PV222
Security Architectures

Lecture 4

Mobile (GSM & UMTS) Security

Acknowledgement

- This lecture is heavily based on a presentation with the same title written by Peter Howard from Vodafone Group R&D.
- Further adaption by Prof Kenny Paterson.
- All errors and inaccuracies are the responsibility of the current presenter.

Objectives of Lecture

- Study the basic features and operation of mobile networks.
- Understand the security issues arising in first generation mobile networks and how these influenced the design of security features in second generation GSM systems.
- Study how authentication and network access control are enabled in GSM.
- Understand the limitations of GSM security and how these are addressed in the design of UMTS standards.

Contents

- Introduction to mobile telecommunications.
- Second generation systems – GSM security.
- Third generation systems – UMTS security.

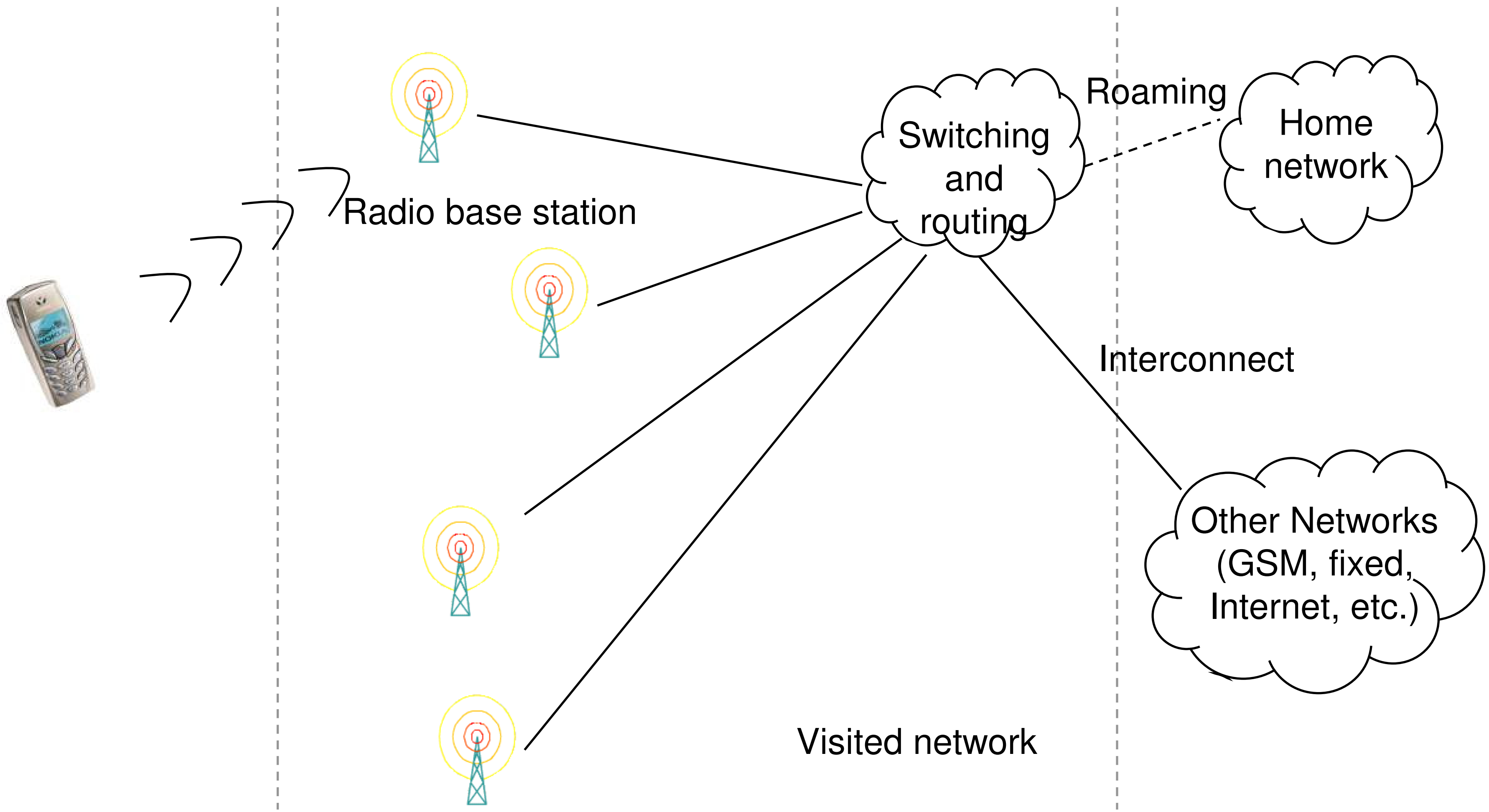
Introduction to Mobile Telecommunications

- Cellular radio network architecture.
- Location management.
- Call establishment and handover.

Cellular Radio Network Architecture

- Radio base stations form a patchwork of radio cells over a given geographic coverage area.
- Radio base stations are connected to switching centres via fixed or microwave transmission links.
- Switching centres are connected to the public networks (fixed telephone network, other GSM networks, Internet, etc).
- Mobile terminals have a relationship with one **home network** but may be allowed to roam in other **visited networks** when outside the home network coverage area.

