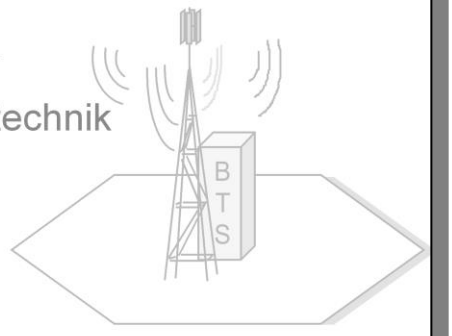
Institut für Kommunikations-Technik

Evolution der öffentlichen Mobilfunknetze (3G/4G)
Chapter VII: Radio Interface Protocols
- Security -

Universität Hannover
Institut für Kommunikationstechnik
Dr.-Ing. Jan Steuer



Leibniz Universität Hannover

Evolution of public radio networks

Institut für Kommunikations-Technik

1. Introduction/Overview GSM/UMTS
2. Basics: Radio Transmission
3. Basics: Radio Network Planning
4. Physical Layer
5. Radio Interface Protocols
6. Architecture / Core Network
7. Security
8. UMTS Evolution / LTE
9. Supplemtary Services

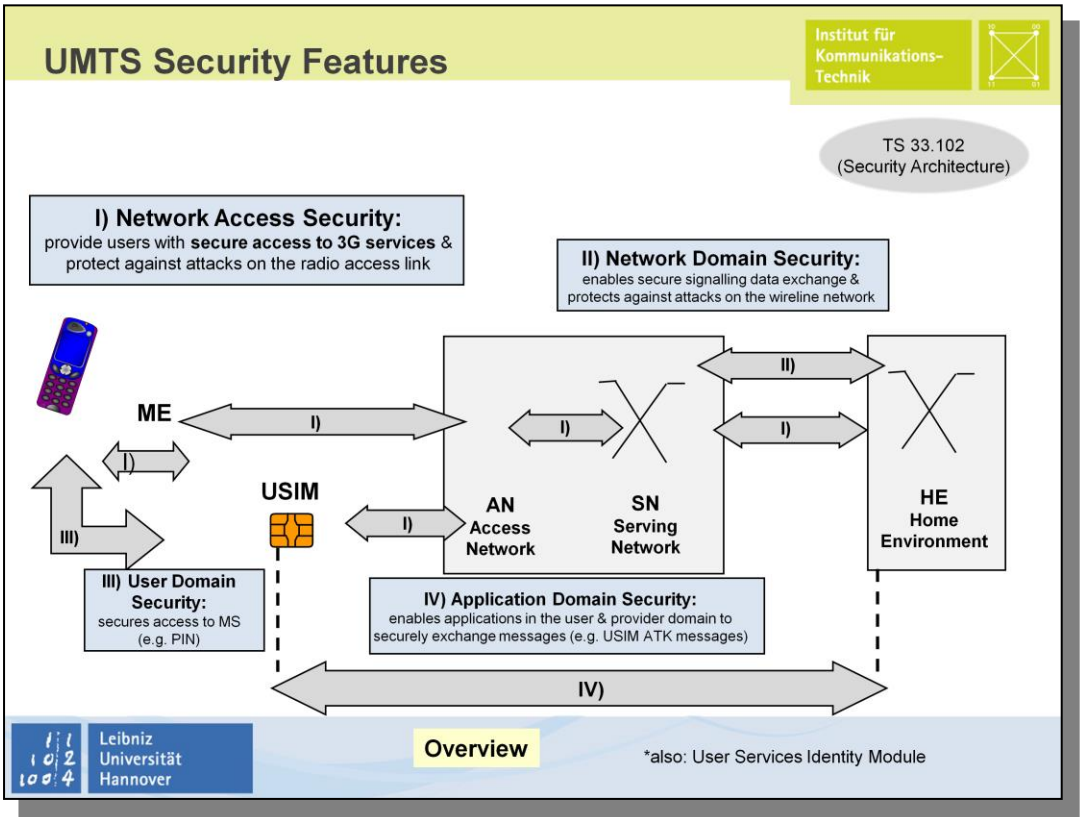
Leibniz Universität Hannover

Outline Part V-III

Institut für Kommunikations-Technik

1. Overview
2. Identities
3. Authentication
4. Ciphering & Integrity

Leibniz Universität Hannover



UMTS Security Features: Overview

Five security feature groups are defined in UMTS (TS 21.133, 33.102, 31.120). Each of these feature groups meets certain threats and accomplishes certain security objectives:

I) Network Access Security

The network access security features, which are defined more precisely in the following chapter, provide users with secure access to UMTS services. Additionally, some of them protect the user and the network against attacks on the radio access link. Currently, User Identity Confidentiality **(P-TMSI, TMSI Allocation),** Entity Authentication **(User/Network Authentication),** Confidentiality **(Ciphering), Data Integrity** and Mobile Equipment Identification **(IMEI Check)** are defined as Network Access Security features.

II) Network Domain Security:

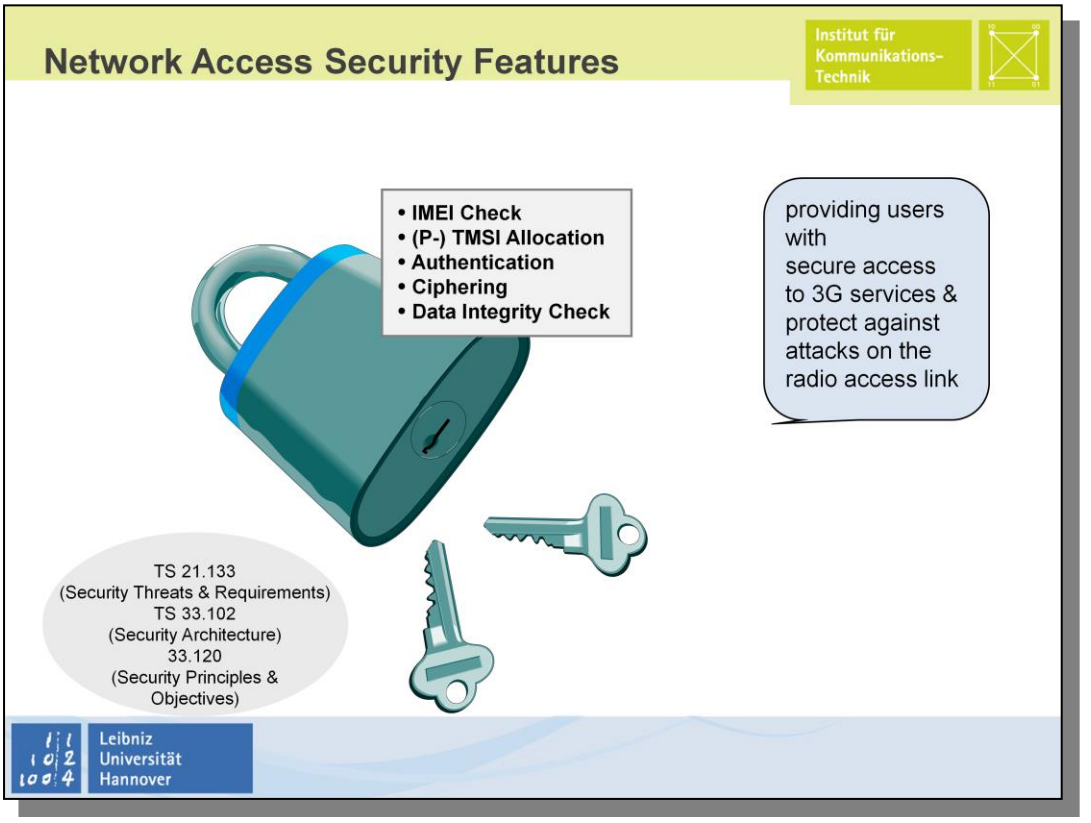
The network domain security features will be defined in future to enable nodes in the provider domain to securely exchange signaling data and protect against attacks on the wire-line network.

III) User Domain Security:

The user domain security features have been defined to enable secure access to the user equipment UE. Currently User-to-USIM Authentication (e.g. PIN; see TS 31.101) and USIM-Terminal Link security (restricting an ME to an authorized USIM by sharing a secret; see TS 22.022) are defined.

IV) Visibility and Configurability of Security:

The visibility & configurability of security features have been defined to enable the user to inform him whether a security feature is in operation. Additionally, the user should be able to decide whether the use and provision of services should depend on the security feature. Examples for visibility are the indication of access network encryption and the indication of the level of security (e.g. 3G or 2G network). Examples for configurability are enabling/disabling User-USIM authentication, accepting/rejection incoming non-ciphered calls, setting-up or not setting-up non-ciphered calls, accepting/rejecting the use of certain ciphering algorithm.



Network Access Security Features

Similar to GSM, the UMTS system provides some mechanism to guarantee the network access security. Some features are still the same as in GSM, others have been enhanced, and also two new aspects have been additionally defined. The following network access security features have been defined in Rel. ´99:

IMEI Check: To prevent the usage of stolen or not allowed mobile equipment, the mobile equipment identification can be checked by the network. This feature remains the same as in GSM.

P-TMSI /TMSI Allocation: To guarantee the user identity confidentiality respectively the user location confidentiality the permanent user identity IMSI is normally not transmitted over the radio interface. The user is normally identified by the temporary identity TMSI/P-TMSI, by which he is known in the serving network. This feature remains the same as in GSM.

Authentication: In UMTS authentication is extended compared to GSM. Additionally to the User Authentication a Network Authentication is introduced. User Authentication is the property that the Serving Network SN checks the real identity of the user, preventing non-authorized access to the network. Network Authentication is a check whether the connected SN is really authorized by the user´s Home PLMN to provide him services. This includes the guarantee that this authorization is recent.

Ciphering: Ciphering prevents eavesdropping of user data and signaling over the radio interface. UMTS ciphering has been enhanced compared to GSM/GPRS.

Data Integrity Check: The Data Integrity Check has been introduced as a new security feature in UMTS. It provides security against unauthorized modification of signaling data respectively the change of data origin.

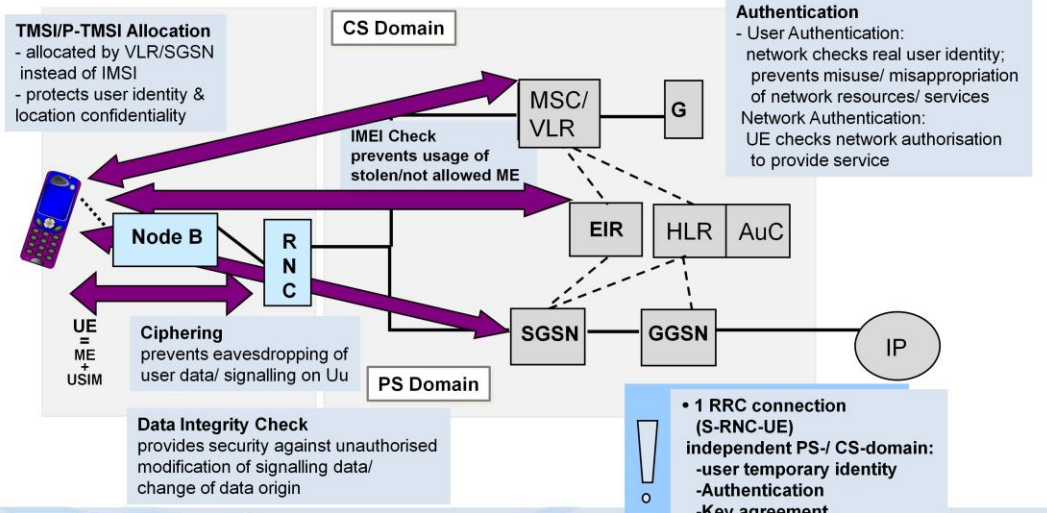
As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in the PS and CS domain. User traffic will be ciphered using the cipher key agreed for the corresponding service domain. Control data will be ciphered and integrity protected using the cipher and integiry keys form either one of the service domains.

The Serving RNC has distribution functionality for the PS and CS domain. Two Iu singaling connections exist, but only one RRC connection.

