Wireless Cellular Network Security: Part 6

Gaurav S. Kasbekar

Dept. of Electrical Engineering

IIT Bombay

References

- D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi, “*LTE Security*”, John Wiley and sons, 2nd edition, 2013.

EPS Authentication and Key Agreement (AKA)

User Identification

- EPS uses the International Mobile Subscriber Identity (IMSI), which is a permanent subscriber identity, to uniquely identify a subscriber
  - ❑ as in GSM and UMTS
- IMSI crucial for EPS security since the permanent authentication key K used in EPS AKA is identified by the IMSI
  - ❑ K is stored in the Authentication Centre (AuC) and in the Universal Subscriber Identity Module (USIM), but nowhere else
  - ❑ this is similar to the case in GSM and UMTS, where the permanent authentication key K_i was identified by IMSI
- For user identity confidentiality, a temporary identity is associated with an IMSI in EPS:
  - ❑ called Globally Unique Temporary UE Identity (GUTI)
  - ❑ recall: in GSM and UMTS, TMSI was used instead of GUTI

User Identity Confidentiality

- EPS protects confidentiality of the user identity as in GSM and UMTS:
    - ❑network assigns the user a temporary identity (GUTI) sent in a message protected from eavesdropping
    - ❑GUTI provides an unambiguous identification of the UE that does not reveal the user’s permanent identity– the IMSI
    - ❑GUTI can be used by the network and the UE during signalling between them, and can be translated by them to IMSI
- MME sends GUTI to UE only after protection for non-access stratum (NAS) signalling has been enabled

Terminal Identification

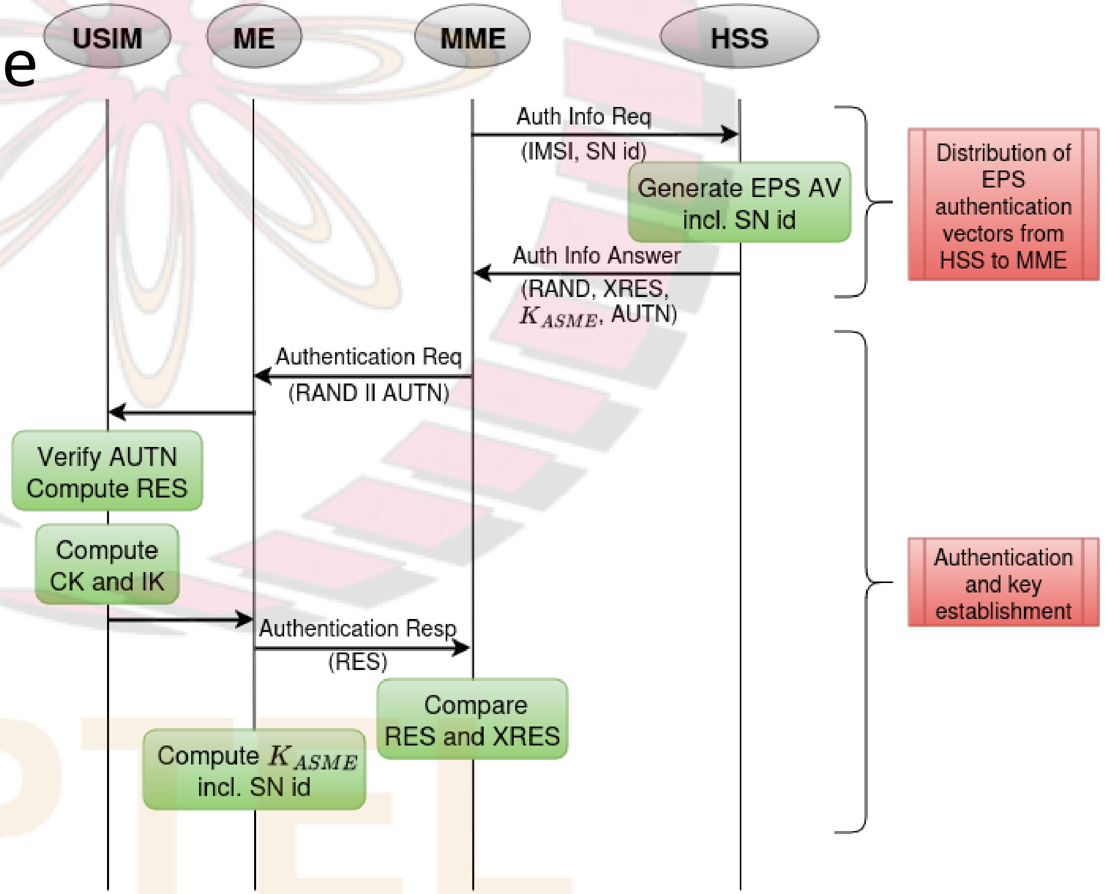
- GSM, 3G and EPS all use the same type of permanent terminal (phone) identity:
  - the International Mobile Equipment Identity (IMEI)
- Uses of IMEI number:
  - Cellular network uses IMEI number to identify phone accessing the network
  - If a mobile phone is stolen, the owner can have his/ her network provider use the IMEI number to blocklist the phone
  - Law enforcement and intelligence services can use an IMEI number as input for tracking phones; are sometimes able to locate a phone with an accuracy of a few meters