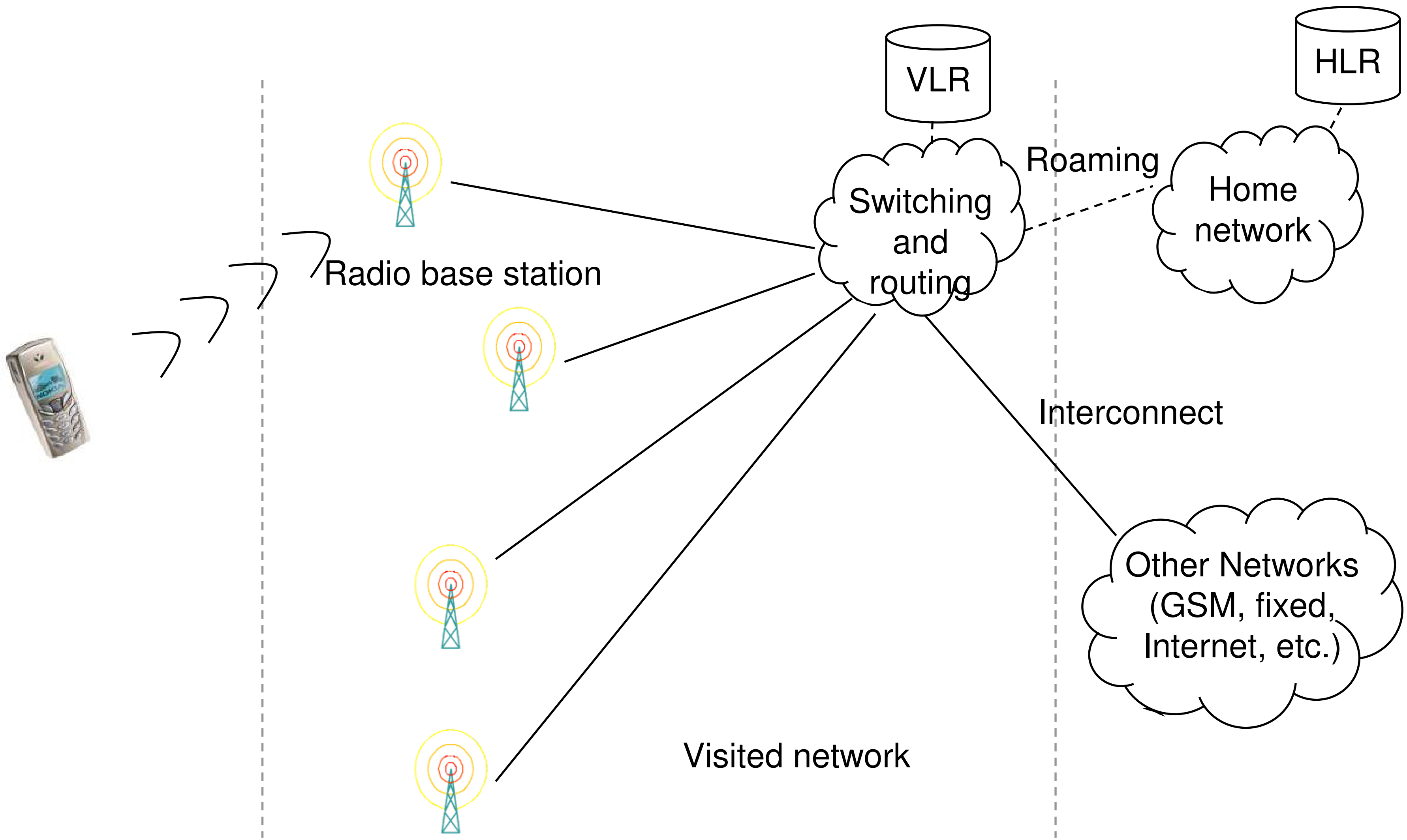
Cellular Radio Network Architecture



Location Management

- The network must know a mobile's location so that incoming calls can be routed to the correct destination.
- When a mobile is switched on, it registers its current location in a **Home Location Register (HLR)** operated by the mobile's home operator.
- A mobile is always roaming, either in the home operator's own network or in another network where a **roaming agreement** exists with the home operator.
- When a mobile registers in a network, information is retrieved from the HLR and stored in a **Visitor Location Register (VLR)** associated with the local switching centre.

Location Management



Call Establishment and Handover

- For mobile originating (outgoing) calls, the mobile establishes a radio connection with a nearby base station which routes the call to a switching centre.
- For mobile terminated (incoming) calls, the network first tries to contact the mobile by **paging** it across its current **location area,** the mobile responds by initiating the establishment of a radio connection.
- If the mobile moves, the radio connection may be re-established with a different base station without any interruption to user communication – this is called **handover.**

First Generation Mobile Phones

- First generation analogue phones (1980 onwards) were extremely insecure.
- Two main problems: Cloning and eavesdropping.
- **Cloning**:
  - 1g phone just announced its identity in clear over the radio link.
  - Easy to pick up phone's identity over the air.
  - Easy to reprogram one phone with another phone's identity.
  - Then all calls are charged to someone else's bill.
  - Loss of revenue for network operator; inconvenience for users, PR damage.

First Generation Mobile Phones

- **Eavesdropping**:
  - Voice traffic transmitted over wireless channel without any confidentiality protection.
  - Equipment to scan and eavesdrop on mobile calls readily available.
  - Compromise of customer privacy.
- Retro-fitting of suitable security mechanisms prohibitively expensive.
- Analogue systems phased out in UK in mid 90's.

Second Generation Mobile Phones – The GSM Standard

- Second generation mobile phones are characterised by the fact that data transmission over the radio link uses **digital** techniques.
- Development of the GSM (Global System for Mobile communications) standard began in 1982 as an initiative of the European Conference of Postal and Telecommunications Administrations (CEPT).
- In 1989 GSM became a technical committee of the European Telecommunications Standards Institute (ETSI).
- First services launched in 1991.
- GSM is the most successful mobile phone standard.
  - >3 billion customers.
  - >80% of the world market.
  - 219 countries source: GSM Association, 2009.

General Packet Radio Service (GPRS)

- The original GSM system was based on circuit-switched transmission and switching.
  - Voice services over circuit-switched bearers.
  - Text messaging.
  - Circuit-switched data services .
    - Charges usually based on duration of connection.
- GPRS is the packet-switched extension to GSM.
  - Sometimes referred to as 2.5G.
  - Packet-switched data services.
    - Suited to bursty traffic.
    - Charges usually based on data volume or content-based.
- Typical data services:
  - Browsing, messaging, download, corporate LAN access.

GSM Security Goals

- GSM was intended to be no more vulnerable to cloning or eavesdropping than a fixed phone.
  - It's a phone not a "secure communications device"!
  - But need to address issues arising from use of a broadcast medium.
- GSM uses integrated cryptographic mechanisms to achieve these goals.
  - Just about the first mass-market equipment to do this.
  - Previously cryptography had been the preserve of the military, security agencies, and businesses worried about industrial espionage, and then banks (but not in mass-market equipment).

GSM Security Features

- Authentication.
  - Network operator can verify the identity of the subscriber making it infeasible to clone someone else's mobile phone.
- Confidentiality.
  - Protects voice, data and sensitive signalling information (e.g. dialled digits) against eavesdropping on the radio path.
- Anonymity.
  - Protects against tracking location of the user or identifying calls made to or from the user by eavesdropping on the radio path.

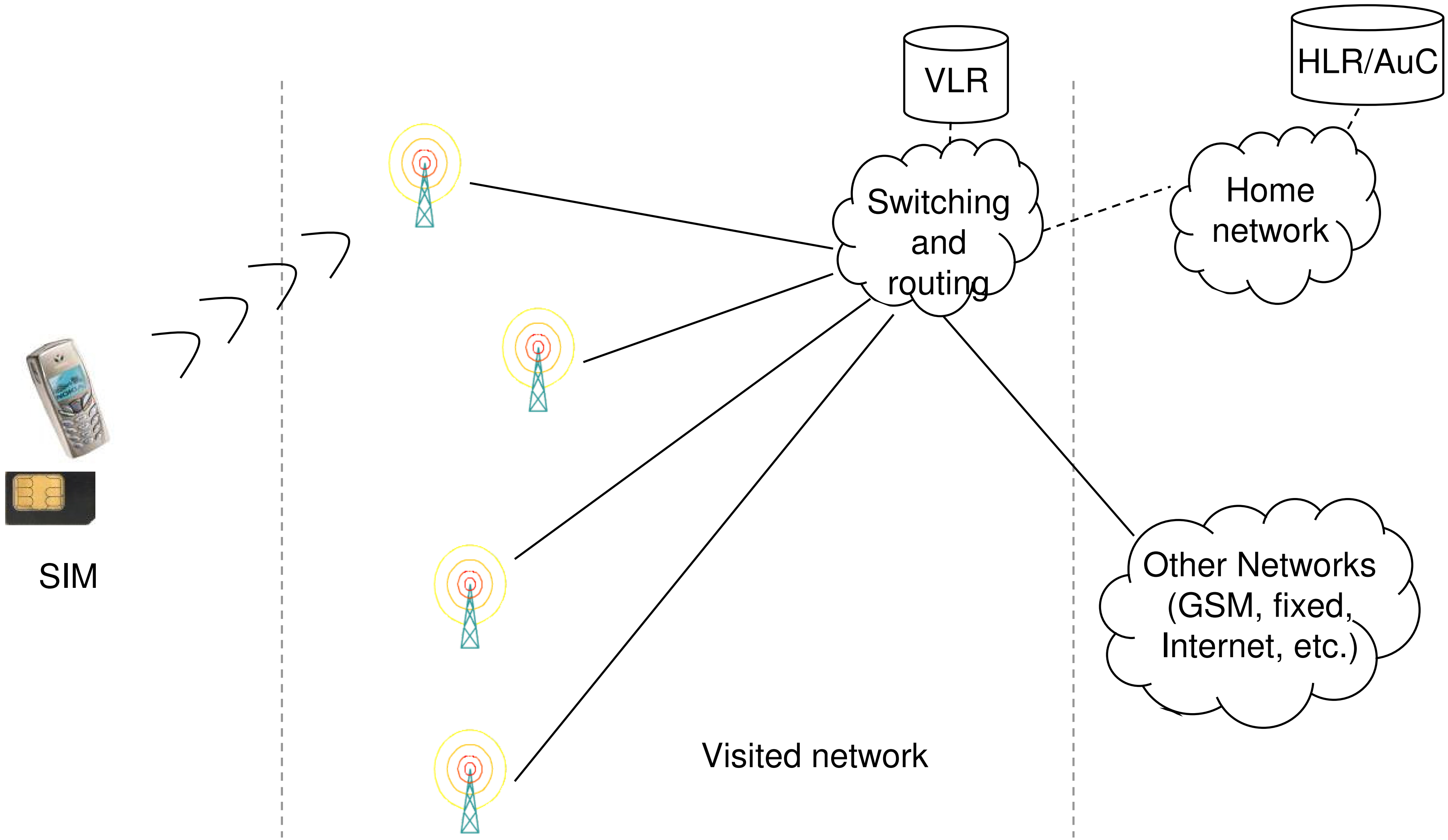
GSM Security Mechanisms

- Authentication.
  - Challenge-response authentication protocol.
  - Encryption of the radio channel.
- Confidentiality.
  - Encryption of the radio channel.
- Anonymity.
  - Use of temporary, variable identities in place of fixed identities.