Network Access Security Features

Institut für Kommunikations-Technik

TS 33.102



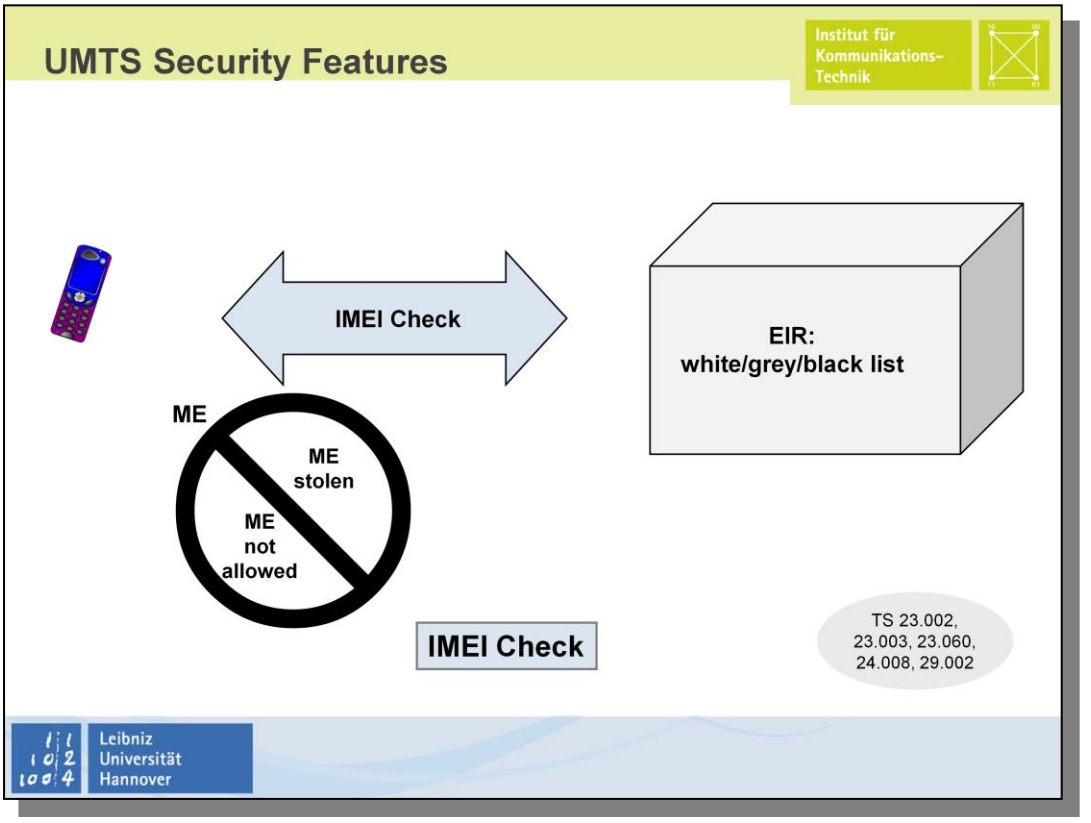
Leibniz Universität Hannover

Outline Part V-III

Institut für Kommunikations-Technik

1. Overview
2. Identities
3. Authentication
4. Ciphering & Integrity

Leibniz Universität Hannover



IMEI Check

The IMEI Check is an optional feature, which can be used to prevent the usage of stolen or not allowed mobile equipment. This feature remains the same as in GSM.

The International Mobile Equipment Identity IMEI identifies uniquely a Mobile Equipment ME. Two versions of IMEI are defined (TS 23.003):
IMEI: The IMEI is composed of a Type Approval Code TAC (6 digits), a Final Assembly Code FAC (2 digits) to identifies the place of manufacture/final assembly, a Serial Number SNR (6 digits) as individual serial number uniquely identifying each equipment within each TAC and FAC and a Spare digit (1 digit) being zero, when transmitted by teh MS/UE.

IMEISV (IMEI & Software Version number): The IMEISV is comprosed of the Type Approval Code TAC, Final Assembly Code FAC, Serial Number SNR and a Software Version Number SVN (2 digits), which identifies the ME software version number.

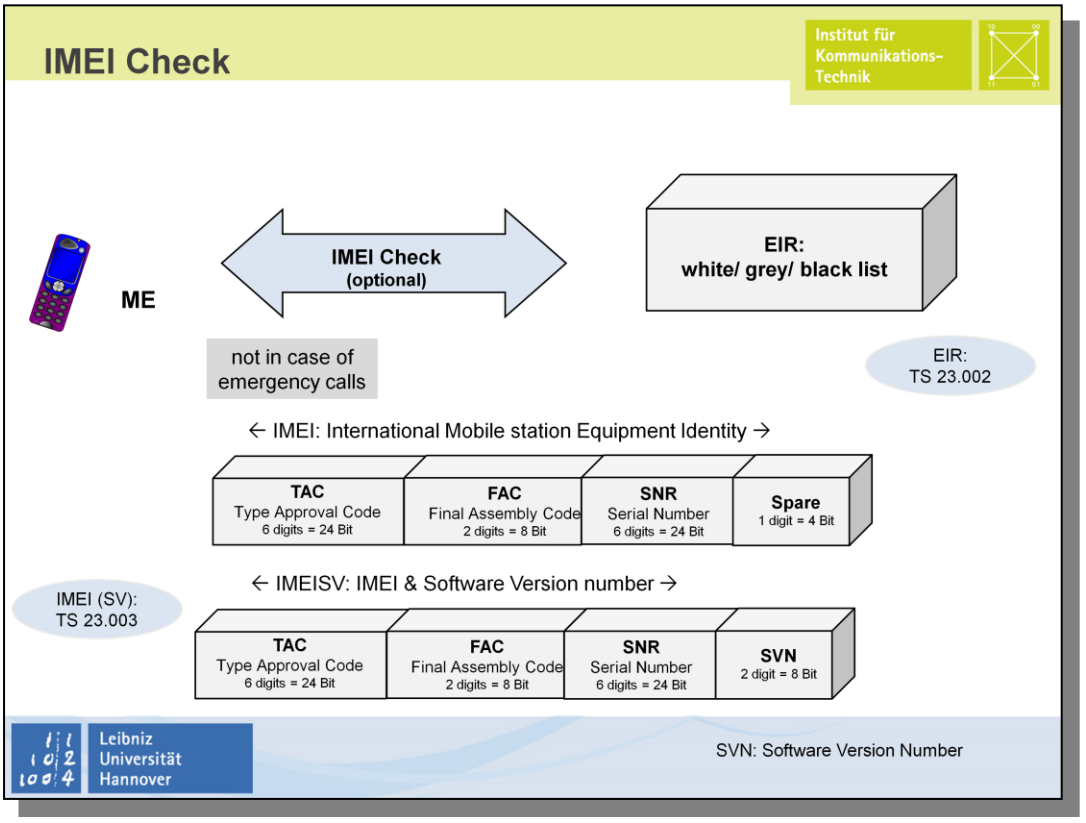
The security requirements of the IMEI are defined in 3GPP TS 22.016.

The IMEI should be surely stored in the ME. In certain cases, the Serving Network SN may request the UE to send it the IMEI. This shall be done only after authentication. In the case of emergency calls, no IMEI check should be performed.

The **Equipment Identity Register EIR** (TS 23.002) is responsible for storing the IMEIs in teh network. The ME is classified as „white listed“, „gray listed“, „black listed“ or it may be unknown as specified in TS 22.016 and TS 29.002.

The white list is composed of all number series of equipment identities that are permitted for use. The black list contains all equipment identities that belong to equipment that need to be barred. Besides the black and white list, administrations have the possibility to use a gray list. Equipment on the gray list are not barred, but are tracked by the network (for evaluation or other purposes).

An EIR shall as a minimum contain a „white list“.



IMEI Check Procedure

The IMEI(SV) shall only be send after authentication (TS 33.102).

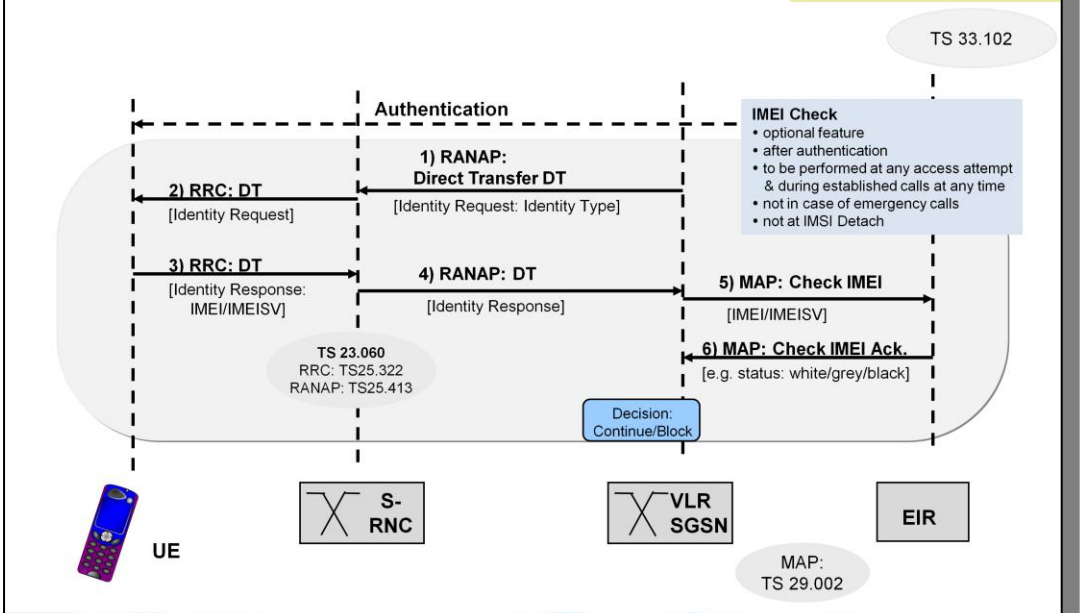
It shall be possible to perform the IMEI check at any access attempt, except IMSI detach, and during an established call at any time when a dedicated radio resource is available, in accordance with the security policy of the PLMN operator (TS 22.016).

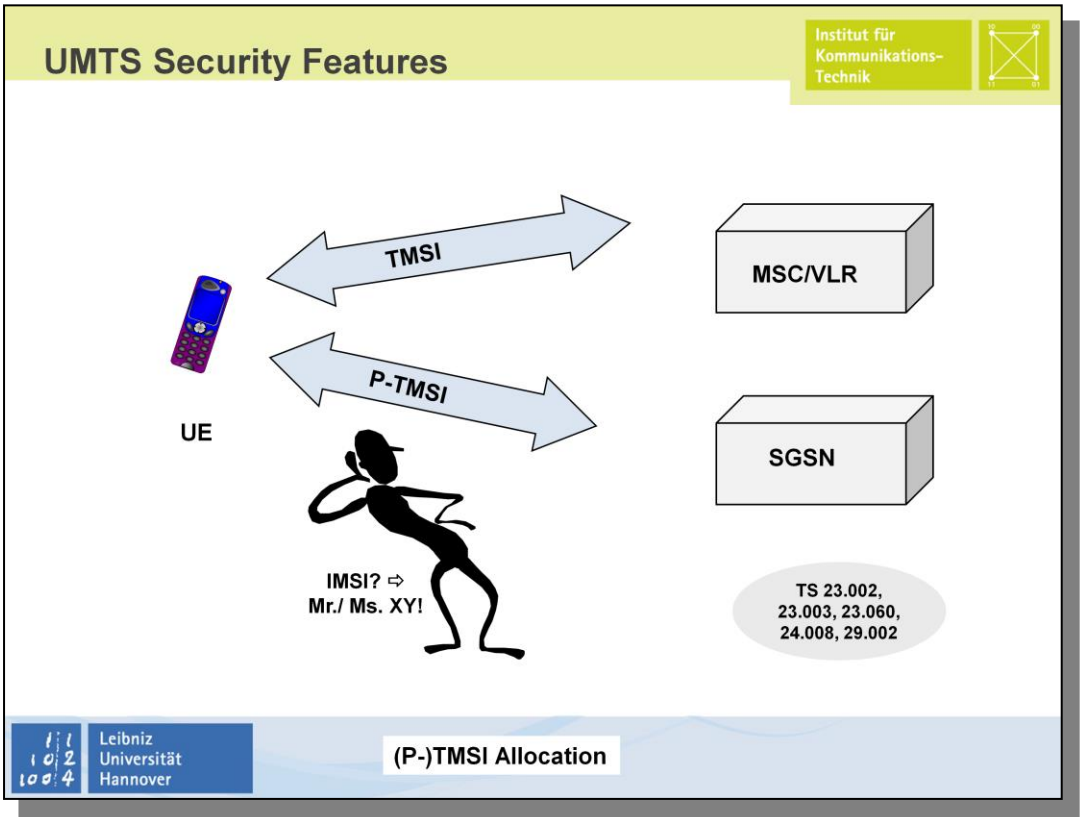
The network shall terminate any access attempt or ongoing call when receiving any of the answers „black-listed“ (i.e., on the black list) or „unknown“ equipment (i.e. not on the white list) from the EIR. An indication of „illegal ME“ shall in these cases be given to the user. Furthermore this is equivalent to an authentication failure hence any call establishment or any location updating is forbidden for the MS/UE, it cannot answer to paging, it is just allowed to perform Emergency Calls.

Emergency calls must never be terminated as a result of the IMEI check procedure.

The procedures to check the IMEI are described in TS 23.060 and TS 29.002.

IMEI Check Procedure





(P-)TMSI Allocation

A unique International Mobile Subscriber Identity IMSI shall be allocated to each mobile subscriber in the GSM system.

To achieve user identity confidentiality and user location confidentiality, the user is normally identified by a temporary identity (Temporary Mobile Subscriber Identity TMSI or Packet-TMSI) by which he is known by the Serving Network SN. To avoid user traceability, which may lead to compromise of user identity confidentiality, the user should not be identified for a long period by means of the same (P-)TMSI (TS 33.102). (P-)TMSI should be used at any Location Update Request, Service Request, Detach Request, connection re-establishment request, etc.