Terminal Identity Confidentiality

- Recall:
  - mechanism for protecting the user identity confidentiality in EPS same as it was in GSM and UMTS
- In contrast, there is an improvement in EPS with respect to GSM and UMTS regarding the terminal identity confidentiality
- In GSM and UMTS, it is possible that:
  - the network requests the terminal identity at any time, even before the signalling protection has been set up
  - without signalling protection already set up, the UE would respond by sending the terminal identity in the clear
  - as a user tends to use the same terminal for an extended period of time, the terminal identity would also give strong hints regarding the user identity
- This is no longer possible in EPS:
  - in EPS, the UE does not send IMEI to the network upon a network request before NAS security has been activated

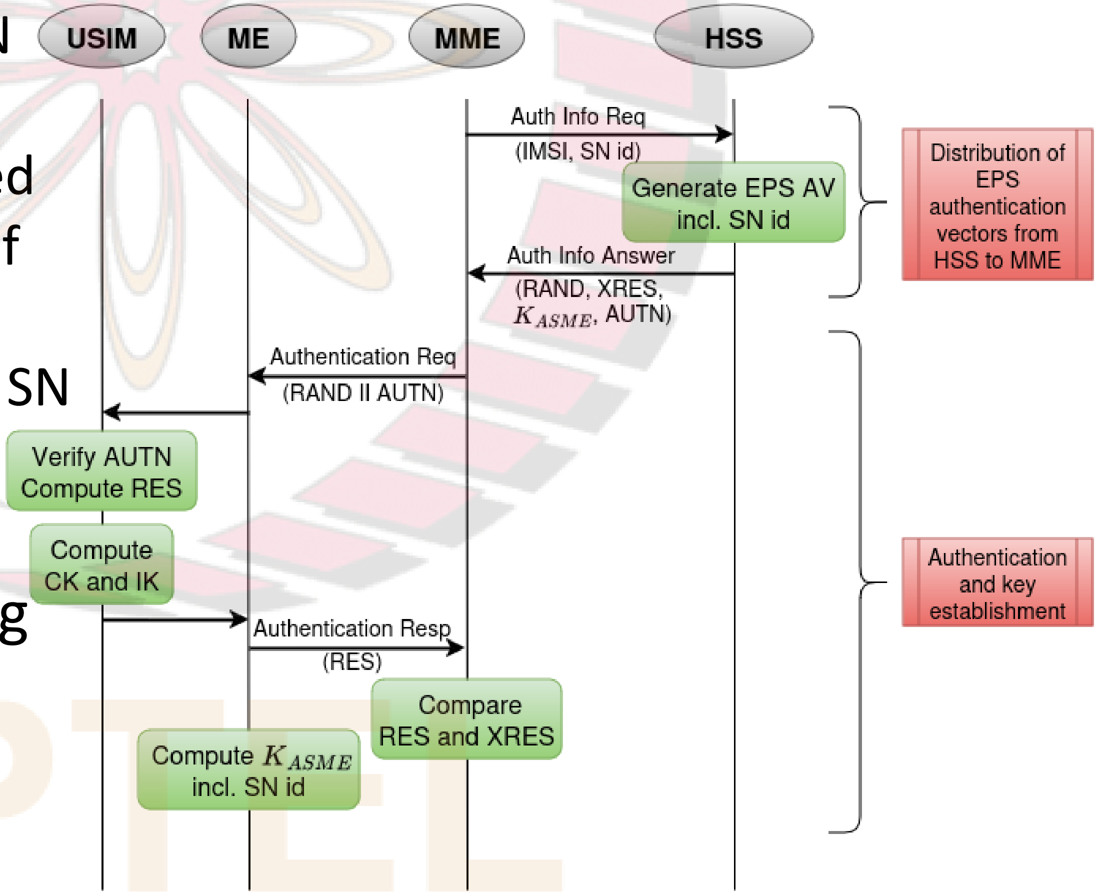
EPS AKA Procedure

- The EPS AKA procedure consists of following:
  - ❑a procedure to generate EPS authentication vectors (AVs) in the Home Subscriber Server (HSS) upon request from the MME, and to distribute them to the MME
  - ❑a procedure to mutually authenticate and establish a new shared key between the serving network (SN) and the UE


USIM
ME
MME
HSS
Auth Info Req
(IMSI, SN id)
Generate EPS AV incl. SN id
Auth Info Answer
(RAND, XRES, K_{ASME}, AUTN)
Distribution of EPS authentication vectors from HSS to MME
Authentication Req
(RAND || AUTN)
Verify AUTN Compute RES
Compute CK and IK
Authentication Resp
(RES)
Compare RES and XRES
Compute K_{ASME} incl. SN id
Authentication and key establishment

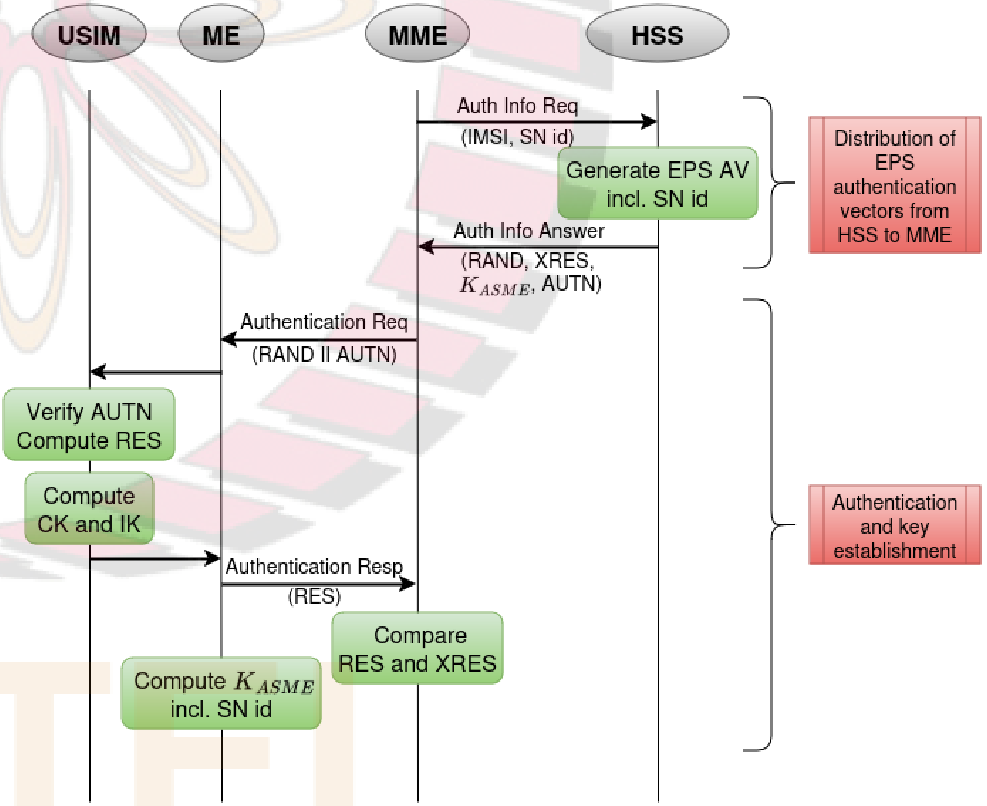
EPS AKA (contd.)