GSM Security Architecture

- Each mobile subscriber is issued with a unique 128-bit secret key (Ki).
- This is stored on a **Subscriber Identity Module (SIM)** which must be inserted into the mobile phone.
- Each subscriber's Ki is also stored in an **Authentication Centre (AuC)** associated with the HLR in the home network.
- The SIM is a tamper resistant smart card designed to make it infeasible to extract the customer's Ki.
  - Even for the customer.
- GSM security relies on the secrecy of Ki.
  - If the Ki could be extracted then the subscription could be cloned and the subscriber's calls could be eavesdropped.

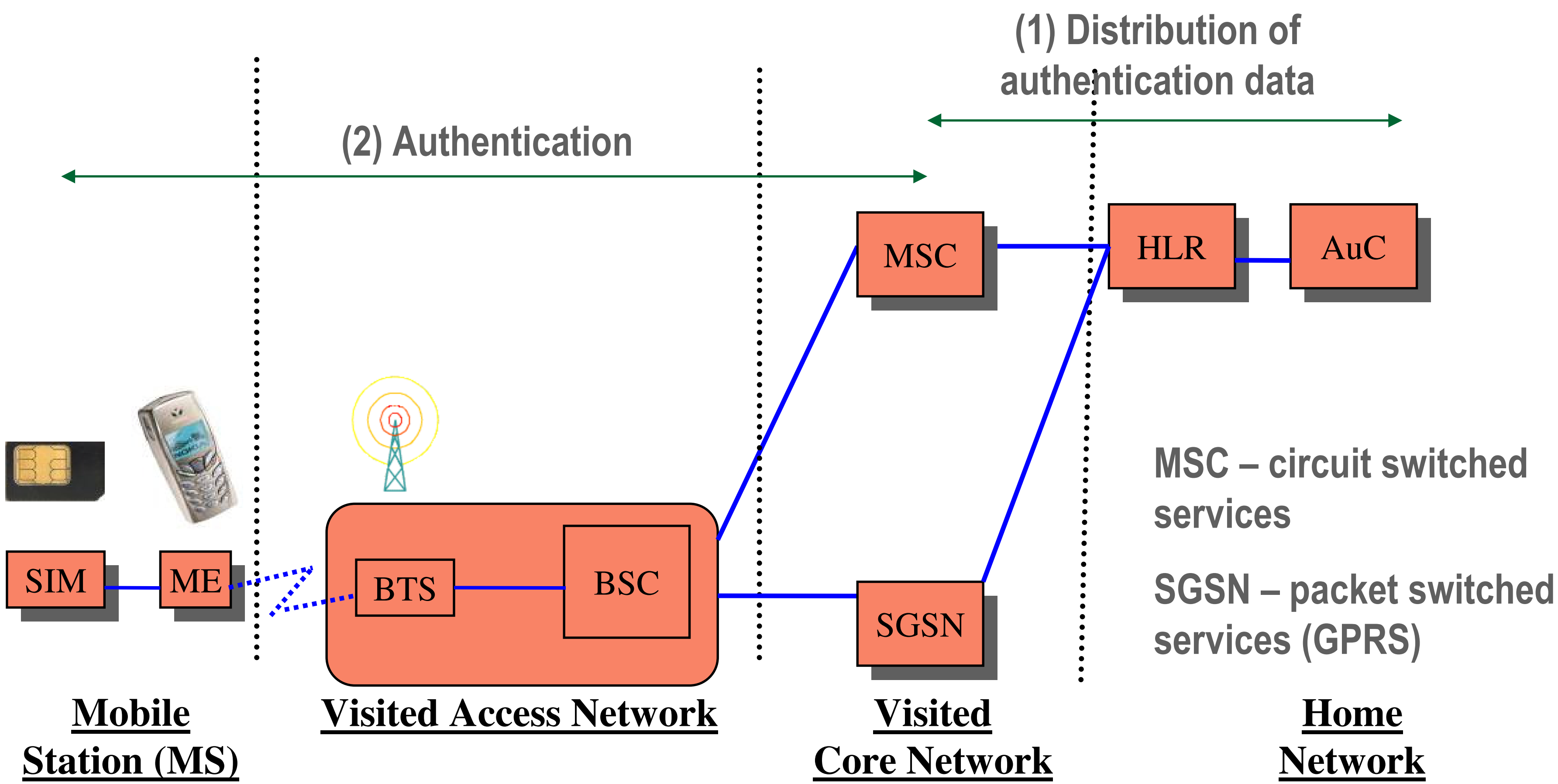
GSM Security Architecture



GSM Authentication Principles

- Network authenticates the SIM to protect against cloning.
- Challenge-response protocol.
  - SIM demonstrates knowledge of Ki.
  - Infeasible for an intruder to obtain information about Ki which could be used to clone the SIM.
- Encryption key agreement.
  - A key (Kc) for radio interface encryption is derived as part of the authentication protocol.
- Authentication can be performed at call establishment allowing a new Kc to be used for each call.