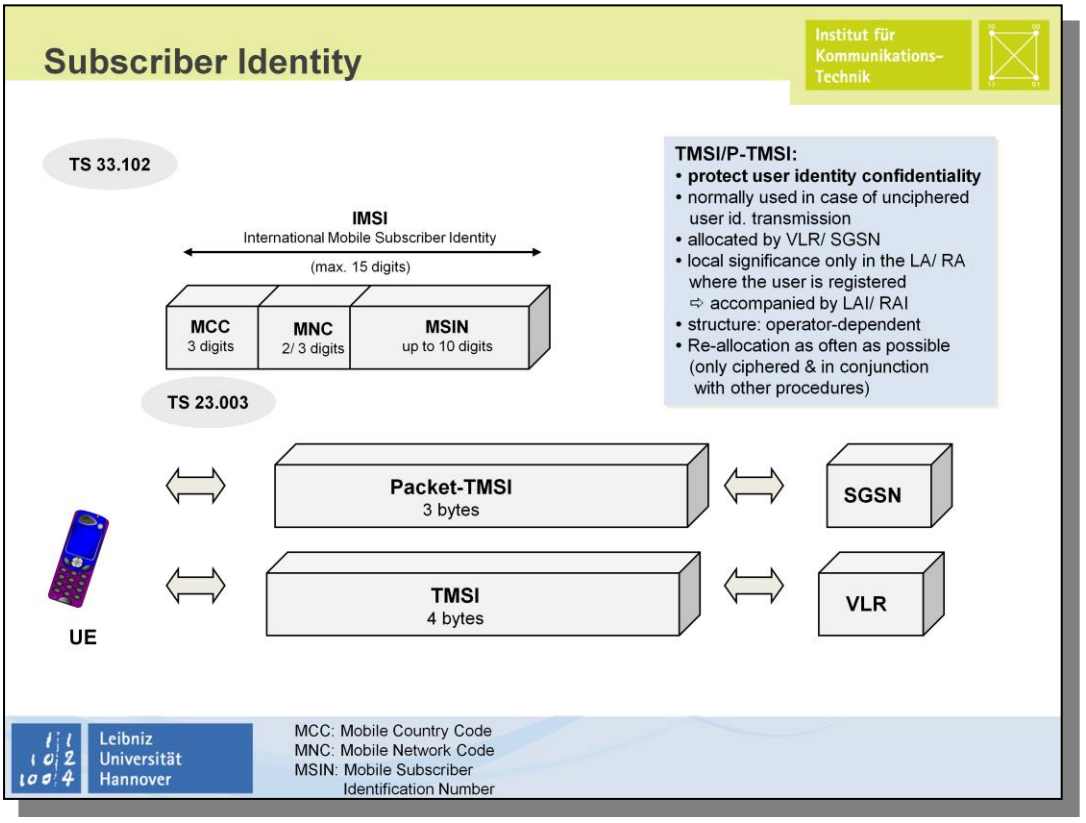
A (P-)TMSI has local significance only in the LAI or RAI in which to user is registered. Outside that area it should be accompanied by an appropriate LAII or RAI in order avoid ambiguities. The association between IMSI and TMSI / P-TMSI is kept by the VLR/SGSN in which the user is registered.

IMSI structure

The IMSI is composed of three parts: Mobile Country Code MCC, Mobile Network Code MNC and Mobile Subscriber Identity Code MSIN. The MCC (3 digits; CCITT administered) identifies uniquely the country of the mobile subscriber. The MNC (2 digits) identifies the Home PLMN of the mobile subscriber. The MSIN identifies the mobile subscriber within a GSM PLMN. The IMSI shall consist of numerical characters (0 through 9) only. The overall number of digits in IMSI shall not exceed 15 digits.

(P-)TMSI structure

Since the (P-)TMSI has only local significance (i.e. within a VLR/SGSN area), the structure and coding of it can be chosen by agreement between operator and manufacturer in order to meet local needs. The P-TMSI/TMSI consists of 3/4 octets. It can be coded using a full hexadecimal representation.



(P-)TMSI Usage & Re-Allocation

The (P-)TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging request, Location Area/Routing Area LA/RA Update Requests, Attach/Detach requests, Service Requests, Connection Re-establishment Requests,…

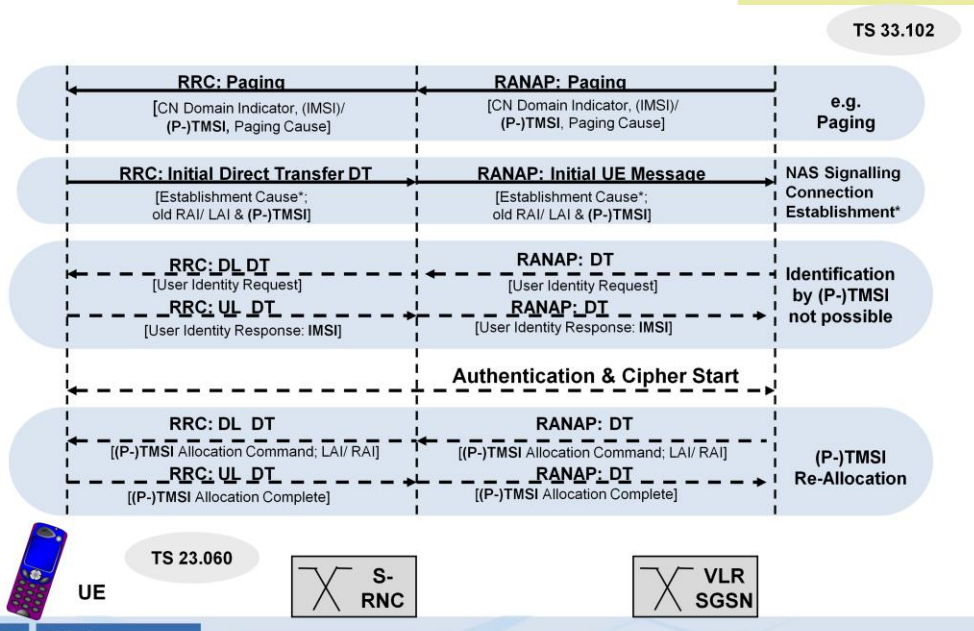
If the user cannot be identified by means of a (P-)TMSI, he is requested to identify himself by his permanent identity IMSI („User Identity Request/Response“).

(P-)TMSI Re-Allocation („(P-)TMSI Allocation Command/Complete“) is performed to allocate a new TMSI/LAI respectively P-TMSI/RAI pair to a user by which be may subsequently be identified on the radio access link. It should be performed after initiation of ciphering. The Re-Allocation is initiated by the VLR/SGSN.

The procedures P-(TMSI) usage & re-allocation procedures and mechanism are described e.g. in TS 23.060 and TS 31.102.

(P-)TSMI Usage & Re-Allocation

Institut für Kommunikations-Technik



Leibniz Universität Hannover

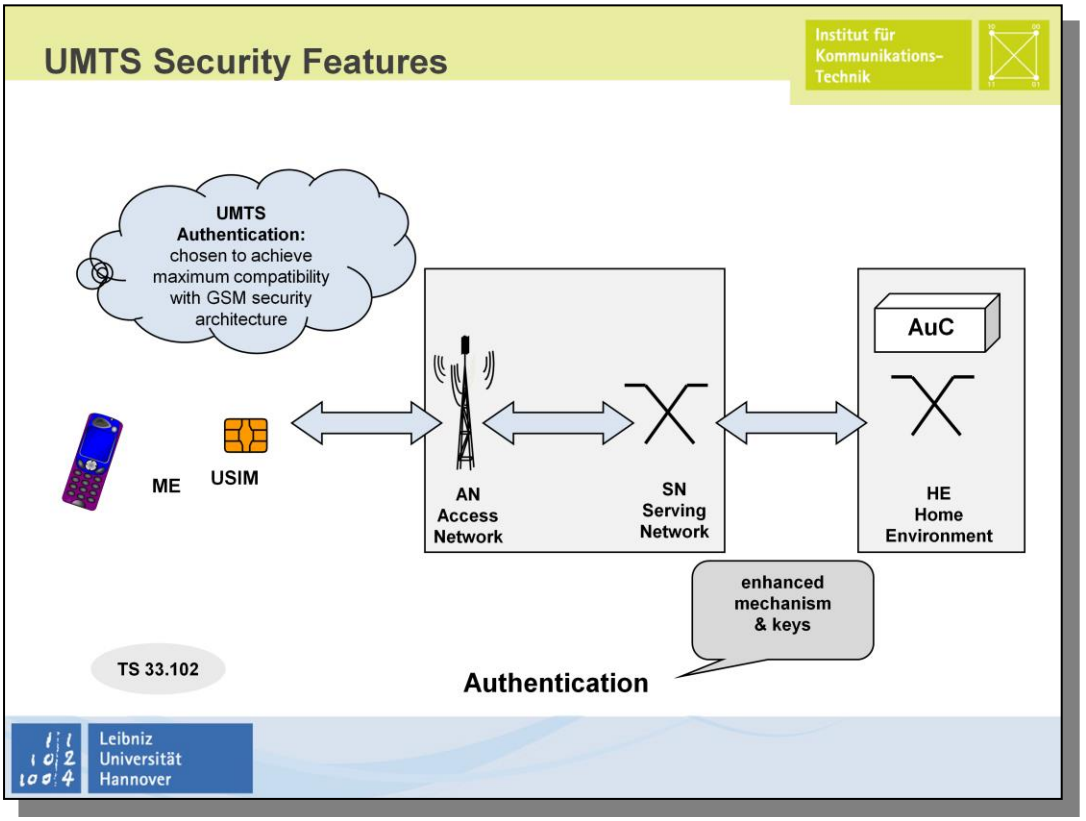
*e.g. LUP, RUP, Attach, Detach, Service Request

Outline Part VI

Institut für Kommunikations-Technik

1. Overview
2. Identities
3. Authentication
4. Ciphering & Integrity

Leibniz Universität Hannover



Authentication

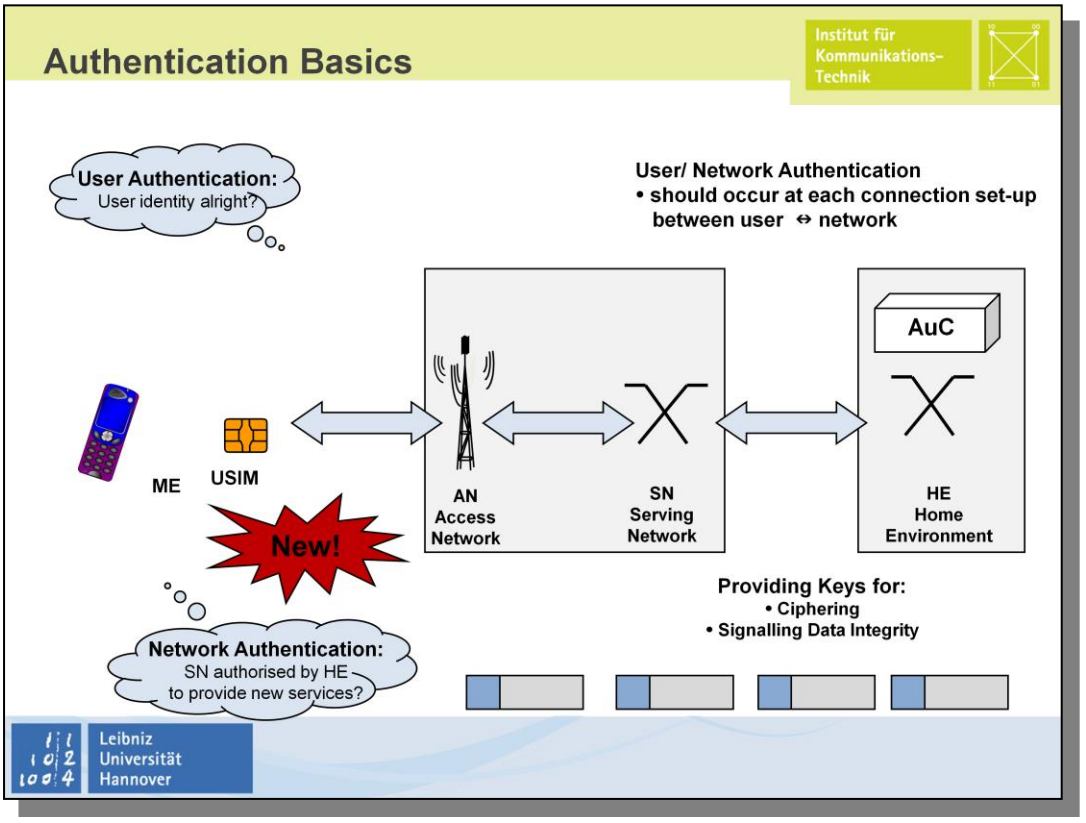
In UMTS different to GSM both sides of the radio transmission check the correct identity of their counterpart. Not only the user identity is checked by the Serving Network SN. Additionally, the authorization of the SN to provide services is checked by the UE. Both, user and network authentication should occur at each connection set-up (TS 33.102).

So the objective of the Authentication process is to enable **User Authentication** similar to the GSM Authentication and additionally **Network Authentication**. Furthermore, the Authentication process provides the **keys for Ciphering and Integrity Check** to the User Equipment UE.

The authentication process should occur at each connection set-up between the user and the network.

It has been chosen in such a way to achieve maximum compatibility with the GSM security architecture and facilitate migration from GSM to UMTS.

Nevertheless, the security mechanism and keys for authentication have been enhanced significantly.



Authentication – Basic Principle

For Authentication, Ciphering and Integrity Check a secret Key K is the pre-requisite. This **secret Key K** is shared between and available only to the USIM and the AuC in the user´s Home PLMN (TS 33.102). The function of K is similar to the GSM individual Key Ki, but it is of enhanced length (K: 128 bit; Ki: 64 bit).

Additionally, several different operator-dependent functions are necessary in the HPLMN´s AuC and in the USIM to generate the so-called Authentication Vector AV, which is necessary for Authentication, Ciphering and Integrity Check. AV is often also denoted as Quintet, in analogy to the GSM Authentication Triples.

