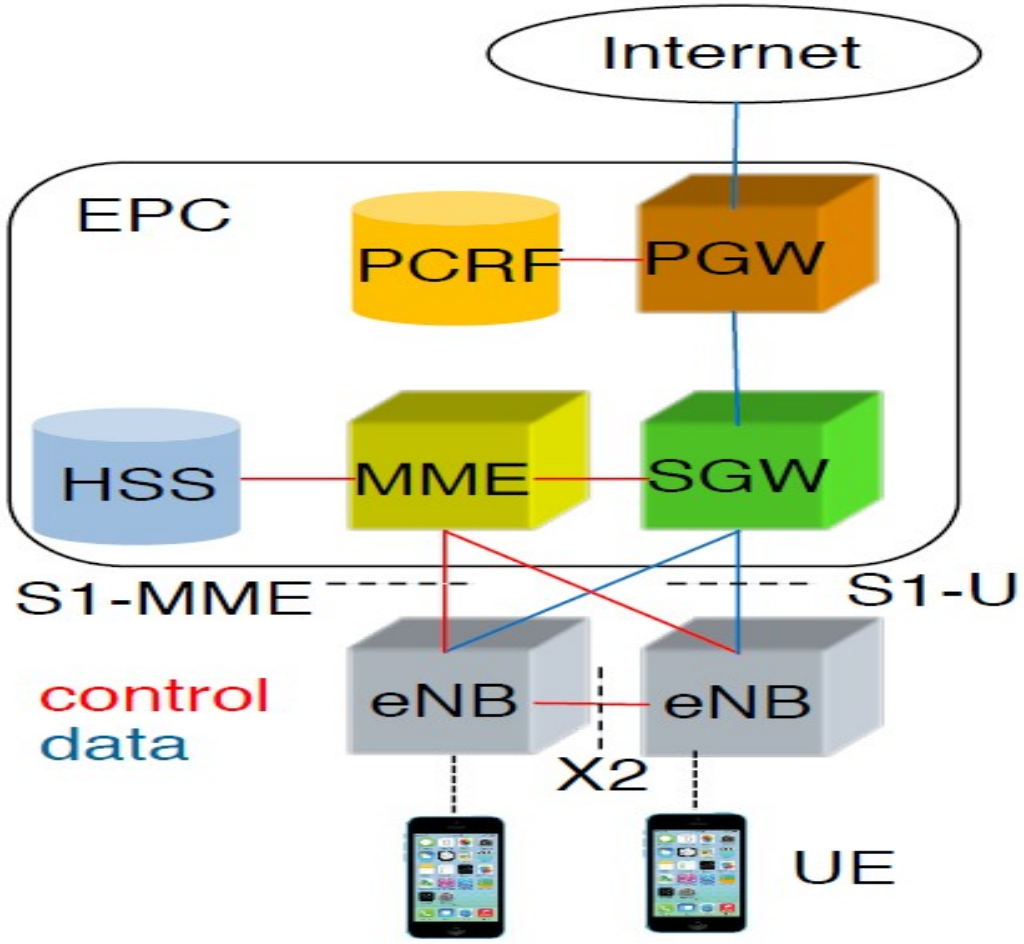
Communication and Distributed Systems Seminar on :

LTE Security

By Anukriti Shrimal
May 09, 2016

LTE network with interfaces



Contents

- LTE Security : Why, What, How
- EPS Architecture
- Design Decisions
- AKA Procedure & Key Hierarchy
- UE Endpoint Security (NAS and AS signalling)
- Base-station Security
- Emergency Call Handling

Why :Threats against EPS

- User Privacy & Identity
- UE tracking
- Handovers.
- Base stations and last-mile transport links.
- Multicast or broadcast signalling.
- Denial of service (DoS).
- Misusing network services.
- Radio protocols.
- Mobility management.
- Manipulation of control plane data.
- Unauthorized access to the network.

These threats have been handled by the guidelines provided by 3GPP standards.

What : High-Level Security Requirements in LTE

The high-level security requirements of can be summarized as follows.

- (H-1) EPS shall provide a high level of security.
- (H-2) Any security lapse in one access technology must not compromise other accesses.
- (H-3) EPS should provide protection against threats and attacks.
- (H-4) EPS shall support authenticity of information between the terminal and the network.
- (H-5) Appropriate traffic protection measures should be provided.
- (H-6) EPS shall ensure that unauthorized users cannot establish communications through the system.

Service-Related Security Requirements in LTE

The more service-related security requirements of can be summarized as follows.

- (S-1) EPS shall allow a network to hide its internal structure from the terminal.
- (S-2) Security policies shall be under home operator control.
- (S-3) Security solutions should not interfere with service delivery or handovers in a way noticeable by end users.
- (S-4) EPS shall provide support for lawful interception.
- (S-5) Rel-99 (or newer) USIM is required for authentication of the user towards EPS.
- (S-6) USIM shall not be required for re-authentication in handovers (or other changes) between EPS and other 3GPP systems, unless requested by the operator.
- (S-7) EPS shall support IP Multimedia Subsystem (IMS) emergency calls (ECs).

Privacy-Related Security Requirements in LTE

The privacy-related requirements can be summarized as follows:

• (P-1) EPS shall provide several appropriate levels of user privacy for communication, location and identity.

• (P-2) Communication contents, origin and destination shall be protected against disclosure to unauthorized parties.

• (P-3) EPS shall be able to hide user identities from unauthorized parties.

• (P-4) EPS shall be able to hide user location from unauthorized parties, including another party with which the user is communicating.

