World Class Standards

3GPP security hot topics: LTE/SAE and Home (e)NB

Valtteri Niemi
3GPP SA3 (Security) chairman
Nokia Research Center, Lausanne, Switzerland

Marc Blommaert
3GPP LTE/SAE security rapporteur
Devoteam Telecom & Media, Herentals, Belgium

4th ETSI Security Workshop - Sophia-Antipolis, 13-14 January 2009

Outline

- Some history and background
- SAE/LTE security: some highlights
- Home (e)NodeB security
- Summary

Some history and background

Some history (1/2)

- For 3GPP Release 99 (frozen 2000), WG SA3 created 19 new specifications, e.g.
  - TS 33.102 “3G security; Security architecture”
  - 5 specifications (out of these 19) originated by ETSI SAGE, e.g. TS 35.202 “KASUMI specification”
- For Release 4 (frozen 2001), SA3 was kept busy with GERAN security while ETSI SAGE originated again 5 new specifications, e.g.
  - TS 35.205-208 for MILENAGE algorithm set
- Release 5 (frozen 2002): SA3 added 3 new specifications, e.g.:
  - TS 33.203 “IMS security”
  - TS 33.210 “Network domain security: IP layer”

Some history (2/2)

- Release 6 (frozen 2005): SA3 added 17 new specifications, e.g.:
  - TS 33.246 “Security of MBMS”
  - TS 33.220-222 “Generic Authentication Architecture”
- Release 7 (frozen 2007): SA3 added 13 new specifications
  - ETSI SAGE created 5 specifications for UEA2 & UIA2 (incl. SNOW 3G spec) (TS 35.215-218, TR 35.919)
- Release 8 (frozen 2008): SA3 has added 5 new specifications, e.g.:
  - TS 33.401 “SAE: Security architecture”
  - TS 33.402 “SAE: Security with non-3GPP accesses”
  - (1-2 more TR’s maybe still be included in Rel-8)

World Class Standards

SAE/LTE security: some highlights

SAE/LTE: What and why?

SAE = System Architecture Evolution

LTE = Long Term Evolution (of radio networks)

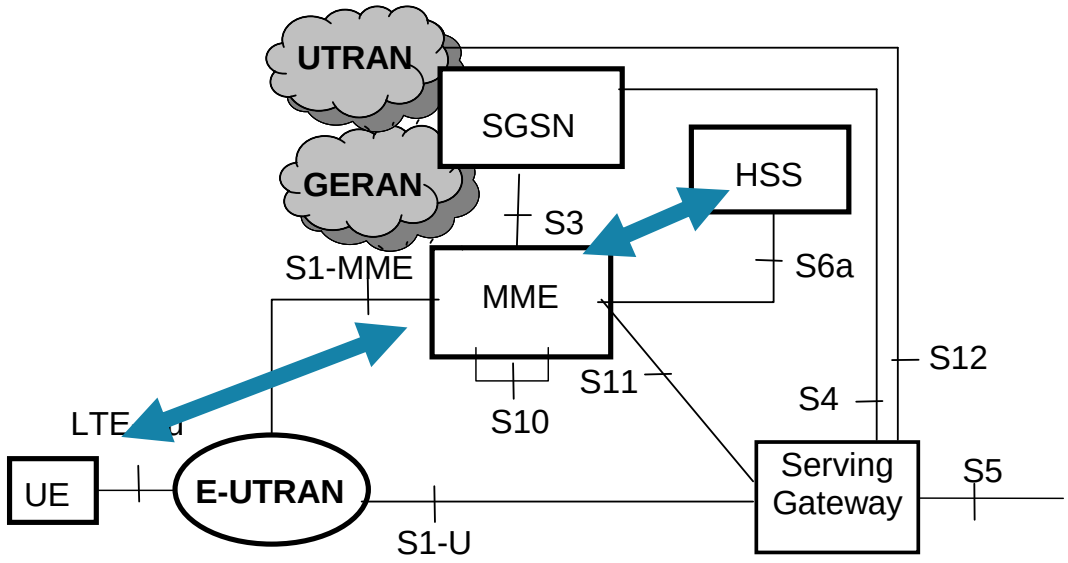
- LTE offers higher data rates, up to 100 Mb/sec
- SAE offers optimized (flat) IP-based architecture

