UMTS security

Helsinki University of Technology
S-38.153 Security of Communication Protocols
k-p.perttula@hut.fi
15.4.2003

Contents

- UMTS Security objectives
- Problems with GSM security
- UMTS security mechanisms
- UMTS and GSM security interoperation
- Summary

3GPP security objectives

- Ensure that 3G security builds on the security of GSM where features that have proved to be needed and that are robust shall be adopted for 3G
- Ensure that 3G security improves on the security of second generation systems by correcting real and perceived weaknesses
- Ensure that new 3G security features are defined as necessary to secure new services offered by 3G

Security Features defined by 3GPP

Technical specifications

- Principles, objectives and requirements

– TS 33.120 Security principles and objectives

– TS 21.133 Security threats and requirements

- Architecture, mechanisms and algorithms

– TS 33.102 Security architecture

– TS 33.103 Integration guidelines

– TS 33.105 Cryptographic algorithm requirements

– TS 35.20x Access network algorithm specifications

- Lawful interception

– TS 33.106 Lawful interception requirements

– TS 33.107 Lawful interception architecture

Technical reports

- Technical reports

– TR 33.900 Guidelines for 3G security

– TR 33.901 Criteria for algorithm design

– TR 33.902 Formal analysis of authentication

Technical specifications and reports are available from www.3gpp.org.

GSM problems to be addressed

- Problems with active attacks using false base stations
- Encryption keys and authentication data are transmitted in clear between and within networks
- Encryption does not extend far enough towards the core network
- The importance of encryption to guard against channel hijack, while acknowledging that encryption may sometimes be switched off (e.g. because some countries may not allow it)
- Data integrity is not provided - data integrity defeats certain false base station attacks and, in the absence of encryption, provides protection against channel hijack
- The terminal identity (the IMEI) is an unsecured identity and should be treated as such
- Fraud and lawful interception were not considered in the design phase of second generation systems but as afterthoughts to the main design work
- Second generation systems do not have the flexibility to upgrade and improve security functionality over time

Problems with GSM Security

- Weak authentication and encryption algorithms (COMP128 has a weakness allowing user impersonation; A5 can be broken to reveal the cipher key)
- Short key length (32 bits)
- No data integrity (allows certain denial of service attacks)
- No network authentication (false base station attack possible)
- Limited encryption scope (Encryption terminated at the base station, in clear on microwave links)
- Insecure key transmission (Cipher keys and authentication parameters are transmitted in clear between and within networks)

3G Security Features (1)

- Mutual Authentication
  - The mobile user and the serving network authenticate each other
- Data Integrity
  - Signaling messages between the mobile station and RNC protected by integrity code
- Network to Network Security
  - Secure communication between serving networks. IPsec suggested
- Wider Security Scope
  - Security is based within the RNC rather than the base station
- Secure IMSI (International Mobile Subscriber Identity) Usage
  - The user is assigned a temporary IMSI by the serving network

3G Security Features (2)

- User – Mobile Station Authentication
  - The user and the mobile station share a secret key, PIN
- Secure Services
  - Protect against misuse of services provided by the home network and the serving network
- Secure Applications
  - Provide security for applications resident on mobile station
- Fraud Detection
  - Mechanisms to combating fraud in roaming situations
- Flexibility
  - Security features can be extended and enhanced as required by new threats and services

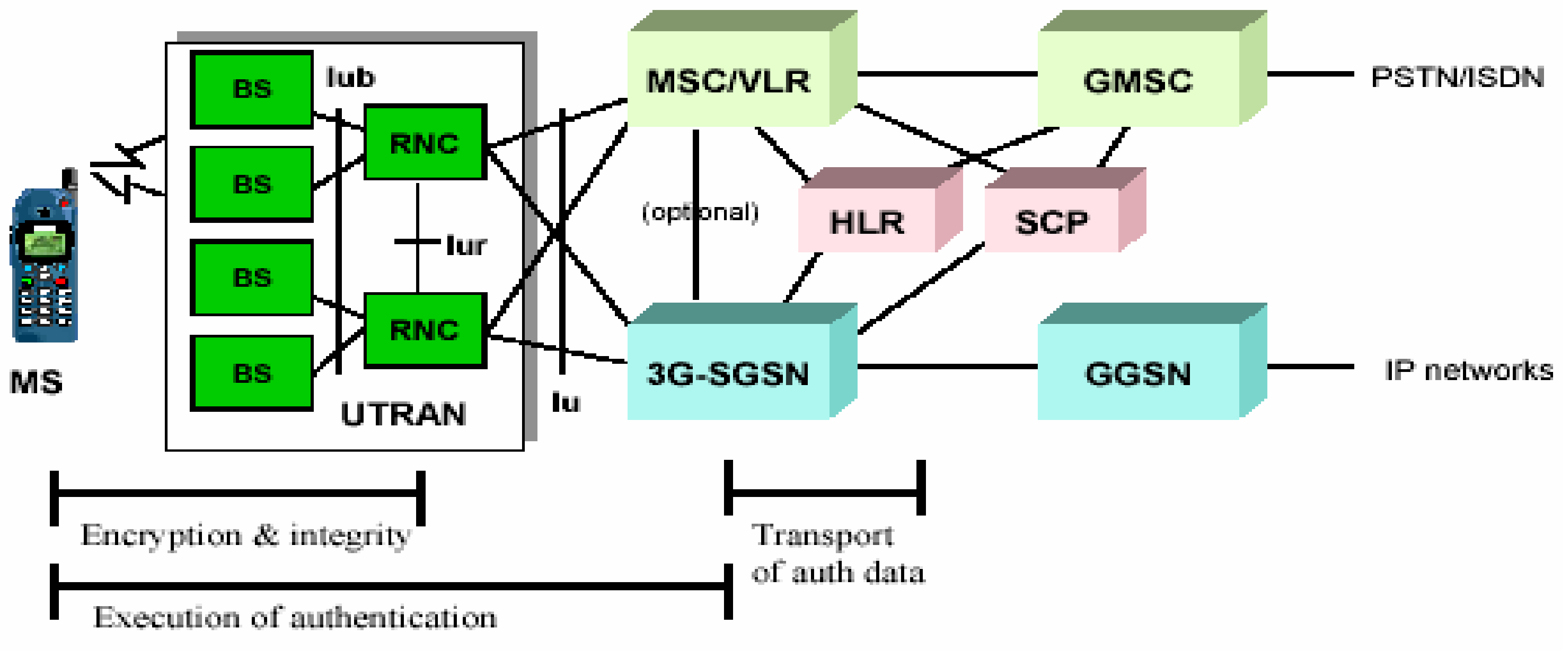
3G Security Features (3)