How : EPS Security Features

UNIVERSITÄT BERN

1. Confidentiality of the User and Device Identities
   - The device identity is sent to the network only after security measures have been activated.
   - Temporary identity (GUTI) is assigned and used for subscriber identity.

2. Authentication between the UE and the Network
   - Two-way authentication, i.e., the network authenticates the user and vice-versa

3. Confidentiality & Integrity of User and Signalling Data
   - Confidentiality & integrity protection mechanism for signalling data between the UE and the core network is mandatory while for user data, integrity protection is optional.

4. Platform Security of the eNodeB
   - Base station setup and configuration must follow platform security requirements by operator and manufacturer.
   - All keys as well as handling of user and control plane data shall take place inside a secure environment.

5. Emergency Calls
   - Legislation dependent

How : EPS Security Features.. Contd.

6. Interworking Security
   - Security should be maintained when there is a change from one system to another

7. Network Domain Security (NDS)
   - Its purpose is to protect the traffic between network elements using mutual authentication, data confidentiality and integrity.

8. Lawful Interception
   - A controlled exception to the other security features
   - The conditions of interception are a matter of the legislation of the country

9. IMS Security for Voice over LTE
   - IP Multimedia Subsystem(IMS) is an overlay system for LTE/3G which uses SIP for voice calls over IP-based network.

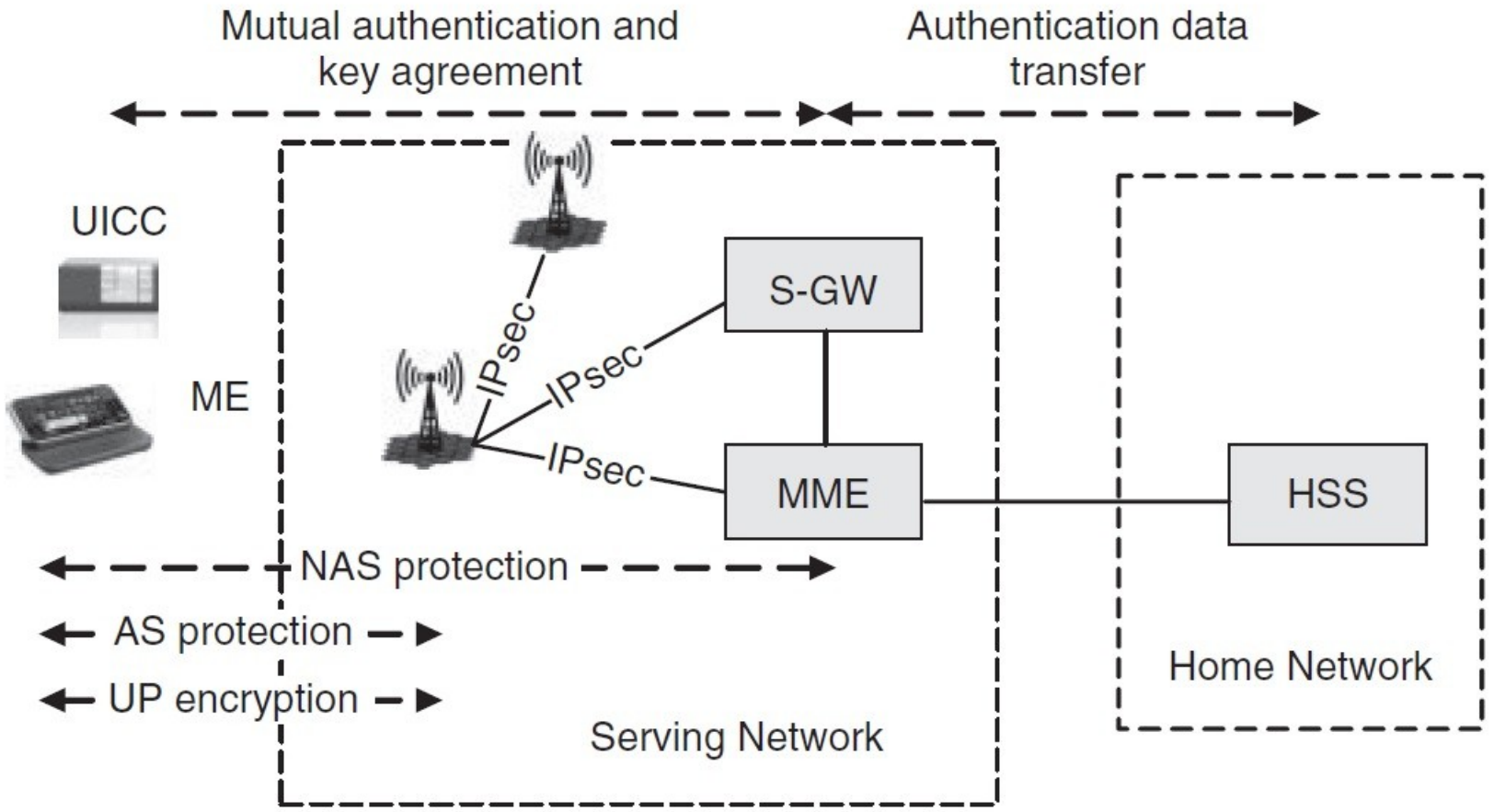
10. Visibility and Configurability of Security
    - Personal Identification Number (PIN)–based access control to the UICC
    - Ciphering indicator to show whether the feature of data confidentiality is applied by the network or not

EPS Security Architecture

EPS security architecture deals with following:

- UE endpoint security :
  - MME triggers the authentication and key agreement (AKA) protocol with the UE to generate K_{ASME}
  - Signalling data between the MME and the UE(NAS) is protected using two derived keys
  - Signalling data between eNB and UE(AS) is protected using two more derived keys from a key sent by MME
  - User plane (UP) data between the eNB and the UE using a third derived key
- S1 Interface security :
  - The signalling data transferred between the UE and the MME over the S1-MME interface can be secured using IPsec
- X2 Interface security :

EPS Security Architecture – Contd.