- Technical terms:
  - E-UTRAN = Evolved UTRAN (LTE radio network)
  - EPC = Evolved Packet Core (SAE core network)
  - EPS = Evolved Packet System (= RAN + EPC)

Implications on security

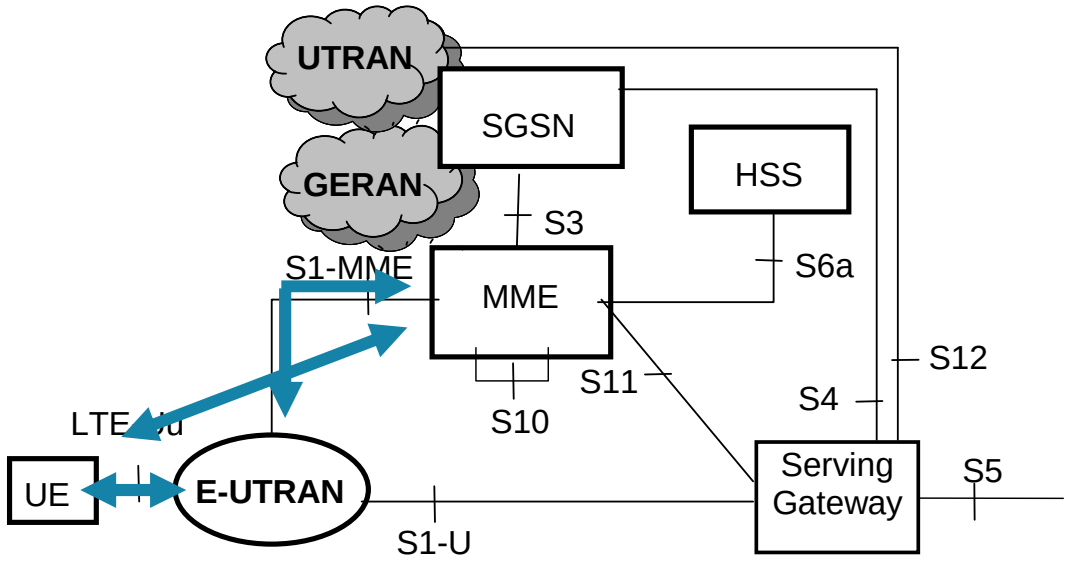
- Flat architecture:
  - All radío access protocols terminate in one node: eNB
  - IP protocols also visible in eNB
- Security implications due to
  - Architectural design decisions
  - Interworking with legacy and non-3GPP networks
  - Allowing eNB placement in untrusted locations
  - New business environments with less trusted networks involved
  - Trying to keep security breaches as local as possible
- As a result (when compared to UTRAN/GERAN):
  - Extended Authentication and Key Agreement
  - More complex key hierarchy
  - More complex interworking security
  - Additional security for eNB (compared to NB/BTS/RNC)