- Visibility and Configurability
  - Users are notified whether security is on and what level of security is available
- Multiple Cipher and Integrity Algorithms
  - The user and the network negotiate and agree on cipher and integrity algorithms. At least one encryption algorithm exported on world-wide basis (KASUMI)
- Lawful Interception
  - Mechanisms to provide authorized agencies with certain information about subscribers
- GSM Compatibility
  - GSM subscribers roaming in 3G network are supported by GSM security context (vulnerable to false base station)

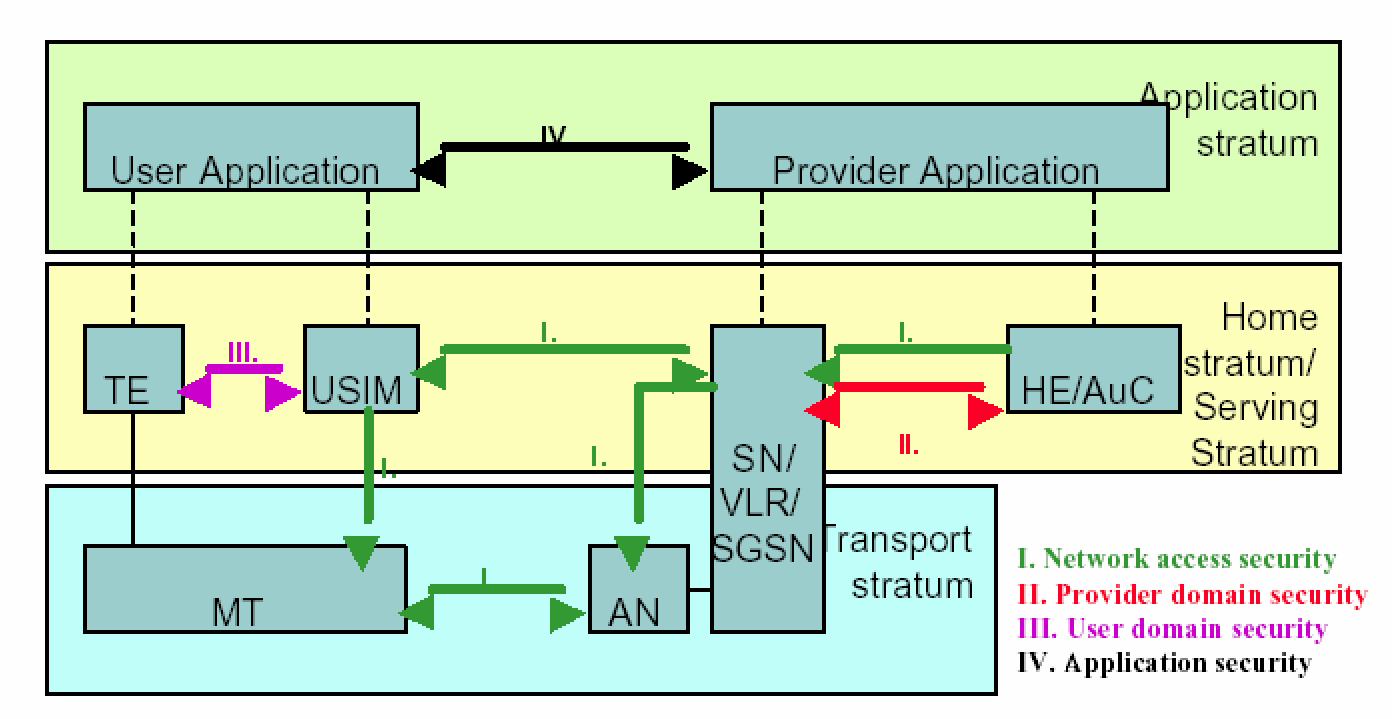
Confidentiality and integrity Key features

