IPLOOK HSS PRODUCT INFORMATION

IPLOOK Technologies

www.iplook.com

IPLOOK HSS Product Information

IPLOOK Technologies / IPLOOK Technologies Co., Limited

Date (2021-01-01)

Document Version (V1.0)

IPLOOK Technologies Co., Limited
Suite 1101, On Hong Commercial Building, 145 Hennessy Road, Wanchai Hong Kong

Content

1. Basic characteristics of EPS HSS

1.1. LTE mobility management

1.1.1. definition

EPS (Evolved Packet System) is the subsequent evolution technology of 3G, which provides users with packet data services with higher rate and lower delay.Support voice, video, data file exchange and other services.

EPS has the following characteristics:

1.The spectrum efficiency is higher, and the advanced OFDM (orthogonal frequency division multiplexing) and MIMO (multiple input multiple output) technologies are adopted.

2.The network is more flat, the signaling plane is completely separated from the user plane, supports end-to-end QoS guarantee, and can perform QoS control on each bearer.

3.Support users' roaming and switching between different access networks, and maintain business continuity.

1.1.2. Dependency

UE	MME	HSS
√	√	√

1.1.2.1. Description of special effect parameters

1.1.2.2. Principle description

The operator signs LTE mobility management for users. The signed services include PDN data and QoS data, which are stored in HSS. In the process of location update or user data insertion, HSS sends the service data to MME / S4-SGSN / 3GPPAAA.

The following is the E-UTRAN initial attach process for mobility management:

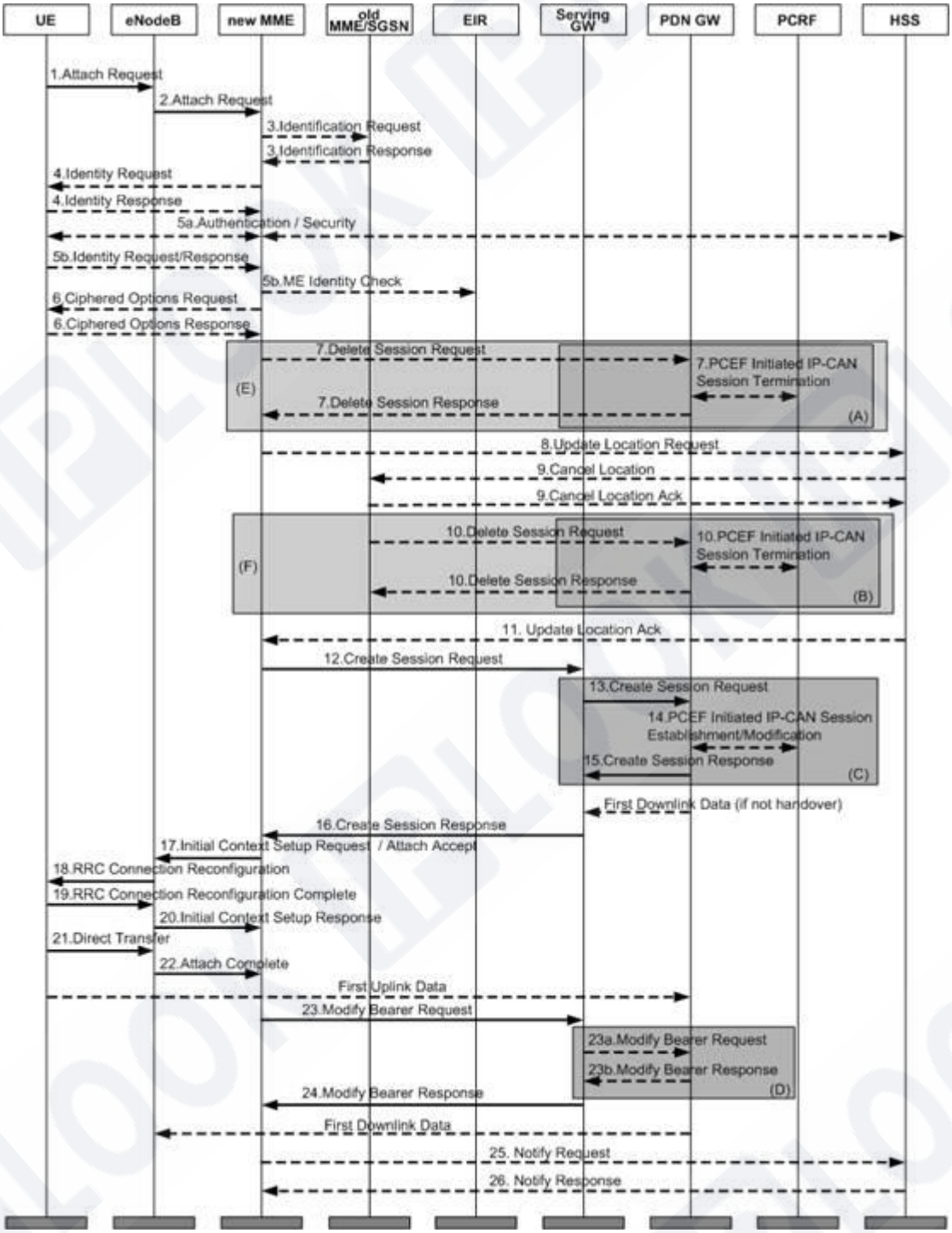


Figure 1.2.4-1 initial attachment process of E-UTRAN

1. The UE initiates an initial attachment request to the eNodeB.

2. ENodeB enables the MME selection process, selects an appropriate MME, and sends an attachment request to this MME.

3. If there is a GUTI ID on the UE and it is found that the current service MME has changed compared with the last time, the current MME deduces the old MME / SGSN address according to the GUTI and sends an "identity request" message to it to obtain the IMSI and MME context of the current UE.

4. If the old and new MMEs do not know the user's IMSI, the MME directly initiates an "identity request" to the UE.

5. a. If the security context or integrity protection of the UE is missing in the network, the authentication and NAS security establishment processes are performed.

b. The UE responds the identity identification to the MME in encrypted form, and performs IMEI legitimacy check if necessary.

6.If the "encryption option" transmission flag bit is carried in the initial attachment request, the MME obtains the "encryption option" from the UE.

7. MME deletes the remaining bearer of this ue on MME.

8. MME initiates a location update request to HSS.

9. HSS sends a location deletion request to the old MME / SGSN.

10.The old MME deletes the bearer activated for this ue on it.

11. HSS returns the location update response to MME, which carries the user's signing data.

12.If the UE carries an APN, the APN is used as the default bearer; otherwise, the contracted APN is used as the default bearer.MME starts the "S-GW selection process"

and selects an appropriate S-GW, so that APN initiates a "session establishment" request to S-GW.

13. The S-GW creates this session and initiates a "session establishment" request to the PDN-GW indicated by the MME.

14. The PDN-GW initiates the IP-CAN session establishment process to the PCRF, thereby obtaining the default PCC rules of the UE.

15. PDN-GW creates this session and generates a billing ID.After the session is established, the PDN-GW can route the user's data packets in the S-GW and data network and start billing.After that, PDN-GW sends a "establish session" response to S-GW.

16. The S-GW sends a "establish session" response to MME.

17. MME returns the "attach accept" response message to eNode.Meanwhile, MME sends an "initial context establishment" request to eNode.

18. The eNodeB initiates a "RRC link reconfiguration" request to the UE, including an attachment confirmation response message.

19. The UE returns the "RRC link reconfiguration complete" response message to eNode.

20. ENodeB sends "initial context response" message to MME.

21. The UE sends the "direct transfer" message to the eNodeB, including the "attachment completion" message.

22. ENodeB forwards the attach complete message to MME.

23.After receiving the "attachment completion" message and the "initial context response" message, MME sends the "modify bearer request" message to S-GW.

a. If the message received by the S-GW contains a handover instruction, a "modify bearer request" message is sent to the PDN-GW, instructing it to iMMEdiately implement the handover from non-3GPP access to 3GPP access, and route subsequent data packets to the S-GW.

b. PDN-GW sends "modify bearing response" message to S-GW.

24. s-gw returns the "modify bearing response" message to MME.