GSM Authentication



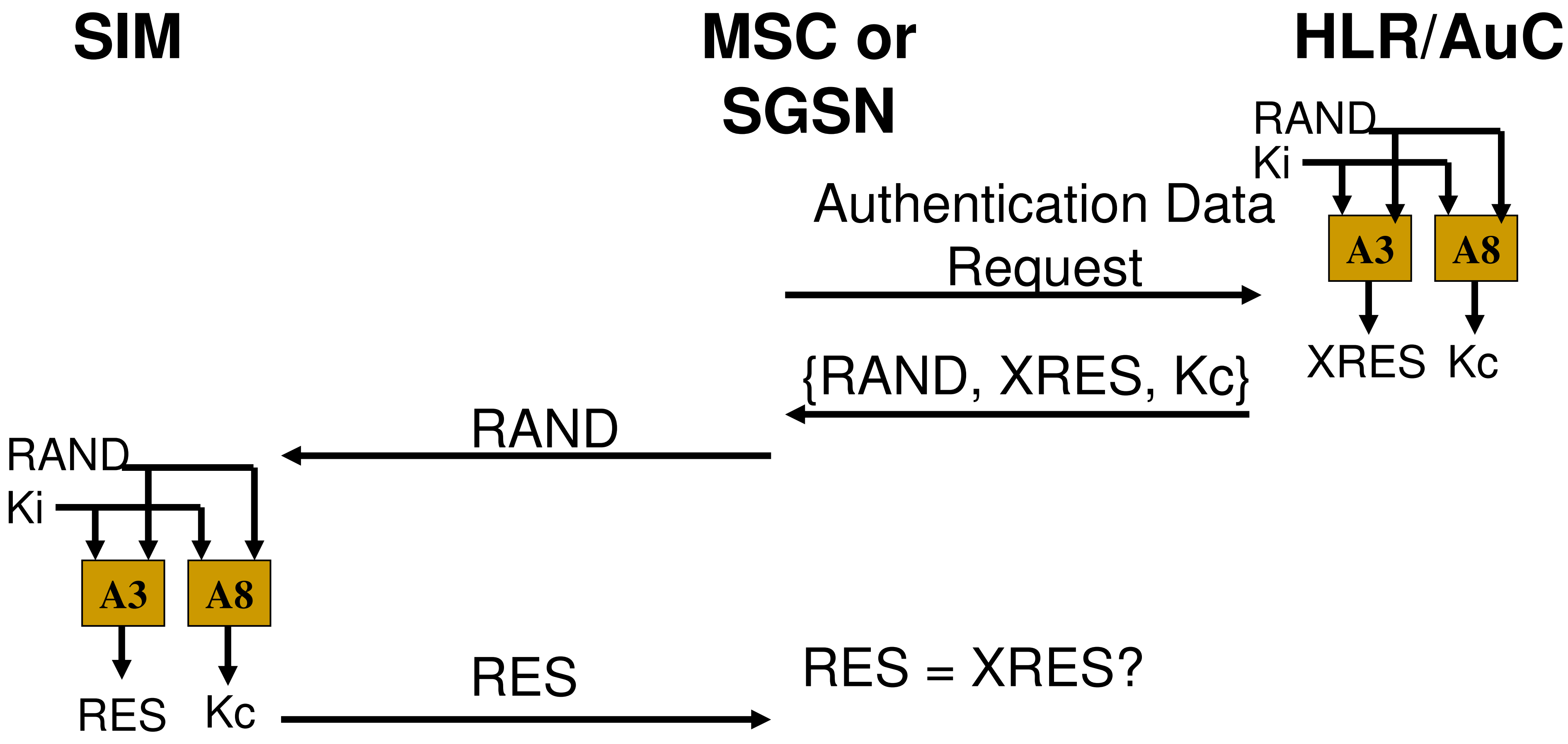
GSM Authentication: Prerequisites

- Authentication centre in home network (AuC) and security module (SIM) inserted into mobile phone share:
  - Subscriber specific secret key, Ki.
  - Authentication algorithm consisting of:
    - Authentication function, A3.
    - Key generating function, A8.
- AuC also has a random number generator.

Entities Involved in GSM Authentication

SIM	Subscriber Identity Module
MSC	Mobile Switching Centre (circuit services) <u>OR</u>
SGSN	Serving GPRS Support Node (packet services)
HLR/AuC	Home Location Register / Authentication Centre

GSM Authentication Protocol



GSM Authentication Parameters

Ki	= Subscriber authentication key (128 bit).
RAND	= Authentication challenge (128 bit).
(X)RES	= $A3_{Ki}$ (RAND).
	= (Expected) authentication response (32 bit)
Kc	= $A8_{Ki}$ (RAND).
	= Cipher key (64 bit).

Authentication triplet = {RAND, XRES, Kc} (224 bits).

Typically sent in batches from AuC to MSC or SGSN.

GSM Authentication Algorithms

- Composed of two algorithms which are often combined into a single algorithm.
  - A3 for user authentication.
  - A8 for encryption key (Kc) generation.
  - COMP128 as an example of a (weak) combined algorithm.
- Algorithms are located in the customer's SIM and in the home network's AuC.
- Standardisation of A3/A8 not required and each operator can choose their own.
  - Visited network provided with copy of XRES by home network; authentication decision based on comparing RES with XRES.

GSM Authentication Policy

- Operators can also set their own policy for when/how often SIMs are authenticated.
- GSM association publishes guidelines.
- For roamers outside home network, could be every call.

Further GSM Authentication Security Issues

- Communications between HLR and MSC/SGSN carried over core network shared by operators.
  - Historically, a trusted network, using SS7 protocols.
  - Increasing use of IP and hence IPSec to secure communications between different network operators' networks.
- AuC requires logical and physical protection.
  - Highly sensitive Ki stored en masse in AuC.
  - Operatives should not have access.
  - File of Ki's typically transported from SIM manufacturer to network operator's AuC in encrypted form; controlled decryption.

GSM Encryption

- Different mechanisms for GSM (circuit-switched services) and GPRS (packet-switched services).

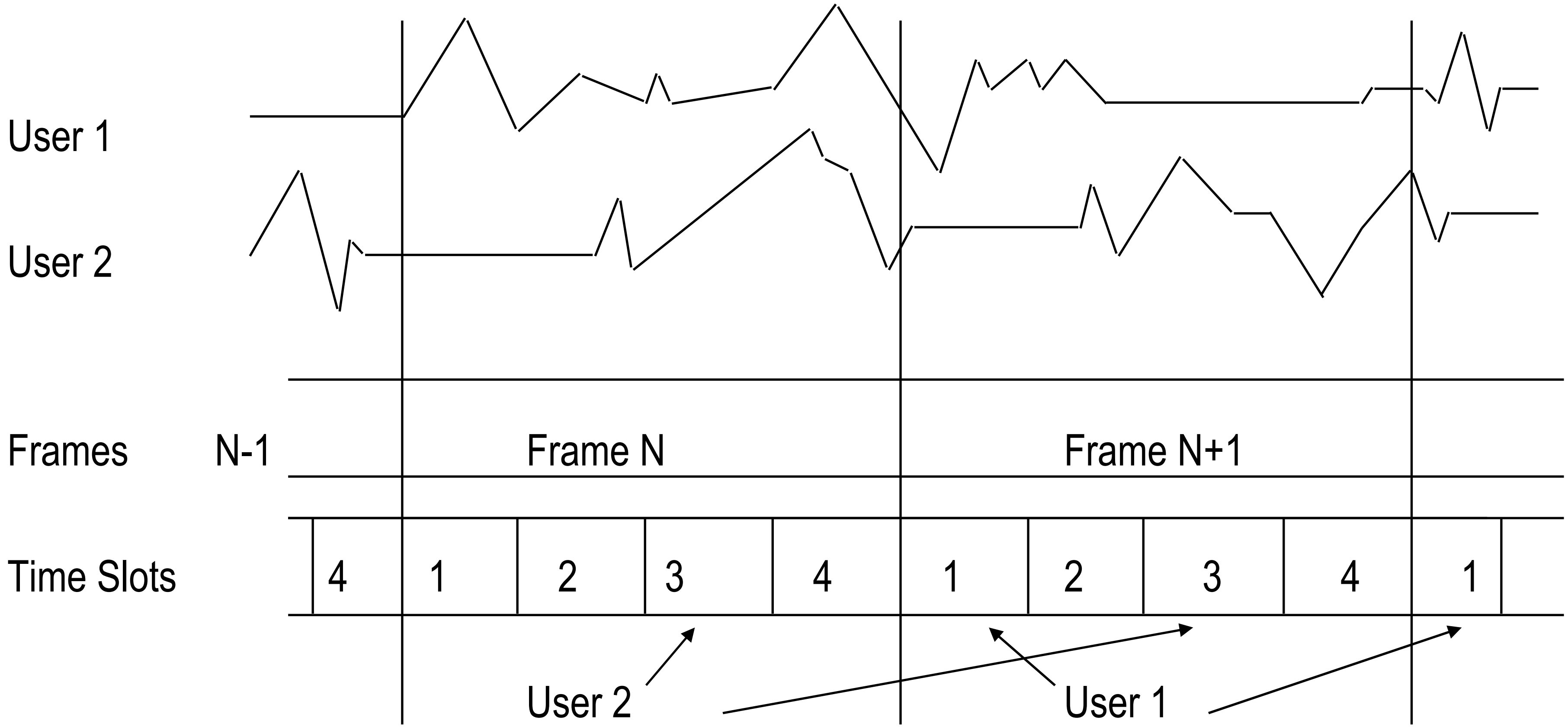
GSM Encryption Principles (Circuit-switched Services)

- Data on the radio path is encrypted between the Mobile Equipment (ME) and the Base Transceiver Station (BTS).
  - Protects user traffic and sensitive signalling data against eavesdropping.
  - Extends the influence of authentication to the entire duration of the call.
  - Scope of encryption is limited, especially in view of typical microwave links from BTS to MSC.
- Uses the encryption key (Kc) derived during authentication.