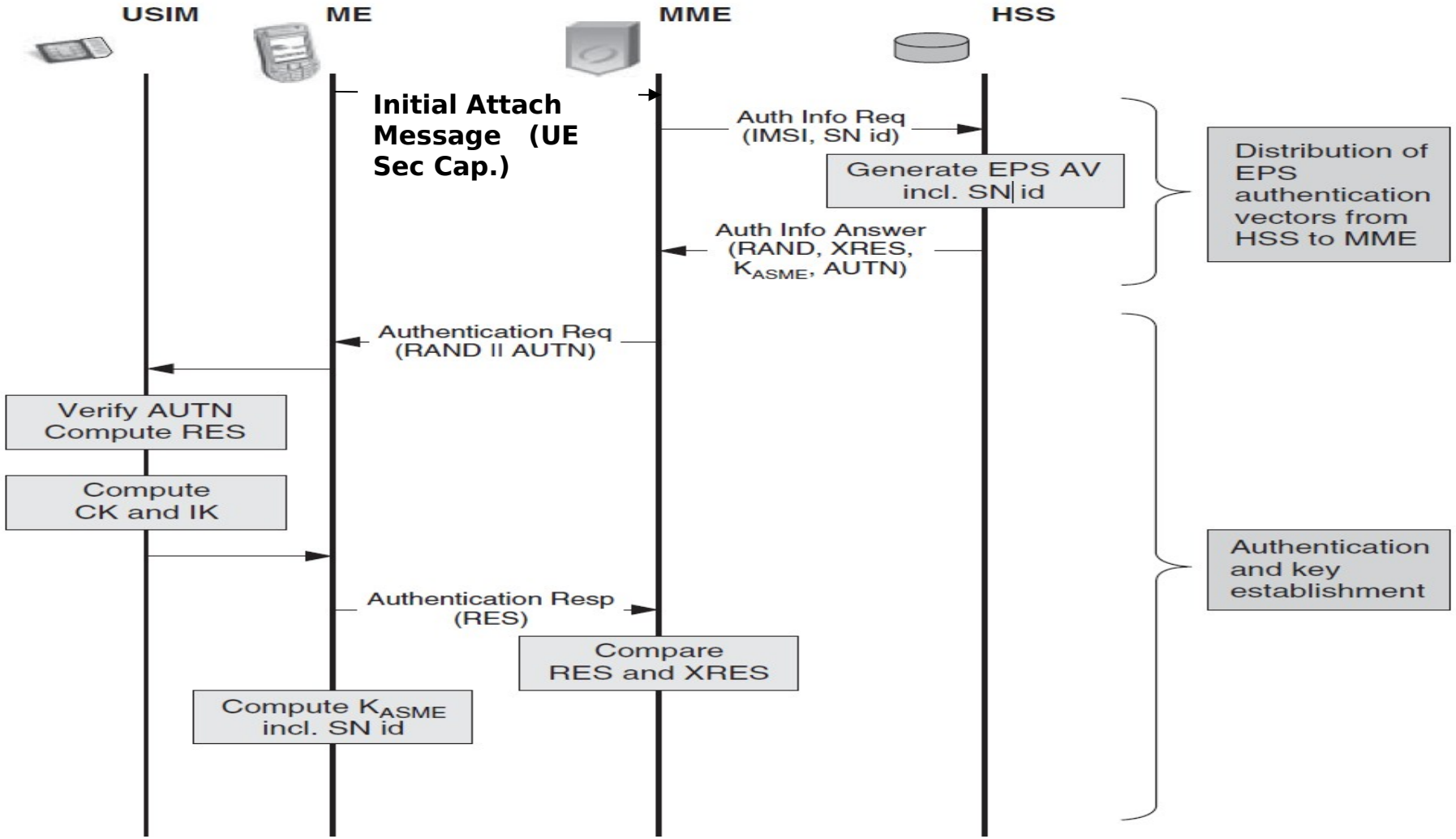
Design Decisions

- Permanent Security Association
  - A permanent key is stored in USIM in UE and also in AuC (HSS). It is never exchanged or visible outside these modules.
- Interfaces between UE and HSS/HLR are completely standardized
  - The interface between the ME and the USIM is fully standardized to allow interoperability
  - AuC is considered part of the HSS
- Reuse of 3G USIMs, but not 2G
  - Authentication & Key agreement (AKA) on EPS is designed to enable reuse of 3G USIMs.
  - 3GPP forbade the use of 3G ME(handset) and 2G SIMs for security advantages.
- Delegated Authentication
  - The actual authentication procedure is done by MME asking information from the HSS
  - The delegation can also happen in a visited network
- Cryptographic Network Separation and Serving Network Authentication
  - Involves binding of any EPS-related cryptographic keys, which leave the HSS, to the identity of the serving network
  - Prevents a spill-over of the effects of the breach to other networks