- Goals achieved by EPS AKA similar to those for UMTS AKA, with following enhancement:
  - ❑ EPS AKA provides implicit SN authentication, which UMTS AKA does not
- Implicit SN authentication achieved as follows:
  - ❑ SN id is one of the inputs used in computation of K_{ASME}
- Home network (HSS):
  - ❑ verifies the identity of a SN requesting AVs and
  - ❑ ensures that the SN id, used as input for computation of key K_{ASME} in AVs, matches the verified identity of the SN to which the AVs are sent
- Hence, a SN cannot obtain AVs with keys corresponding to the id of another SN
  - ❑ thus, SN authentication achieved


USIM
ME
MME
HSS
Auth Info Req
(IMSI, SN id)
Generate EPS AV incl. SN id
Auth Info Answer
(RAND, XRES, K_{ASME}, AUTN)
Distribution of EPS authentication vectors from HSS to MME
Authentication Req
(RAND || AUTN)
Verify AUTN Compute RES
Compute CK and IK
Authentication Resp
(RES)
Compare RES and XRES
Compute K_{ASME} incl. SN id
Authentication and key establishment

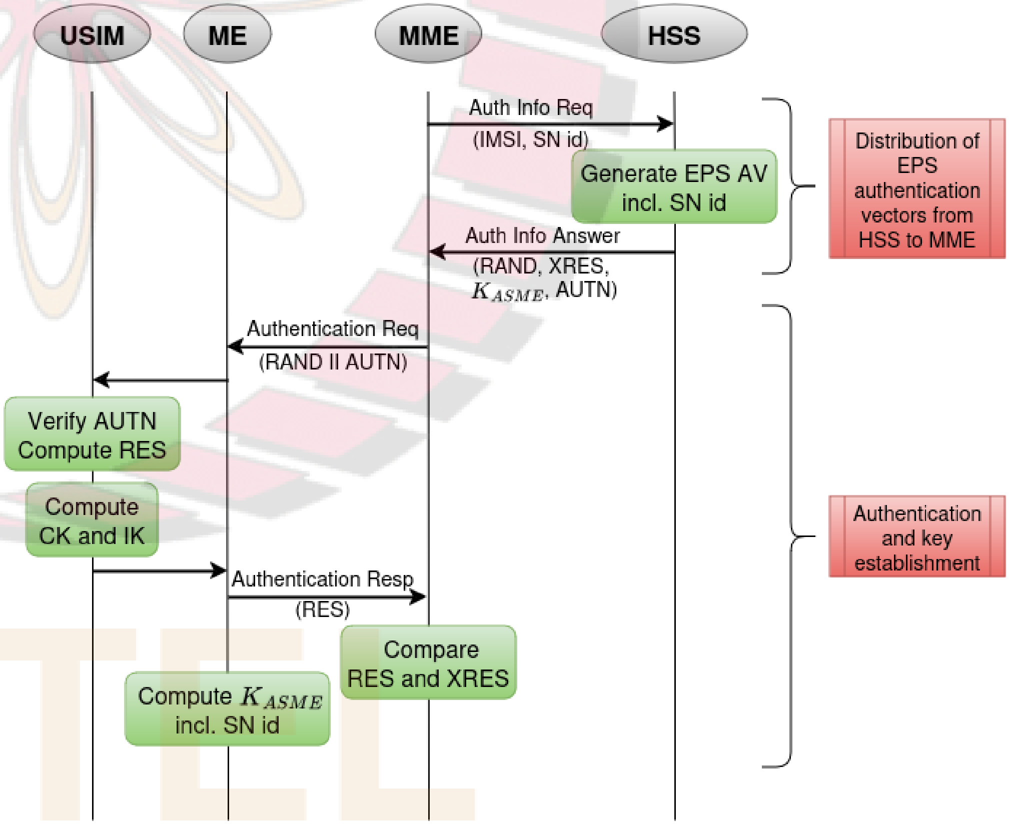
EPS AKA (contd.)

- The MME invokes the procedure by requesting EPS AVs from the HSS
- The Authentication Information Request includes the IMSI and the SN id of the requesting MME
- SN id is required for the computation of K_{ASME} in the HSS
- Upon receipt of the Authentication Information Request from MME:
  - ❑ the HSS may have pre-computed AVs available and retrieve them from the HSS database, or
  - ❑ it may compute them on demand
- The HSS sends an Authentication Information Answer back to the MME:
  - ❑ contains an ordered array of *n* EPS AVs $(1, \ldots, n)$
  - ❑ if $n > 1$, the EPS AVs are ordered based on sequence number