Encryption Mechanism

- Encryption is performed by applying a stream cipher called A5 to the GSM TDMA frames, the choice being influenced by:
  - Limitations of handset.
  - Speech coder.
  - Error propagation.
  - Low tolerance of delay.
  - Handover issues.

Time Division Multiple Access (TDMA)



Encryption Function

- For each TDMA frame, A5 generates consecutive sequences of 114 bits for encrypting/decrypting in the transmit/receive time slots.
  - Encryption and decryption is performed by applying the 114 bit keystream sequences to the contents of each frame using a bitwise XOR operation.
- A5 generates the keystream as a function of Kc and the ‘frame number’.
  - So the cipher is re-synchronised to every frame.
- The TDMA frame number repeats after about 3.5 hours, hence the keystream starts to repeat after 3.5 hours.
  - New cipher keys can be established to avoid keystream repeat.

Managing the Encryption

- BTS instructs ME to start ciphering using the *cipher* command *.*
- At same time BTS starts decrypting.
- ME starts encrypting and decrypting when it receives the *cipher* command.
- BTS starts encrypting when *cipher* command is acknowledged.

Strength of the Encryption

- Cipher key (*Kc*) 64 bits long but 10 bits are typically forced to zero in SIM and AuC .
  - 54 bits effective key length.
  - Reflecting regulatory climate at time of GSM design/introduction.
- Full length 64 bit key now possible.
- The strength also depends on *which* A5 algorithm is used.

GSM Encryption Algorithms

- Currently defined algorithms are: A5/1, A5/2 and A5/3.
- The A5 algorithms are standardised so that mobiles and networks can interoperate globally.
- All GSM phones currently support A5/1 and A5/2.
- Most networks use A5/1, some use A5/2.
- A5/1 and A5/2 specifications have restricted distribution but the details of the algorithms have been reverse engineered and extensive cryptanalysis has been conducted.
- A5/3 is new and openly published - expect it to be phased in over the next few years.

GPRS Encryption

- Differences compared with GSM circuit-switched.
  - Encryption terminated further back in network at SGSN.
  - Encryption applied at higher layer in protocol stack.
    - Logical Link Layer (LLC).
  - New stream cipher with different input/output parameters.
    - GPRS Encryption Algorithm (GEA).
  - GEA generates the keystream as a function of the cipher key and the 'LLC frame number'.
    - So the cipher is re-synchronised to every LLC frame.
  - LLC frame number is very large so keystream repeat is not an issue.

GPRS Encryption Algorithms

- Currently defined algorithms are: GEA1, GEA2 and GEA3.
- The GEA algorithms are standardised so that mobiles and networks can interoperate globally.
- GEA1 and GEA2 specifications have restricted distribution.
- GEA3 is new – expect it to be phased in over the next few years.

GSM User Identity Confidentiality (1)

- User identity confidentiality on the radio access link.
  - Temporary identities (TMSIs) are allocated and used instead of permanent identities (IMSIs).
- Helps protect against:
  - Tracking a user's location.
  - Obtaining information about a user's calling pattern.

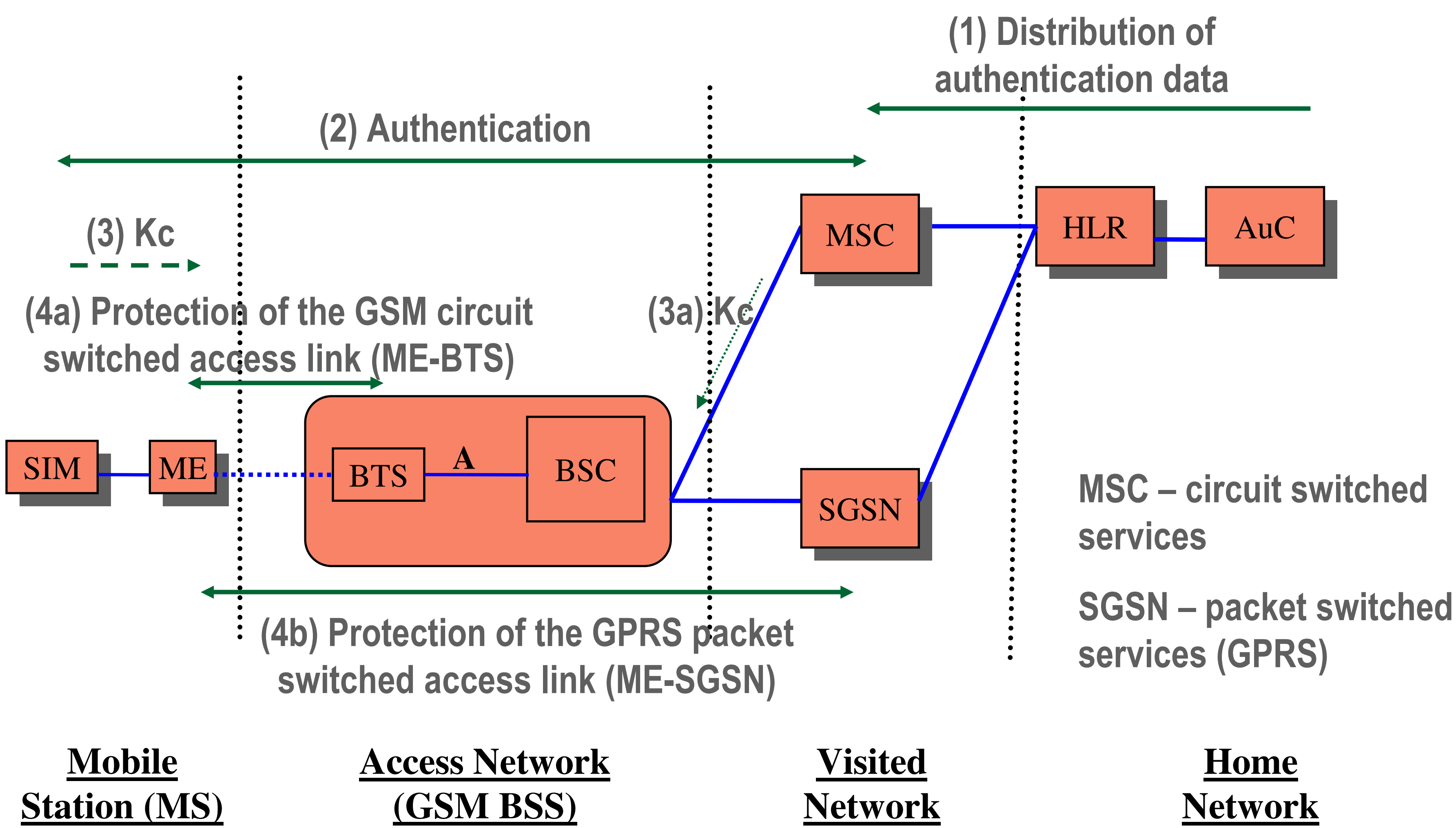
IMSI: International Mobile Subscriber Identity.

TMSI: Temporary Mobile Subscriber Identity.

GSM User Identity Confidentiality (2)

- When a user first arrives on a network he uses his IMSI to identify himself.
- When network has switched on encryption it assigns a temporary identity TMSI 1.
- When the user next accesses the network he uses TMSI 1 to identify himself.
- The network assigns TMSI 2 once an encrypted channel has been established.