- Common to ciphering and integrity
  - Secret key cryptography
  - Key length 128 bits (GSM: 54-64 bits)
  - Public algorithms (GSM: secret algorithm)
- Termination points
  - User side: Mobile equipment
  - Network side: Radio Network Controller(GSM: base station)
- Applied to
  - Confidentiality signaling and user data
  - Integrity signaling data

UMTS system architecture (R99) is based on GSM/GPRS



Security architecture overview



I. Network access security
II. Provider domain security
III. User domain security
IV. Application security

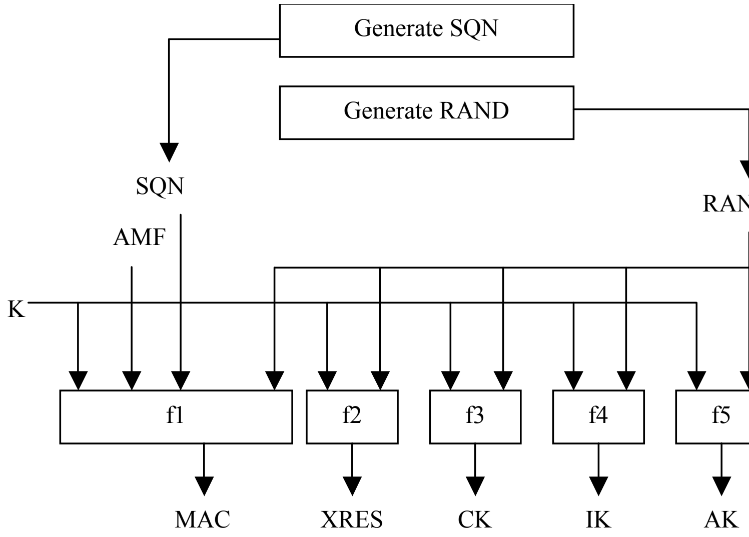
Authentication and key agreement Prerequisites

- AuC and USIM share
  - permanent secret key K
  - message authentication functions f1, f1*, f2
  - key generating functions f3, f4, f5
- AuC has a random number generator
- AuC has scheme to generate fresh sequence numbers
- USIM has scheme to verify freshness of received sequence numbers