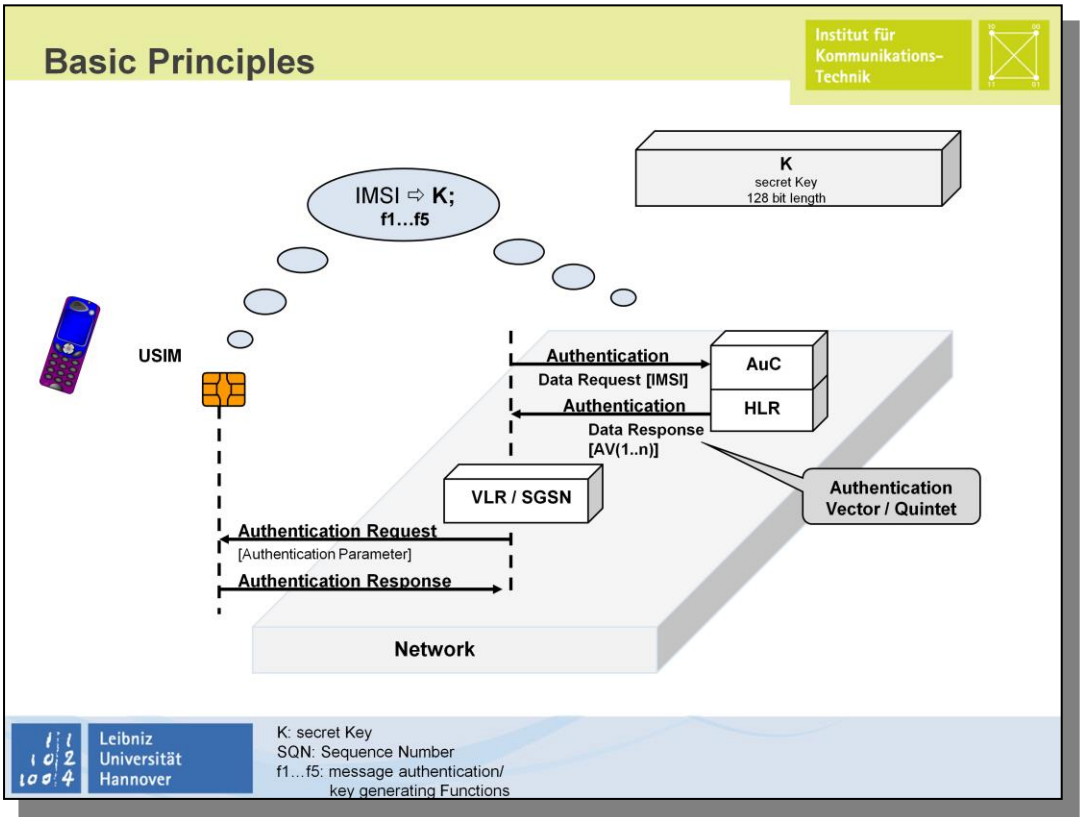
Authentication is performed independently in the CS or PS domain.

If no Authentication Vectors correlated to the user are stores in the serving VLR/SGSN, VLR/SGSN are initiating the Authentication process with an „Authentication Data Request“ via the HLR of the user´s HPLMN to the AuC. The „Authentication Data Request“ shall include the IMSI. On basis of this order, the AuC generates a set of n Authentication Vectors AVs. This AVs are send back in an „Authentication Data Response“ from Auc via HLR to the VLR/SGSN.

The VLR/SGSN stores the Authentication Vectors AVs and continues the Authentication sending some Authentication parameter to the USIM („Authentication Request“). The UE stores the parameter, calculates keys for ciphering and integrity check and performs the network authentication. If the network authentication is successfully completed the UE answers with „Authentication Response“ to the VLR/SGSN request, delivering a parameter for user authentication. VLR/SGSN perform user authentication.

If user authentication is successful, VLR/SGSN continue with connection set-up.

If user´s AVs are already stored in the VLR/SGSN, „Authentication Data Request“ and „Authentication Data Response“ are not necessary in the Authentication process.



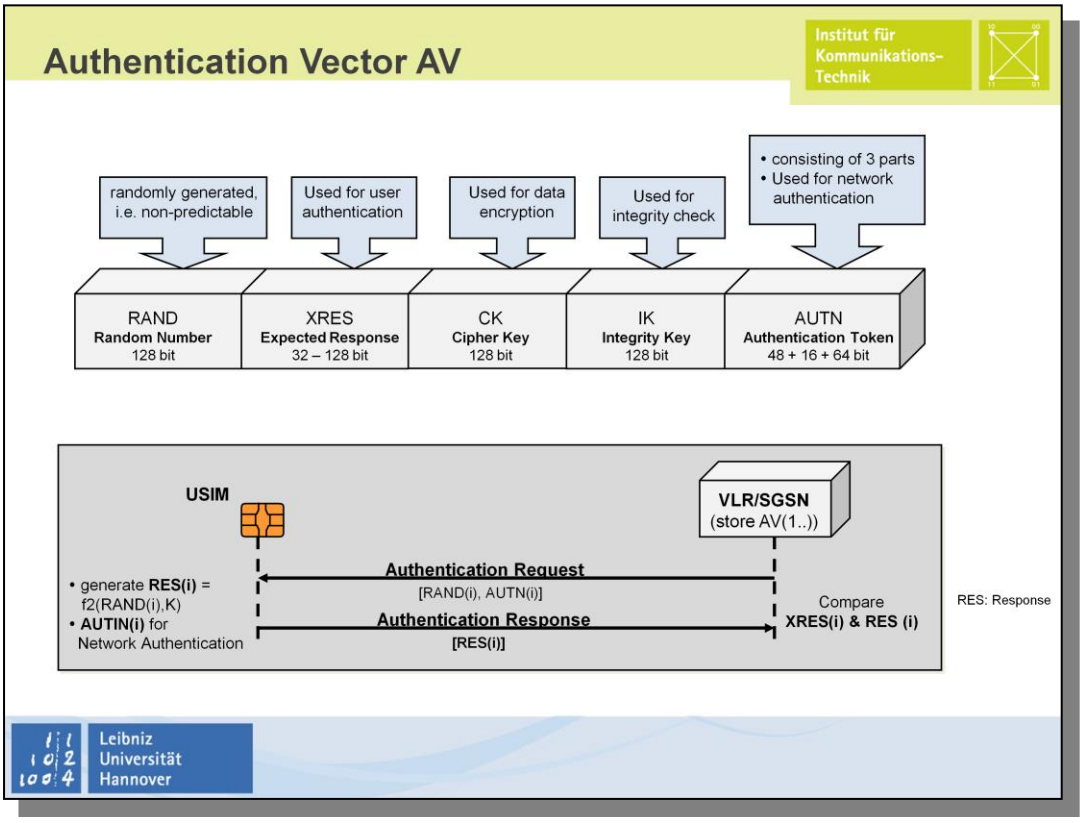
Authentication Vector AV

Each Authentication Vector consists of the following components (TS 33.102):

- a **Random Number RAND**, which is randomly generated, i.e. non-predictable. It´s length is 128 bit.
- an **Expected Response XRES**, which is used for User Authentication. It shall have a flexible length of 32 -128 bit.
- a **Cipher Key CK**, which is necessary for Ciphering. It shall have a fixed length of 128 bit.
- an **Integrity Key IK**, which is used for Signaling Data Integrity Check. It´s length is 128 bit.
- an **Authentication Token AUTN**, which is used for Network Authentication. AUTN consists of three different parts, described later on. Ist total length is 128 bit.

A set of n Authentication Vestors AVs is send on VLR/SGSN request from HLR/AuC to VLR/SGSN. The AVs are stored in the VLR/SGNS. Each AV is good for one authentication and key agreement (for ciphering & integrity check) between the VLR/SGSG and the USIM.

When the VLR/SGSN initiates an Authentication and key agreement, it selects the next AV and sends the parameters RAND and AUTN to the UE. The USIM checks whether AUTN can be accepted (**Network Authentication)** and computes a **Response RES**. RES is send back to the VLR/SGSN. The VLR/SGSN compare the received RES with the AV parameter XRES **(User Authentication).** If they are equal, User Authentication is successfully completed.



Generation of Authentication Vectors AVs

After receiving the „Authentication Data Request“ from the VLR/SGSN, the AuC generates new Avs (TS 33.102). Every AV consists of the following five parameters:

Random Number RAND, Expected Response RES, Cipher Key CK, Integrity Key IK and Authentivation Token AUTN.

Random Number RAND: The AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

Expected Response XRES: The secret Key K, RAND and f2 are necessary to compute XRES. XRES = f2 (K, RAND); f2 is a (possibly truncated) message authentication function. XRES is used for User Authentication.

Cipher Key CK: K, RAND and f3 are used to compute CK. CK = f3 (K, RAND); f3 is a key generating functions. CK is used for Ciphering.

Integrity Key IK: K, RAND and f4 are used to compute IK. IK = f4 (K,RAND); f4 is a key generating function. IK is used for Signaling Data Integrity Check.

Authentication Token AUTN: K, RAND, SQN, AMF and f5 are necessary to compute AUTN. AUTN consists of three parts: AUTN = SQN * AK II AMF II MAC.

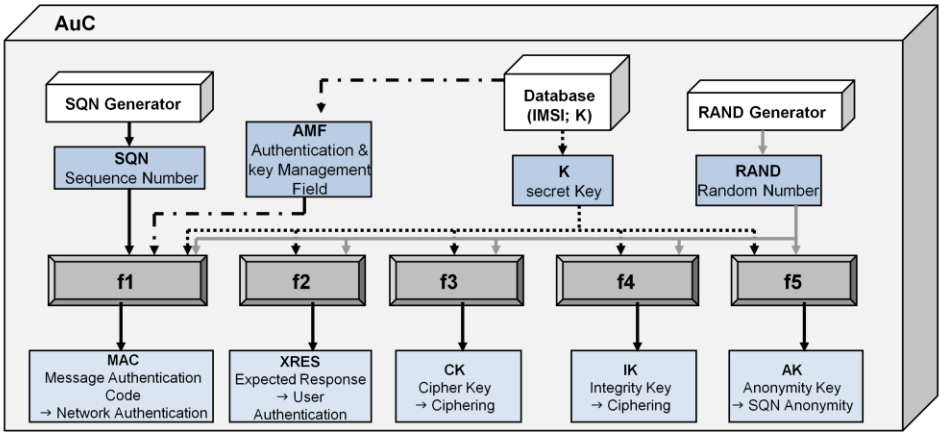
The first part of AUTN is calculated by an „exclusive or“ (XOR) connection of the Sequence Number SQN and the Anonymity Key AK. AK = f5 (K, RAND); f5 is a key generating function or f5 = 0. AK is used to conceal SQN as the latter may exponse the identity and location of the user. The concealment of SQN is to protect against passive attacks only. If no concealment is needed then f5 = 0 (AK = 0).

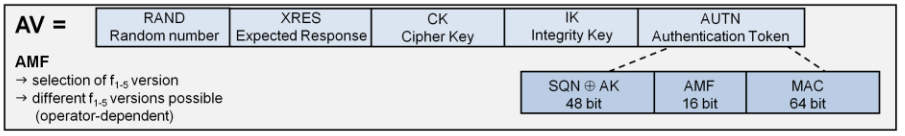
The second part of AUTN is the **Authentication and key Management Field AMF**. AMF is part of the user´s database in the AuC. Operator-dependent, different f1..f5 algorithm may be defined. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The third part of AUTN is the Message Authentication Code MAC. MAC = f1 (K, SQN, RAND, AMF); f1 is a message authentication function.

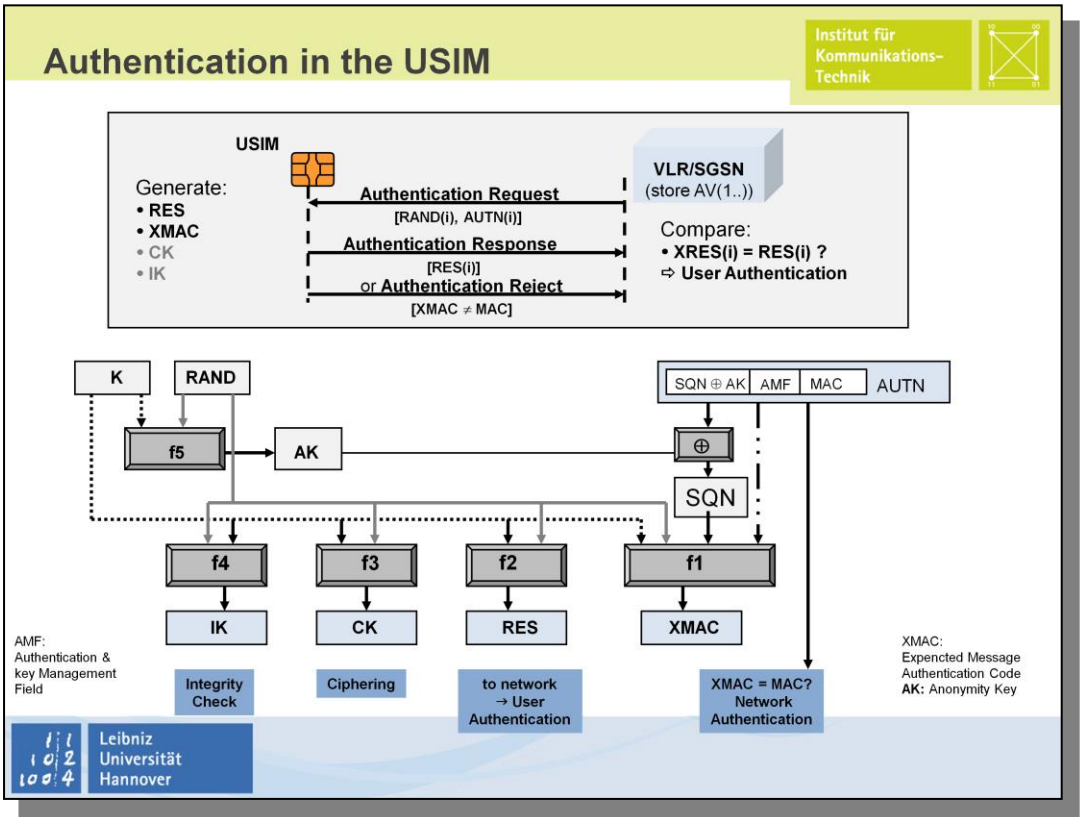
AV Generation

Institut für Kommunikations-Technik





Leibniz Universität Hannover



Authentication in the USIM

With the „Authentication Request“ message, the authentication parameter RAND and AUTN are transmitted from the VLR/SGSN to the USIM. The purpose of this procedure is to authenticate user & network and to establishment a new pair of cipher and integrity keys CK & IK between the VLR/SGSN and the USIM.