GSM Radio Access Link Security



Significance of the GSM Security Features

- Effectively solved the problem of cloning mobiles to gain unauthorised access.
- Addressed the problem of eavesdropping on the radio path - this was incredibly easy with analogue, but is now much harder with GSM.

Limitations of GSM Security (1)

- Security problems in GSM stem by and large from design limitations on what is protected.
  - Design only provides *access security.*
    - Communications and signalling in the fixed network portion aren't protected.
  - Design does not address *active attacks*, whereby network elements (e.g. base-station) may be impersonated.
    - False base-station attack considered unrealistic at design time.
    - Cost and size of equipment has since drastically reduced, making such attacks more realistic.
  - Design goal was only ever to be *as secure as the fixed networks* to which GSM systems connect.

Limitations of GSM Security (2)

- Failure to acknowledge limitations by some operators.
  - The terminal is an unsecured environment.
    - So trust in the terminal identity is misplaced.
    - Issues with pay-as-you-go phones.
  - Disabling encryption does not just remove confidentiality protection, it also increases risk of radio channel hijack.
  - Standards don't address everything - operators must themselves secure the systems that are used to manage subscriber authentication key.
- Lawful interception only considered as an afterthought.

Specific GSM Security Problems (1)

- Ill-advised use of COMP128 as the A3/A8 algorithm by some operators.
  - Vulnerable to collision attack.
  - Key can be determined if the responses to about 160,000 chosen challenges are known.
    - Later improved to about 50,000.
  - Still requires long period of access to user's SIM.
  - Attack published on Internet in 1998 by Briceno and Goldberg.
  - Software tools for cloning COMP128 SIMs are widely available.

Specific GSM Security Problems (2)

- The GSM cipher A5/1 is becoming vulnerable to:
  - Exhaustive search on its 54 bit key.
  - Advances in cryptanalysis:
    - Algorithm reverse engineered in 1999.
    - Time-memory trade-off attacks by Biryukov, Shamir and Wagner (2001) and Barkan, Biham and Keller (2003).
    - Statistical attack by Ekdahl and Johansson (2002), Maximov, Johansson and Babbage (2004).

Specific GSM Security Problems (3)

- The GSM cipher A5/2:
  - Algorithm reverse engineered in 1999.
  - Then “broken” in 1999 (Goldberg, Wagner and Green).
  - Improvements by Barkan, Biham and Keller (2003), including a ciphertext-only attack.
  - A5/2 now offers virtually no protection against passive eavesdropping.
  - Cipher key can be discovered in near real time using a very small amount of known plaintext.
  - Same key is used whether A5/1 or A5/2 is encryption algorithm.
    - Allows man-in-the-middle attack where mobile forced to use weaker A5/2, Kc is then obtained by cryptanalysis, and then same Kc is used in an A5/1 network to masquerade as a legitimate user.
    - A false base-station threat.
  - A5/2 is being removed from new terminals.

False Base Station Threats

- IMSI Catching.
  - Force mobile to reveal its IMSI in clear.
- Intercepting mobile-originated calls by disabling encryption.
  - Encryption controlled by network and user generally unaware if it is switched on or off.
  - False base station masquerades as network with encryption switched off.
  - Calls relayed to called party e.g. via fixed network.
  - Cipher indicator on phone helps guard against attack.

Lessons Learnt From GSM Experience

- Security must operate without user assistance, but the user should know it is happening.
- Base user security on smart cards.
- Possibility of an attack is a problem even if attack is unlikely.
- Don't relegate lawful interception to an afterthought.
- Develop open international standards.
- Use published algorithms, or publish any specially developed algorithms.

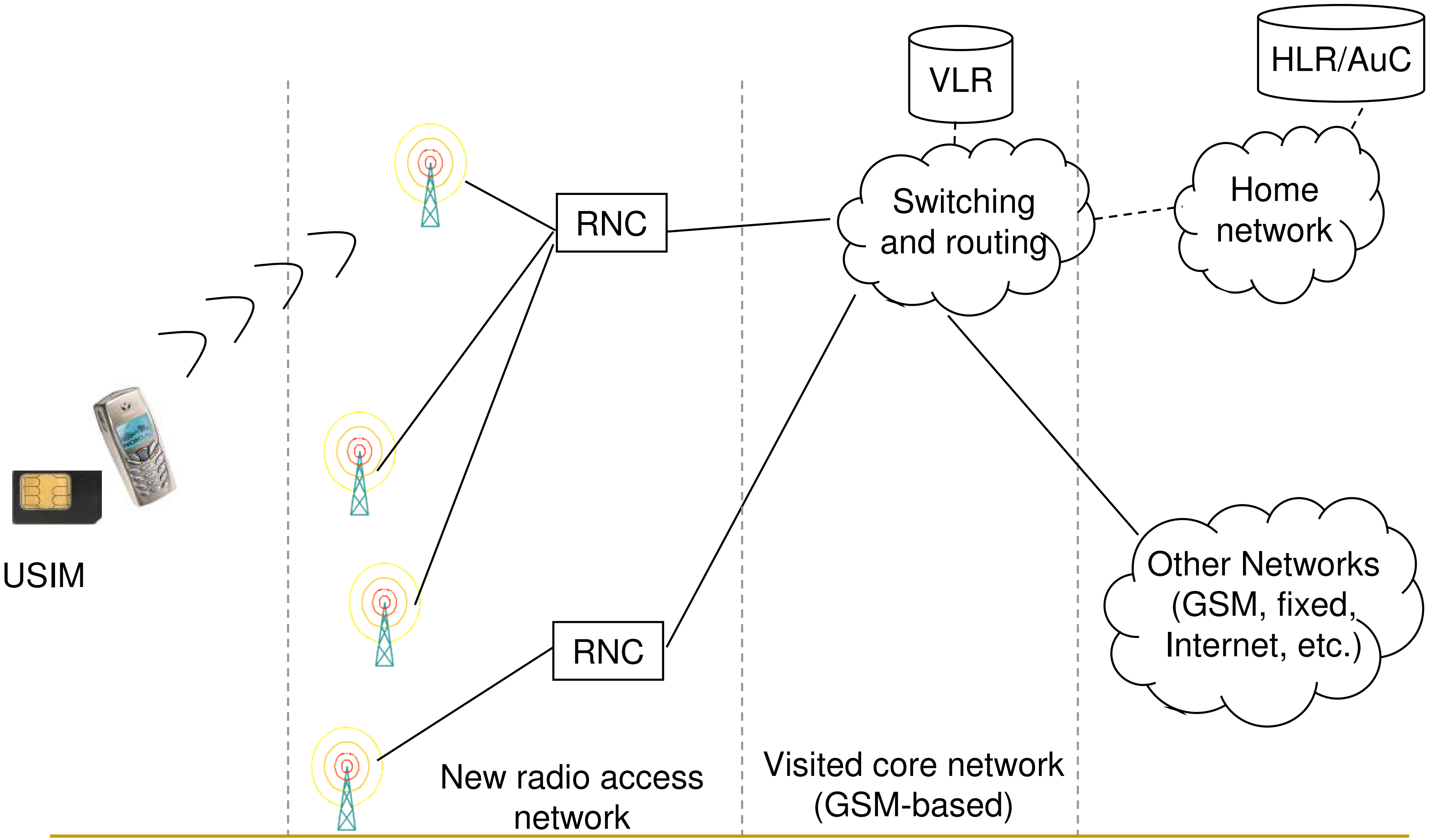
Third Generation Mobile Phones – The UMTS Standard

- Third generation (3G) mobile phones are characterised by higher rates of data transmission and a richer range of services.
- Universal Mobile Telecommunications System (UMTS) is one of the new 3G systems.
  - CDMA2000 another major 3G system.
- UMTS introduces a new radio technology into the access network.
  - Wideband Code Division Multiple Access (W-CDMA).
  - Connected to evolution of GSM/GPRS core network.
- UMTS statistics:
  - 137 million subscribers at October 2007.
  - 182 networks in 81 countries at October 2007.
  - Source: GSACOM website.