Authentication and Key Agreement

128 bit secret key K is shared between the home network and the mobile user

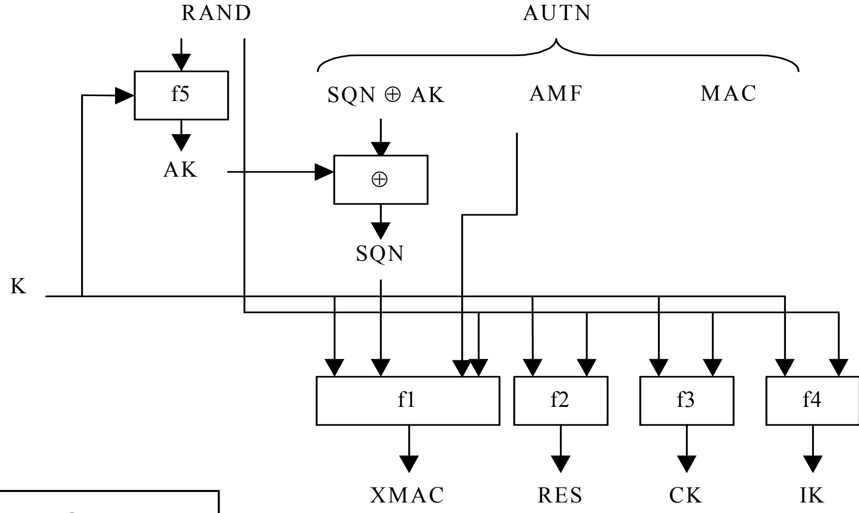
Home Network

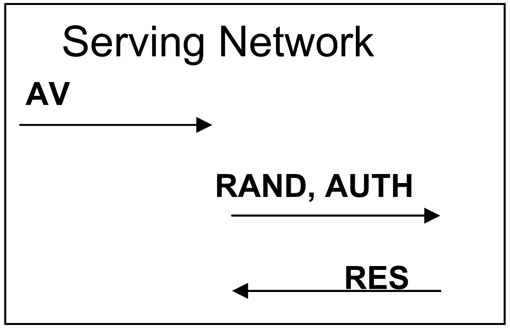


AUTN := SQN ⊕ AK || AMF || MAC

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

Mobile station





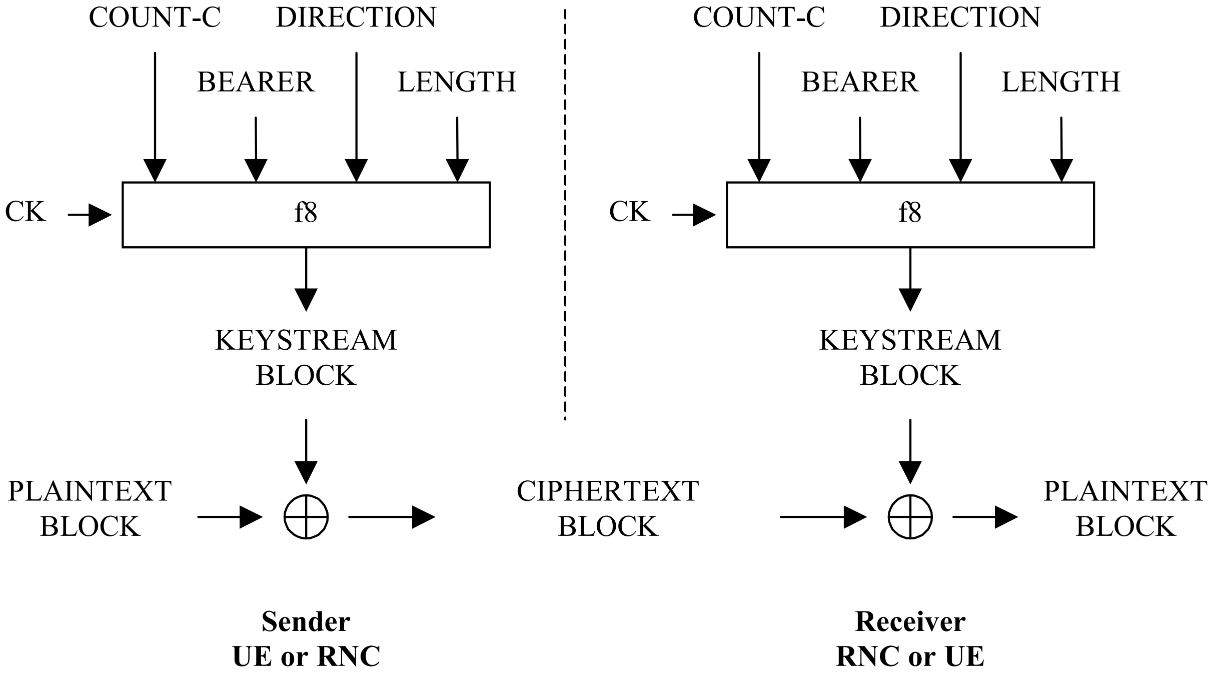
Verify MAC = XMAC

Verify that SQN is in the correct range

Encryption

Signaling and user data protected from eavesdropping. Secret key, block cipher algorithm (KASUMI) uses 128 bit cipher key.

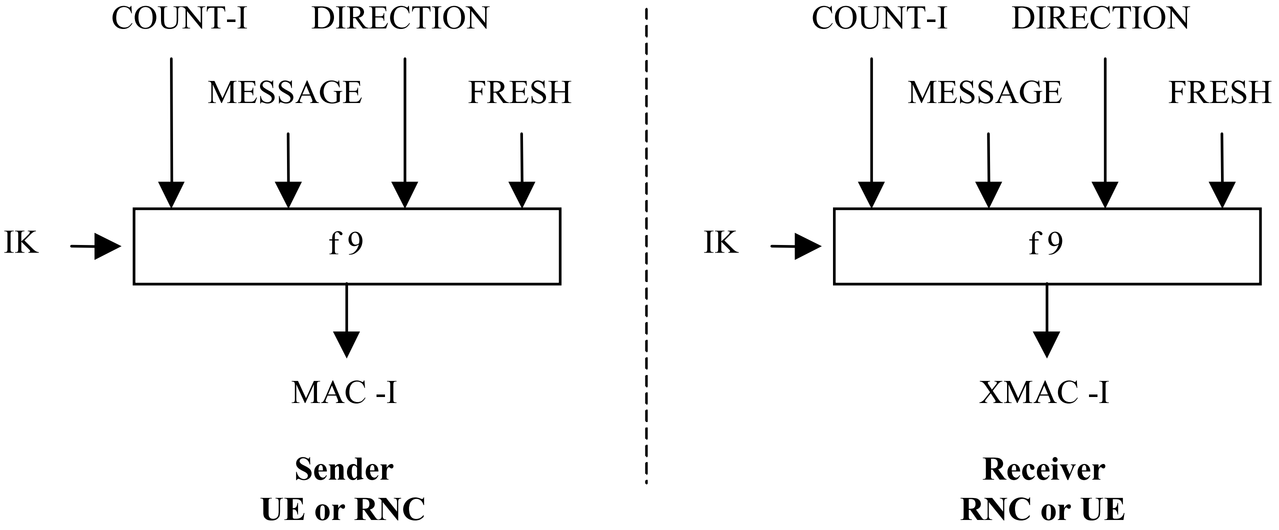
At the mobile station and RNC (radio network controller)



Integrity Check

Integrity and authentication of origin of signalling data provided. The integrity algorithm (KASUMI) uses 128 bit key and generates 64 bit message authentication code.