25. MME reports the currently selected PDN-GW identity to HSS for subsequent application between and non-3GPP access.

26. HSS stores the PDN-GW identity in the database and returns a response message to MME.

The following is the tracking area update process of mobility management:

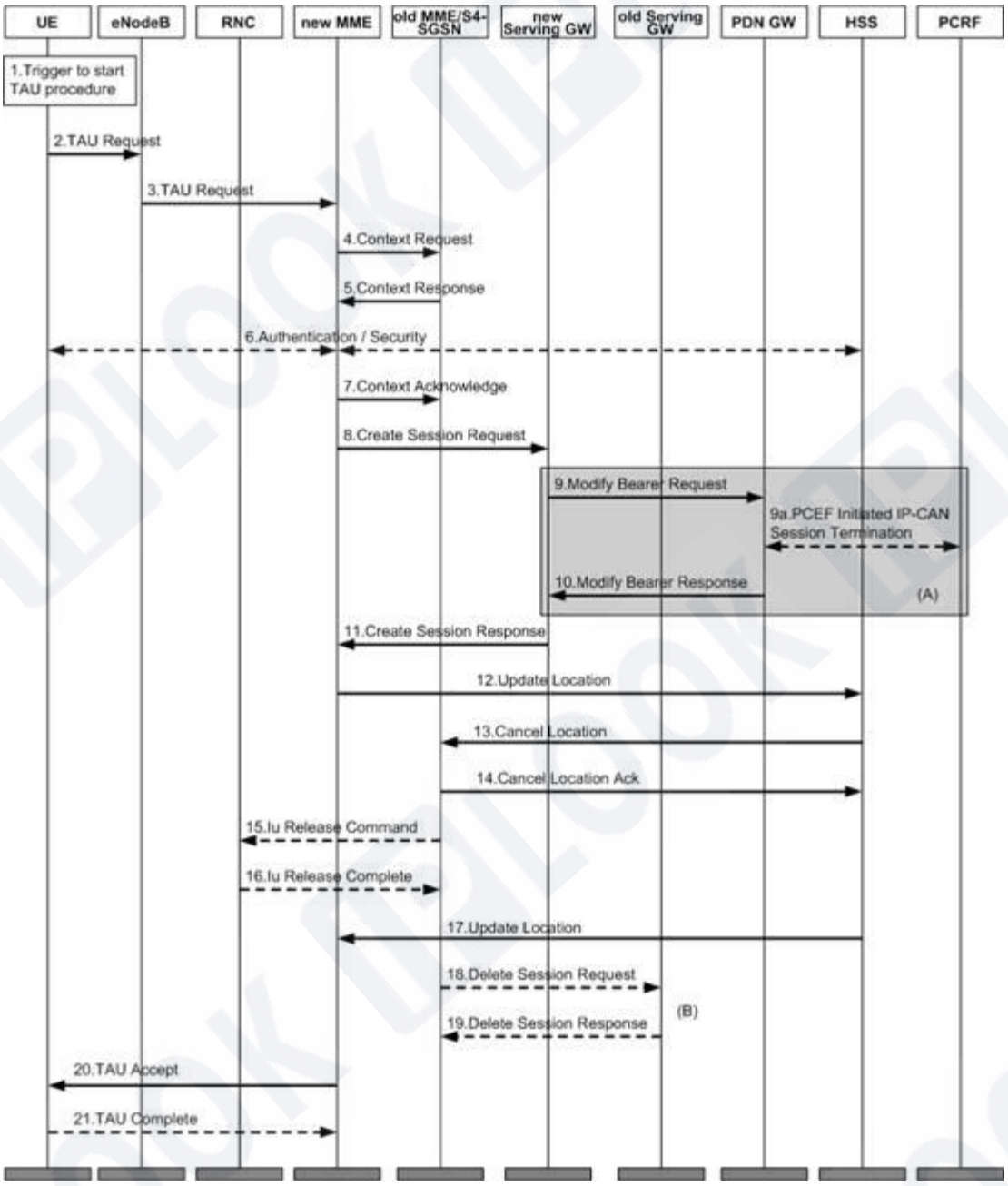


Figure 1.2.4-2 update process of tracking area

1. An event has occurred that caused the initial attachment (for example, entering a new tracking area).

2. The UE initiates a "tau request" to the eNode.

3. ENodeB identifies the current service MME according to the information carried in the request message and forwards the "tau request" to the MME.

4. MME derives the MME / S4-SGSN address of the previous service according to GUTI and sends a "context request" to it to obtain user information.

5. The old MME / S4-SGSN sends the relevant information of the current user to the new MME.

6. If the integrity check of the TAU request message fails, the authentication process will be initiated.

7. The new MME sends a "context confirmation message" to the old MME / S4-SGSN, and the old MME / S4-SGSN selects a new S-GW for the UE according to this message.Meanwhile, the old MME / S4-SGSN marks its own UE context as invalid.

8. MME starts the "S-GW selection process" and selects an appropriate S-GW, so that APN initiates a "session establishment" request to S-GW.

9. The S-GW creates this session and sends a "modify bearer request" to the PDN-GW indicated by the MME.

a. The PDN-GW initiates the IP-CAN session establishment process to the PCRF, thereby obtaining the default PCC rules of the UE.

10. PDN-GW updates its own session context and sends a "establish session" response to S-GW.

11. The S-GW updates its session context and sends a "establish session" response to MME.And transmit the uplink data packet from eNodeB to PDN-GW.

12. MME sends location update message to HSS and supports location update between MMES.

13. HSS sends cancellation location registration to the old MME.

14. The old MME deletes its own MM context and sends a "cancel location registration response" message to HSS.

15. The old S4-SGSN receives the "context confirmation message" and returns the "IU release" message to the RNC.

16. RNC returns the response message "IU release completed".

17. HSS sends a location update response message to MME.

18. The old MME / S4-SGSN sends a "delete session request" to the old S-GW and instructs the S-GW not to initiate the session deletion process to the PDN-GW.

19. The S-GW returns the "delete session response" message.And discard all data packets cached for the UE.

20. The MME returns a TAU complete message to the UE.

21. If the "TAU complete" message contains GUTI, the UE returns the "TAU complete" response message to the MME.

The following is the E-UTRAN detachment process initiated by UE:

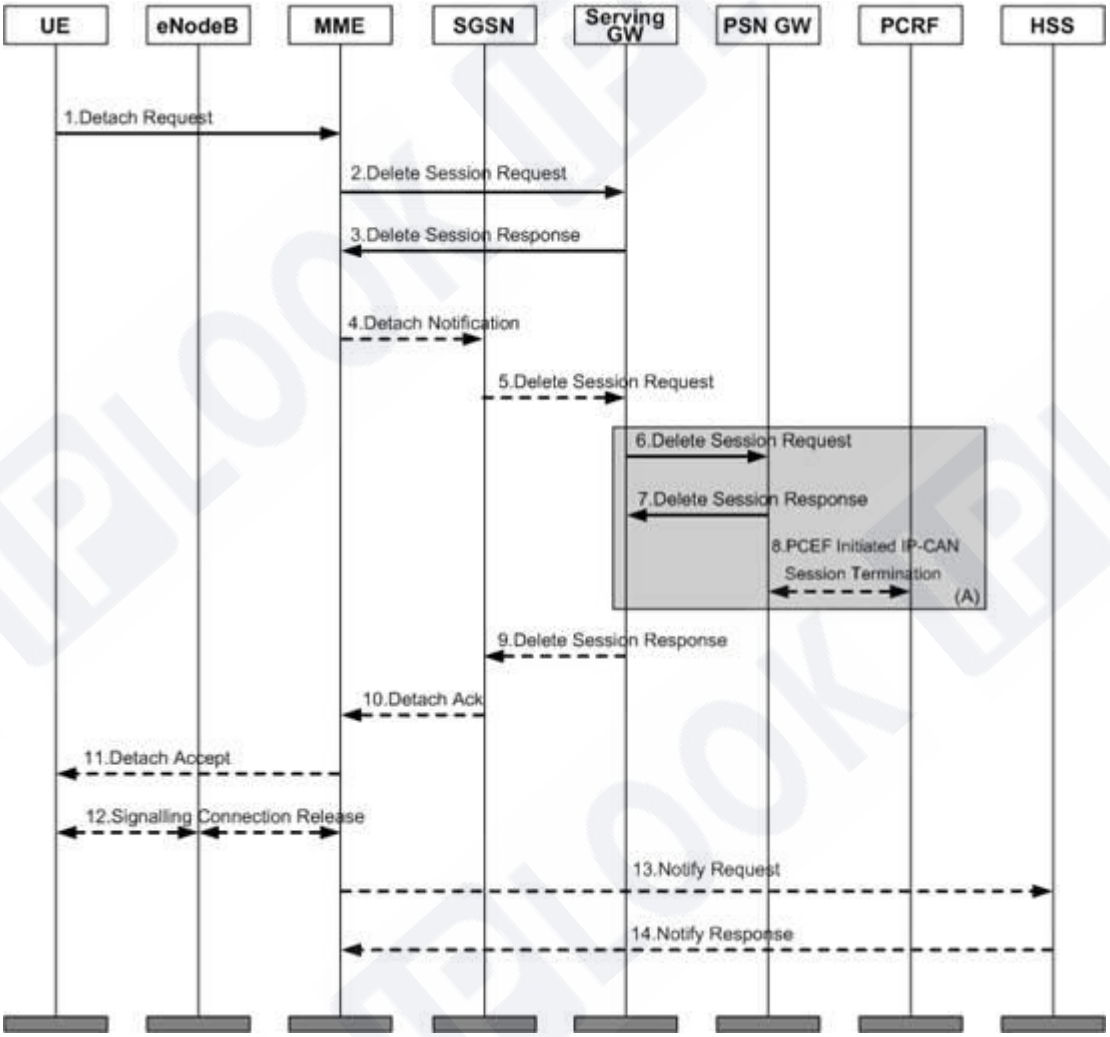


Figure 1.2.4-3 E-UTRAN detachment process initiated by UE

1. The UE sends a "detachment request" to the MME.

2. The MME sends a "delete session request" to the S-GW, and the S-GW deactivates all bearers of the UE.

3. The S-GW returns the "delete session response" message.

4. If ISR is activated, MME sends a "detachment indication" message to its associated SGSN and indicates complete detachment.