Principles of UMTS Security

- Build on the security of GSM.
  - Adopt the security features from GSM that have proved to be needed and that are robust.
  - Try to ensure compatibility with GSM to ease inter-working and handover.
- Correct the problems with GSM by addressing security weaknesses.
- Add new security features.
  - To secure new services offered by UMTS.
  - To address changes in network architecture.

UMTS Network Architecture



GSM Security Features to Retain and Enhance in UMTS

- Authentication of the user to the network.
- Encryption of user traffic and signalling data over the radio link.
  - New algorithm – open design and publication.
  - Encryption terminates at the radio network controller (RNC).
    - Further back in network compared with GSM.
    - Protects data on potentially vulnerable microwave links.
  - Longer key length (128-bit).
- User identity confidentiality over the radio access link.
  - Same IMSI/TMSI mechanism as GSM.

New Security Features for UMTS

- Mutual authentication and key agreement.
  - Extension of user authentication mechanism.
  - Provides enhanced protection against false base station attacks by allowing the mobile to authenticate the network.
- Integrity protection of critical signalling between mobile and radio network controller.
  - Provides enhanced protection against false base station attacks by allowing the mobile to check the authenticity of certain signalling messages.
  - Extends the influence of user authentication when encryption is not applied by allowing the network to check the authenticity of certain signalling messages.

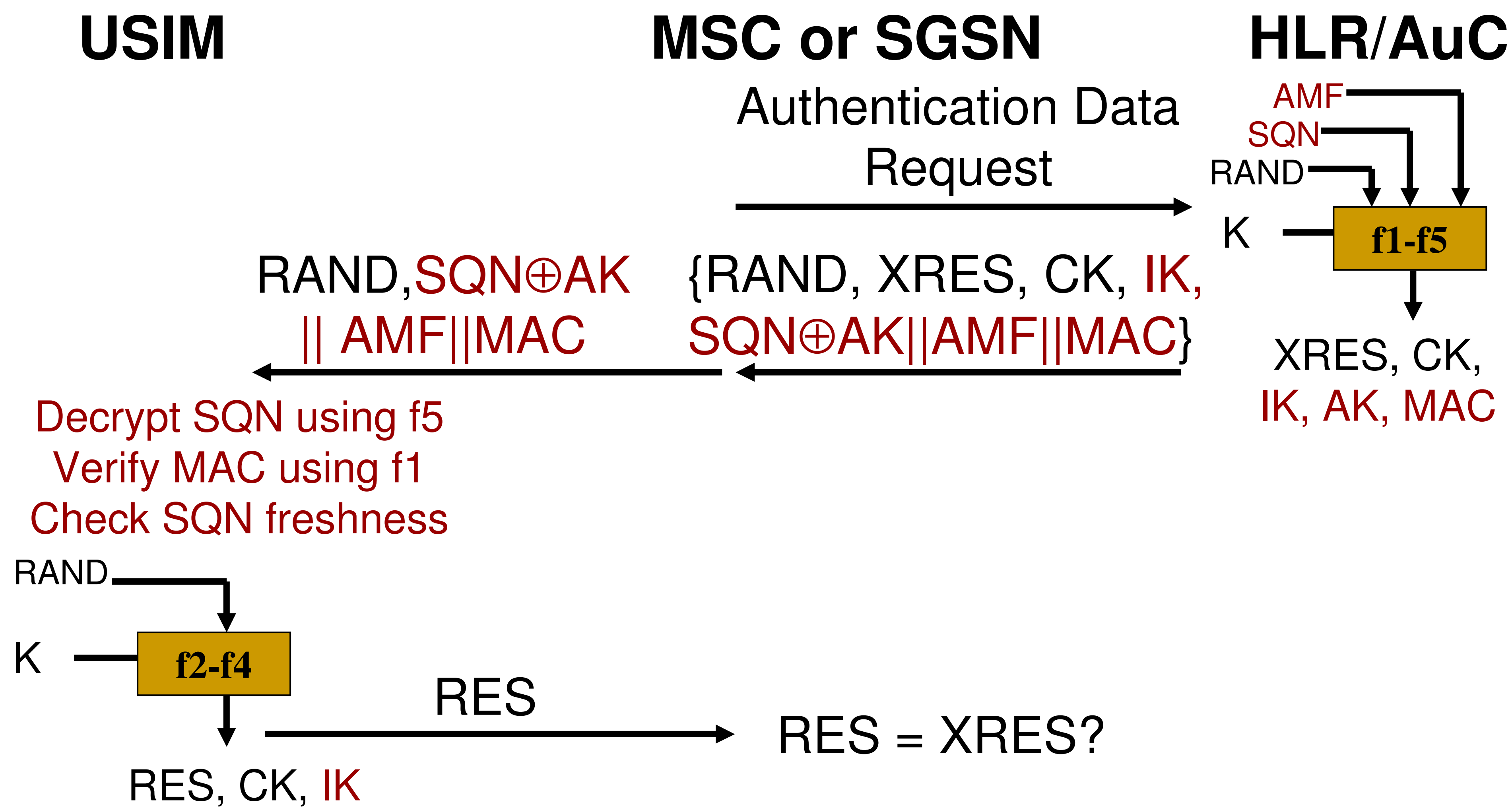
UMTS Authentication: Protocol Objectives

- Provides authentication of user (USIM) to network and network to user.
- Establishes a cipher key and integrity key.
- Assures user that cipher/integrity keys were not used before.
- Inter-system roaming and handover.
  - Backwards compatible with GSM: similar protocol.
  - Compatible with other 3G systems due to the fact that the other main 3G standards body (3GPP2 for CDMA2000) has adopted the same authentication protocol.

UMTS Authentication: Prerequisites

- AuC and USIM share:
  - Subscriber specific secret key, K:
  - Authentication algorithm consisting of:
    - Authentication functions, f1, f1*, f2.
    - Key generating functions, f3, f4, f5, f5*.
- AuC has a random number generator.
- AuC has a sequence number generator.
- USIM has a scheme to verify freshness of received sequence numbers.

UMTS Authentication



UMTS Authentication Parameters

K	= Subscriber authentication key (128 bit)
RAND	= User authentication challenge (128 bit)
SQN	= Sequence number (48 bit)
AMF	= Authentication management field (16 bit)
MAC	= $f1_K$ (SQN||RAND||AMF) = Message Authentication Code (64 bit)
(X)RES	= $f2_K$ (RAND)
	= (Expected) user response (32-128 bit)
CK	= $f3_K$ (RAND) = Cipher key (128 bit)
IK	= $f4_K$ (RAND) = Integrity key (128 bit)
AK	= $f5_K$ (RAND) = Anonymity key (48 bit)
AUTN	= SQN⊕AK|| AMF||MAC = Authentication Token (128 bit)

Authentication quintet = {RAND, XRES, CK, IK, AUTN} (544-640 bit)

- typically sent in batches to MSC or SGSN

UMTS Authentication Notes

- Protocol achieves mutual authentication with only 2 messages.
  - 3 message protocol would have been undesirable.
- Authentication of SIM using identical mechanism to GSM.
  - Compare RES to XRES, both generated using RAND and subscriber key K.
- Authentication of network via MAC on sequence number SQN.
  - SQN encrypted with AK to enhance anonymity of users.
- AMF carries operator-specific management field.

UMTS Authentication Algorithms

- Authentication algorithms f1-f5 located in the customer's USIM and in the home network's AuC.
- Standardisation not required and each operator can choose their own.
- An example algorithm set, called MILENAGE, has been made available.
  - Open design and evaluation by ETSI's algorithm design group, SAGE.
  - Open publication of specifications and evaluation reports.
  - Based on Rijndael which was later selected as the AES.