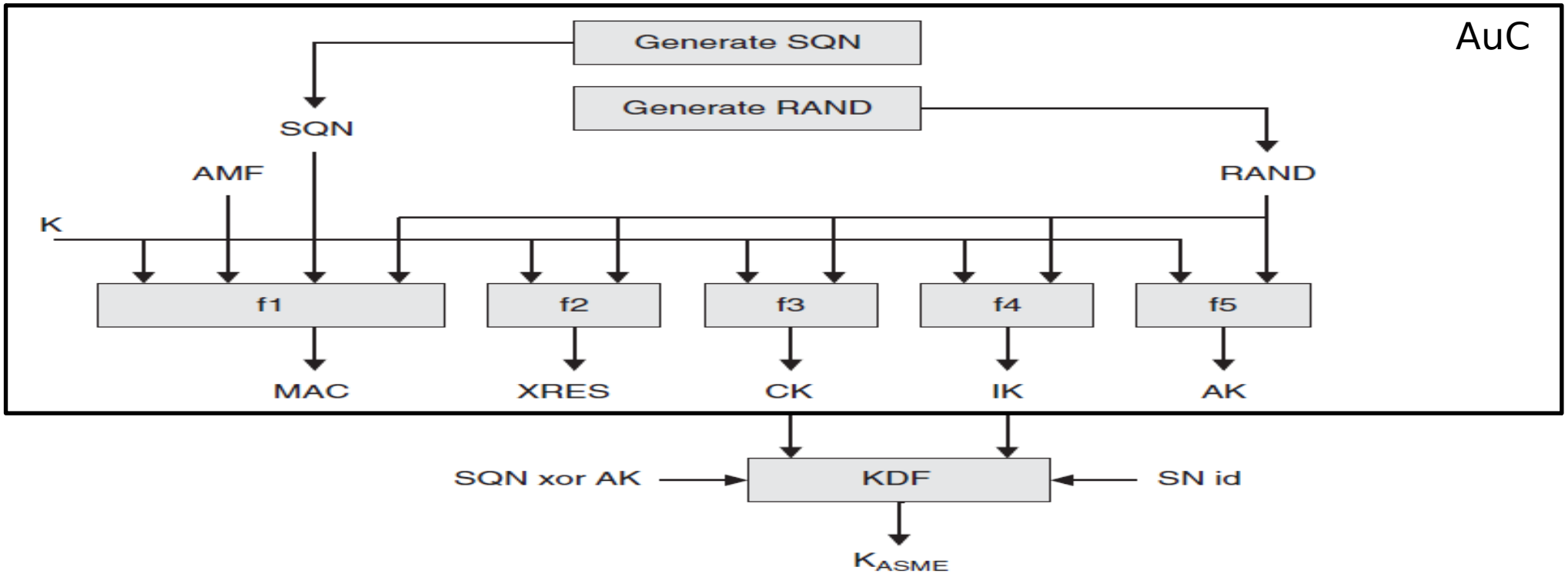
Design Decisions ..Contd.

- Reuse of the Fundamental Elements of UMTS AKA
- Termination Point for Encryption and Integrity Protection Extending from the UE
  - It has been applied in multiple levels with each level having a different end-point
  - User plane security is terminated security at the eNB
  - AS security extends between the UE and the eNB
  - NAS signalling starts from UE and ends at MME.
- Homogeneous Security Concept for Heterogeneous Access Networks
  - EPS provides a framework(EAP) for connecting heterogeneous access networks to the EPC.
  - EAP allows carrying authentication messages over a variety of transports
- New key hierarchy and Key separation in Handovers
  - Introduction of a new local master key K_{ASME} obtained from 3Gs (IK, CK) pair
  - Introduction of intermediate key KeNB given to eNB from MME, and other keys derived from it.
  - During handovers, the key is modified before forwarding to avoid its derivation in the forwarded element.

EPS authentication and key agreement (AKA)



