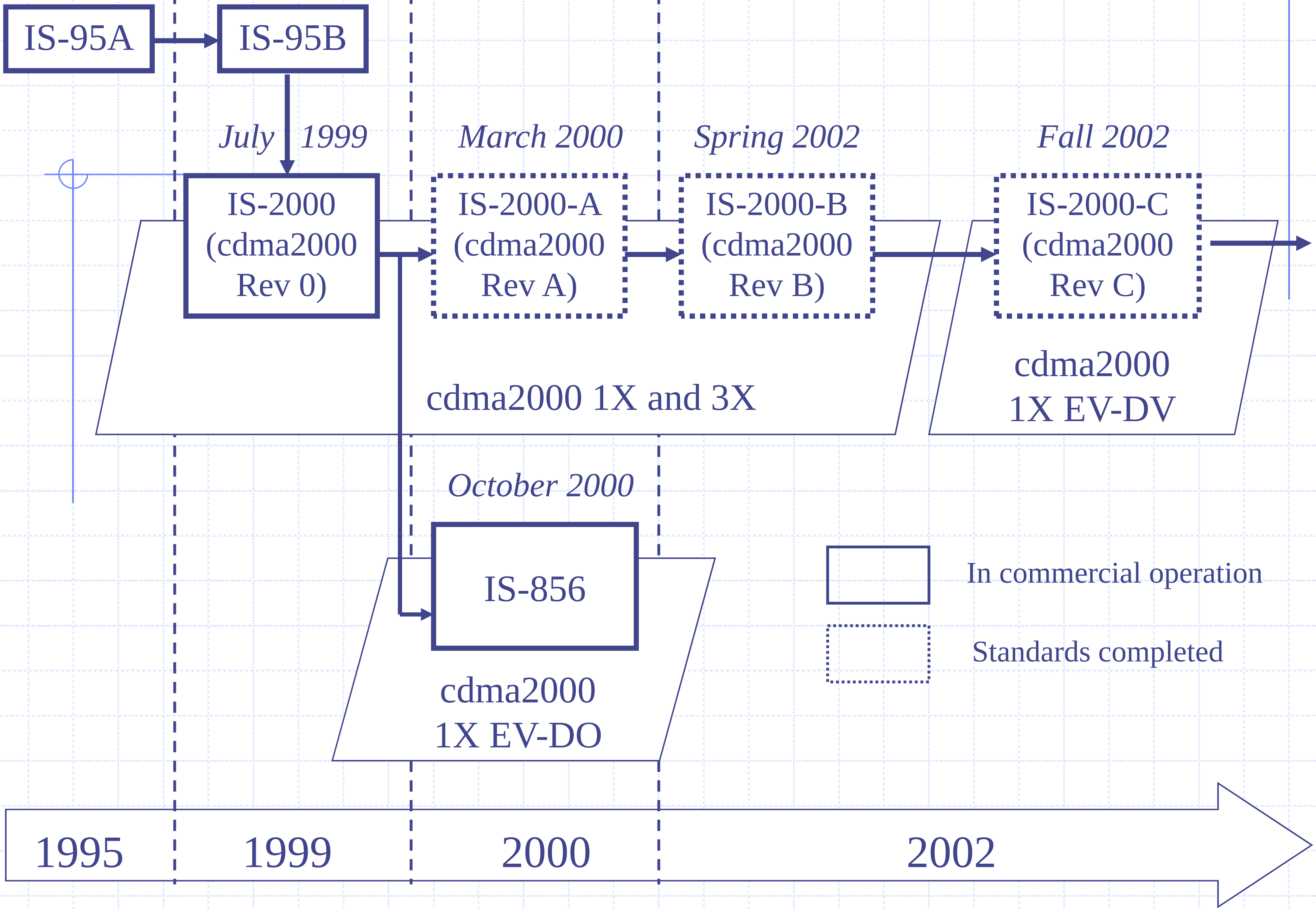
5.8 Security in 3GPP2

5.8.1 Network Access Security

5.8.2 Network Domain Security

3GPP2 Security

- Network Access Security
  - AKA
  - Privacy
  - Integrity
- Network Domain Security
  - IPsec
  - AAA