USIM
ME
MME
HSS
Auth Info Req
(IMSI, SN id)
Generate EPS AV incl. SN id
Auth Info Answer
(RAND, XRES, K_{ASME}, AUTN)
Authentication Req
(RAND II AUTN)
Verify AUTN Compute RES
Compute CK and IK
Authentication Resp
(RES)
Compare RES and XRES
Compute K_{ASME} incl. SN id
Distribution of EPS authentication vectors from HSS to MME
Authentication and key establishment

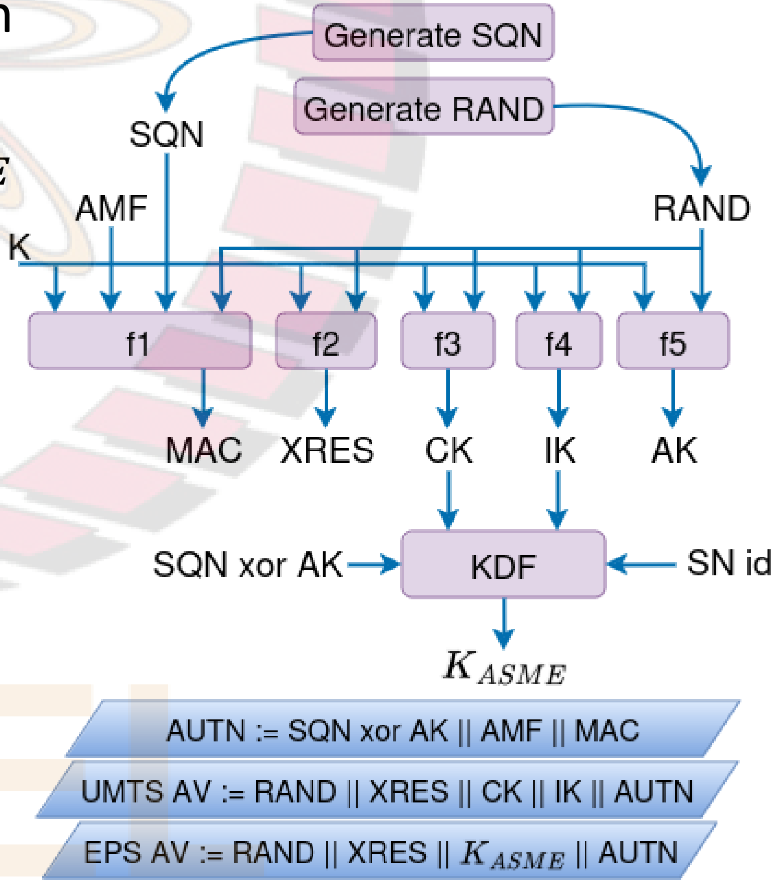
EPS AKA (contd.)

- LTE standard recommends *n* =1; so typically only one AV is sent at a time
  - ❑ recall: in GSM and UMTS AKA, five AVs are sent at a time
- This is because the need for frequently contacting the HSS for fresh AVs has been reduced in EPS through the availability of the local master key K_{ASME}
  - ❑ K_{ASME} is not used for encryption or message integrity; hence, not exposed like Ciphering Key (CK) and Integrity Key (IK) in UMTS
  - ❑ hence does not need to be renewed very often
- Based on the local master key, and keys derived from it, an MME can offer secure services even when links to the HSS are unavailable
- Pre-computed AVs no longer usable when the user moves to a different SN owing to the binding of the local master key K_{ASME} to the SN id
- Each EPS AV is used for one run of the AKA procedure between the MME and the USIM


USIM
ME
MME
HSS
Auth Info Req
(IMSI, SN id)
Generate EPS AV incl. SN id
Auth Info Answer
(RAND, XRES, K_{ASME}, AUTN)
Distribution of EPS authentication vectors from HSS to MME
Authentication Req
(RAND II AUTN)
Verify AUTN Compute RES
Compute CK and IK
Authentication Resp
(RES)
Compare RES and XRES
Compute K_{ASME} incl. SN id
Authentication and key establishment