Upon receipt of RAND and AUTN the USIM first computes the Anonymity Key AK = f5 (K, RAND) and retrieves the Sequence Number SQN. SQN = (SQN XOR AK) XOR AK.

Second, the USIM calculates the Expected Message Authentication Code XMAC. XMAC = f1 (K, SQN, RANF, AMF). For network authentication, XMAC is compared with MAC (included in AUTN). If they are different, the USIM sends back the „ Authentication Reject“ message to the VLR/SGSN and abandons the connection set-up. „Authentication Reject“ includes an indication of the cause for the rejection. In the case of „Authentication Reject“, the VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR.

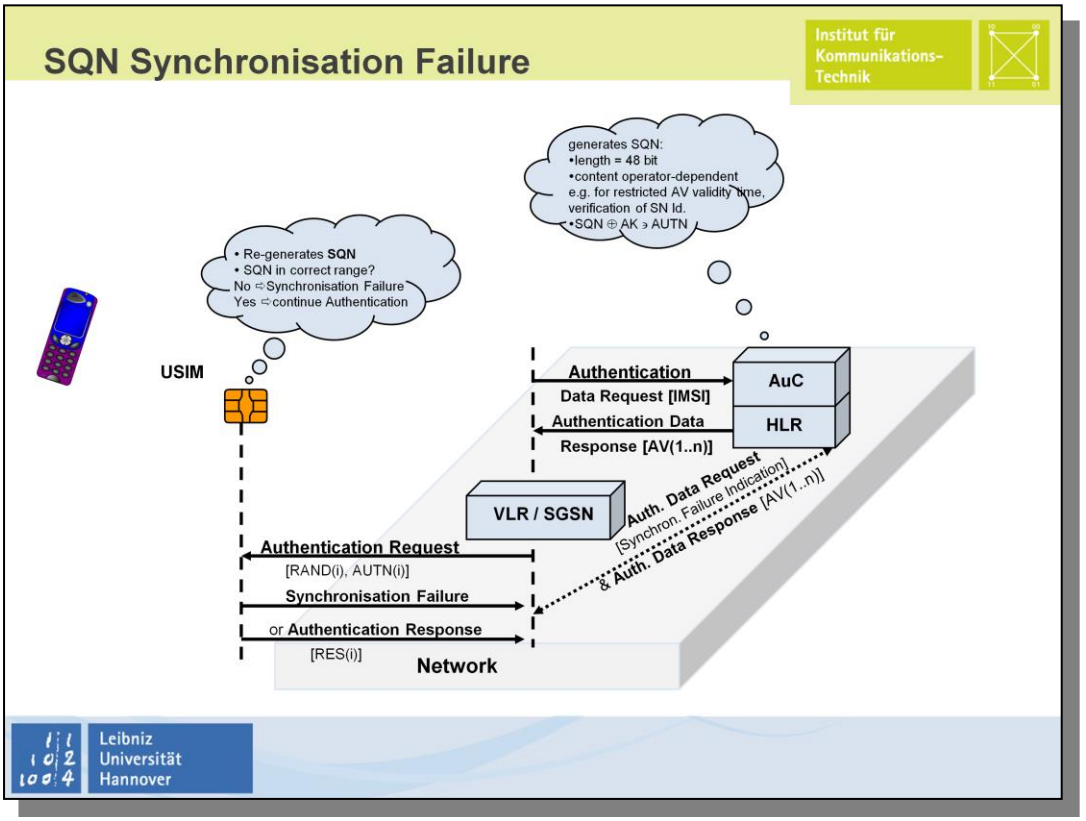
If the network authentication is all right, the USIM verifies that the received SQN is in the correct range.

If the USIM considers SQN to be not in the correct range, it sends „Synchronization Failure“ back to the VLR/SGSG including the appropriate parameter, and abandons the connection set-up.

If SQN is in the correct range, the USIM computes RES. RES = f2 (K, RAND).

Furthermore, the USIM calculates the Cipher Key CK = f3 (K, RAND) and the Integrity Key IK = f4 (K, RAND). CK and IK are stored in the USIM for the following ciphering of user data and integrity check of signaling data.

Finally, RES is included in the „Authentication Response“ message and sends back from the USIM to the VLR/SGSN. The VLR/SGSN needs the RES for User Authentication. If RES = XRES from the selected AV, the authentication of the user has been successful. If they are different, the VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR.



Synchronization Failure

At the beginning of the Authentication process, the AuC generates the Sequence Number SQN. SQN shall have a length of 48 bit. The structure & content of SQN is operator-dependent. SQN may contain information used to restrict the Authentication Vector AV validity time or to verify the Serving Network SN Identity.

SQN, being a part of AUTN, is transmitted via VLR/SGSN („Authentication Data Response“) to the USIM („Authentication Request“).

The USIM regenerates SQN and verifies that the received SQN is in the correct range.

If the USIM considers SQN to be not in the correct range, it sends the „Synchronization Failure“ message back to the VLR/SGSN including the appropriate parameter, and abandons the connection set-up.

Upon receiving a „Synchronization Failure“ message from the UE, the VLR/SGSN sends an „Authentication Data Request“ with a Synchronization Failure Indication to appropriate parameter received from the UE.

The AuC checks the parameter, generates a fresh set of AVs and sends them with an „Authentication Data Response“ message to the VLR/SGSN.

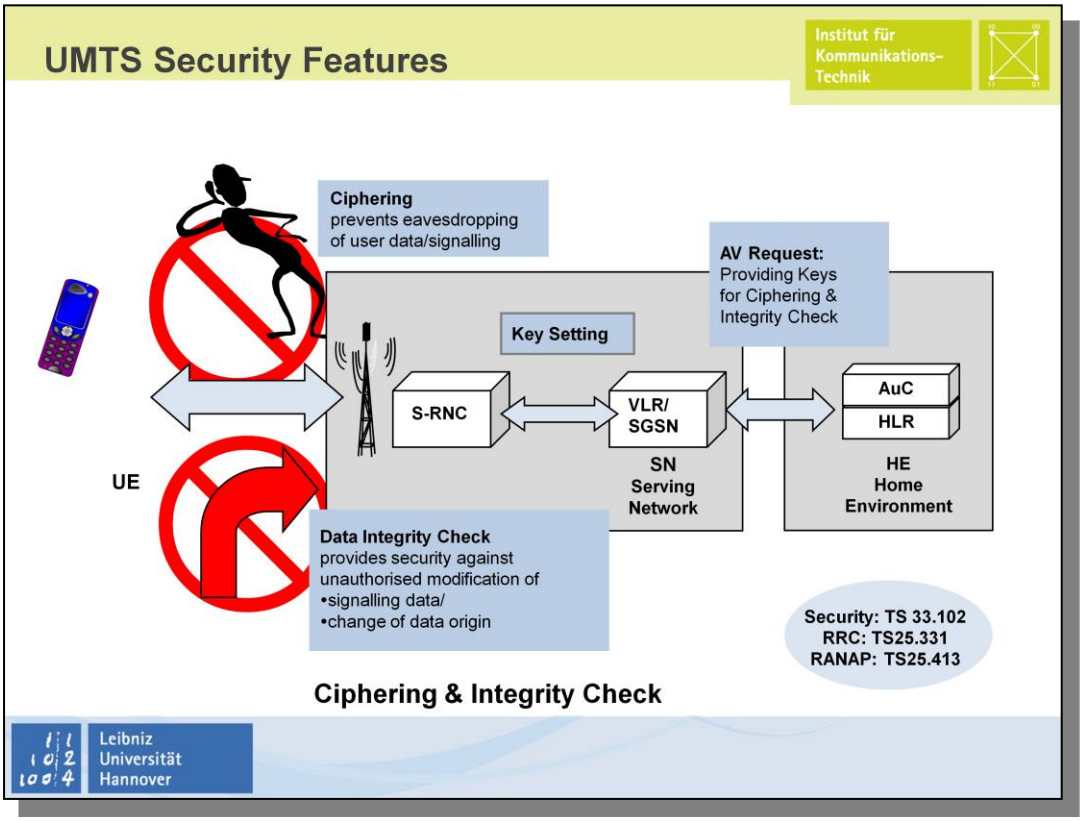
Whenever the VLR/SGSN receives a new set of AVs from the AuC in a „Authentication Data Response“ to an „Authentication Data Request“ with Synchronization Failure Indication it deletes the old AVs for that UE. The VLR/SGSN may now start a new authentication process to the UE bades on a new AV from the AuC.

Outline Part V-III

Institut für Kommunikations-Technik

1. Overview
2. Identities
3. Authentication
4. Ciphering & Integrity

Leibniz Universität Hannover



Ciphering & Integrity Check

To start the security features Ciphering (optional) & Integrity Check (mandatory), three steps are necessary:

Connection Establishment

At the connection start the RRC Connection Establishment also informs the network about the UEs security capabilities. They includes the MEs UMTS Encryption Algorithms UEAs and UMTS Integrity Algorithms UISs. In Rel.`99 only 2 UEAs and 1 UIA are defined (TS 33.102): UEA0= „no encryption“, UEA1=Kasumi encryption, UIA1=Kasumi algorithm. The S-RNC stores the UEs security capabilities.

Authentication & Key Generation in UE

Authentication & key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber, i.e. (P-)TMSI or IMSI, is known by the VLR/SGSN.

The security parameter RAND is transmitted with the „Authentication Request“ message from the VLR/SGSN to the UE. The USIM uses RAND to generate the Cipher Key CK for ciphering and the Integrity Key IK for integrity check. Now CK & IK are available in the USIM and in the VLR/SGSN.

Security Mode Set-Up

Sending the „Security Mode Command“ to the S-RNC, the VLR/SGSN initate integrity & ciphering. This command includes the IK & CK to be used.

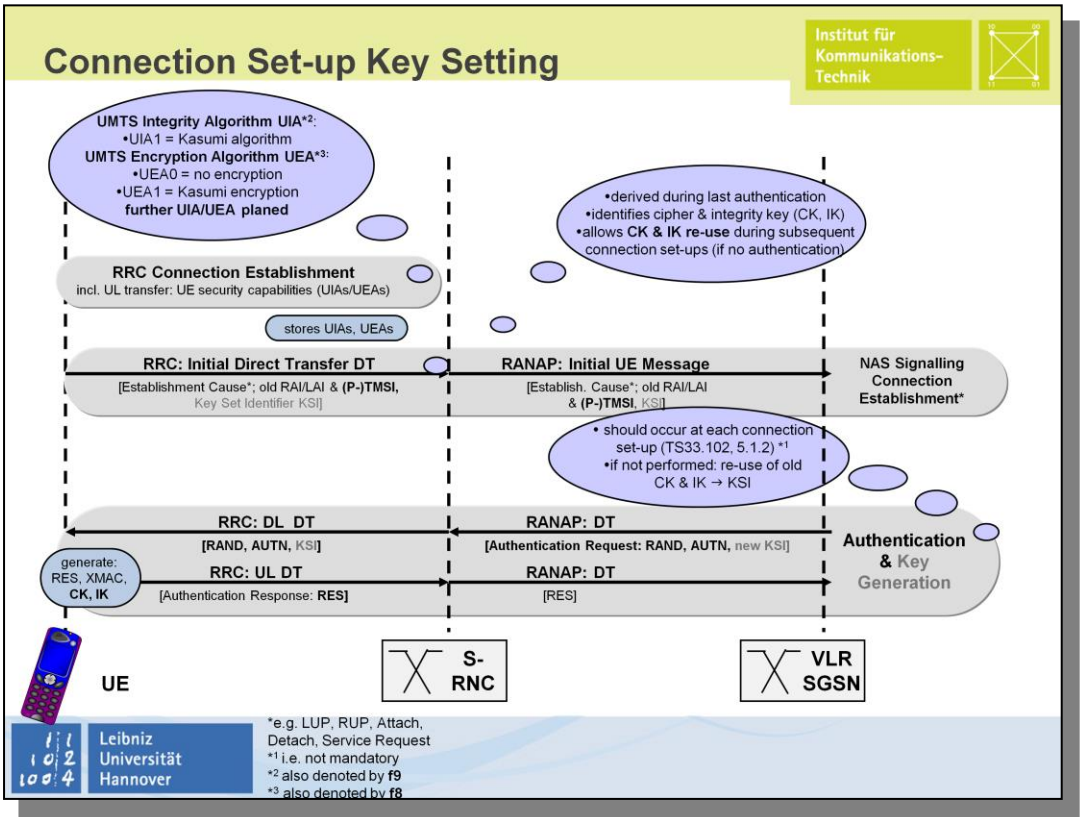
The S-RNC decides which UEA & UIA will be used, taking into account the UEs security capabilities. If the requirements in the „Security Mode Command“ cannot be fulfilled, the S-RNC sends a „Security Mode Reject“ message to the VLR/SGSN.

Next, the S-RNC starts the DL integrity protection. It is mandatory to start integrity protection of signaling messages at each new signaling connection establichment between the UE and the VLR/SGSN (exceptions listed in TS 33.102).

The S-RNC sends the „Security Mode Command“ to the UE. This message includes the selected UIA and also UEA, if ciphering shall be started. Furthermore, parameter for integrity check, an indication on the core domain (CS/PS) and optionally the time of cipher start are included.