Authentication and key agreement



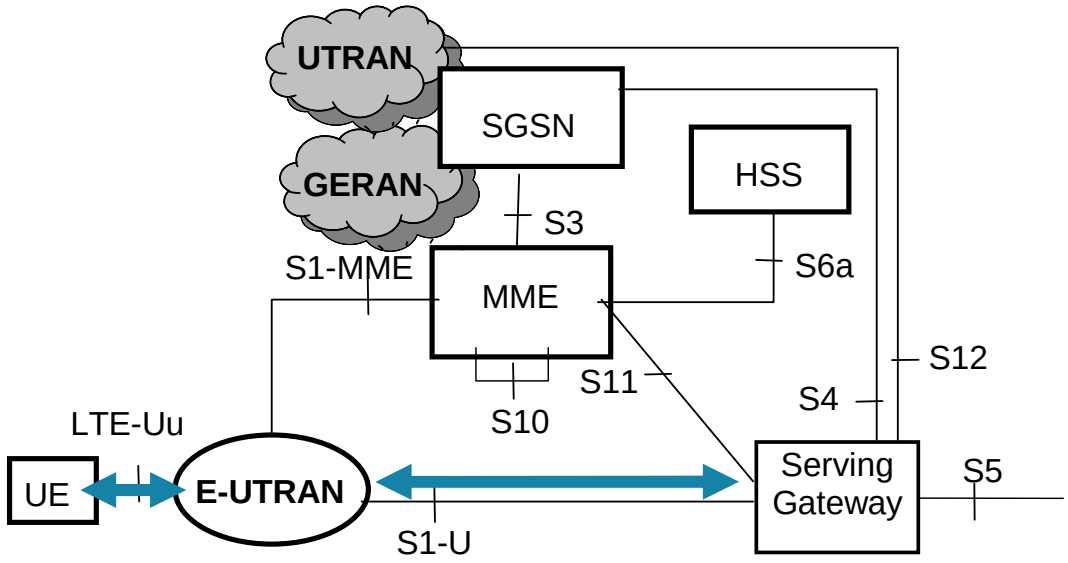
- HSS generates authentication data and provides it to MME
- Challenge-response authentication and key agreement procedure between MME and UE

Confidentiality and integrity of signalling



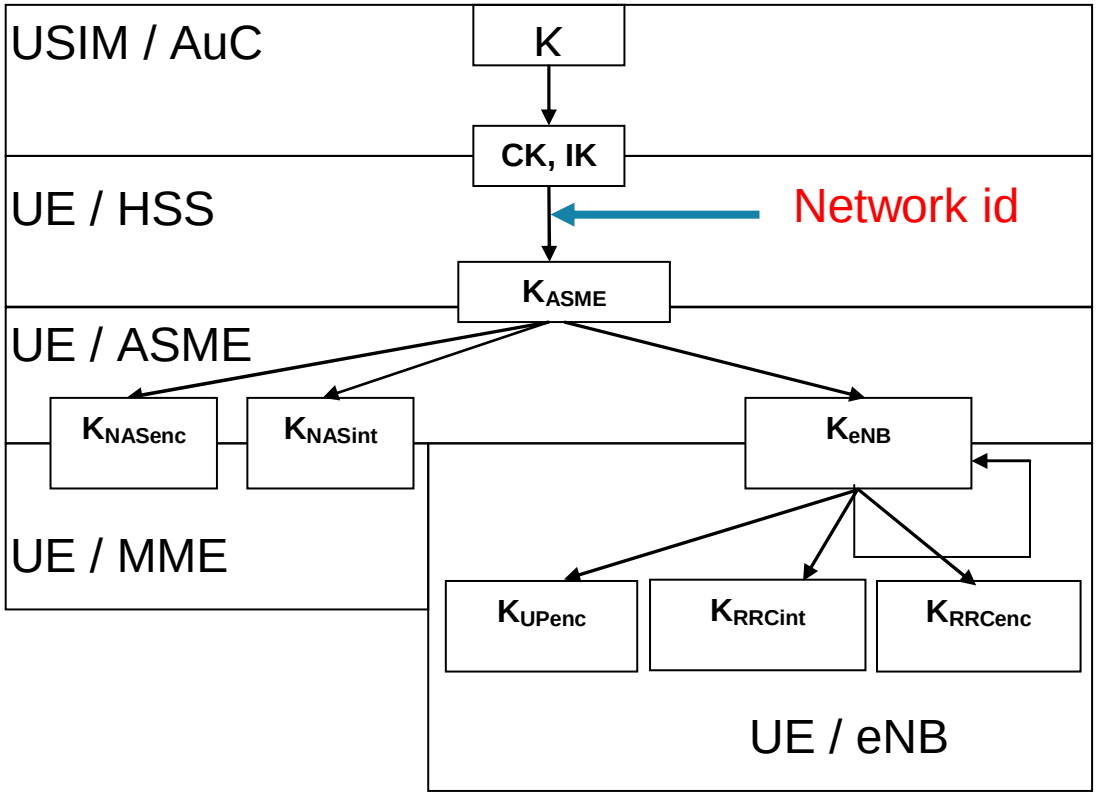
- RRC signalling between UE and E-UTRAN
- NAS signalling between UE and MME
- S1 interface signalling
  - protection is not UE-specific
  - optional to use