5. The SGSN sends a "delete session request" to the S-GW, and the S-GW deactivates all PDP contexts of the UE.

6. The S-GW deactivates the IDR and sends a "delete session request" to the PDN-GW.

7. PDN-GW returns "delete session response" to S-GW.

8. The PDN-GW sends the "IP-CAN session termination" process to the PCRF to notify it that the EPS bearer has been released.

9. PDN-GW returns "delete session response" to SGSN.

10. SGSN returns the "detachment confirmation message" to MME.

11. MME returns the "detachment confirmation" message to UE.

12. MME sends "S1 release" command to eNodeB.

13. After receiving the "delete session response" message sent by S-GW, MME sends a "notification request" to HSS to instruct HSS to delete the PDN-GW identity corresponding to the saved APN.

The following is the process of inserting user data:

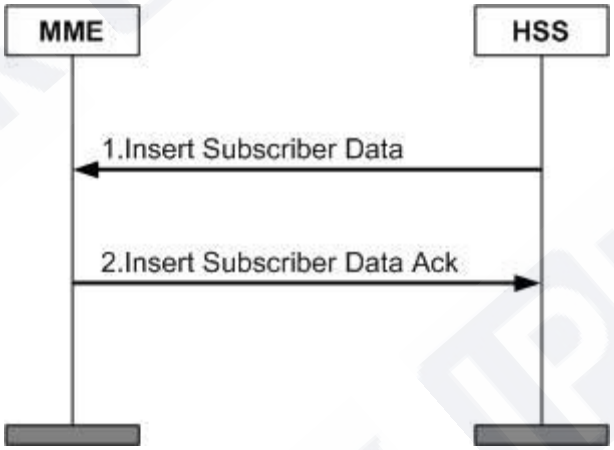


Figure 1.2.4-4 process of inserting user data

1. If the user's subscription data changes, HSS sends a "insert user data" request to MME.

2. MME updates its saved user subscription data and sends the "insert user data response" message.MME performs corresponding operations according to the new data issued by HSS. For example, if the new data does not allow users to roam in the current network, MME initiates the "detachment" process.

1.2. EAP-AKA authentication function

1.2.1. definition

Authentication refers to the process of network checking the legitimacy of users. It is a part of mobile network security management. It is used to realize the confidentiality and data integrity of mobile network.EPS-AKA (evolved packet system authentication and key agreement) authentication refers to the authentication of LTE network.

1.2.2. Dependency

UE	MME	HSS
√	√	√

1.2.3. Description of special effect parameters

1.2.4. Principle description

EPS-AKA authentication occurs when EPS users access the LTE network.

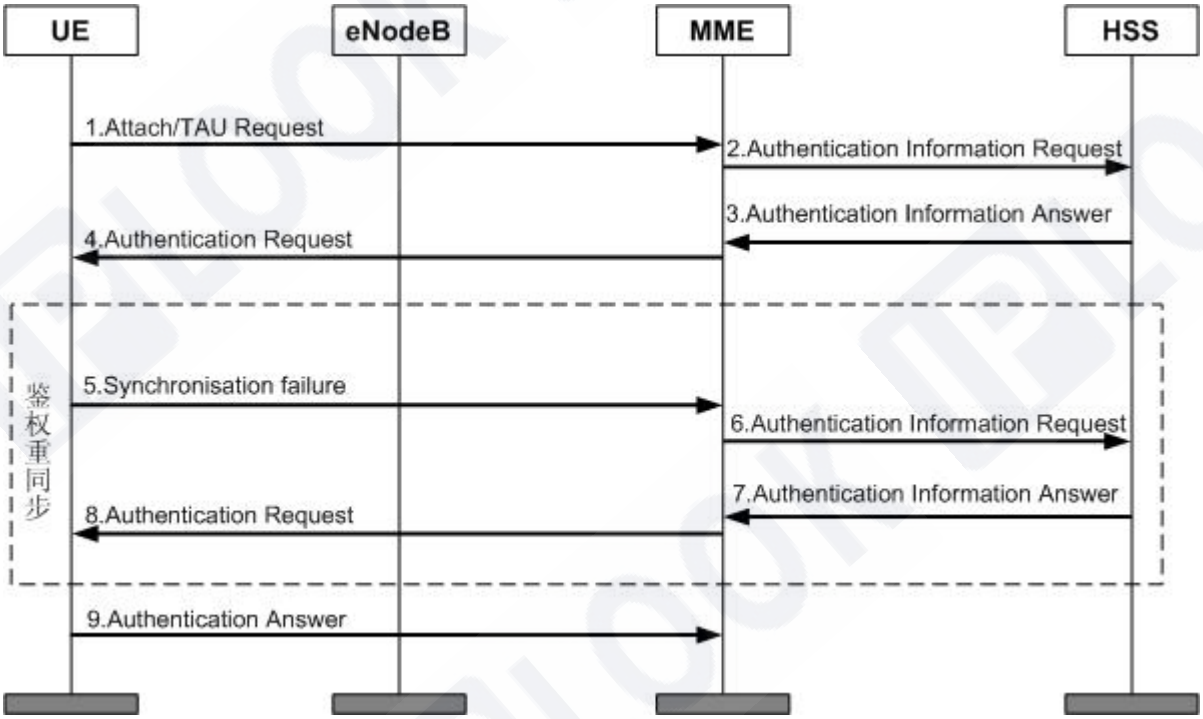


Figure 1.2.4-1 EPS-AKA authentication process

The authentication process is as follows:

1. The UE sends an attach request message to the eNodeB to attach to the LTE / SAE network or sends a tau request message to update the location;ENodeB sends the attach request message or tau (tracking area update) request message sent by UE to MME in advance.

2. MME sends an authentication information request message to HSS to initiate an authentication vector request, including IMSI, service network ID Sn ID (such as MCC + MNC) and network access type (such as E-UTRAN).

3. After receiving the message, HSS starts to calculate the EPS authentication vector, which calculates the root key K in the EPS authentication vector according to the service network ID and CK / IK_ASME and returned to MME through authentication information answer message, which carries a complete set of authentication vector quadruplets {RAND, AUTN, XRES, K_ASME}. If multiple sets of authentication vectors need to be returned, they are sorted according to the sequence number Sqn (sequence number);Since the access network type is E-UTRAN, HSS sets the "separator" in the AMF field in autn to 1 to inform ue that the authentication vector is only used for AKA processes of LTE / SAE. If the "separator" is set to 0, the vector is only used for non LTE / SAE contexts (such as GSM and UMTS).

4. MME selects a set of authentication vectors from the database according to the first in first out criterion for this AKA process, and saves XRES and K_ASME in the authentication vector,sends an authentication request message to the UE, and the UE transmits the RANDom number RAND and authentication token autn in the authentication vector AV (authentication vector) contained in the message to the USIM card. In addition, the message also assigned K_ASME's identification KSI (key set identifier) to UE.

5. After receiving the AUTN and RAND from the network side, USIM calculates the SQN and compares it with the maximum Sqn number SQN_{MS} stored by itself to ensure that the new SQN must be greater than the SQN_{MS}, so as to ensure that the received authentication vector is a new and unused authentication group.When the received SQN is less than or equal to the SQN_{MS} saved by USIM, it sends a synchronization

failure message to MME, takes the SQN_{MS} saved by itself as the input parameter, calculates the AUTS parameter （AUTS = SQN_{MS} ⊕f5*$_K$（RAND） || f1*$_K$（SQN_{MS} || RAND || AMF））, and initiates the authentication weight synchronization process to the network side.

6. After receiving the synchronization failure message sent by UE, MME sends authentication information request message to HSS again;The Requested-EUTRAN-Authentication-Info parameter contains Re-Synchronization-Info AVP, which is composed of RAND and AUTS.