The UE verifies the received „Security Mode Command“ message (Integrity Check) and starts UL integrity protection.

Finally, the UE sends „Security Mode Complete“ to the S-RNC. The security mode set-up is terminated with the „Security Mode Complete“ message, which is send from the S-RNC to the VLR/SGSN. This message includes the selected UIA & UEA.



Data Integrity Check: Basic Principle

The Data Integrity Check is used between the UE and the VLR/SGSN to protect signaling data against unauthorized modification and change of data origin.

It is mandatory to start intergrity protection at each new signaling connection establishment between the UE and the VLR/SGSN. Exceptions (e.g emergency call) are listed in TS 33.102.

Integrity protection starts after the „Security Mode Command“. The messages „Security Mode Command“, „Security Mode Complete“ and all following messages are integrity protected.

The principle of the Integrity Check is the following:

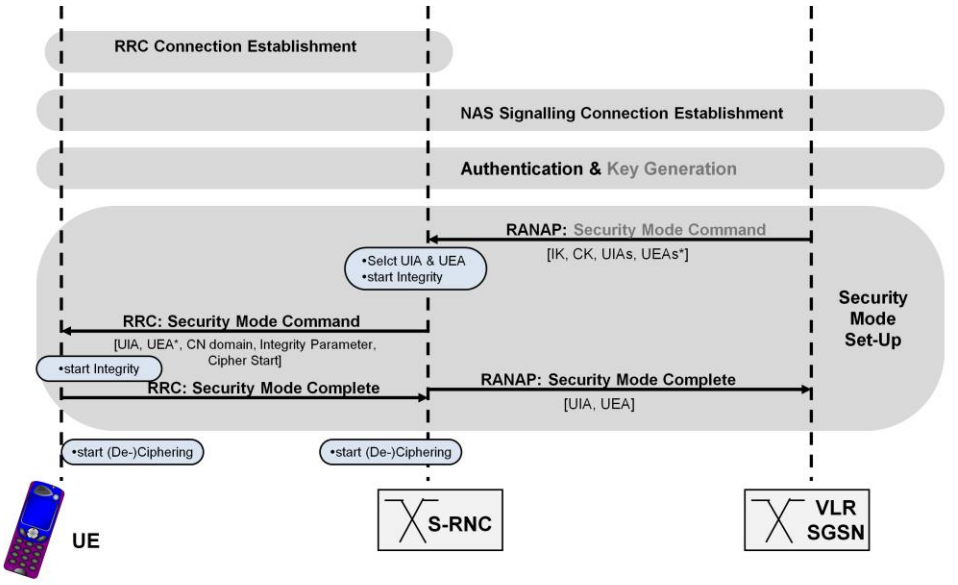
The signaling data to be protected and the Integrity Key IK are used in the transmitter (UE or S-RNC) as input for the UMTS Integrity Algorithm UIA. The result of this calculation is a kind of a check sum of this data. This checks sum is appended to the signaling data to be transmitted.

Signaling data and appended check sum are send from transmitter (UE or S-RNC) to receiver (S-RNC or UE).

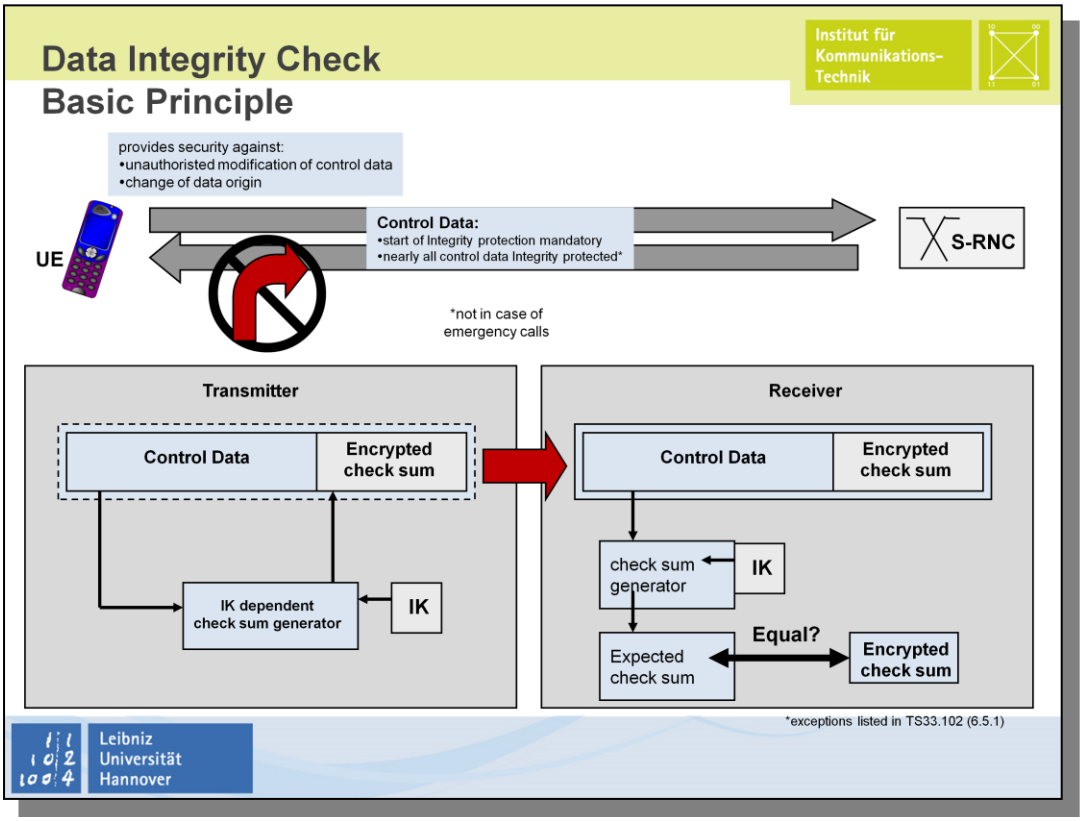
In the receiver, the signaling data and the IK (stored in the receiver) are again used as input for the same UIA. The newly generated check sum (expected check sum) is compared to the transmitted check sum.

If during transmission signaling data are modified or someone tries to simulate the users signaling, the expected check sum and the transmitted check sum differ and the non-authorized modification becomes visible.

Connection Set-up Security Mode Set-up



*UEs GSM cipher algorithm also included (GSM MS classmark)



Data Integrity Check – UMTS Integrity Algorithm UIA

The UMTS Integrity Algorithm UIA (different types of UIA can be used; currently only UIA 1 using a Kasumi algorithm is defined; see TS 33.102/6.5.6) is often also denoted as f9.

The transmitter (UE or S-RNC) uses the Control Data and the integrity parameter **Integrity Key IK, Integrity Sequence Number COUNT-I,** a random value generated by the network side **FRESCH** and the direction bit **DIRECTION** as input for f9.

Based on these input parameters the transmitter computes the **Message Authentication Code for data Integrity MAC-I** (i.e. the check sum):

MAC-I = f9 (Control Data, IK, COUNT-I, FRESCH, DIRECTION).

The MAC-I is appended to the control data and transmitted over the radio link.

The receiver computes the Expected Message Authentication Code for data Integrity XMAC-I in the same way as the transmitter computed MAC-I. The data integrity of the control data is checked by comparing XMAC-I with the received MAC-I.

Remarks to the integrity parameter:

Integrity Key IK: There may be one IK for CS connections IK (CS) and one for PS connections IK(PS). The data integrity of radio bearers for user data is not protected.

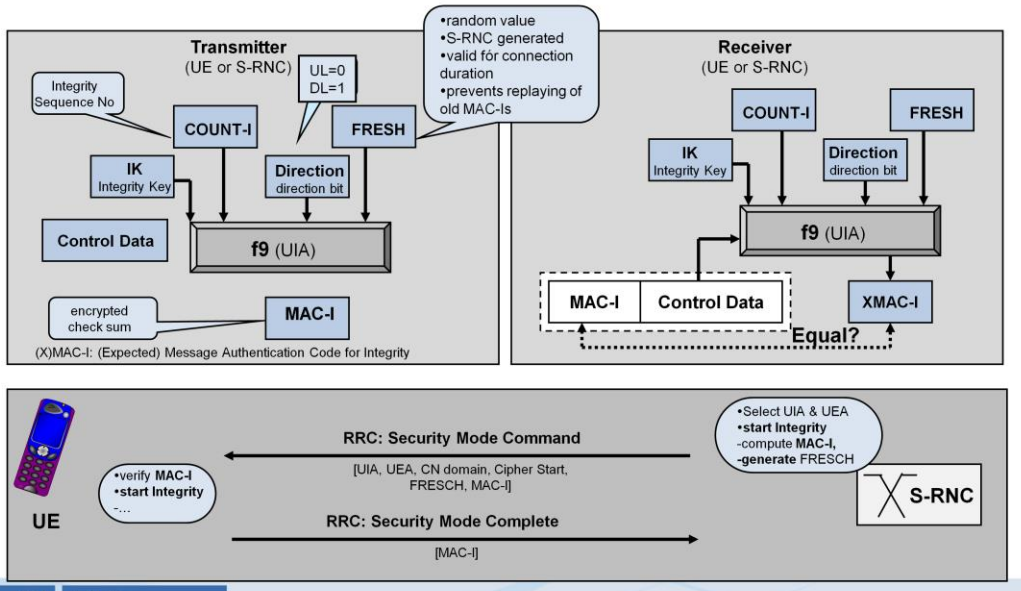
FRESCH: There is only one FRESCH parameter value per user. The input parameter FRESCH protects the network against replay of signaling messages by the UE. At connection set-up the S-RNC generates a random value FRESCH and sends it to the UE in the RRC „Security Mode Command“ message. The value FRESCH is subsequently used by the UE and S-RNC throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

COUNT-I: the integrity sequence number COUNT-I is comprosed on basis of the RRC sequence number RRC SN and the RRC Hyperframe Number RRC HFN.

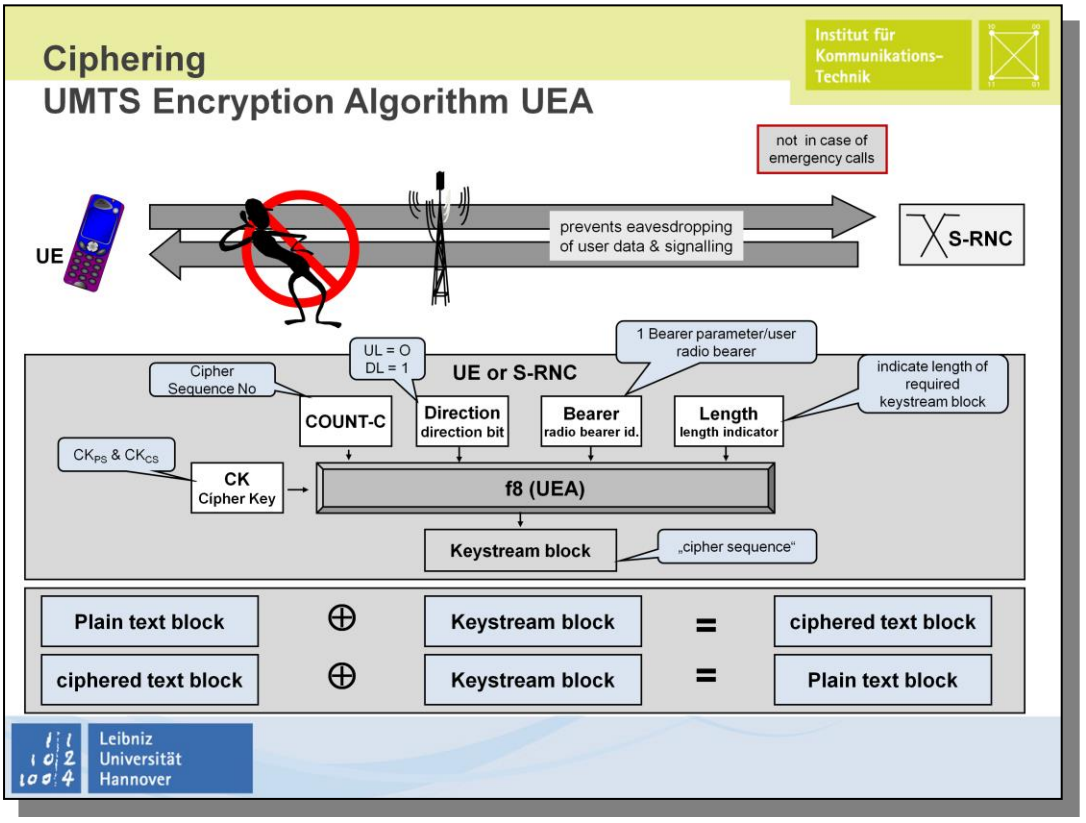
DIRECTION: the direction identifier bit indicates UL or DL direction (DIRECTION = 0 for UL and 1 for DL).

Data Integrity Check
UMTS Integrity Algorithm UIA

Institut für Kommunikations-Technik



Leibniz Universität Hannover



Ciphering – UMTS Encryption Algorithm UEA

Similar to GSM, UMTS performs encryption of user data and signaling to prevent eavesdropping ón the radio interface.

For CS and PS data encryption is performed between the S-RNC and the UE.

Like in GSM the „plain text" is ciphered in the transmitter connecting it via XOR operation with a cipher sequence (UMTS: Keystream Block). The ciphered text block is transmitted via radio interface. In the receiver the plain text is recovered connectiong the ciphered text block via XOR operation with the cipher sequence/Keystream Block.

The algorithm producing the Keystream Block is the UMTS Encryption Algorithm UEA. UEA is often denoted as f8 Different UEA implementations are possible Currently only UEA0 (no ciphering) and UEA1 (Kasumi encryption) are avaiable.