EPS : Generation of UMTS and EPS authentication vectors

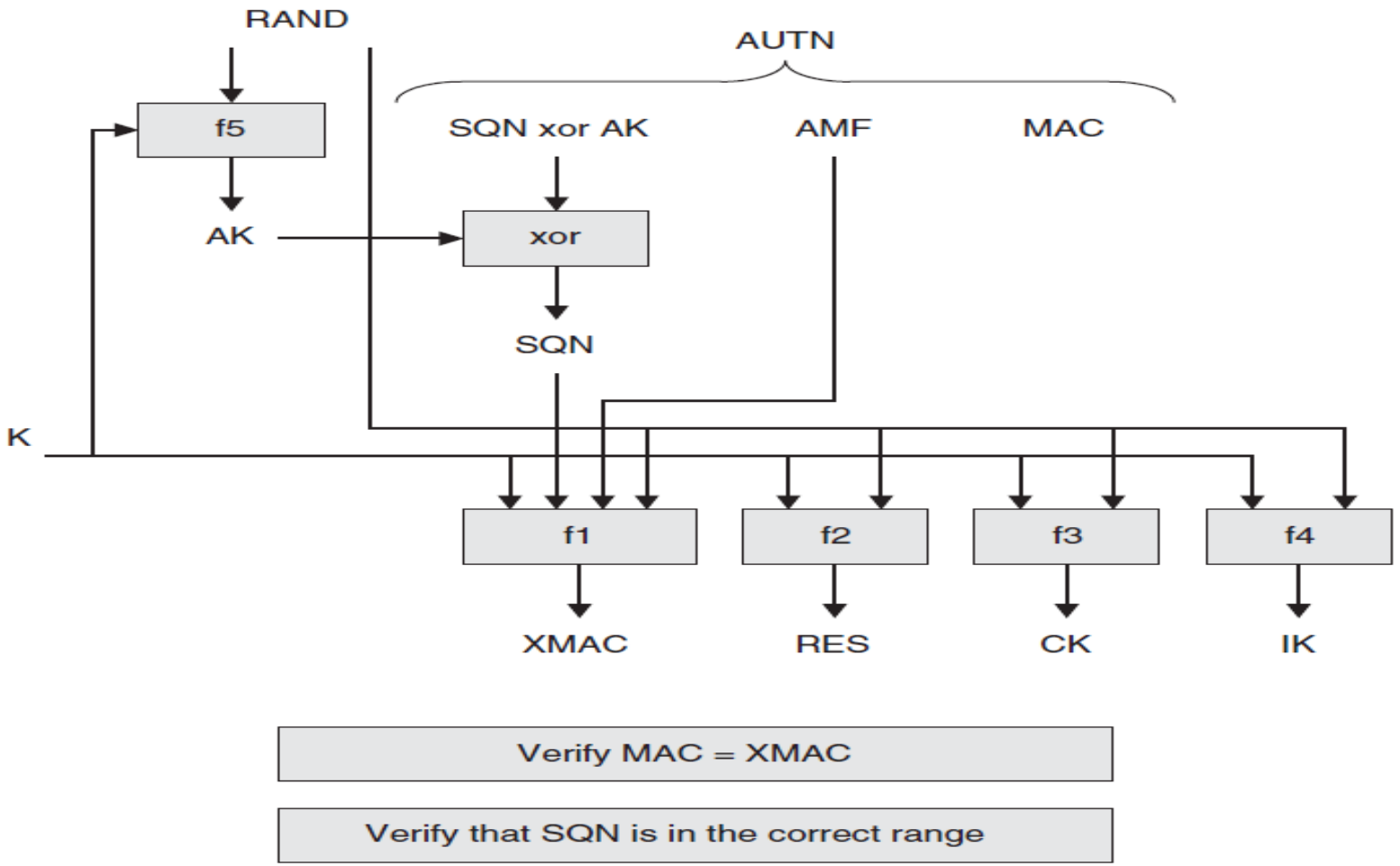


AUTN := SQN xor AK || AMF || MAC

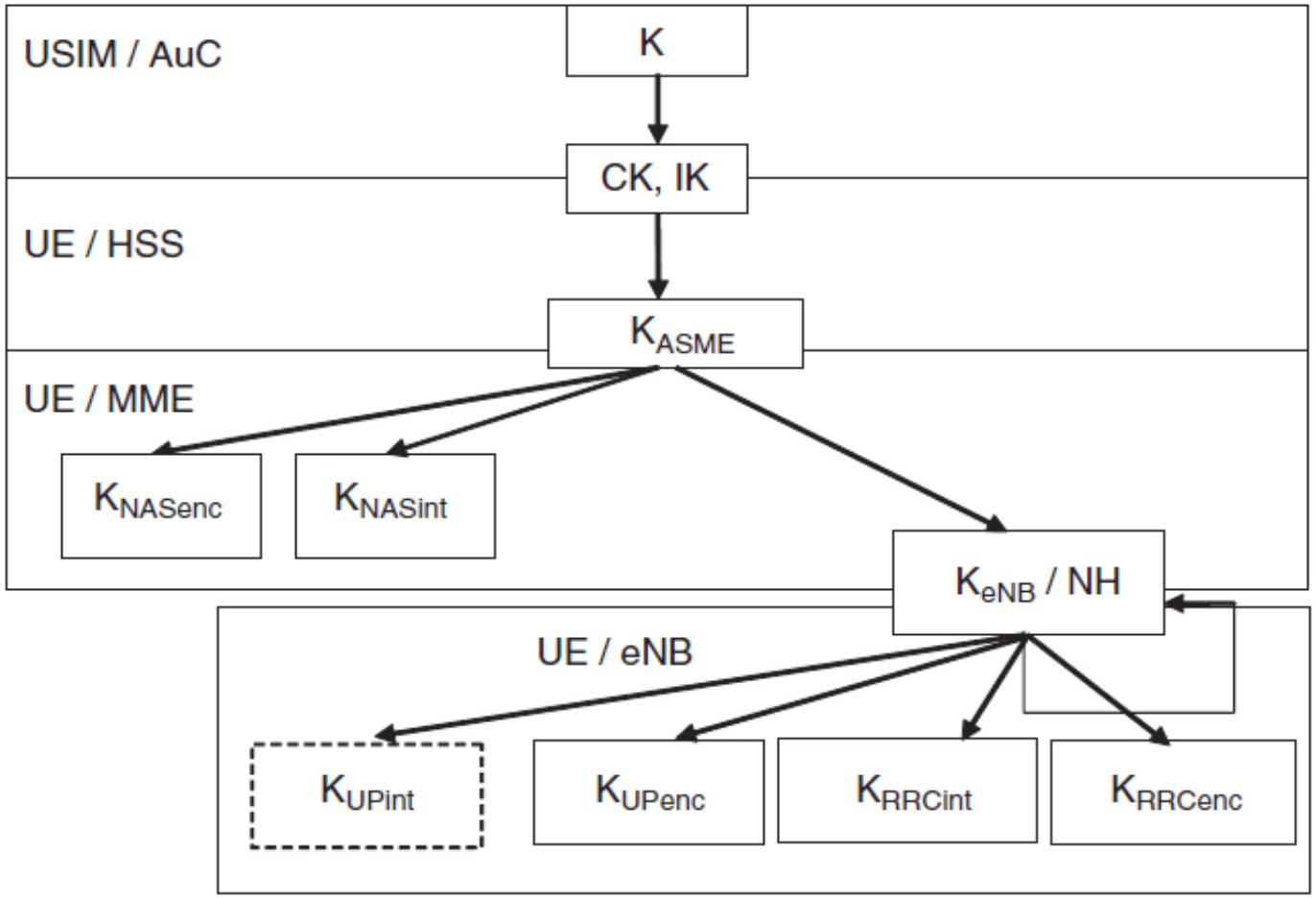
UMTS AV := RAND || XRES || CK || IK || AUTN