User plane confidentiality



- S1-U protection is not UE-specific
  - (Enhanced) network domain security mechanisms (based on IPsec)
  - Optional to use
- Integrity is not protected for various reasons, e.g.:
  - performance
  - limited protection for application layer

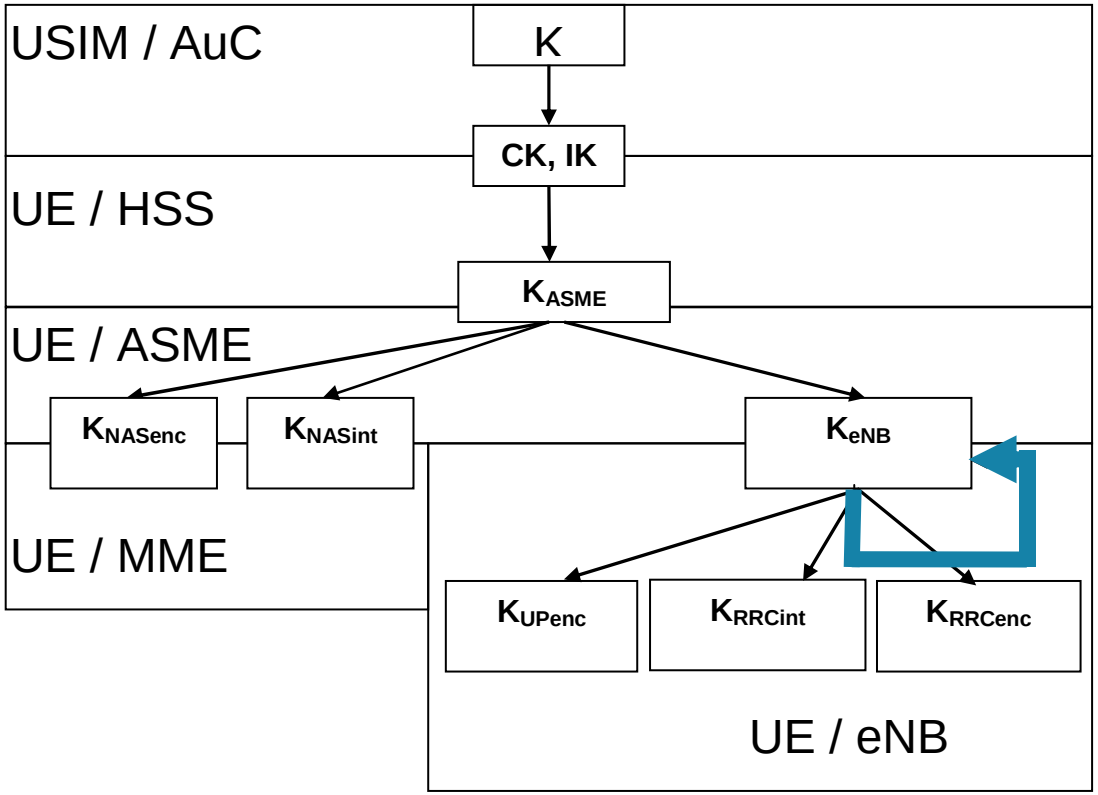
Cryptographic network separation (1/2)



Cryptographic network separation (2/2)

- Authentication vectors are specific to the serving network
  - → AV's usable in UTRAN/GERAN cannot be used in EPS
- AV's usable for UTRAN/GERAN access cannot be used for E-UTRAN access
  - Solution by a "separation bit" in AMF field
- On the other hand, Rel-99 USIM is sufficient for EPS access
  - → ME has to check the "separation bit" (when accessing E-UTRAN)
- As one consequence, "EAP-AKA' " was created in IETF