The UMTS keystream block is generated in the UE ans S-RNC feeding the cipher paramter **Cipher Key CK, Ciphering Sequence Number COUNT-C**, bearer identity **BEARER**, transmission direction **DIRECTION** and the length of the keystream **LENGTH** into f8.

Keystream Block = f8 (CK, COUNT-C, BEARER, DIRECTION, LENGTH).

Remarks on the cipher parameter:

Cipher Key CK: There may be one CK for CS connection CK(CS) and one for PS connections CK(PS).

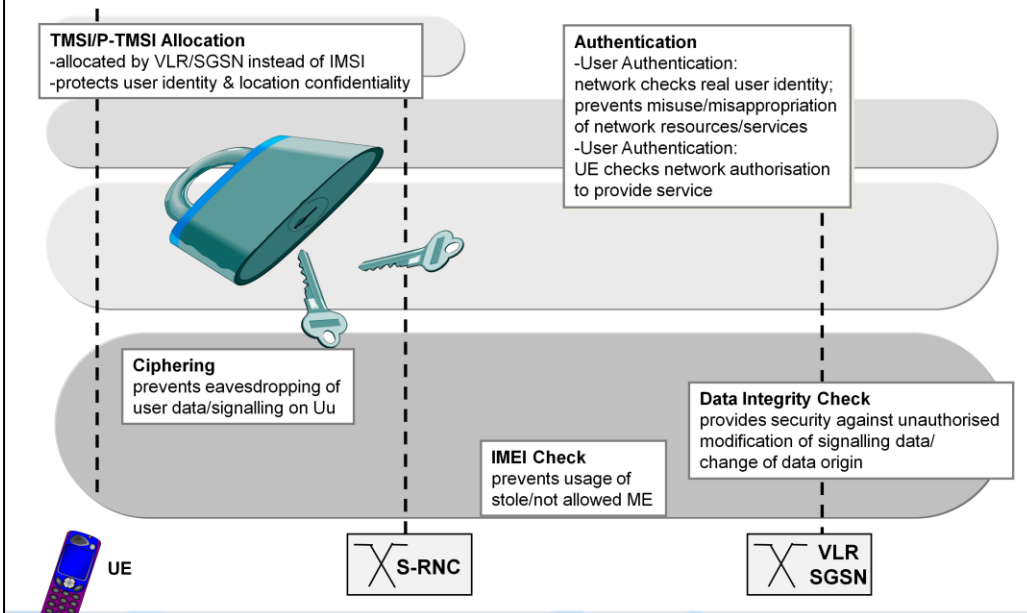
COUNT-C: The ciphering sequence number COUNT-C is generated by MAC or RLC frame and sequence information.

BEARER: the radion bearer identifier BEARER is input to avoid that for different keystream an identical set of input parameter values is used.

DIRECTION: the direction identifier bit indicates UL or DL direction (DIRECTION = O for UL and 1 for DL).

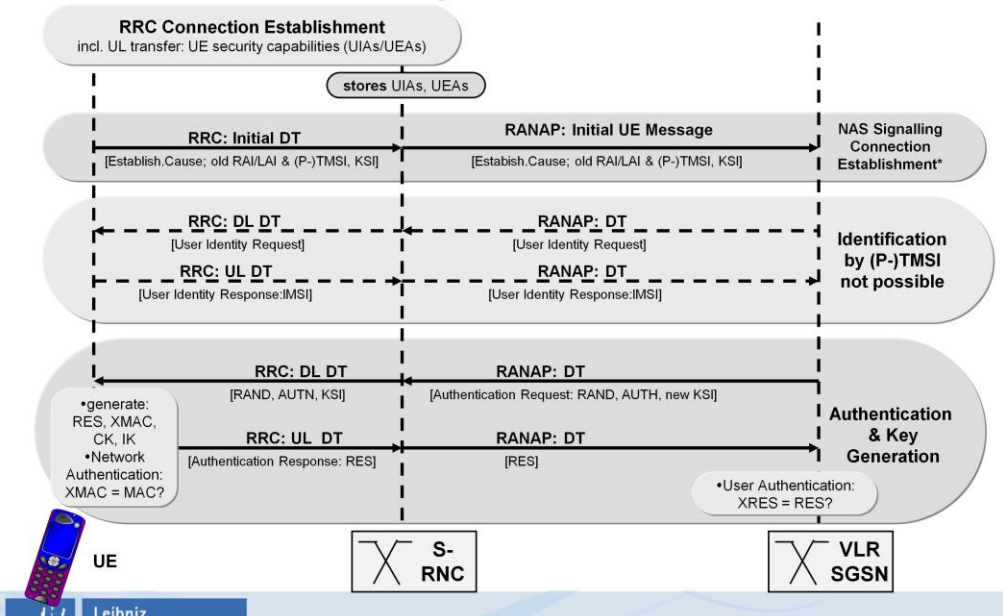
LENGTH: The length indicator LENGTH indicates the length of the required keystream block. LENGTH shall affect only the lenght of the Keystream block, not the actual bits in it.

Summary


TMSI/P-TMSI Allocation
-allocated by VLR/SGSN instead of IMSI
-protects user identity & location confidentiality
Authentication
-User Authentication:
network checks real user identity;
prevents misuse/misappropriation
of network resources/services
-User Authentication:
UE checks network authorisation
to provide service
Ciphering
prevents eavesdropping of
user data/signalling on Uu
Data Integrity Check
provides security against unauthorised
modification of signalling data/
change of data origin
IMEI Check
prevents usage of
stole/not allowed ME
UE
S-RNC
VLR
SGSN

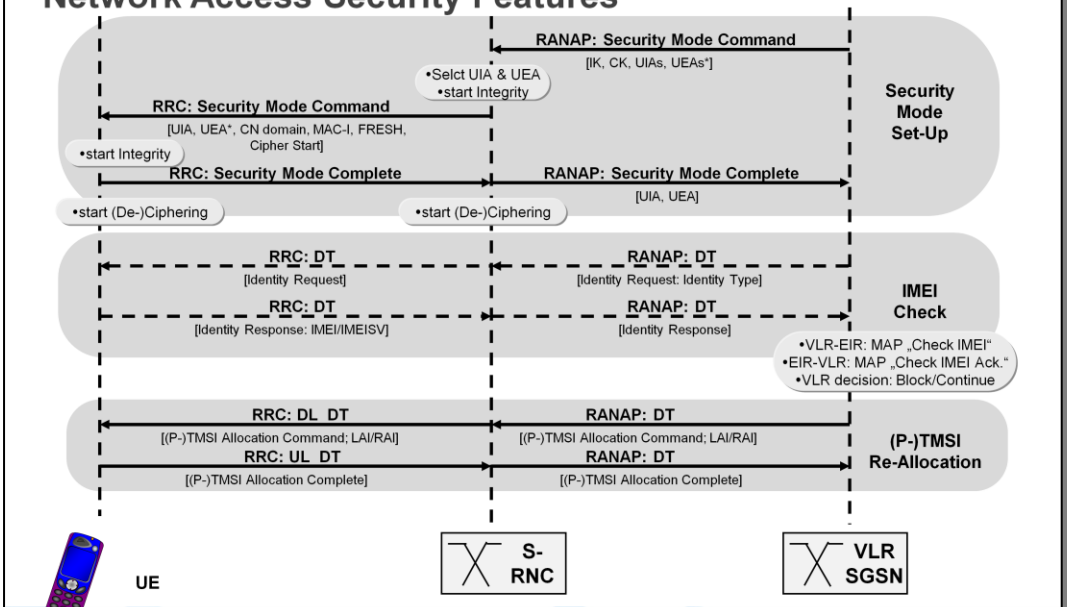
Summary I

Network Access Security Features



Summary II

Network Access Security Features

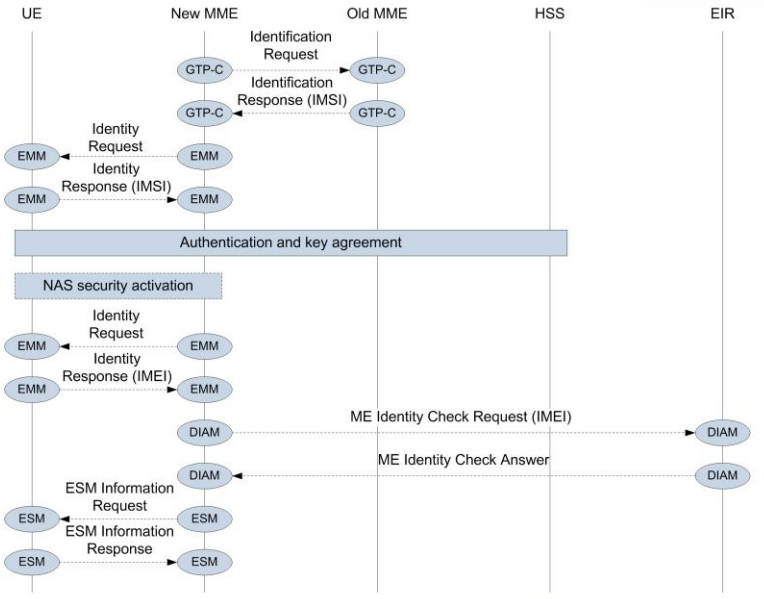


*UEs GSM cipher algorithm
also included (GSM MS classmark)

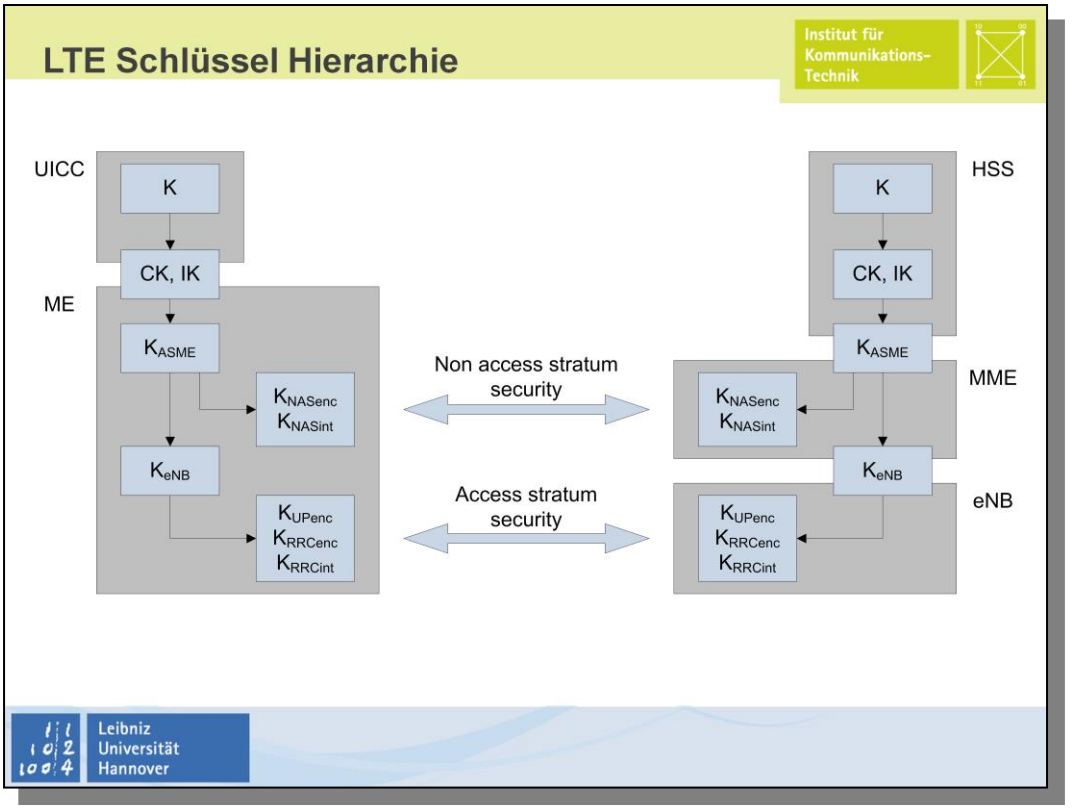
LTE Security Procedures

Identifikations- und Sicherheitsprozeduren

Institut für Kommunikations-Technik



Leibniz Universität Hannover



UICC Universal Integrated Circuit Card

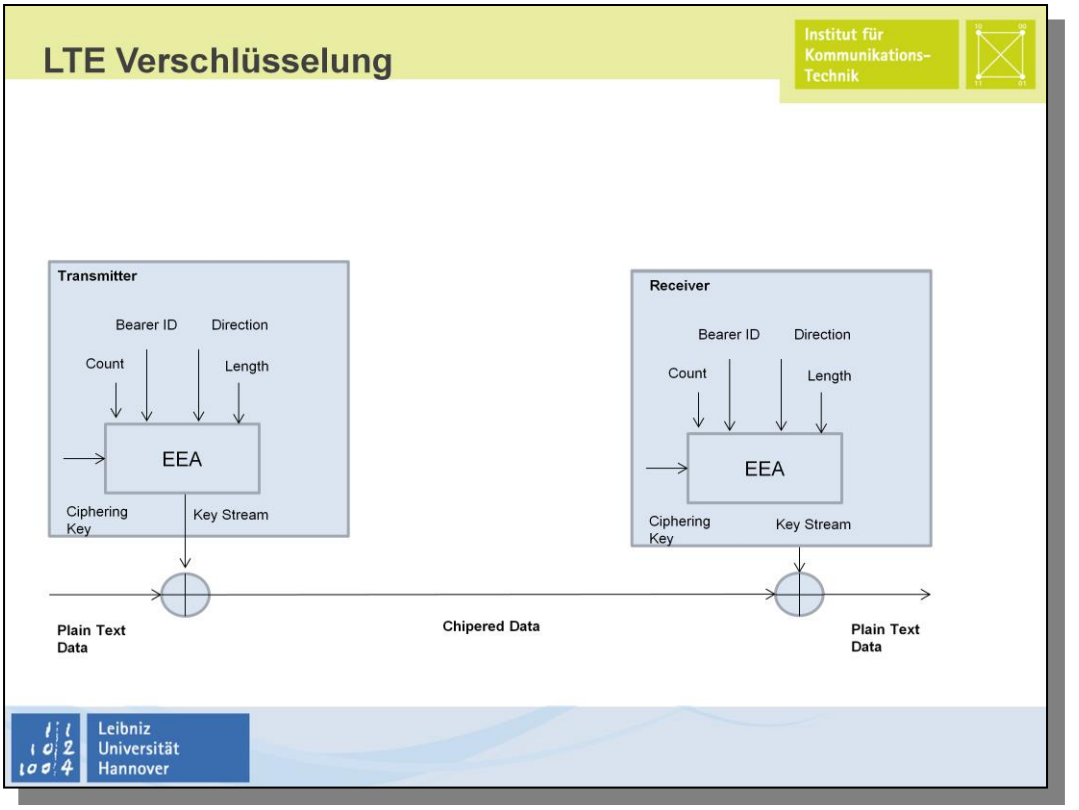
K Secret

CK und IK werden abweichend zu UMTS verwendet

Ableitung des K_{ASME} (access security management entity) Key

K_{NASenc}	Verschlüsselungs Key
K_{NASint}	Integritäts-Key, beide für das Non-Access Stratum
K_{UPenc}	Ciphering Data
K_{RRCenc}	Ciphering RRC Signallling
K_{RRCint}	Integritätsprüfung RRC Signalling