7. HSS parses the SQN_{MS} saved by USIM from the AUTS and verifies the AUTS. If the verification is passed, the SQN_{HE} saved in SAE-HSS and tracking the UE is set as the SQN_{MS} of the UE, and based on this, a new SQN and authentication vector are generated and returned to MME, while ensuring that the new SQN can be accepted by USIM.

8. MME saves XRES and K_ASME in the authentication vector, sends the authentication request message to the UE again, and the UE transmits the RANDom number RAND and authentication token AUTN in the authentication vector AV (authentication vector) contained in the message to the USIM card. In addition, the message also assigns K_ASME's identification KSI (key set identifier) of to UE.

9.When USIM confirms that the received authentication group is an unused authentication group, it calculates whether the autn is correct according to the random number RAND, so as to authenticate the network. Then it calculates the RES according

to the random number RAND and AUTN, and sends it to MME in the response message authentication answer. If the MME checks if RES is consistent with XRES, the network authenticates the UE.In addition, the USIM card also calculates CK / IK through AUTN and RAND and transmits it to the UE. The UE calculates K_ASME in combination with CK / IK and service network ID and store.

1.3. Roaming local breakout function

1.3.1. definition

The roaming local breakout function allows users to access the network directly using the PDN GW (packet data network gateway) of the roaming place without detouring back to the home place for network access.

1.3.2. Dependency

UE	MME	HSS
√	√	√

1.3.3. Description of special effect parameters

1.3.4. Principle description

The PDN GW used by the user to access the network is mainly selected by MME / S4 SGSN / AAA, and HSS is only responsible for the storage and distribution of signing information.

1. By signing this feature, users can access the network using PDN GW in roaming and home places.

2. Without signing this feature, users can only access the network using the PDN GW of their home location.

The effectiveness of this feature needs to be determined by the local breakout attribute based on APN level and the local breakout attribute based on UE PLMN level. The relationship between the two is as follows:

1. If the user does not sign up for the UE PLMN template, the local breakout attribute of APN level shall prevail.

2. If the user signs up for the UE PLMN template, but the template does not define the PLMN ID of the current user, the local breakout attribute of APN level shall prevail.

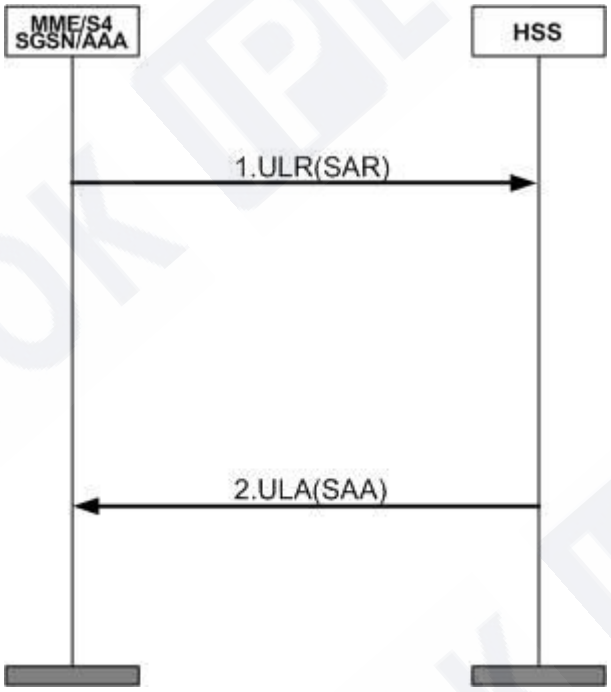
3. If the user signs up for the UE PLMN template, the template contains the current PLMN ID of the user and defines the local breakout attribute of the UE PLMN level, that is, the local breakout function is allowed only when the two local breakout attributes are set to allow the user to access the PDP / PDN network from the VPLMN.

Business process:

1. If the user does not sign up for roaming local breakout on the network, HSS will send the relevant user signing data to MME / S4 SGSN / AAA through the location update process.

2. If the user signs up / goes to sign up for roaming local breakout on the network, HSS will notify MME / S4 SGSN / AAA to update the relevant user signing data through the independent user data insertion process.

Distribute relevant user signing data through the location update process:



1.3.4-1Figure distribution of relevant user signing data through location update process

1. MME / S4 SGSN / AAA sends a location update request to HSS. The interaction between AAA and HSS is completed through the SAR process (the server assignment request).

2. Return the response message update location answer with successful location update, and bring relevant user data in the response message. The interaction between AAA and HSS is completed through the SAA process (the server assignment answer).

Issue relevant user signing data through the independent user data insertion process:

1. HSS sends the relevant user signing data to MME / S4 SGSN / AAA through the independent insertion user data process IDR (PPR), in which the interaction between AAA and HSS is completed through the PPR process (the push profile request).

2. MME / S4 SGSN / AAA returns the response message of IDA (PPA) to HSS. The interaction between AAA and HSS is completed through the push profile answer.

1.4. PLMN based roaming restrictions

1.4.1. definition

Roaming restriction service based on PLMN (public land mobile network) means that the system manages user mobility according to the requirements of operators, networks or users, and restricts users to allow or prohibit access to other operators' networks.

This service is generally used to limit the access range of users to the networks of other operators that have signed roaming agreements with this operator.

1.4.2. Dependency

UE	MME	HSS
√	√	√

1.4.3. Description of special effect parameters

1.4.4. Principle description

In S6a / S6d location update process, PLMN based roaming restriction process:

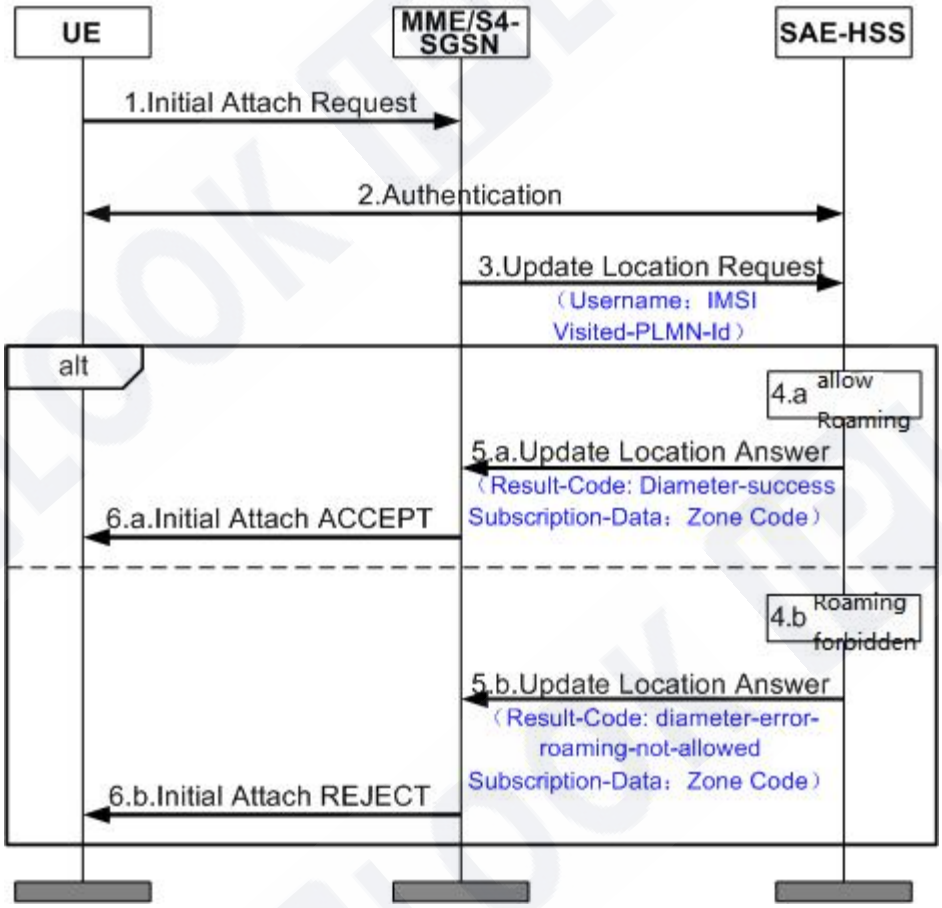


Figure 1.4.4-1 roaming restriction flow chart based on PLMN

1. When the mobile user leaves the PLMN area to another PLMN area, it will send an initial attach request to MME.

2. MME / S4-SGSN initiates an authentication operation for the user to determine the legitimacy of the user.

3. After successful authentication, MME / S4-SGSN sends a location update request ULR (update location request) to SAE-HSS.

4. SAE-HSS determines whether the user is roaming allowed or roaming prohibited according to the IMSI and visited PLMN ID carried in the location update request message.

5. SAE-HSS returns ULA (update location answer) response message.

a. Roaming is allowed, and the AVP of "result code" carried in the returned ula message is "diameter success".

b. Roaming is prohibited, and the AVP of "result code" carried in the returned ula message is "diameter error roaming not allowed".