At the mobile station and RNC (radio network controller)



Confidentiality and integrity Algorithms - KASUMI

- KASUMI
  - Design authority: ETSI SAGE
  - Based on the block cipher MISTY (Mitsubishi)
  - KASUMI is the Japanese for “MIST”
- Two modes of operation
  - f8 for encryption
  - f9 for data integrity protection
- Reviewed by three independent teams of experts
- Reviews were unanimously positive
- Published on ETSI/3GPP web site

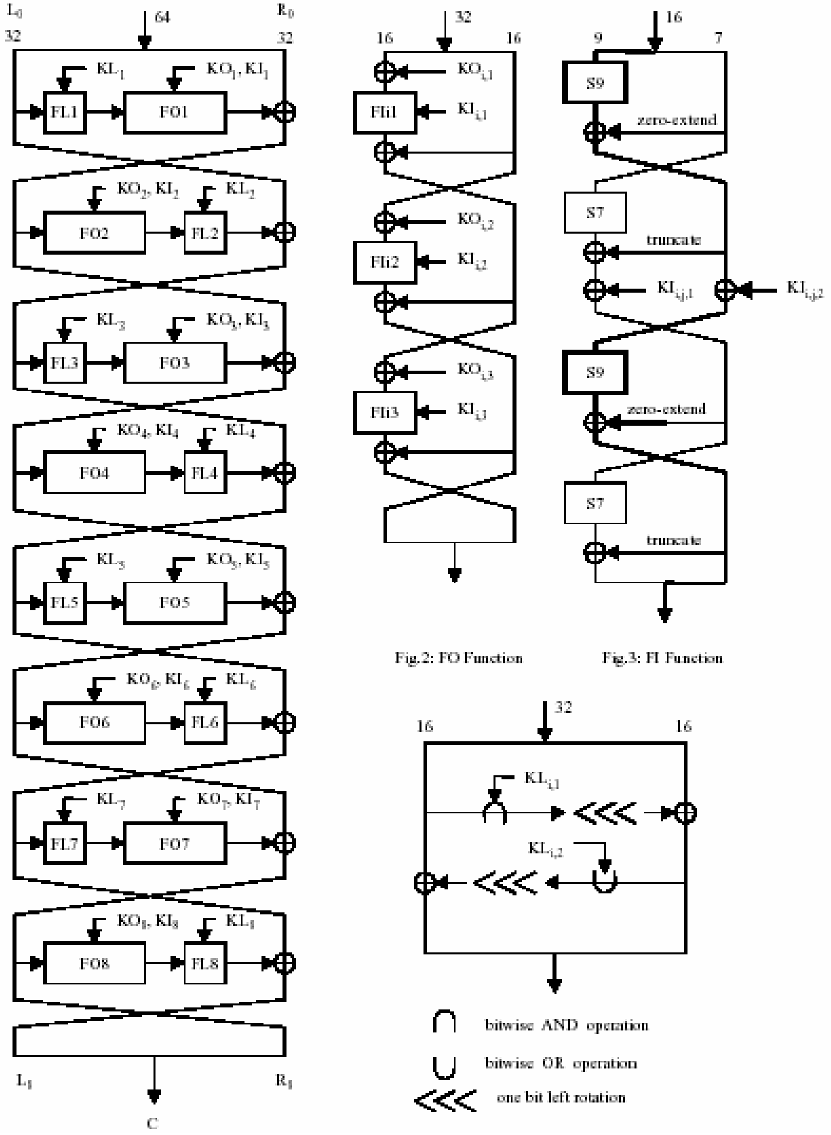


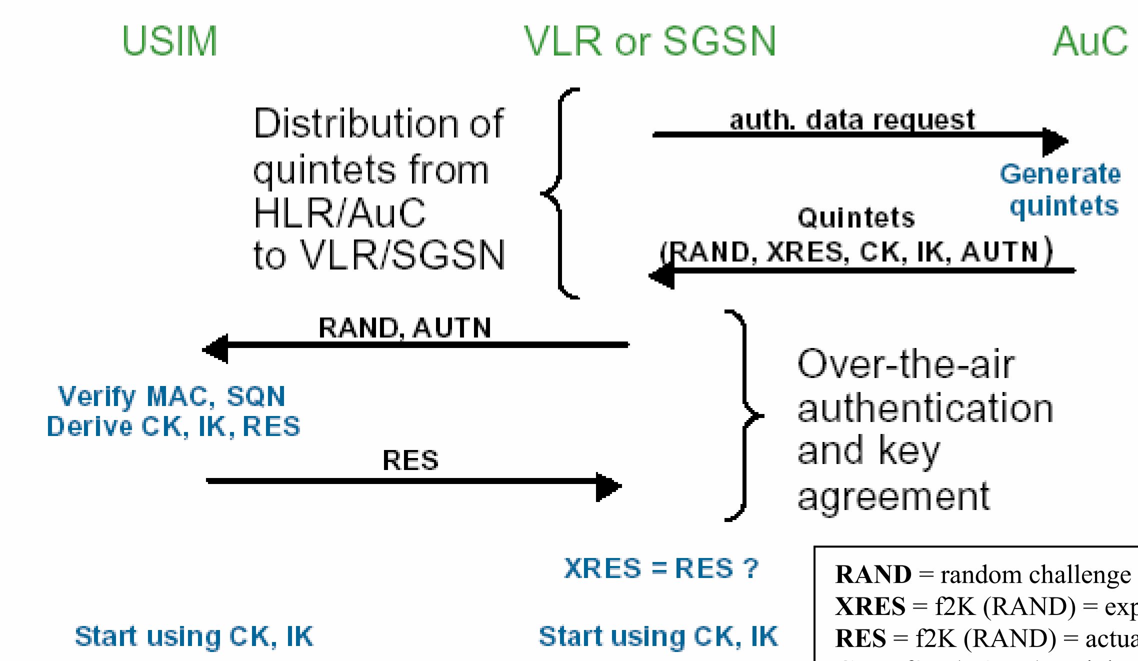
Fig.2: FO Function

Fig.3: FI Function

Ref: 3GPP TS 35.202 V3.1.1

Picture. KAZUMI algorithm

Complete message flow for successful AKA



USIM

VLR or SGSN

AuC

Distribution of quintets from HLR/AuC to VLR/SGSN

auth. data request

Generate quintets

Quintets (RAND, XRES, CK, IK, AUTN)