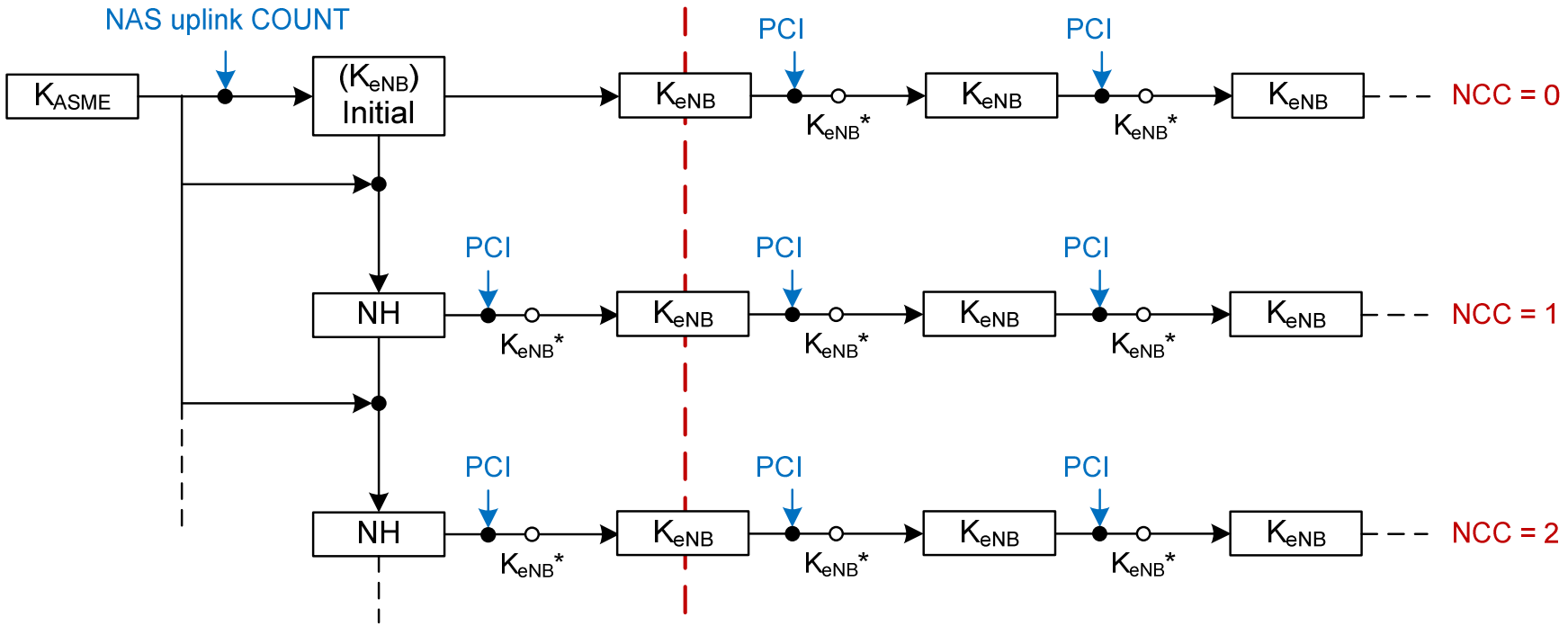
Handovers without MME involvement (1/2)



Handovers without MME involvement (2/2)

- Handovers are possible directly between eNB's for performance reasons
- If keys would be passed as such, all eNB's in a "HO chain" would know all the keys → one compromised eNB would compromise all eNB's in the "HO chain"
- Countermeasures:
  - One-way function used before key is passed (***Backward security***)
  - MME is involved after the HO for further key passes (***Forward security***, effective after two hops)
  - When MME involved already during the HO, Forward security is effective already after one hop

K_{eNB} derivations



Interworking with UTRAN/GERAN (1/2)

- UE may be registered in both SGSN and MME simultaneously

  → when moving from one system (*source*) to the other (*target*)

  both

  cached keys (created earlier in the *target* system)

  and

  mapped keys (converted from the keys in the *source* system)