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

Verification in the USIM

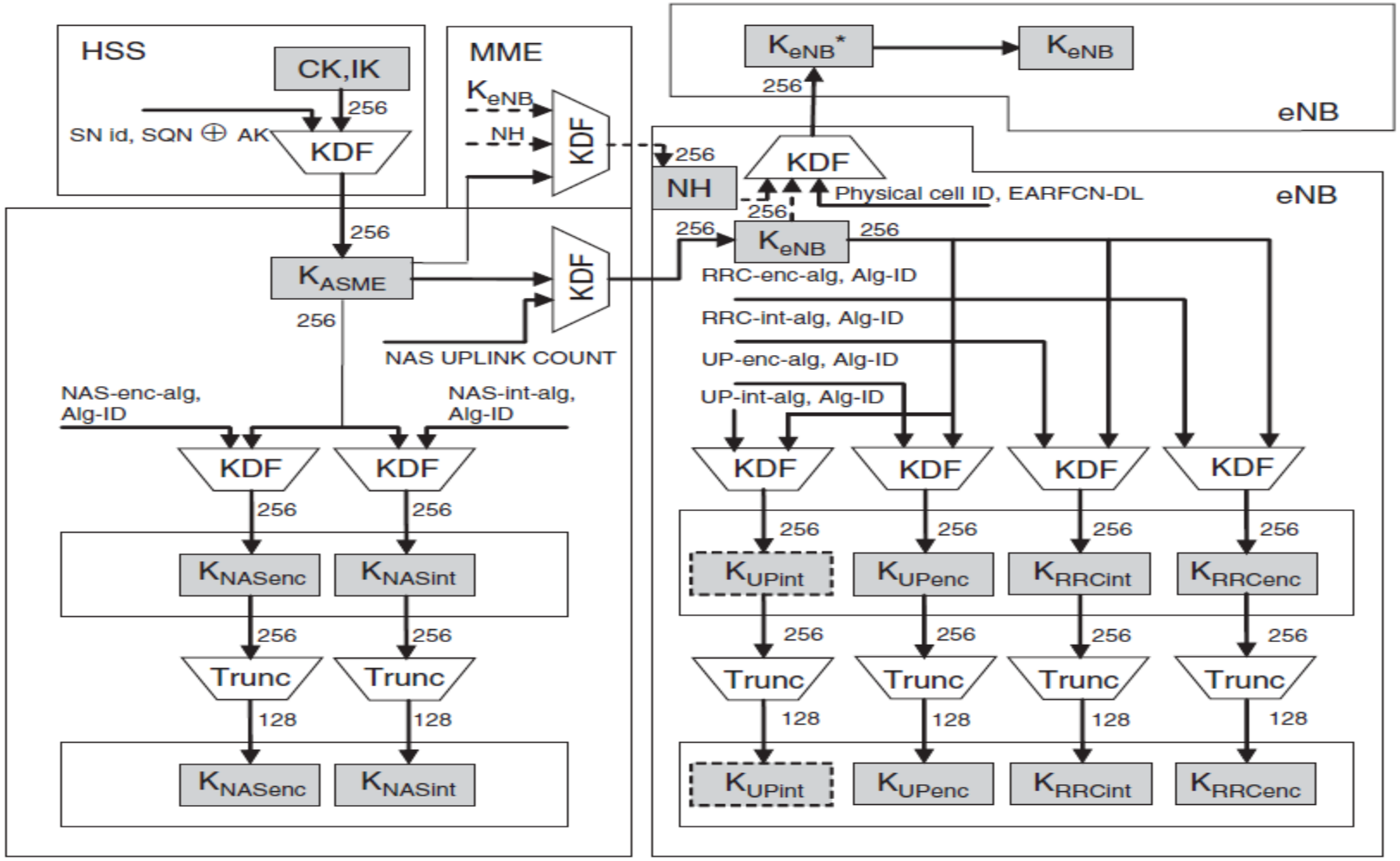


Key Hierarchy

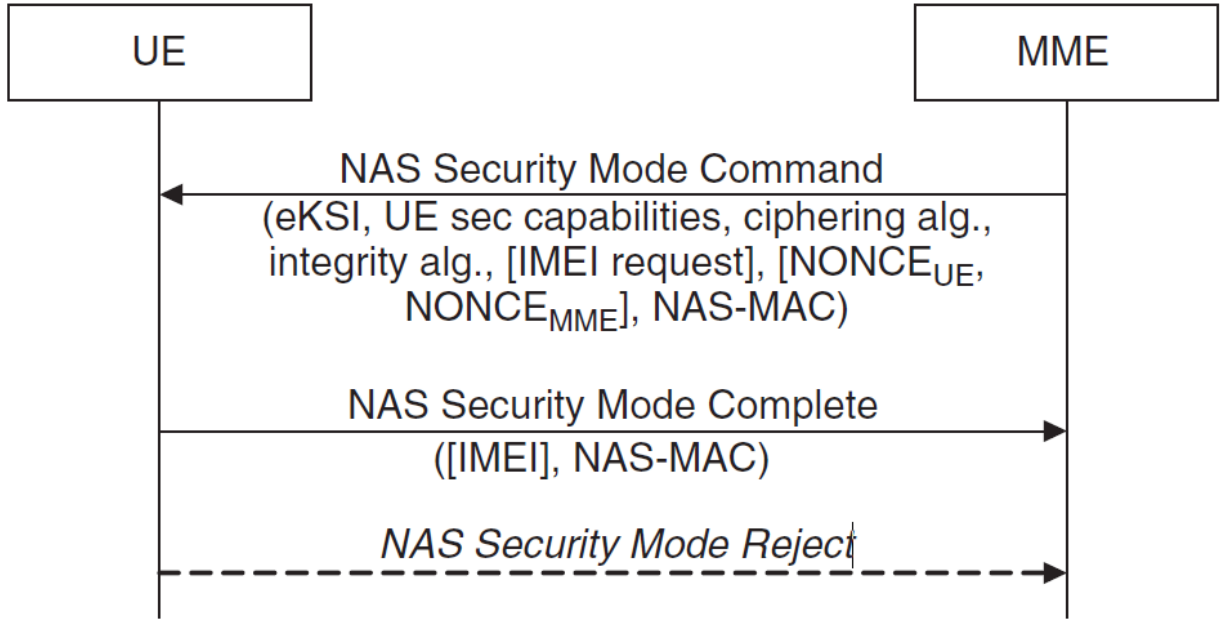


- Each key is generated using the key above it along with some additional parameters.
- The generation functions are one-way, i.e., the key on lower level cannot be used to derive key on higher level.