RAND, AUTN

Verify MAC, SQN
Derive CK, IK, RES

RES

Over-the-air authentication and key agreement

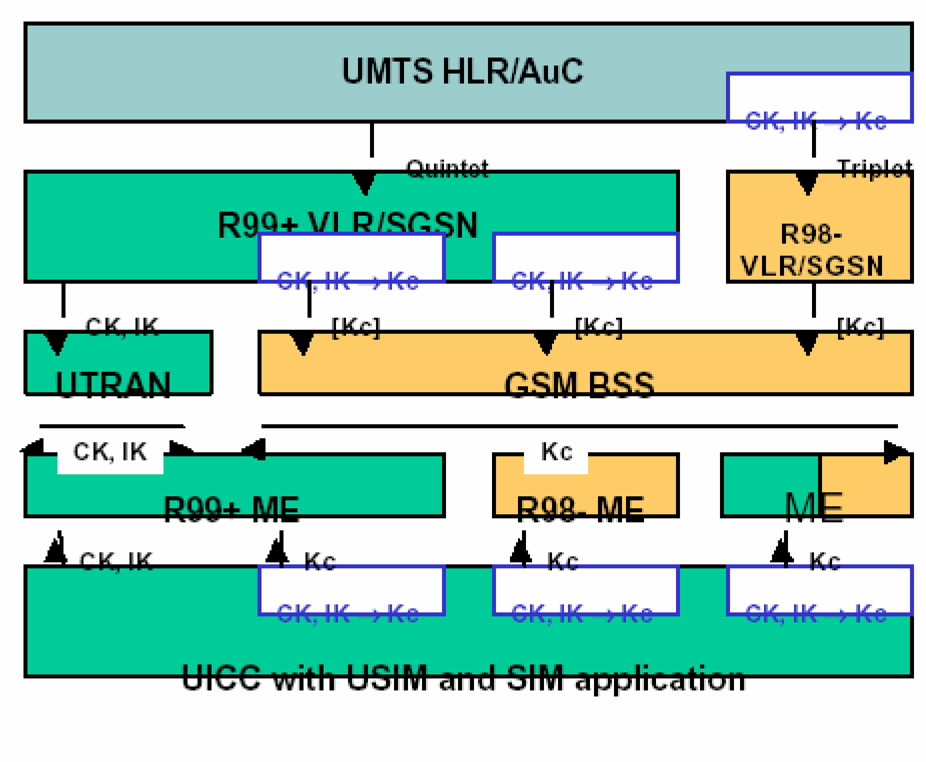
XRES = RES ?

Start using CK, IK

Start using CK, IK

RAND = random challenge generated by AuC
XRES = f2K (RAND) = expected user response computed by AuC
RES = f2K (RAND) = actual user response computed by USIM
CK = f3K (RAND) = cipher key
IK = f4K (RAND) = integrity key
AK = f5K (RAND) = anonymity key
SQN = sequence number
AMF = authentication management field
MAC = f1K(SQN || RAND || AMF) = message authentication code computed over SQN, RAND and AMF
AUTN = SQNÅAK || AMF || MAC = network authentication token, concealment of SQN with AK is optional
Quintet = (RAND, XRES, CK, IK, AUTN)