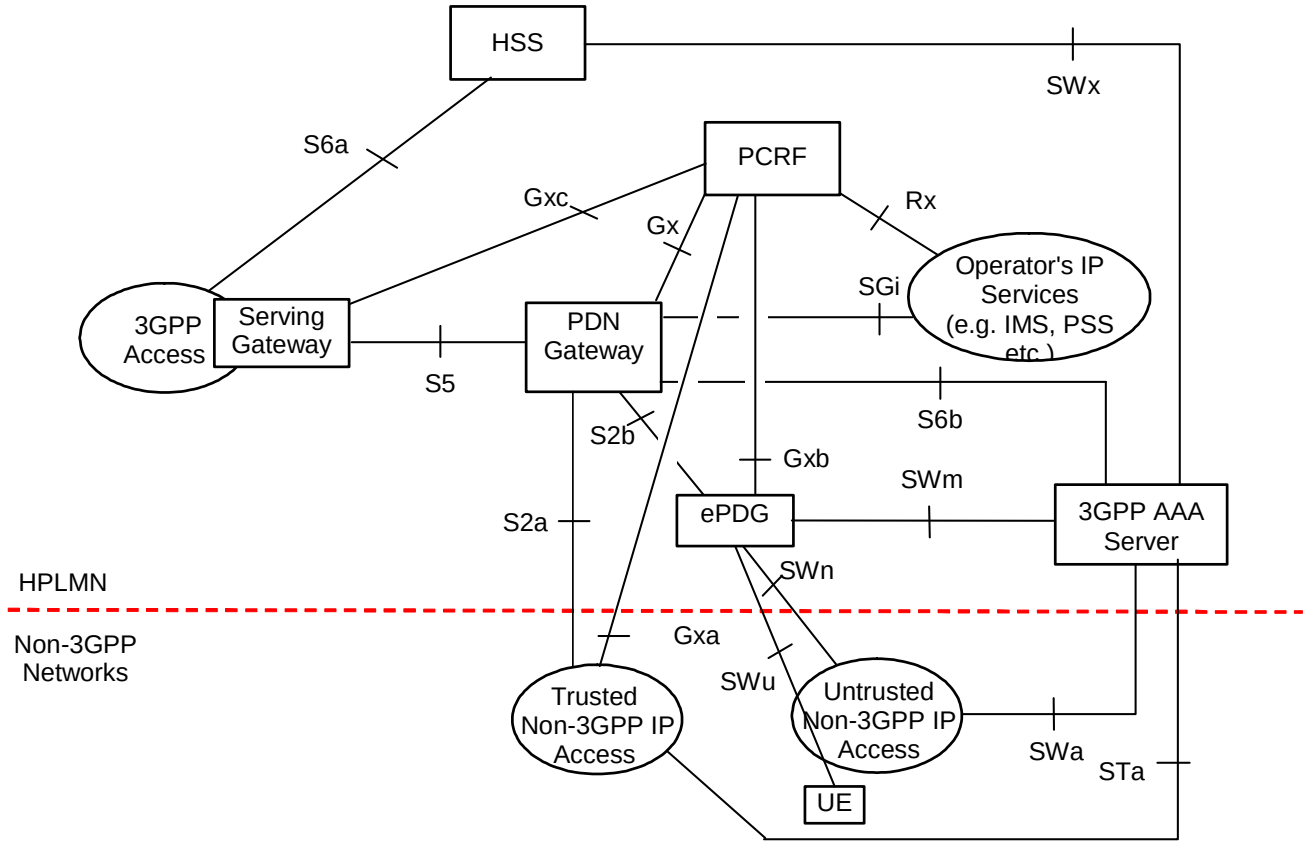
  may exist

  - Note: cached keys only for Rel-8 SGSN, not for legacy SGSN

Interworking with UTRAN/GERAN (2/2)

- **Idle mode transition**
  - From E-UTRAN to UTRAN: either *mapped* or *cached* keys are used (depending on the identity used in *Routing Area Update Request*)
  - From UTRAN to E-UTRAN: *cached* keys are used *but* an exceptional case exists also
- **Handover**
  - From E-UTRAN to UTRAN: *mapped* keys are used
  - From UTRAN to E-UTRAN: *mapped* keys are used *but* it is possible to activate the *cached* keys after HO completed (using *key-change-on-the-fly* procedure)

Inter-working with non-3GPP networks (1/2)



Extract from TS 23.402 (one of several architecture figures)

Inter-working with non-3GPP networks (2/2)