IS-95A
IS-95B
July 1999
March 2000
Spring 2002
Fall 2002
IS-2000 (cdma2000 Rev 0)
IS-2000-A (cdma2000 Rev A)
IS-2000-B (cdma2000 Rev B)
IS-2000-C (cdma2000 Rev C)
cdma2000 1X and 3X
cdma2000 1X EV-DV
October 2000
IS-856
cdma2000 1X EV-DO
In commercial operation
Standards completed
1995
1999
2000
2002

5.8.1.1 Authentication and Key Agreement (AKA)

- cdma2000 1x and 3x (Rev B and earlier): IS-41 CAVE
- Enhanced Subscriber Authentication (ESA): 1x EV-DV (Rev C)
  - Similar to 3GPP AKA
- cdma2000 1x EV-DO: PPP Challenge Handshake Authentication Protocol (CHAP)

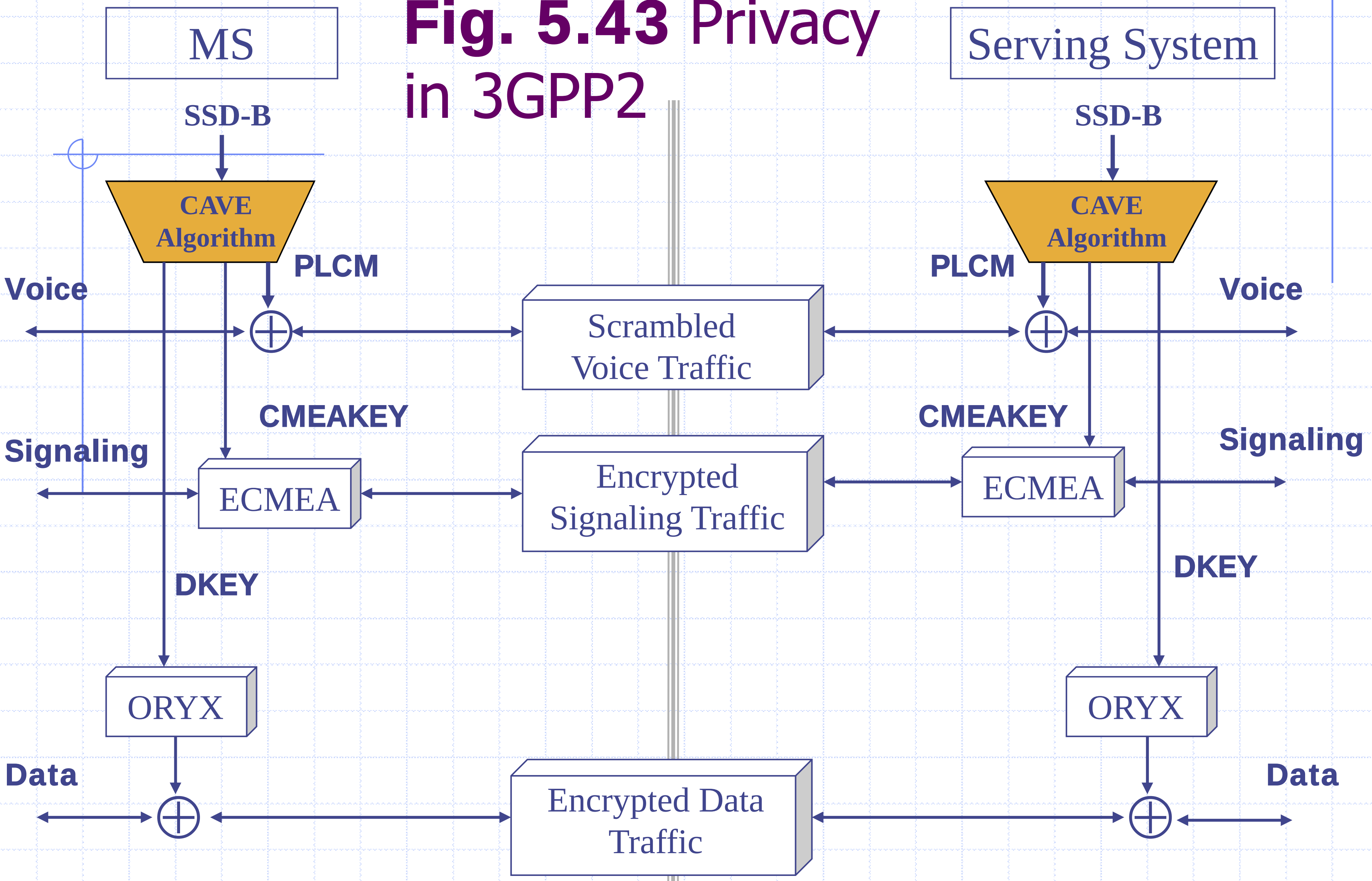
Enhanced Subscriber Authentication (ESA)