6. MME / S4-SGSN returns the initial attach message to the user.

a. Roaming is allowed, and the initial attach accept message is returned to the user. The user's location is updated successfully.

b. Roaming is prohibited, and the initial attach reject message is returned to the user. The user location update fails.

1.5. Equipment status management

1.5.1.1. 1.1.1definition

EIR (Equipment Identity Register) is an independent network element device used to store the status information of IMEI (international mobile station equipment identity).The device status management function refers to the function that EIR can detect the legitimacy of the network to the terminal device by checking the status information of the terminal IMEI, so as to control whether the mobile device can access the network.

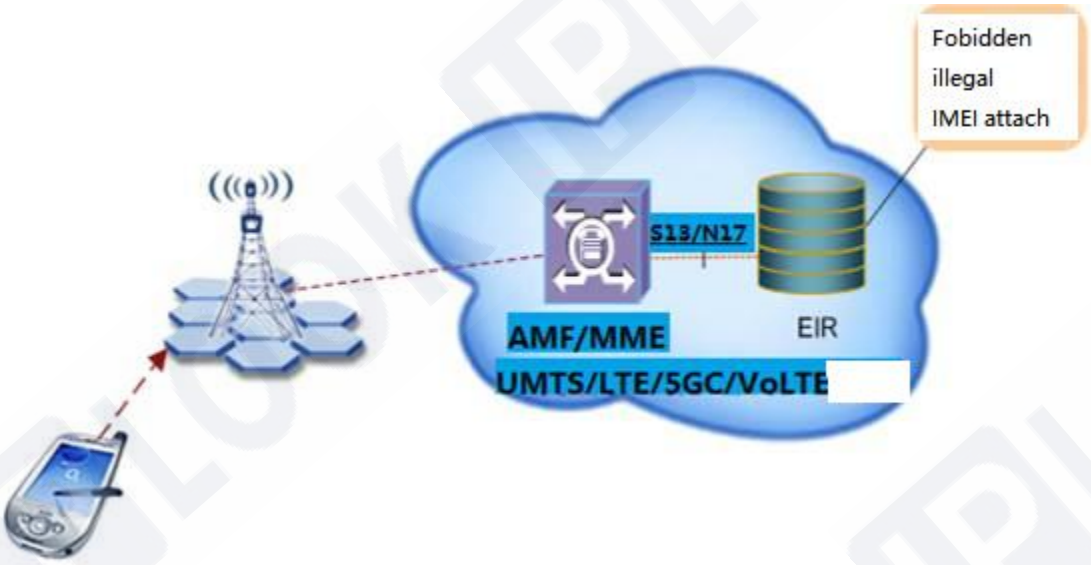


Figure 1.1.1-1 Schematic diagram of equipment status management function

1.5.1.2. 1.1.2Application scenario

When the operator needs to restrict the use of mobile devices in a batch of IMEI segments, the status of devices in this IMEI segment can be configured as blacklist status;When the operator allows the mobile equipment in an IMEI section to be available, the equipment status in this IMEI section can be configured as white list status;When the user's mobile equipment is stolen, it can provide the equipment identification IMEI to the corresponding eir business hall and report the loss. Eir can configure the equipment status corresponding to this IMEI to the blacklist status to restrict its access to the network;When the mobile device held by the user is an illegal device (such as a fake machine or an unauthenticated mobile device), EIR can restrict its access to the network.

In addition to the black-and-white list, operators can customize the functions supported by the gray list if necessary.

This function can be applied to LTE network, 5GC network and volte network.

1.5.1.3. 1.1.3 Dependency

UE	MME/AMF
√	√

1.5.1.4. 1.1.4Description of special effect parameters

category	parameter
Equipment status management parameters	IMEI = international mobile device number
	Status = current status of equipment (white list, blacklist, gray list)

1.5.1.5. 1.1.5Principle description

IMEI status information

IMEI number is represented by a 14 digit decimal number, which is used to uniquely identify a mobile device.The EIR stores the IMEI status information of the mobile device, including the following three types:

- White table status: indicates that this mobile device is a legal device, and MME / AMF will allow it to access the network.
- Black table status: indicates that this mobile device is an illegal device, and MME / AMF will deny its access to the network.

- Gray table status: indicates whether the mobile device can access the network, which will be determined by the operator.

According to different application network types, the implementation principle is described according to business process 1 (LTE network and volte network) and business process 2 (5GC network).

Business process 1LTE Network and volte Network)

When detecting the legitimacy of the mobile device, MME will obtain the IMEI number from the mobile device and send me identity check req (ECR) message to eir to check the device status. Eir queries the device status information and returns the status information to MME. MME will judge whether the mobile device is legitimate according to the status returned by eir, and then decide whether to allow the mobile device to access the network.

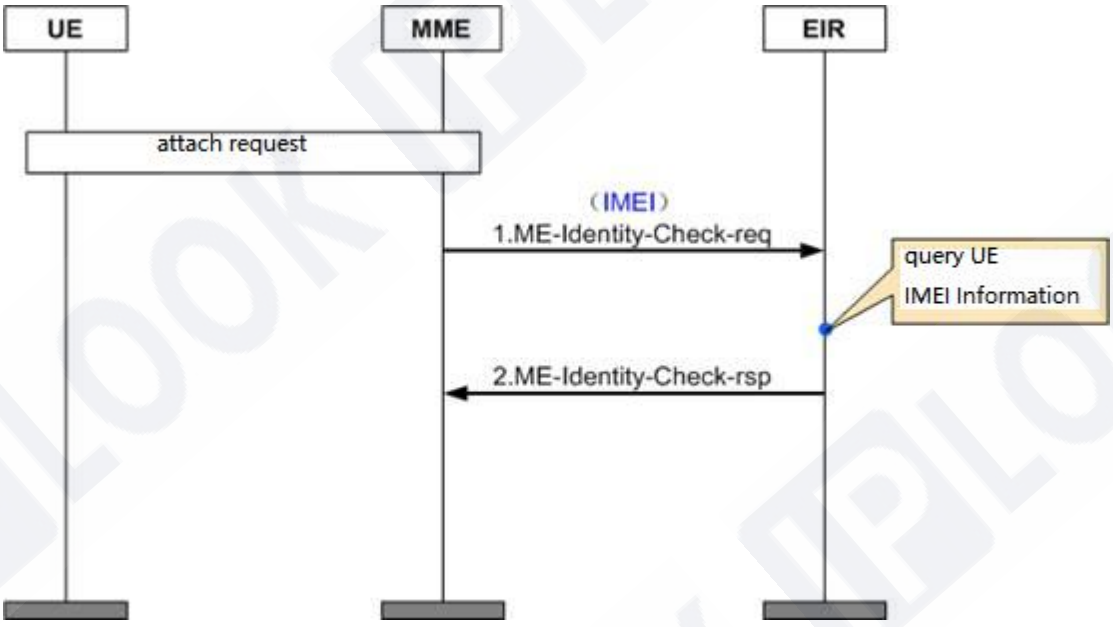


Figure 1.1.5-1ECR message interaction diagram

1.After initiating the network access request, MME sends ME-Identity-Check-req message to eir, and carries the IMEI number of the UE in the request message.

2. After receiving the request message, the EIR first looks up the IMEI number. If it exists, set the status information of the IMEI to the status queried in the database. If it does not exist, set the status information of the IMEI to unknown.The IMEI status message of the MS is carried in the me identity check RSP message.

Business process 2(5GC Network)

When detecting the legitimacy of a mobile device, AMF will obtain the IMEI number from the mobile device and send a GET .equipment-status?pei={pei}&supi={supi} message to 5G-EIR to check the device status. 5g-eir queries the device status information and returns the status information to AMF. AMF judges whether the mobile device is legitimate according to the status returned by EIR,Then decide whether to allow the mobile device to access the network.