- Three options for mobility between 3GPP and non-3GPP networks:
  - Proxy Mobile IP: no user-specific security associations between the Proxy and Home Agent
  - Client MIPv4: tailor-made security mechanisms are used
  - Dual Stack MIPv6: IPsec with IKEv2 is used between UE and HA
- IPsec tunnel (with evolved Packet Data Gateway) is used in case the non-3GPP network is untrusted by the operator (of EPS network)
- Authentication is run by EAP-AKA or EAP-AKA' procedures, in both cases based on USIM

Home (e) Node B security

Home (e)NB architecture

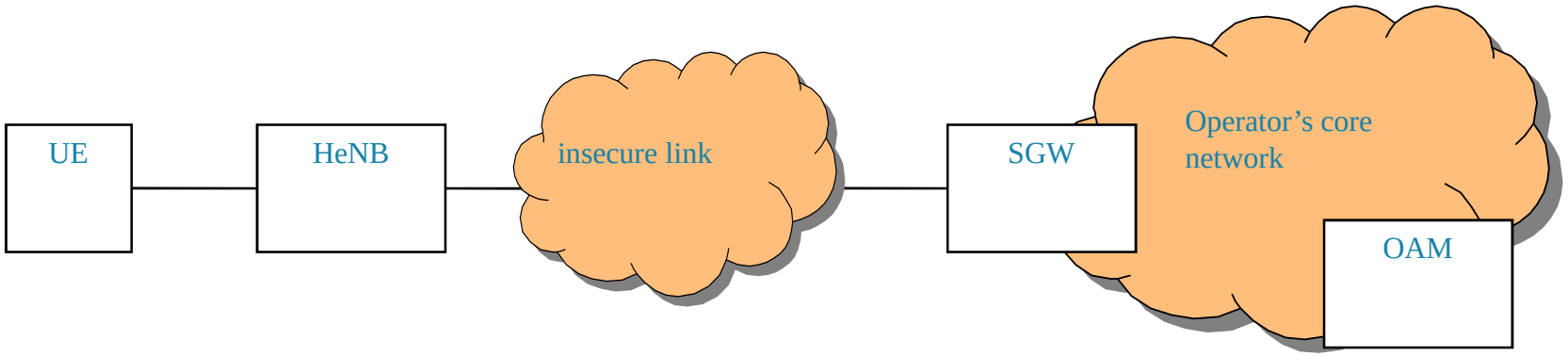


Figure from draft TR 33.820

One of the key concepts: *Closed Subscriber Group*

Note: Rest of the talk: Home (e)NB denoted by HeNB

Threats

- Compromise of HeNB credentials
  - e.g. cloning of credentials
- Physical attacks on HeNB
  - e.g. physical tampering
- Configuration attacks on HeNB
  - e.g. fraudulent software updates
- Protocol attacks on HeNB
  - e.g. man-in-the-middle attacks
- Attacks against the core network
  - e.g. Denial of service
- Attacks against user data and identity privacy
  - e.g. by eavesdropping
- Attacks against radio resources and management

Several sources of Security Requirements

- (Additional) requirements for eNB due to SAE/LTE security architecture (TS 33.401)
- Requirements stemming from threats due to home placement (TR 33.820)
- Requirements due to *Closed Subscriber Group* concept

Countermeasures

- Mutual authentication between the HeNB and the (rest of) network
- Security tunnel establishment for backhaul link
- *Trusted Environment* inside HeNB
  - e.g. secure execution
- Access Control mechanisms (for Closed Subscriber Groups)
- Security mechanisms for OAM
- *Hosting party* authentication (if used) with *Hosting Party Module*
- *etc..*

Summary

Summary

- SAE/LTE security
  - New architecture and business environment require enhancements to 3G security
  - Radio interface user plane security terminates in base station site
  - Cryptographic separation of keys
  - Forward/backward security in handovers
  - Different security mechanisms in many inter-working cases with both 3GPP and non-3GPP access networks
- Home (e)NB security
  - New architecture with more exposed locations of NB's
  - New types of threats
  - Many new countermeasures needed

For more information:

www.3gpp.org