- ESA Requirements
  - The *root authentication key* should be known only to the MS and the Authentication Center (AC) in the home network.
  - The ESA should employ 128-bit authentication key and support mutual authentication.
  - The ESA should be backward compatible with CAVE.
  - The ESA should be able to negotiate the cryptographic algorithms.
  - The ESA algorithm should be published openly and commercially available, and should have been scrutinized thoroughly.
- TR-45 has adopted 3GPP AKA as the basis

5.8.1.2 Privacy

- cdma2000 1x and 3x (Rev 0 and Rev A): IS-41 CAVE
- Enhanced Subscriber Privacy (ESP): Rev B and later
  - 128-bit Rijndael AES
- cdma2000 1x EV-DO: AES

Fig. 5.43 Privacy in 3GPP2



Enhanced Subscriber Privacy (ESP)

- Keys for ESP may be based on the root authentication key but should be cryptographically decoupled from the keys used for authentication.
- The privacy key in MS can be modified under control of the home system.
- Keys for ESP are changed with each new security association.
- Privacy keys for each call are established at the time when a mobile is authenticated.
- Privacy keys for control channel are established after a mobile is authenticated successfully.

5.8.1.3 Integrity

- cdma2000 1x and 3x (Rev B and earlier): no integrity service
- cdma2000 1x EV-DV (Rev C):
  - Similar to 3GPP UIA
- cdma2000 1x EV-DO: no integrity service

5.8.2 Network Domain Security

- For both Simple IP and Mobile IP access mechanisms, IP network authentication of the mobile station is via a static security association between the mobile station and the home IP network.
- For Mobile IP, the service provider network shall use the Foreign Agent Challenge to authenticate and authorize the mobile station.
- For Simple IP the service provider network may use CHAP or PAP to authenticate and authorize the mobile station;
  - if the mobile station does not support CHAP or PAP, there is no IP network authentication.