Generation of Authentication Vectors

- Recall: a UMTS AV consists of:
  - ❑ a random 128-bit string (RAND), an expected response (XRES), a CK, an IK, and an authentication token (AUTN)
- In contrast, EPS AV consists of:
  - ❑ RAND, XRES, a local master key K_{ASME} and an AUTN
- Fig. shows generation of a UMTS AV by AuC, and generation of an EPS AV from this UMTS AV by HSS
- The AuC generates UMTS AVs for EPS AKA in exactly the same format as for UMTS AKA
- The HSS part outside the AuC derives K_{ASME} from CK and IK; in particular:
  - ❑ When the HSS receives the UMTS AV from the AuC, the HSS applies the KDF to CK, IK, SN id and, for technical cryptographic reasons, (SQN xor AK)
  - ❑ The result of the application of KDF is the key K_{ASME}
  - ❑ CK and IK can then be deleted in the HSS; they must never leave HSS



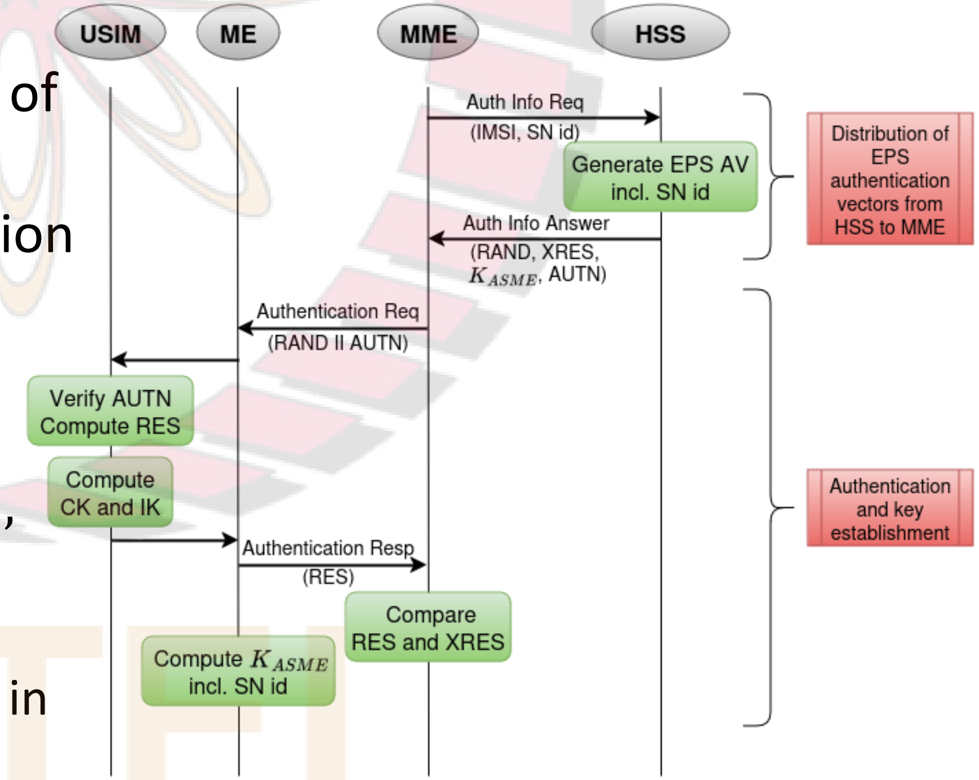
AUTN := SQN xor AK || AMF || MAC

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

EPS AV := RAND || XRES || K_{ASME} || AUTN

Mutual Authentication and Establishment of Shared Key between Serving Network and UE

- Purpose of this procedure is:
  - ❑ mutual authentication of user and MME,
  - ❑ establishment of a new local master key K_{ASME} between MME and UE
- K_{ASME} is subsequently used for deriving keys for the protection of user plane (UP) data, RRC signalling and NAS signalling
- Procedures used in EPS for handling of authentication requests and verification in USIM and authentication responses are same as in UMTS
- Difference:
  - ❑ when the ME receives (CK, IK) from the USIM, the ME computes K_{ASME}, using the same KDF and the same input parameters as the HSS
  - ❑ after this, CK and IK can be deleted in the ME


USIM
ME
MME
HSS
Auth Info Req
(IMSI, SN id)
Generate EPS AV incl. SN id
Auth Info Answer
(RAND, XRES, K_{ASME}, AUTN)
Distribution of EPS authentication vectors from HSS to MME
Authentication Req
(RAND II AUTN)
Verify AUTN Compute RES
Compute CK and IK
Authentication Resp
(RES)
Compare RES and XRES
Compute K_{ASME} incl. SN id
Authentication and key establishment