- All key derivations except the one from K to CK, IK are standardized as they happen outside of USIM.
- All the key derivations carried out in the UE share the same core cryptographic function.

EPS Key Generation



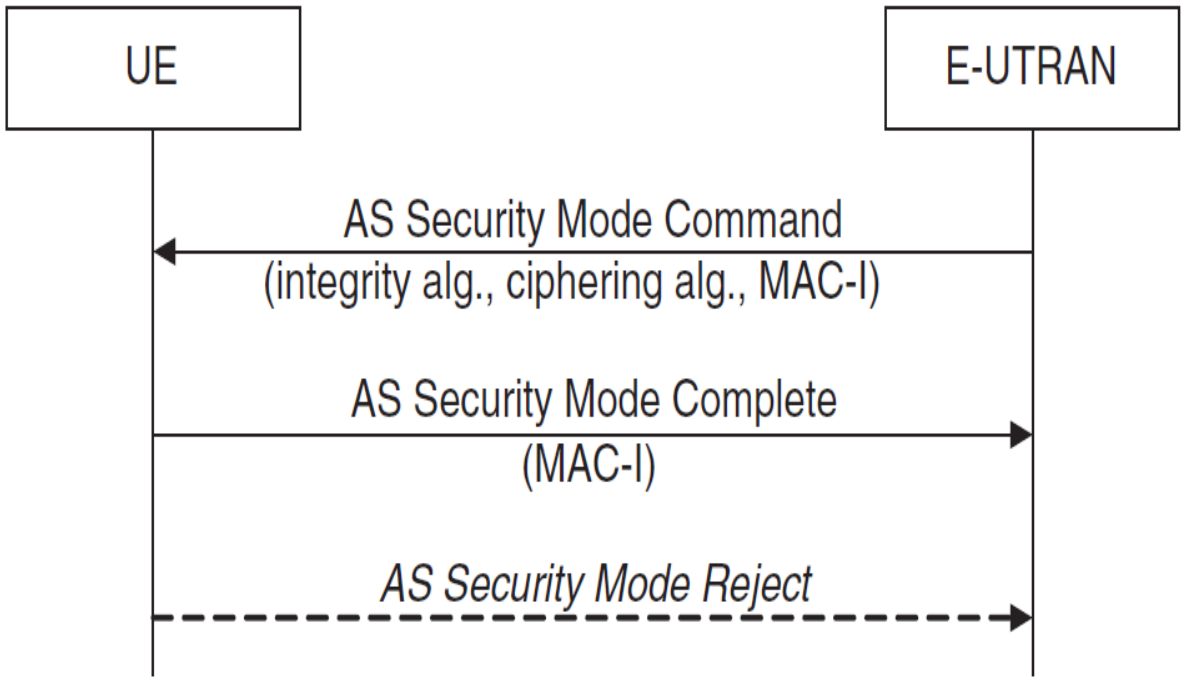
NAS Signalling (Integrity and protection)