Fig. 5.44 Security architecture for circuit-switching domain

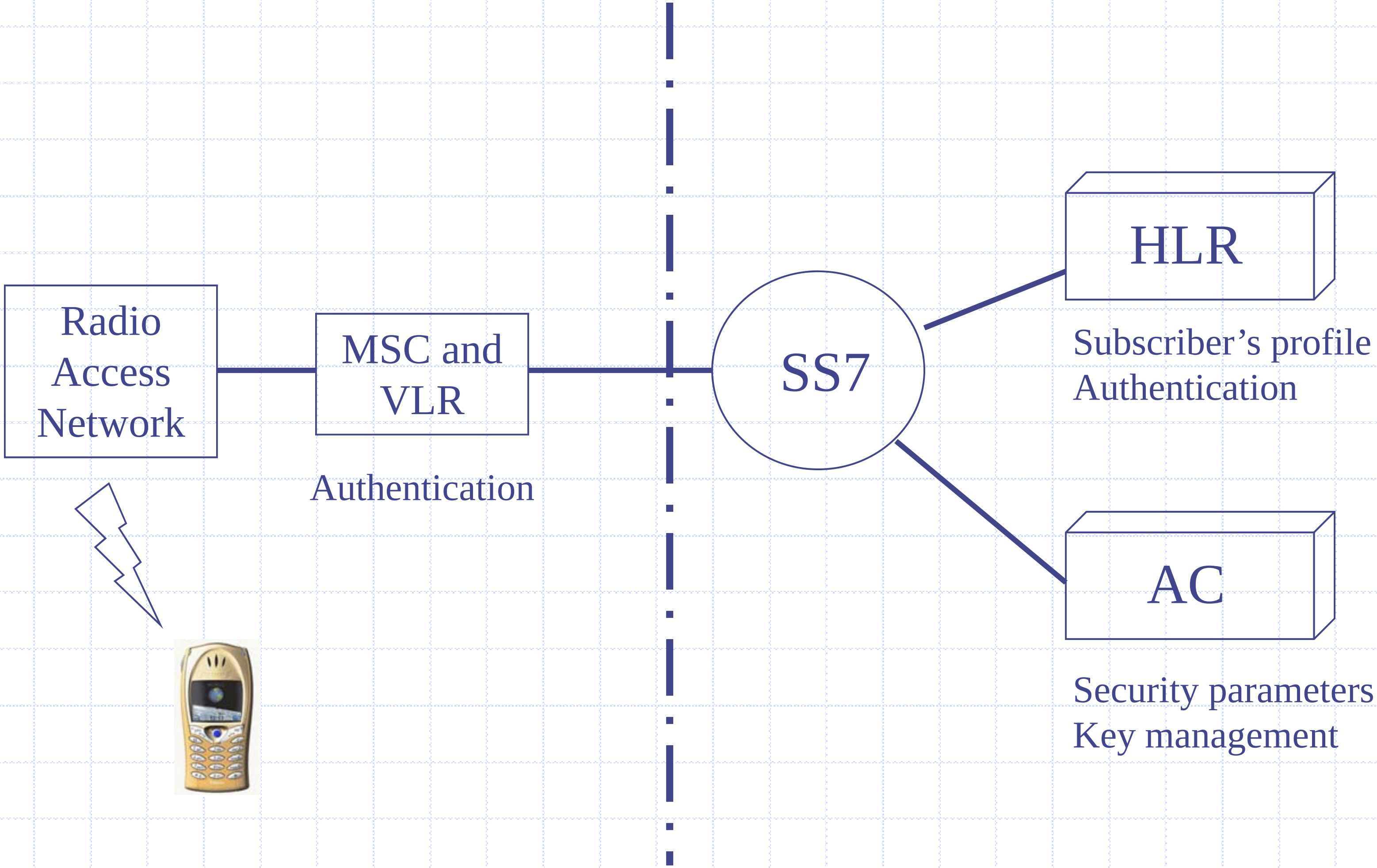
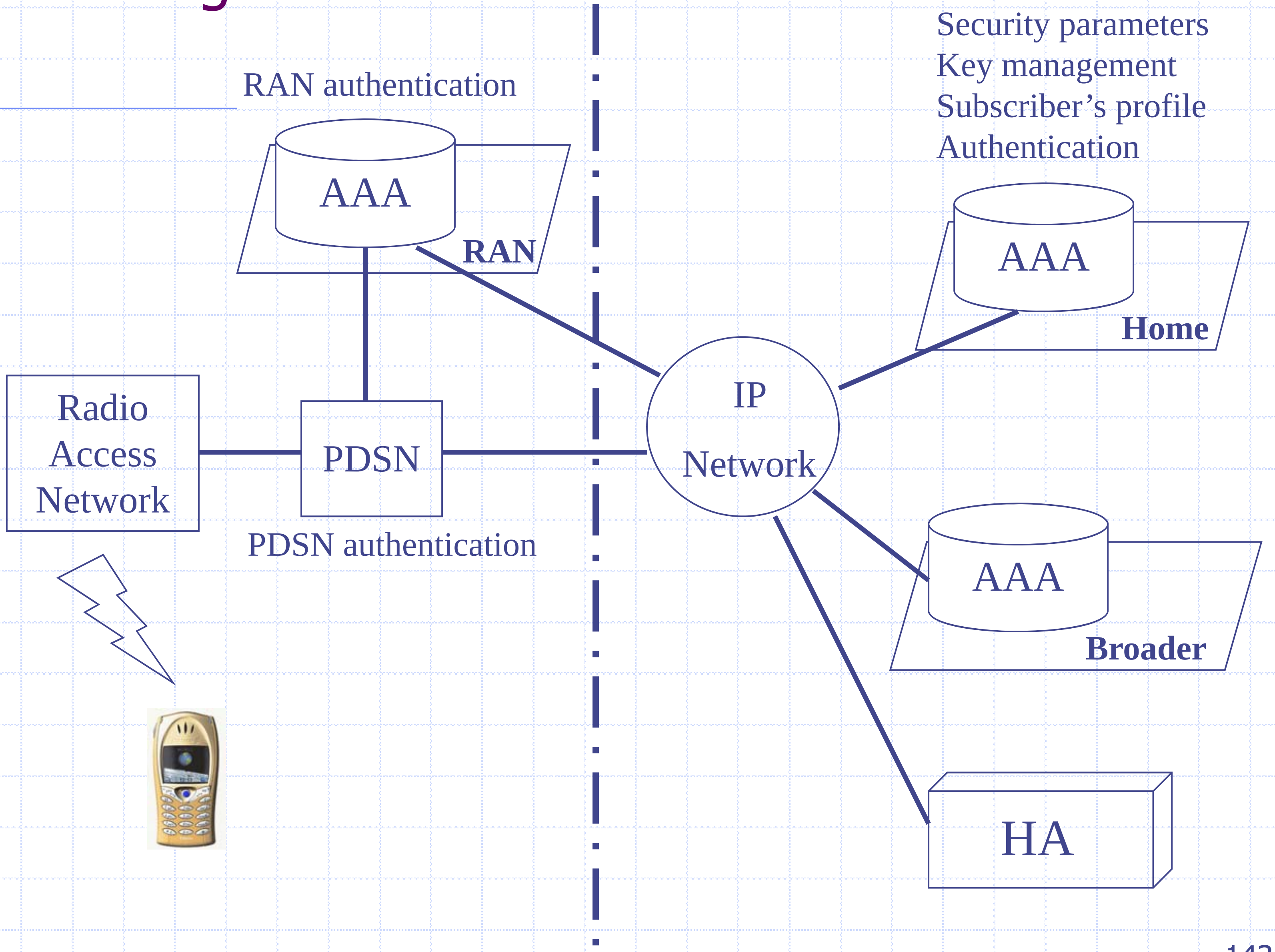