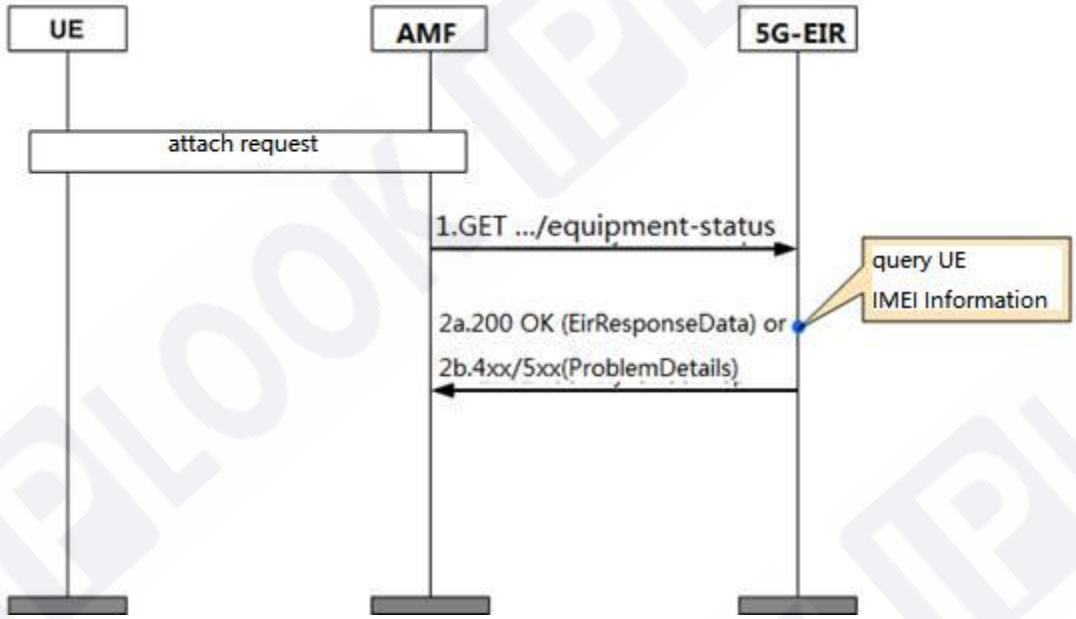


Figure 1.1.5-25g get device status message interaction diagram

1.After initiating the network access request, AMF sends a GET .equipment-status message to 5G-EIR, and carries the PEI (IMEI or imeisv) number of the UE in the request message.

2a.5G-EIR first looks up the PEI (IMEI or imeisv) number after receiving the request message. If it exists, it returns 200 OK and the status information of the IMEI is the status queried in the database.

2B. If PEI (IMEI or imeisv) does not exist, the message "404 not found" and the "problemdetails" object are carried in the message, and the "detail" in the object is set to "error_equipment_unknown".

1.5.1.6. 1.1.6Beneficiary

Operators can increase their operating revenue through the equipment status management function.

Through the equipment status management function, operators prohibit illegal terminals (such as cottage machines) from outside the network, which can protect network security and reliability.

By providing equipment status management function, operators can provide security services for end users and attract more users to the network.For example, operators can monitor users' stolen mobile phones through the device status management function to prevent users' mobile phones from being stolen or online information disclosure.When a user's mobile phone is stolen, he can report the loss of the mobile phone IMEI to the business hall, limiting his access to the network, so as to improve the security of the mobile phone.

1.6. Authentication data configurable

1.6.1. definition

The configurable functions of authentication parameters mainly include supporting the configuration of C1 ~ C5 and R1 ~ R5 parameters

1.6.2. Dependency

UE	MME	HSS
√		√

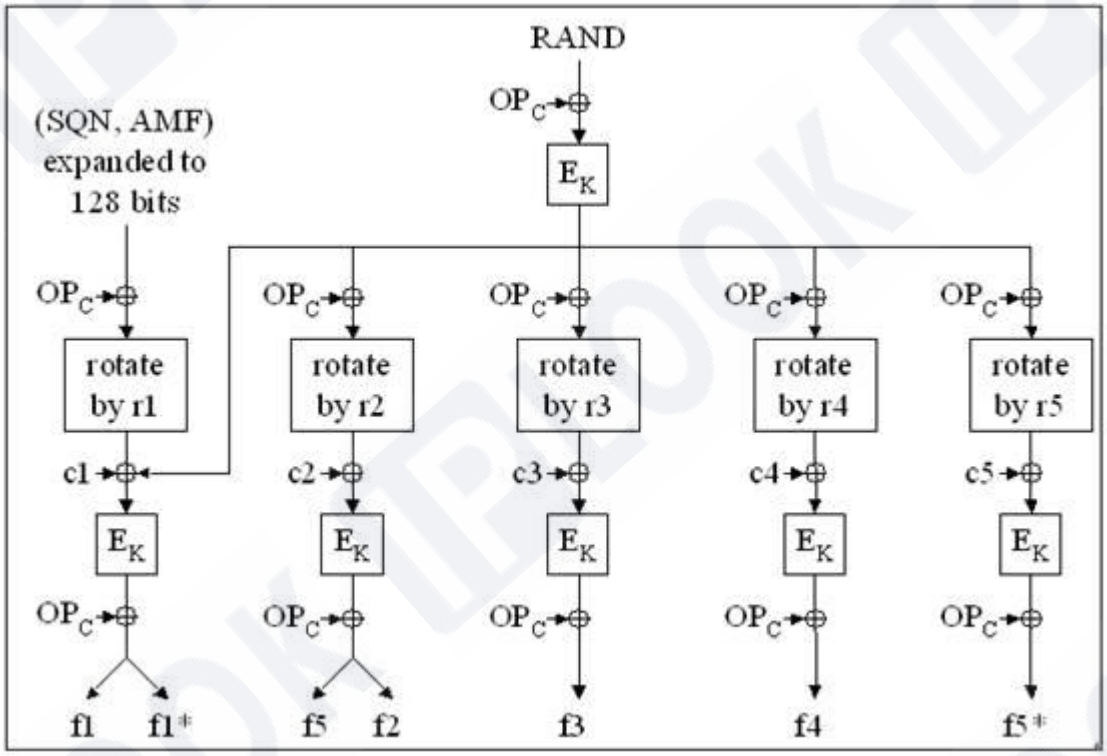
1.6.3. Description of special effect parameters

When some operators have high security requirements, they may use customized C1 ~ C5 and R1 ~ R5 parameters as the input of authentication milenage algorithm to improve the security of users.

1.6.4. Principle description

In the calculation process of milenage algorithm, C1 ~ C5 and R1 ~ R5 parameters will be used. These parameters can be customized by operators to enhance the security of the algorithm.The calculation process of the specific algorithm is shown in the following figure:

Calculation process of f1，f1*，f2，f3，f4，f5 and f5*



1.7. ODB service

1.7.1. definition

ODB (operator determined barring) refers to the blocking determined by the operator, which means that the service capability of the user to access the GSM / UMTS / LTE network is set for the user by the PLMN (public land mobile network) network operator.

1.7.2. Dependency

UE	MME	HSS
√	√	√

1.7.4. Principle description

1.8. Access type restriction function

1.8.1. definition

The access type restriction function is a function provided to operators to control the access rights of mobile users to different networks.

Access types can be divided into:

· UTRAN(Universal Terrestrial Radio Access Network)

- GERAN(GSM/EDGE Radio Access Network)
- GAN(Generic Access Network)
- I-HSPA-Evolution(Internet High Speed Packet Access-Evolution)
- EUTRAN(Evolved Universal Terrestrial Radio Access Network)

HO-To-Non3GPP-AccessHO To Non 3rd Generation Partnership Project Access

When a mobile user opens an account, the operator configures the user's ard (access restriction data) data on HSS according to the access type selected by the user, so as to control the mobile user to access different types of networks.

1.8.2. Dependency

UE	MME	HSS
√	√	√

1.8.3. Description of special effect parameters

This feature can be applied to 2G / 3G networks or LTE networks

1.8.4. Principle description

·The user accesses the LTE network and checks the ARD function when the location is updated

1. The mobile user sends an initial attach request to the MME.
2. MME initiates an authentication operation for the user to determine the legitimacy of the user.
3. After successful authentication, MME initiates update location to HSS.
4. HSS returns the response message of update location, which contains the ard data of the user.
5. MME determines whether the user is allowed to access the network according to the user's ard data. If it is determined that it is not allowed, it returns the initial attach reject message to the user, and the user's location update fails.
6. If the user allows access, the initial attach accept message is returned to the user, and the user location is updated successfully.

1.9. Roaming restrictions in user area

1.9.1. definition

EPS (evolved packet system) user area roaming restriction, that is, EPS user roaming is restricted according to the area roaming template or the cell location accessed by the user for the first time.
Zone Code is the roaming area code of the user area planned by the operator. A roaming area template can have up to 20 Zone Codes.
There are two user area roaming restriction schemes provided by EPS HSS, namely static area roaming restriction and dynamic area roaming restriction. The flexible area roaming restriction function can not only realize different roaming experiences of users, but also enable operators to flexibly and efficiently manage user mobility.
Static area roaming limit means that the user has signed up for a fixed area roaming template planned by the operator (the Zone Code list and roaming cell range have been determined at the time of signing up and cannot be changed automatically).EPS HSS sends the Zone Code list signed by the user to the MME where the user is located. After receiving the Zone Code list, MME limits the roaming status of the user according to the Zone Code and roaming restriction policy (blacklist or whitelist) of the roaming area where the user is located.