Interoperation between UMTS and GSM

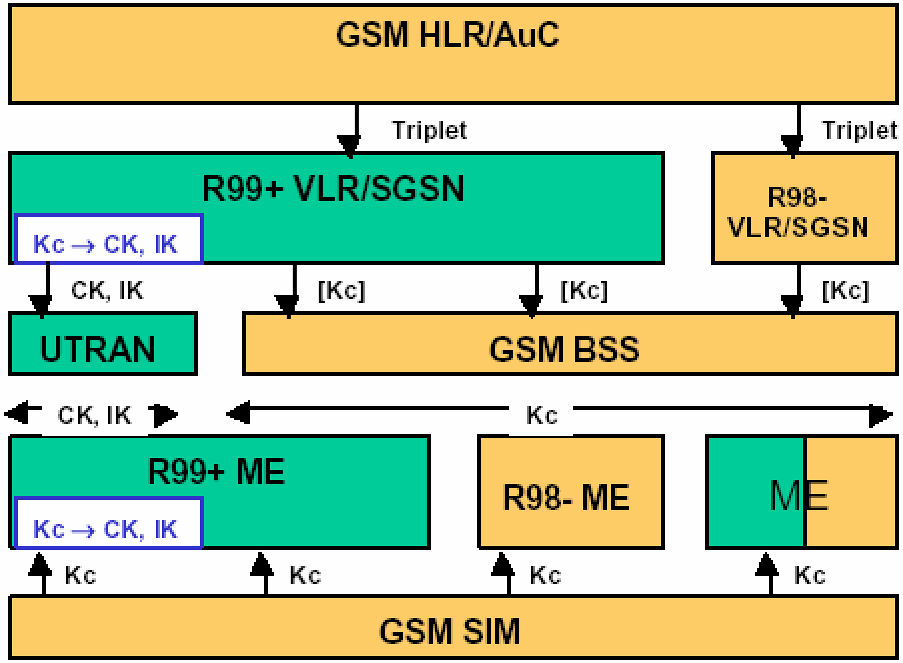


- UMTS AKA
  R99+ VLR/SGSN
  and UICC
- GSM AKA
  Otherwise

- CK, IK
  UTRAN
- Kc
  Otherwise

- Standard function
  c3: CK, IK → Kc

Interoperation between UMTS and GSM



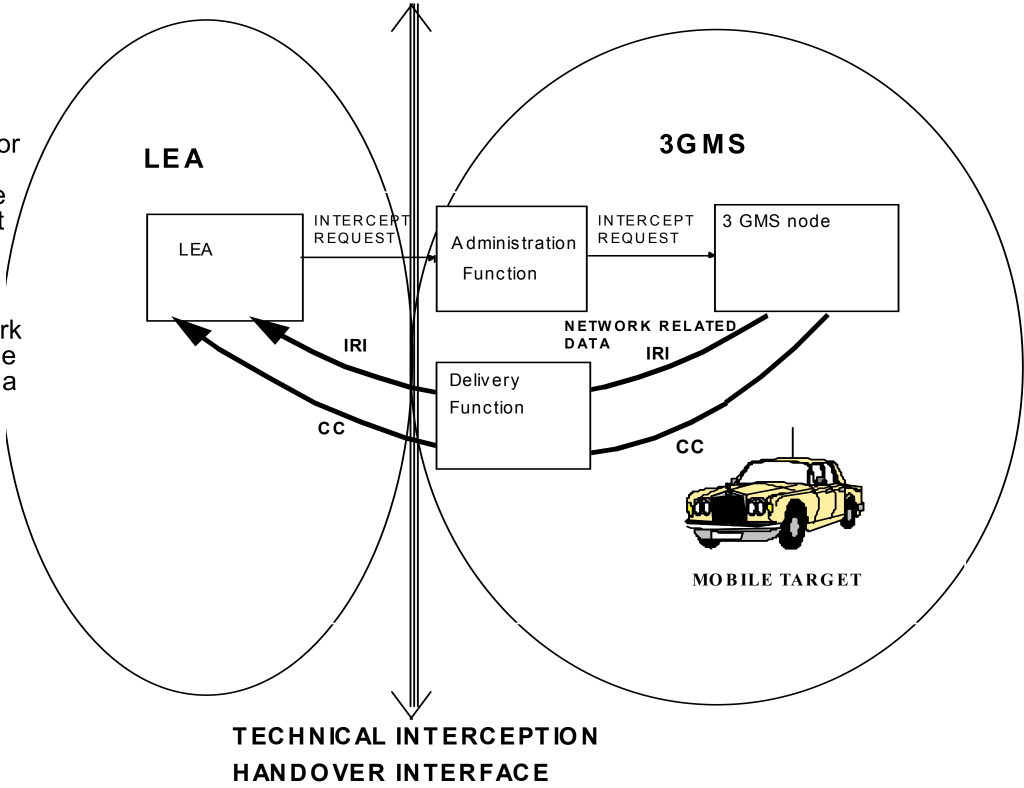
- UMTS AKA
  never
- GSM AKA
  always
- CK, IK
  UTRAN
- Kc
  Otherwise
- Standard functions
  c4: Kc → CK
  c5: Kc → IK

IPSEC

- Network level safety protocol standardized by IETF
- Obligatory in IPv6
- IPSEC used in all-IP UMTS
- IP traffic between networks can be protected with IPSEC between security gateways
- Native IP-protocols will be protected with IPSEC, like GTP
- Why it's needed?
  - Spoofing
  - One machine masquerades as another
  - Sniffing
  - Eavesdropping between two or more parties
  - Session high-jacking
  - Using above techniques one user could take over an established connection (man in the middle attack)

Lawful Interception

- Lawful interception plays a crucial role in helping law enforcement agencies to combat criminal activity.
- 3GMS shall provide access to the intercepted Content of Communications (CC) and the Intercept Related Information (IRI) of the mobile target on behalf of Law Enforcement Agencies (LEAs).
- A mobile target in a given 3GMS can be a subscriber of that 3GMS, or a user roaming from another 3GMS or from any other network capable of using that 3GMS (such as a GSM or mobile satellite). The intercepted CC and the IRI can only be delivered for activities on that given 3GMS.
- For interception, there needs to be a means of identifying the target, correspondent and initiator of the communication. Target Identities used for interception shall be MSISDN, IMEI and IMSI. When network encryption is introduced, it shall be a national option as to whether the network provides the CC to the agency decrypted, or encrypted with a key available to the agency.
- Location Dependent Interception, (LDI) allows a 3GMS to service multiple interception jurisdictions within its service area. Multiple law agencies with their own interception areas can be served by the 3GMS. All the information or rules given for interception within a 3GMS apply to interception within an IA when Location Dependent Interception is invoked. A target may be marked in one or more different IAs within the same 3GMS. Interception is not required nor prohibited by this standard when Location Dependent Interception is active and the location of the target subscriber is not known or available.