Fig. 5.45 Security architecture for packet-switching domain



PPP Session Authentication

- The PDSN should support CHAP and PAP.
- The PDSN should also support a configuration option to allow an MS to receive Simple IP service without CHAP or PAP.

PDSN

- The PDSN should support IPsec and IKE.
- A SA between the PDSN in a visited network and the mobile’s Mobile IP HA may be established using X.509-based certificates.
- Alternatively, a shared secret for IKE may be statically configured or dynamically provisioned by the mobile’s Home AAA server.
- IPsec ESP is preferred over AH
  - To insure backward compatibility, AH should also be implemented.
- The PDSN should act as a AAA client for the AAA server.

Authentication, Authorization and Accounting (AAA)

- May support both the IP domain and the legacy circuit-switching domain.
- Provide IP based Authentication, Authorization, and Accounting
- Maintains security associations with peer AAA entities to support intra- and/or inter-administrative domain AAA functions

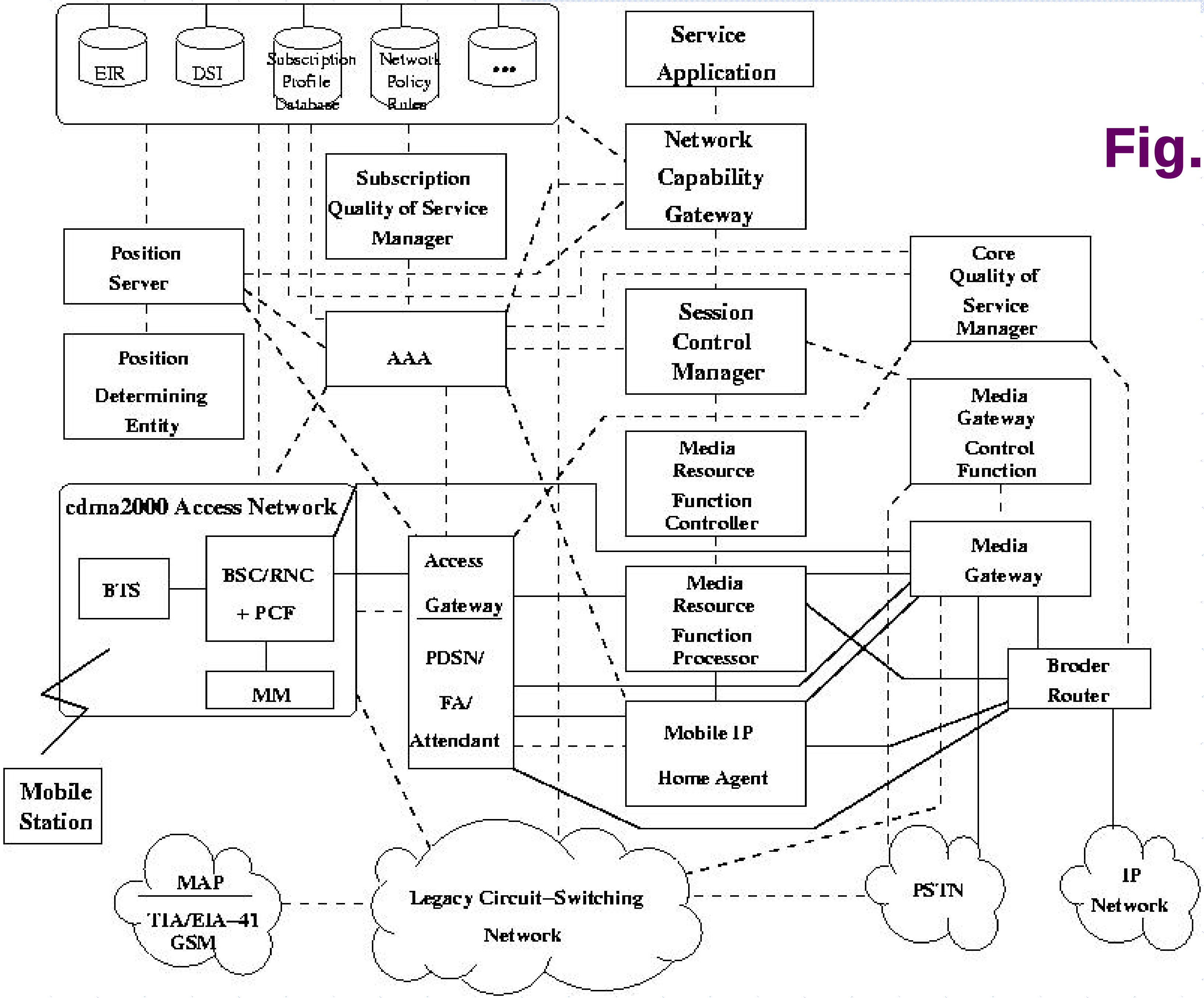

EIR
DSI
Subscription Profile Database
Network Policy Rules
•••
Service Application
Network Capability Gateway
Subscription Quality of Service Manager
Position Server
Position Determining Entity
AAA
Core Quality of Service Manager
Session Control Manager
Media Gateway Control Function
Media Resource Function Controller
cdma2000 Access Network
BTS
BSC/RNC + PCF
MM
Access Gateway
PDSN/ FA/ Attendant
Media Resource Function Processor
Media Gateway
Mobile IP Home Agent
Broder Router
Mobile Station
MAP
TIA/EIA-41 GSM
Legacy Circuit-Switching Network
PSTN
IP Network

Fig. 5.46