Dynamic area roaming restriction means that when a user signs up, the range of the roaming area is not determined, but the area centered on the cell (including adjacent cells) is automatically locked as the roaming active area of the user according to the cell location when the user UE (user equipment) first accesses, and a regional subscription Zone Code list is generated at the same time.EPS HSS sends the user area signing code list to the MME where the user is located. After receiving the user area signing code list, MME limits the user's roaming status according to the user area signing code and roaming restriction policy (blacklist or white list) in the user's roaming area.

1.9.2. Dependency

UE	MME	HSS
√	√	√

1.9.3. Description of special effect parameters

1.9.4. Principle description

The specific business implementation is mainly completed by MME, and HSS is only responsible for the storage and distribution of signing information.

·If the user signs up for static area roaming restrictions when he is not on the network, HSS will distribute the list of zone codes signed by the user to MME through the location update process.

·If the user is in the network and signs up for static area roaming restrictions, HSS will send the user's modified zone code list to MME through IDR / IDA message.

·If the user is in the network and signs up for static area roaming restrictions, HSS notifies MME to delete the user's zone code list information through DSR / DSA message.

1.10. General configuration APN function

1.10.1. definition

When signing an APN (access point name) for a user, the wildcard "*" is used to indicate the universal APN.After signing the universal APN, the user can select the appropriate APN access network according to the actual situation.

1.10.2. Dependency

UE	MME	HSS
√	√	√

1.10.3. Description of special effect parameters

1.10.4. Principle description

The specific business implementation is mainly completed by MME, and HSS is only responsible for the storage and distribution of signing information.

operation flow

·If the user signs up for the general distribution APN when he is not in the network, HSS will issue the general distribution APN signed by the user to MME through the location update process.

·If the user is in the network and signs up for universal APN, HSS sends the universal APN signed by the user to MME through IDR / IDA message.

·If the user is in the network and signs up for universal APN, HSS notifies MME to delete the user's universal APN information through DSR / DSA message.

1.11. Multi HPLMN function

1.11.1. definition

HPLMN (home public land mobile network) management function is mainly to provide users with operations of adding, deleting, modifying and querying system HPLMN information

1.11.2. Dependency

UE	MME	HSS
√	√	√

1.11.3. Description of special effect parameters

1.11.4. Principle description

The HPLMN function mainly involves four operations: add, delete, modify and query.The message processing mainly involves the processing of location registration messages.When the user signs up for ODB service, compare the VPLMN brought by the message with multiple HPLMN records saved in the database:

·If there is a match, it is considered to be the home domain.

·If none of them match, it is considered a visiting domain (roaming).

2. IMS HSS basic features

2.1. Registration restrictions

2.1.1. definition

Registration restriction refers to the function of controlling whether a user is allowed to register in the IMS network on HSS.After opening an account, IMS users can prohibit user registration by setting user registration permission.When a user accesses the IMS network, HSS will judge whether to allow access to the IMS network and enjoy IMS multimedia services according to the Registration Authority signed by the user.

2.1.2. Dependency

UE	IMS	HSS
√	√	√

2.1.3. Description of special effect parameters

2.1.4. Principle description

After setting this feature, users cannot register. The process of registering restricted features in the registration scenario is as follows:

1: the UE sends a register request message to the P-CSCF at the place where the user visits.

2: the P-CSCF sends a register request message to the I-CSCF where the user belongs.

3: after receiving the register request message, I-CSCF sends UAR message to HSS to query the address of S-CSCF.

4: after receiving the UAR message, HSS judges the user's permission. If registration is not allowed, HSS will return the UAA message to I-CSCF, and the error code (parameter_authorization_rejected) contained in the message indicates that the user is not allowed to register.

5: the I-CSCF returns a 403 (Forbidden) message to the P-CSCF where the user visits. In the warning header field, it indicates that the user does not have registration permission, and the registration fails.

6: the P-CSCF returns a 403 (Forbidden) message to the UE, indicating that the user does not have registration permission and registration fails.

2.2. IMS roaming restrictions

2.2.1. definition

IMS roaming restriction means that HSS matches the roaming information signed by the user with the roaming area information at the time of user registration. If it fails, it limits the roaming range of the user by checking the default restriction policy information to realize the system's management of user mobility.

When the IMS mobile user enters the roaming allowed area, the IMS system allows the user to register.

When the IMS mobile user enters the roaming prohibition area, the IMS system prohibits the user from registering.

When an IMS mobile user enters an area that is neither roaming allowed nor roaming prohibited, it needs to be processed by checking the default restriction policy information. If the roaming allowed policy is signed, the IMS system allows the user to register. If the roaming prohibited policy is signed, the IMS system prohibits the user from registering.

The operator configures network1.com and network2.com roaming areas on HSS, and sets network1.com as roaming prohibited area and network2.com as roaming allowed area;No network3.com related data is configured on HSS, but the operator sets it to allow roaming.

2.2.2. Dependency

UE	IMS	HSS
√	√	√

2.2.3. Description of special effect parameters

This feature is suitable for various IMS access networking modes. The processing method of this feature is the same under different access networking modes. Operators can limit the roaming range of users through this feature. Its application scenarios include:

1. Users in the defined roaming allowed area are allowed to register and access the IMS network.
2. In the defined no roaming area, the user is not allowed to register.
3. In areas where roaming permission or prohibition is not defined, you need to check the default restriction policy information. If the information is roaming permission, the user is allowed to register; otherwise, the user is prohibited from registering.

2.2.4. Principle description

The HSS stores the user's roaming address list, user roaming permission information and default restriction policy information.

HSS matches the roaming information (e.g. user.Hytera.com) in the user's registration message initiated by the visiting network with the roaming permission information signed by the user in HSS (e.g. Hytera.com). If it fails, the user's roaming permission is obtained by checking the default restriction policy information.Introduce the principle of IMS roaming restriction in the registration process.According to roaming permission and roaming prohibition, it is divided into the following two scenarios:

Roaming prohibition

1: the UE sends a register request message to the P-CSCF at the place where the user visits.

2: after receiving the register request, the P-CSCF of the visiting place fills the visiting network address configured on the P-CSCF into the register message, and then sends the register request to the I-CSCF of the user's home. The p-visited-network-id header field carries the visiting network address of the P-CSCF.

3: I-CSCF determines the registration request message according to the register message, sends the UAR message to HSS to query the address of S-CSCF, and puts the visited network address in the p-visited-network-id header field in the UAR message.

4: HSS obtains the visiting network address information from the user signing data and matches it with the visiting network address carried in the UAR message.

5: the I-CSCF returns a 403 (Forbidden) message to the P-CSCF where the user visits. In the warning header field, it indicates that the user cannot register in the roaming prohibition area, and the registration fails.

6: the P-CSCF returns a 403 (Forbidden) message to the UE, indicating that the user cannot register in the roaming prohibition area, and the registration fails.

Roaming allowed

1: the UE sends a register request to the P-CSCF where the user visits.

2: after receiving the register request, the P-CSCF of the visiting place fills the visiting network address configured on the P-CSCF into the register message, and then sends the register request to the I-CSCF of the user's home. The p-visited-network-id header field carries the visiting network address.

3: I-CSCF determines the registration request message according to the register message, sends the UAR message to HSS to query the S-CSCF, and puts the visited network address in the p-visited-network-id header field in the UAR message.

4: HSS obtains the visiting network address information from the user signing data and matches it with the visiting network address carried in the UAR message.

If the visiting network address signed by the user is matched and the address is a roaming allowed area.

If the visiting network address signed by the user is not matched, HSS will check the default restriction policy information, which is roaming allowed.

In the above two cases, HSS judges that the user is in the roaming allowed area and allows the user to roam and register in the area. HSS will return UAA message to I-CSCF, which carries the address or capability set of S-CSCF.

5: after I-CSCF queries the address of S-CSCF, I-CSCF sends the register request message to S-CSCF to continue the registration process.

2.3. IMS AKA authentication

2.3.1. definition

IMS AKA authentication is a mechanism for IMS network to authenticate IMS users (UES) using ISIM (IP multimedia services identity module) card.This mechanism enables two-way authentication between IMS user (UE) and IMS network.That is, the IMS network needs to authenticate the IMS user (UE), and the IMS user (UE) also needs to authenticate the IMS service network.The identity used for user authentication in the IMS network is the user private identity IMPI (IP multimedia private identity).IMS authentication parameters include authentication vector quintuples.

2.3.2. Dependency

UE	IMS	HSS
√	√	√

2.3.3. Description of special effect parameters

This feature needs to be enabled only when the IMS network needs to authenticate IMS users (UE) using ISIM cards in the network.

2.3.4. Principle description

IMS user (UE) has opened an account in HSS and signed the feature. The home network performs IMS AKA authentication for IMS users through the initial user registration process. The implementation principle of authentication is as follows:

1: the UE initiates the registration request message register and carries the authentication authorization header domain.
2: P-CSCF receives the registration request message and sends it to I-CSCF.