UMTS Encryption Principles

- Data on the radio path is encrypted between the Mobile Equipment (ME) and the Radio Network Controller (RNC).
  - Protects user traffic and sensitive signalling data against eavesdropping.
  - Protection deeper into core network than in GSM/2.5g.
  - Extends the influence of authentication to the entire duration of the call.
- Uses the 128-bit encryption key (CK) derived during authentication.
  - CK passed from USIM to ME after authentication.

UMTS Encryption Mechanism

- Encryption applied at MAC or RLC layer of the UMTS radio protocol stack depending on the transmission mode:
  - MAC = Medium Access Control.
  - RLC = Radio Link Control.
- Stream cipher used, UMTS Encryption Algorithm (UEA).
- UEA generates the keystream as a function of the cipher key, the bearer identity, the direction of the transmission and the 'frame number'.
  - So the cipher is re-synchronised to every MAC/RLC frame.
  - The frame number is very large so keystream repeat is not an issue.

UMTS Encryption Algorithm

- Two standardised algorithms: UEA1 and UEA2.
  - Located in the customer’s phone (not the USIM) and in every radio network controller.
  - Standardised so that mobiles and radio network controllers can interoperate globally.
    - Same reasoning as in GSM.
  - UEA1 based on a stream-cipher mode of operation of a block cipher called KASUMI.
  - UEA2 is a new algorithm introduced in case a vulnerability discovered in UEA1.
    - Based on Snow3G block cipher.

UMTS Integrity Protection Principles

- Protection of some radio interface signalling.
  - Protects against unauthorised modification, insertion and replay of messages.
  - Applies to security mode establishment and other critical signalling procedures.
  - Prevents false base station from deselecting encryption.
- Helps extend the influence of authentication when encryption is not applied.
- Uses the 128-bit integrity key (IK) derived during authentication.
- Integrity applied at the Radio Resource Control (RRC) layer of the UMTS radio protocol stack.
  - Signalling traffic only.

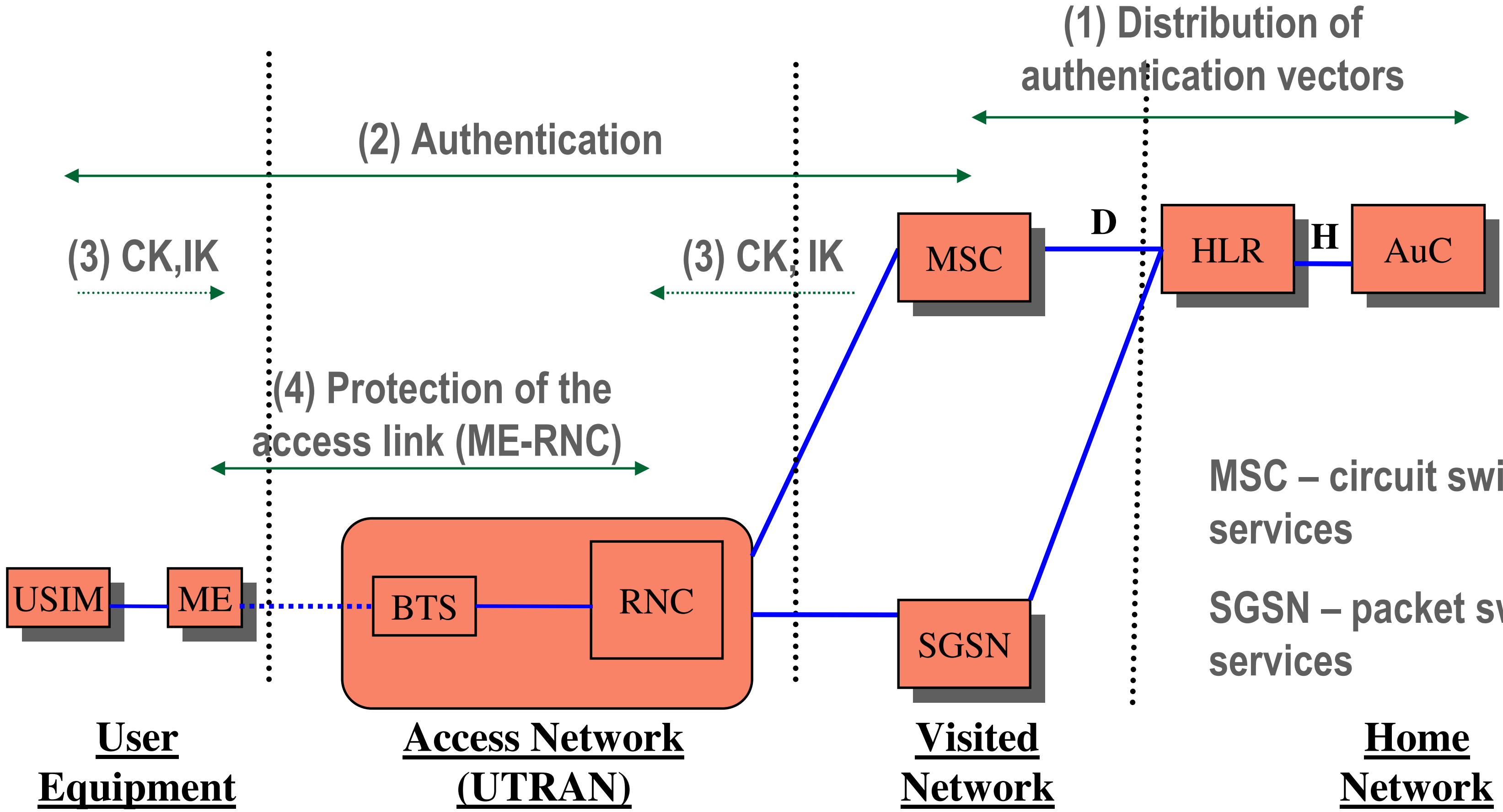
UMTS Integrity Protection Algorithm

- Two standardised algorithms: UIA1 and UIA2.
  - Located in the customer's phone (not the USIM) and in every radio network controller.
  - Integrity key (IK) passed from USIM to ME after authentication.
  - Standardised so that mobiles and radio network controllers can interoperate globally.
  - UIA1 based on a mode of operation of KASUMI.
  - UIA2 is a new algorithm introduced in case a vulnerability discovered in UIA1.
    - Again based on Snow3G block cipher.

UMTS Encryption and Integrity Algorithms

- Open design and evaluation of UEA/UIA algorithms by ETSI SAGE.
- Open publication of specifications and evaluation reports.
- No export restrictions on terminals, and network equipment exportable under licence in accordance with international regulations.

UMTS Radio Access Link Security



MSC – circuit switched services

SGSN – packet switched services

Summary of UMTS Radio Access Link Security

- New and enhanced radio access link security features in UMTS:
  - New algorithms – open design and publication.
  - Encryption terminates at the radio network controller.
  - Mutual authentication and integrity protection of critical signalling procedures to give greater protection against false base station attacks.
  - Longer key lengths (128-bit).

Other 3GPP Security Standards

- Security architecture for IP multimedia sub-system (IMS).
  - Provides security for services like presence, instant messaging, push to talk, rich call, click to talk, etc.
- Security architecture for WLAN inter-working.
  - (U)SIM-based security for WLAN network access.
- Security architecture for Multimedia Broadcast/Multicast Service (MBMS).
  - Provides secure conditional access to multicast services.

Further Reading

- 3GPP standards, http://www.3gpp.org/ftp/specs/latest.
  - TS 43.020 – for GSM security features.
  - TS 33.102 – for UMTS security features.
- UMTS Security by Valtteri Niemi and Kaisa Nyberg ISBN: 0-470-84794-8.
- A large collection of GSM/UMTS resources and links at: http://www.brookson.com/gsm/contents.htm.