NAS Security Mode Command Procedure

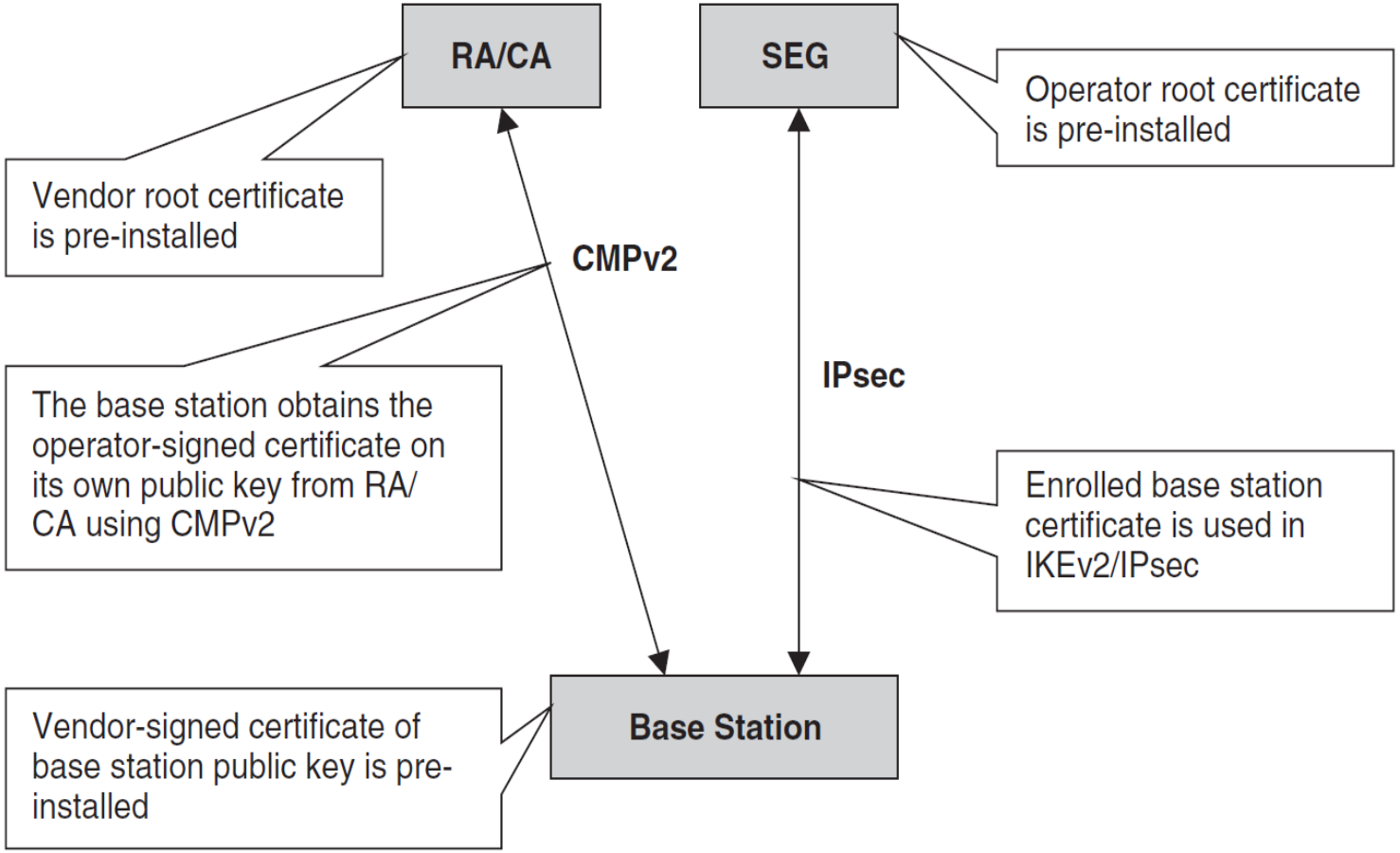
- NAS security command is integrity-protected but not ciphered.
- eKSI (evolved Key Set Identifier) used to identify the K_{ASME}
- The UE can derive the K_{NASenc} and K_{NASint} from K_{ASME}
- Integrity and replay protection for NAS messages is part of the NAS protocol itself.

AS Level / RRC Signalling and User data



- AS Security mode is integrity protected.
- The UE verifies the MAC and replies with Complete/Reject message unciphered.
- Both user-plane data and RRC signalling are carried over PDCP protocol
- AS-level integrity and replay protection is verified both in the UE and in the base station.
- If verification fails at UE, RRC connection re-establishment is used for recovery

Base Station Enrollment Architecture



- Manufacturer provided base-station is installed and connected to the network
- The base station must provide the RA/CA with a proof of possession for the private key
- Certifying Authority (CA):
  - Authenticates & authorize base station
  - Generates/signs certificate for BS
- Integrity & confidentiality carried over Certificate Management Protocol (CMPv2)

Emergency Call Handling - Features

Features of emergency calls:

- Regulations on emergency calls vary between different countries, such as whether unauthenticated emergency calls are permitted or not.
- Regulations of some countries require that it is possible to always make an emergency call with UE, even when there is no valid SIM or USIM.
- A limited service state, is used to describe situations in which a UE cannot obtain normal service but can only be used for emergency purposes.
- A voice solution for EPS is provided by IMS ((IP Multimedia Subsystem) also used in VoLTE
- On the bearer level, there are specific emergency bearers that support IMS emergency sessions.

Emergency Call Handling - Security

Security measures to make normal but still unauthenticated calls:

- UE in limited service state can only use emergency bearers.
- Emergency bearers are limited to an emergency APN and a specific emergency-aware PDN GW.
- This specific PDN GW allows only traffic to and from IMS entities that handle emergency services.
- The P-CSCF on the IMS side checks that all IMS traffic to and from the specific PDN GW is indeed for emergency purposes and selects a suitable E-CSCF for the further handling of the requests, including finding an appropriate PSAP for the session.

Open issues/topics

- Security during mobility
- Ciphering and encryption algorithms
  - Null Algorithms
  - Ciphering algorithms : AES, UEA1, UEA2 (based on SNOW)
  - Intergrity algorithms : 128-EIA1, 128EIA2
- Interworking with GSM and 3G networks
  - The keys are designed to be backward compatible
  - Systems are designed to be able to differentiate the mode of operation.
- Security for Voice over LTE
  - SIP authentication
  - IMS AKA procedure

References

- **LTE Security, Second Edition By** Dan Forsberg, Günther Horn, Wolf-Dietrich Moeller, Valtteri Niemi
  http://onlinelibrary.wiley.com/book/10.1002/9781118380642

- **http://www.3gpp.org/DynaReport/33102.htm**

- **Lectures on LTE by Dr. Braun**

THANK YOU!

Questions?