3: I-CSCF queries the address of S-CSCF from HSS and sends the registration request message to S-CSCF.After receiving the registration request message, S-CSCF does the following:
·If there is no available authentication vector in the S-CSCF, the S-CSCF will send an authentication vector set request to HSS with the required number of authentication vectors m ($1 \leq m \leq 5$).
·If an authentication vector is available in the S-CSCF, execute 8.

4: after HSS receives the authentication vector set request from S-CSCF, it determines that the authentication mode of the user is IMS AKA authentication according to the authentication scheme parameter value in the message as "digest-AKAv1-md5", calculates the authentication quintuple according to the authentication information signed by the user, and returns n authentication vectors sorted based on serial number to S-CSCF, where n is equal to or less than m.
5: S-CSCF selects an authentication vector from the authentication vector set according to the first in first out principle and sends 401 authentication challenge (authentication request of S-CSCF to UE) to I-CSCF. The message contains parameters IMPI, RAND, AUTH, IK and CK, and the authentication vector is contained in the www-authenticate header field.At the same time, S-CSCF calculates XRES according to the authentication vector and saves it.
6: I-CSCF forwards 401 authentication challenge to P-CSCF.
7: the P-CSCF receives the 401 authentication challenge, takes out the IK and CK and saves them, and continues to send the remaining parameters RAND, AUTN and IMPI in the message to the UE.

8: the UE receives the 401 authentication challenge, calculates the XMAC according to the autn and RAND, compares it with the MAC value in the autn to see if it is consistent, and compares the serial number Sqn in the autn.After the UE authenticates the network, the UE uses RAND to calculate the authentication response RES, places it in the authorization header domain, and sends it to the P-CSCF through a registration message.

9: P-CSCF receives the authentication response and sends it to I-CSCF. I-CSCF queries the address of S-CSCF from HSS and sends the authentication response to S-CSCF.After the S-CSCF receives the authentication response, check whether the actually received authentication response RES and the expected authentication response XRES are the same.

10: S-CSCF sends SAR message to HSS, updates the registration flag of UE in HSS, and HSS returns SAA to S-CSCF.
·If the UE's IMPU is not currently registered, HSS updates the registration flag to registered.
·If the IMPU is currently registered, HSS will keep the registration mark unchanged.
·If the IMPU is in the implicit registry, HSS will treat all impus in the implicit registry as registered.
11: after the S-CSCF receives the SAA, the S-CSCF sends a 200 (OK) registration success response message to the UE through the I-CSCF and P-CSCF, and the user registration is completed.

2.4. Alias IMPU function

2.4.1. definition

An alias IMPU group is a collection of two or more impus.In the alias IMPU group, all impus belong to the same implicit registration set and share the same service profile.In HSS system, an alias IMPU group is identified by alias ID.
The IMPU roaming permission and registration permission in the alias IMPU group are the same, and the same IMPI is associated.

2.4.2. Dependency

UE	IMS	HSS
√	√	√

2.4.3. Description of special effect parameters

2.4.4. Principle description

Alias IMPU group refers to a collection of impus that share service profiles in the implicit registration set of IMPUs.
HSS supports the establishment of alias IMPU group in the IMPU sharing service profile in an implicit registration set through portal client, and uses alias ID to represent the ID number of alias IMPU group.

The AS can download the alias IMPU group through the UDR (user data request) / UDA (user data answer) message of the Sh interface, and subscribe to the alias IMPU group through the SNR (subscribe notifications request) / SNA (subscribe notifications answer) message.If the subscribed alias IMPU group changes, HSS needs to send PNR (push notification request) message to notify AS.
The S-CSCF downloads the alias IMPU group through the SAR (server assignment request) / SAA (server assignment answer) message of the CX interface.If the subscribed alias IMPU group changes, HSS needs to send PPR (push profile request) message to inform S-CSCF.

2.5. Transparent number and alias transparent data function

2.5.1. definition

Transparent data refers to the data related to IMS contracted users stored by as in HSS.These data are defined by as and transparent to HSS, so they are called transparent data.The purpose of this mechanism is to make use of the storage function of HSS and reduce the complexity of as data management.As can download transparent data through UDR (user data request) / UDA (user data answer) messages, update transparent data through PUR (profile update request) / PUA (profile update answer) messages, and subscribe to and unsubscribe from transparent data through SNR (subscribe notifications request) / SNA (subscribe notifications answer) messages.If the subscribed transparent data changes, HSS will send a PNR (push notification request) message to notify as.
Alias transparent data refers to the transparent data shared by IMPUs in the alias IMPU group.

2.5.2. Dependency

UE	IMS	HSS
√	√	√

2.5.3. Description of special effect parameters

2.5.4. Principle description

AS cooperates with HSS to store user business related data on HSS.As downloads transparent data through UDR / UDA messages, updates transparent data through PUR / PUA messages, and subscribes and unsubscribes transparent data through SNR / SNA messages.When the subscribed transparent data changes, HSS will send PNR message to notify AS.

When issuing services on the AS, if there is no transparent data of the current user locally, download the transparent data through UDR.

When the AS processes third-party registration or supplementary services, if there is no transparent data of the current user locally, it downloads transparent data through UDR or downloads and subscribers to transparent data through SNR.

When the data on HSS is subscribed to by multiple AS at the same time, one of the AS will update the transparent data on HSS through pur after modifying the user signing data. At this time, HSS will notify other AS subscribing to this data through PNR.

Transparent data and alias transparent data are data stored in HSS by as.These data are defined by as and transparent to HSS.

HSS saves transparent data and alias transparent data, and supports the maintenance of these data through portal interface and Sh interface.

2.6. BSF obtains user authentication data through Zh interface

2.6.1. definition

This feature supports BSF ne to request user authentication information from IMS-HSS NE through MAR (multimedia authentication request) message in Zh interface, and IMS-HSS sends user authentication vector and security setting information to BSF ne through MAA (multimedia authentication answer).

2.6.2. Dependency

UE	IMS	HSS
√	√	√

2.6.3. Description of special effect parameters

2.6.4. Principle description

The business process supporting BSF to obtain user authentication data through Zh interface is as follows:

1: the UE sends an authentication request to the BSF NE and carries the IMPI user ID in the request message.
2: after receiving the request from the UE, the BSF NE sends a MAR message to the IMS-HSS to request the authentication vector.
3: after receiving the Zh interface Mar message, IMS-HSS queries the IMSI corresponding to the IMPI carried in the Mar message, sends an AIR message to the SAE-HSS through the S6a interface, and obtains the authentication vector of the corresponding IMSI user in SAE-HSS.
4: After receiving the air message, SAE-HSS returns the user's authentication information to IMS-HSS through AIA message authentication info AVP.
5: The IMS-HSS sends a MAA message to the BSF. In the MAA message, SIP auth data item AVP carries the authentication vector, and GBA usersecsettings AVP carries the guss signing information signed in IMS-HSS.
6: the BSF ne saves the user's corresponding authentication vector and GUSS signing information for the user's subsequent business processes.
7: the BSF ne sends the obtained authentication information to the UE.

2.7. SIM / USIM card authentication

2.7.1. definition

SIM / USIM card authentication is a mechanism that supports PS / CS domain users to authenticate when accessing IMS network under the situation of coexistence of HSS and HLR.

Although the integration of HSS and HLR is the trend of network evolution, in order to make maximum use of the existing network equipment of operators, the coexistence of HSS and HLR will last for a long time. IMS network needs to support the access of PS / CS domain users.In this authentication mode, HSS will only save the user data of the IMS domain (such as the user ID impi and IMPU of the GSM or UMTS user opening an account in the IMS domain), and HLR will save the user data of the PS / CS domain (such as the IMSI, MSISDN and authentication data of the PS / CS domain user).

When a PS / CS domain user requests registration with the IMS core network, HSS needs to request an authentication vector from the HLR and send it to the S-CSCF.This requires HSS to retrieve the corresponding PS / CS domain user ID IMSI according to the user's IMPI / IMPU, and send a MAP message to HLR to request authentication vector. This authentication method of requesting authentication vector from HLR is called SIM / USIM card authentication, or early AKA authentication. In case of GSM authentication, the authentication vector returned from HLR to HSS is an authentication triplet;In case of UMTS authentication, the authentication vector returned from HLR to HSS is authentication quintuple.

2.7.2. Dependency

UE	IMS	HSS
√	√	√

2.7.3. Description of special effect parameters

2.7.4. Principle description

UE indicates that the PS / CS domain user has opened an account in HSS and signed the feature. When the PS / CS domain user initiates the registration process, only the PS / CS domain user authenticated by SIM / USIM card can access the IMS network.HSS and HLR interact through MAP messages, and authentication information is stored in HLR.