34



UICC Universal Integrated Circuit Card

K Secret

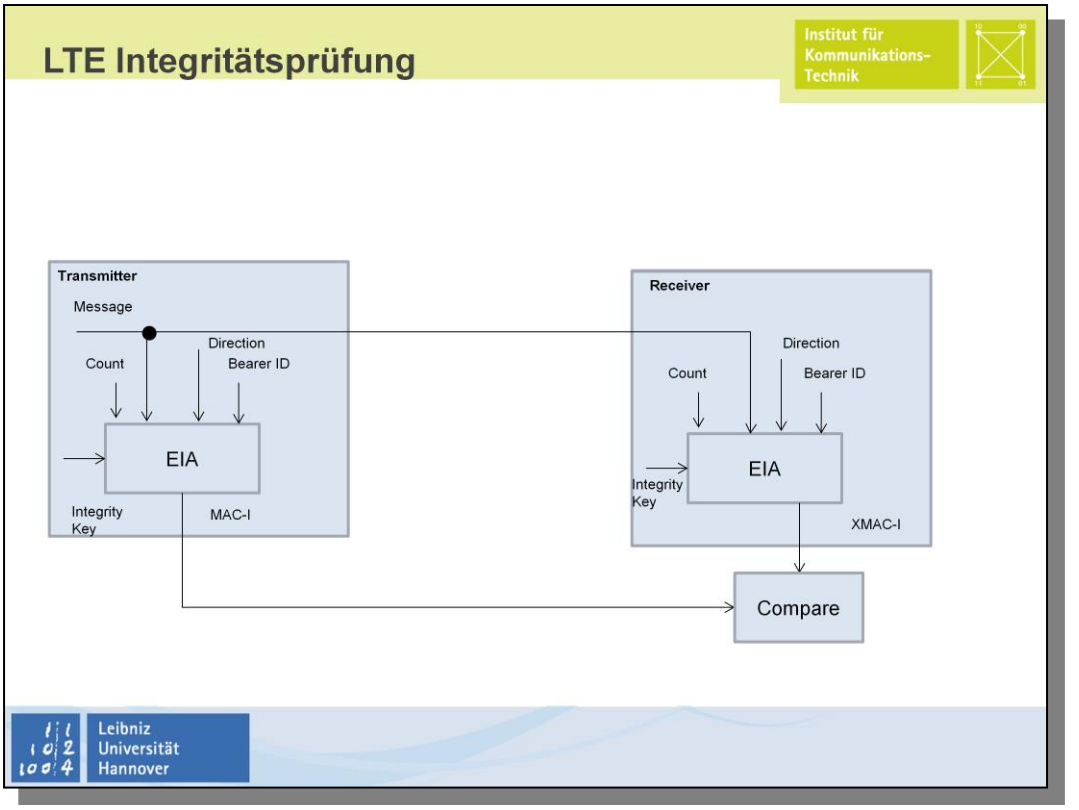
CK und IK werden abweichend zu UMTS verwendet

Ableitung des K_{ASME} (access security management entity) Key

K_{NASenc}	Verschlüsselungs Key
K_{NASint}	Integritäts-Key, beide für das Non-Access Stratum
K_{UPenc}	Ciphering Data
K_{RRCenc}	Ciphering RRC Signallling
K_{RRCint}	Integritätsprüfung RRC Signalling

TS 33.401

35



UICC Universal Integrated Circuit Card

K Secret

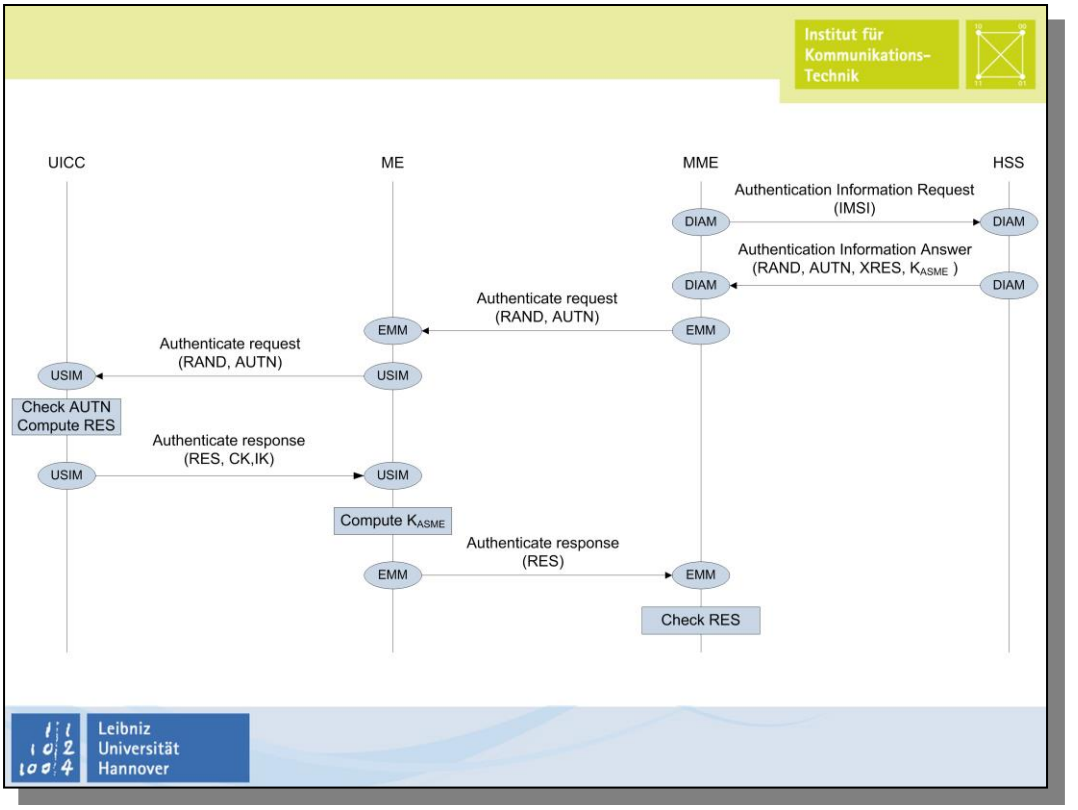
CK und IK werden abweichend zu UMTS verwendet

Ableitung des K_{ASME} (access security management entity) Key

K_{NASenc}	Verschlüsselungs Key
K_{NASint}	Integritäts-Key, beide für das Non-Access Stratum
K_{UPenc}	Ciphering Data
K_{RRCenc}	Ciphering RRC Signallling
K_{RRCint}	Integritätsprüfung RRC Signalling

TS 33.401

36


Institut für Kommunikations-Technik
UICC
ME
MME
HSS
Authentication Information Request (IMSI)
DIAM
DIAM
Authentication Information Answer (RAND, AUTN, XRES, K_{ASME})
DIAM
DIAM
Authenticate request (RAND, AUTN)
EMM
EMM
Authenticate request (RAND, AUTN)
USIM
USIM
Check AUTN
Compute RES
Authenticate response (RES, CK,IK)
USIM
USIM
Compute K_{ASME}
Authenticate response (RES)
EMM
EMM
Check RES
Leibniz Universität Hannover

Institut für Kommunikations-Technik

Lawful Interception

Leibniz Universität Hannover

Why intercept

- Why Intercept?
  - Crime investigation
  - Crime prevention
  - Intelligence gathering
- Why not?
  - Privacy
    - Abuse by Government
    - Blackmail
    - Identity theft
  - Security
    - Interception is about enabling eavesdropping on communications
    - LI compromises network security

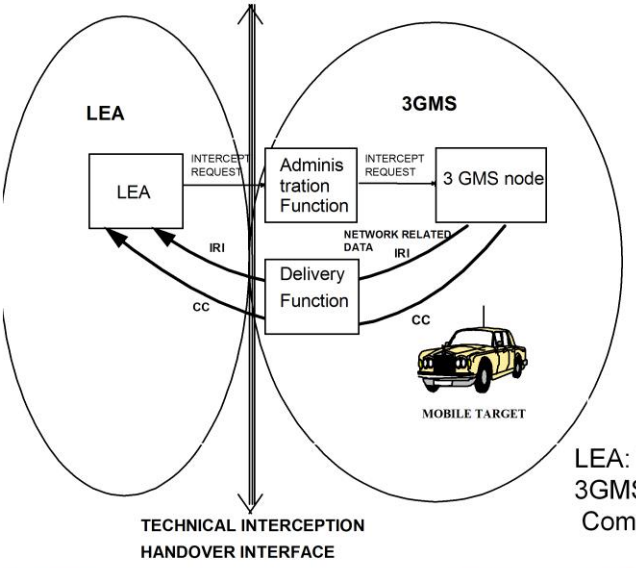
Telecommunications Companies & Lawful Interception

Institut für Kommunikations-Technik

- Provide interception in the public access network
  - PSTN, GSM, GPRS, UMTS...
- Carry the main load of interception
  - Until recently, telecommunications companies were either heavily regulated (US) or a government department (Europe)
  - Telecommunications companies have the resources needed to provide interception
- Highly standards oriented
  - LI is defined in great detail by international standards
  - There are LI standards for all public access network technologies

Leibniz Universität Hannover

Overview



LEA: Law Enforcement Agencies
3GMS: Third Generation Mobile Communications System

Types of intercepted information

Institut für Kommunikations-Technik

- **IRI**: Intercept Related Information
  - Information associated with telecommunication services involving the target identity
  - Often most important part of the intercept
    - LEAs usually more interested in who is talking to who rather than in what they are saying
    - 90% of warrants (in the US) are IRI only
- **CC**: Content of Communication
  - Information exchanged between two or more users of a telecommunications service
    - Voice, SMS, videoconferencing, data packets…
  - Can be cross referenced to the warrant and any associated Intercept Related Information

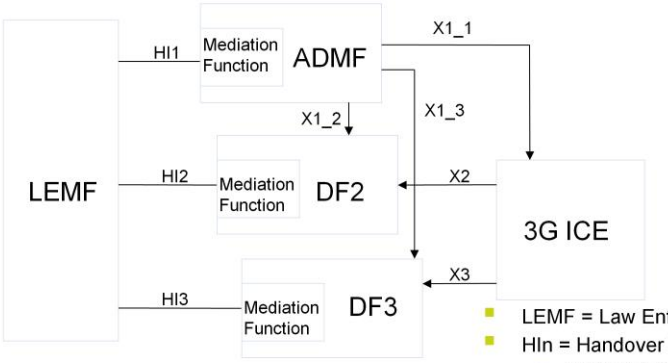
Leibniz Universität Hannover

LI Architecture (ETSI)

- ETSI defines three Handover Interfaces between the Network Operator and the LEA
  - **HI1**: Administrative Information
  - **HI2**: Intercept Related Information
  - **HI3**: Content of Communication

Lawful Interception Architecture

Institut für Kommunikations-Technik



- LEMF = Law Enforcement Monitoring Facility
- HIn = Handover Interfaces
  - described in TS 33.108
- ADMF = Administration Function
- DFn = Delivery Functions
  - DF2: Delivery Function for IRI
  - DF3: Delivery Function for CC
- ICE = Intercepting Control Elements
  - either MSC, GMSC, CSCF, SGSN, GGSN, HLR...

Leibniz Universität Hannover

Sources

- **3GPP TS 33.106** Lawful Interception requirements
- **3GPP TS 33.107** Lawful interception architecture and functions
- **3GPP TS 33.108** Handover interface for Lawful Interception

- **3GPP TR 21.905** Vocabulary for 3GPP Specifications
- **Document 496Y1104(01)** - Council Resolution of 17 January 1995 on the lawful interception of telecommunications
- **Lawful Interception - Historical context and future challenges for Internet Service Providers** - Dr. Philip Branch
- **Introduction on ETSI, Lawful Interception standardisation, Activities in ETSI/TC LI** - Peter van der Arend; Chairman ETSI/TC LI