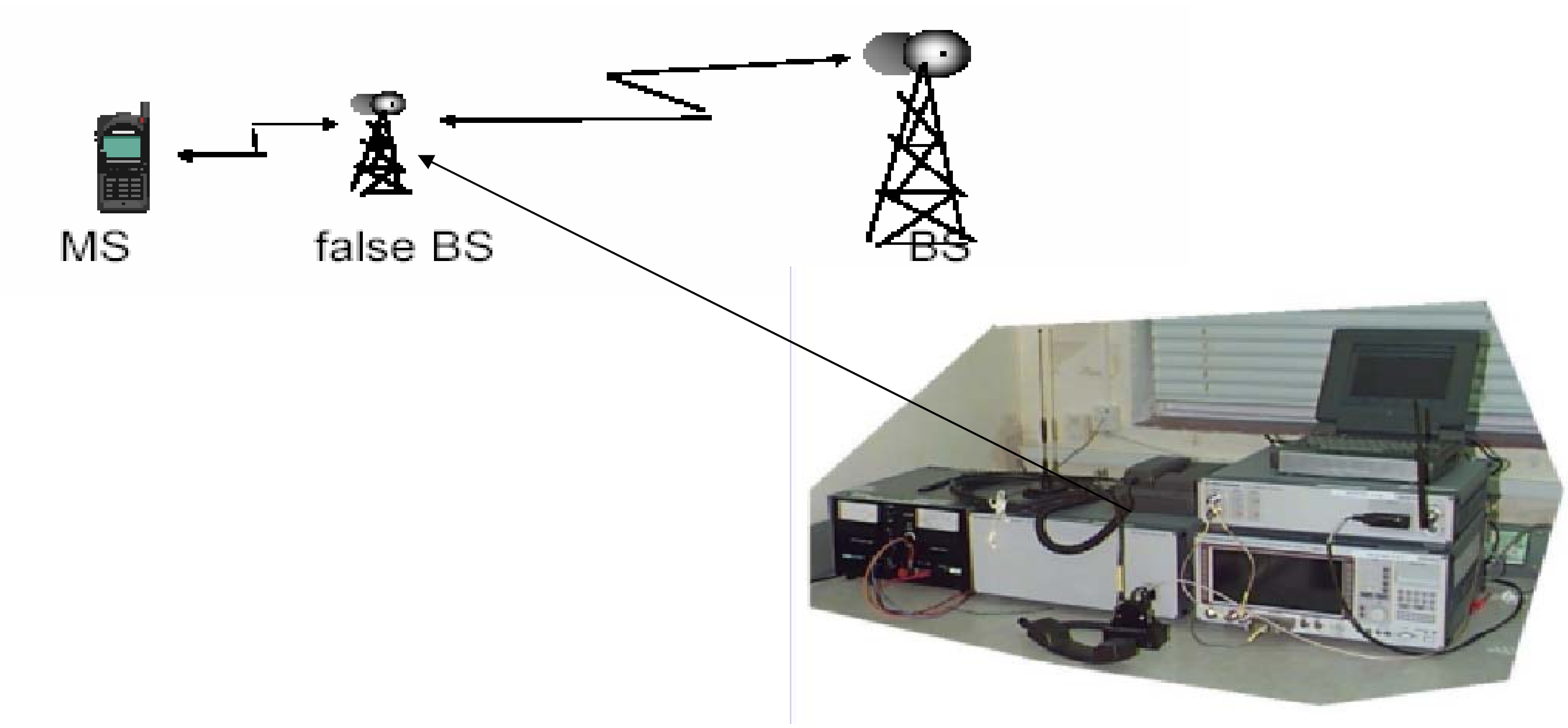


CC = Content of Communication
IA = Interception Area
IRI = Intercept Related Information

Problems with 3G Security

- All that can happen to a fixed host attached to the Internet could happen to a 3G terminal
- IMSI is sent in cleartext when the user is registering for the first time in the serving network (trusted third party can be a solution)
- A user can be enticed to camp on a false BS. Once the user camps on the radio channels of a false BS, the user is out of reach of the paging signals of SN
- Hijacking outgoing/incoming calls in networks with disabled encryption is possible. The intruder poses as a man-in-the-middle and drops the user once the call is set-up

Active attack(false BS)



Summary

- Inherits good practices from GSM
- UMTS R99 offers better subscriber safety than GSM
- New features are bilateral authentication and signaling integrity check
- Algorithms are public and longer keys are used
- Safety mechanisms between networks standardized in UMTS R4/R5
- Subscriber safety in IP Multimedia systems
  - IPSEC is new mechanisms in IP-based networks
  - Independent from radio technology
  - Utilized methods that are already in use