World Class Standards

3GPP Security: LTE/SAE and Home (e)NB

Charles Brookson
ETSI OCG Security Chairman

with special thanks to

Valtteri Niemi
Nokia Corporation
3GPP SA3 Security Chairman

Dionisio Zumerle
ETSI
3GPP SA3 Security Secretary

Introduction

- 3GPP SA Working Group 3 (3GPP SA3)
  - specifying security mechanisms and functions
  - in 3G UMTS, SAE/LTE systems and beyond
- ETSI: one of the founding Standards Developing Organizations of 3GPP
- ETSI OCG Security: transversal security co-ordination ad hoc group of ETSI

SAE/LTE security

SAE/LTE implications on security

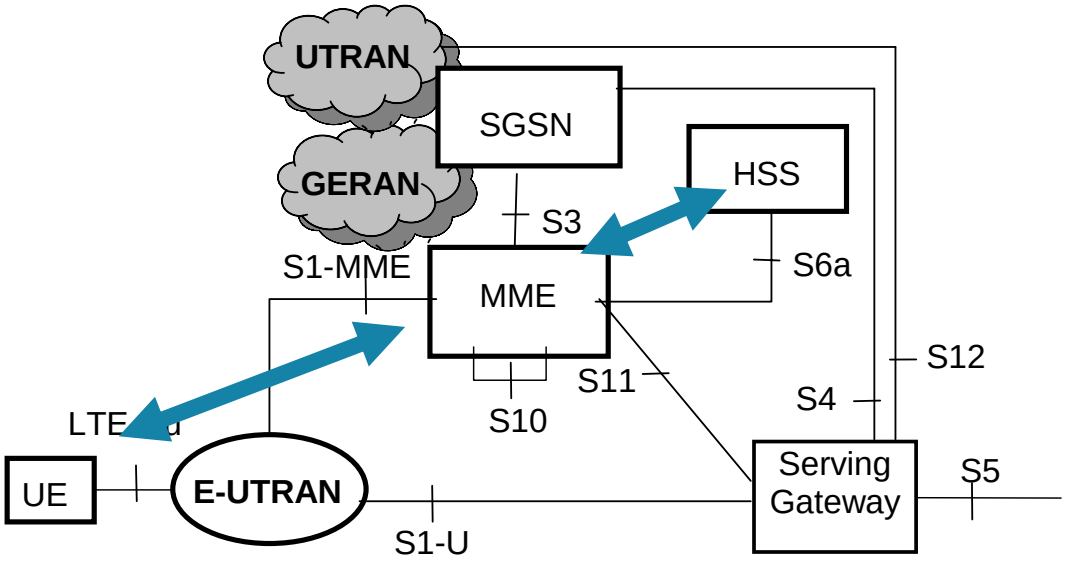
- Security implications due to
  - *Flat architecture*: RAN protocols terminate in eNB
  - Interworking with legacy and non-3GPP networks
  - Allowing eNB placement in untrusted locations
  - New business environments with less trusted networks involved
  - Trying to keep security breaches as local as possible

- Extended Authentication and Key Agreement
- More complex key hierarchy
- More complex interworking security
- Additional security for eNB (compared to NB/BTS/RNC)

Security functions

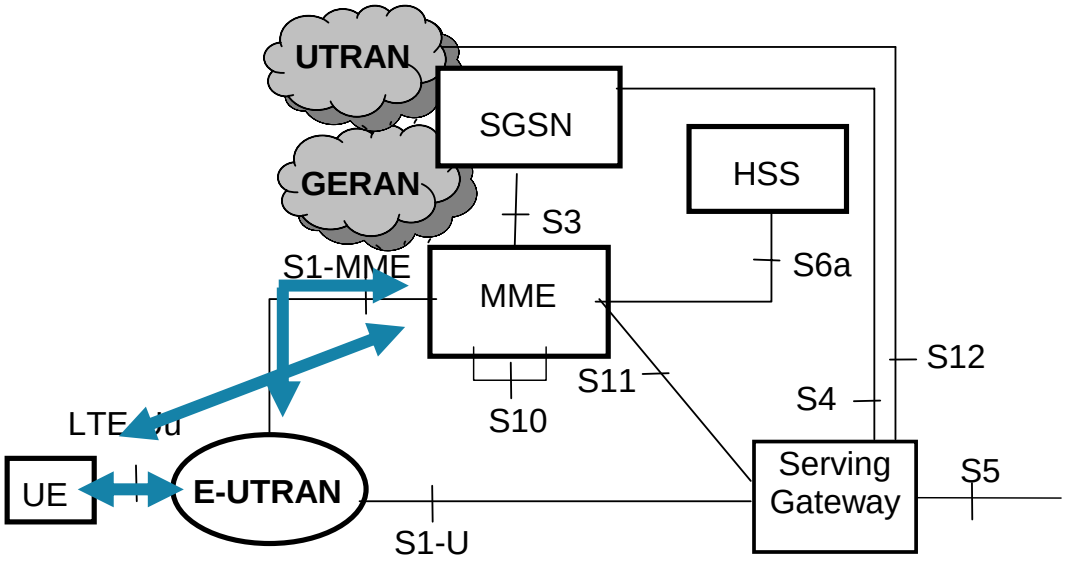
- Authentication and key agreement
  - UMTS AKA re-used for SAE
  - SIM access to LTE is explicitly excluded (USIM R99 onwards allowed)
- Signalling protection
  - For core network (NAS) signalling, integrity and confidentiality protection terminates in MME (Mobility Management Entity)
  - For radio network (RRC) signalling, integrity and confidentiality protection terminates in eNodeB
- User plane protection
  - Encryption terminates in eNodeB
  - Separate protection in on network interfaces
- Network domain security used for network internal interfaces

Authentication and key agreement



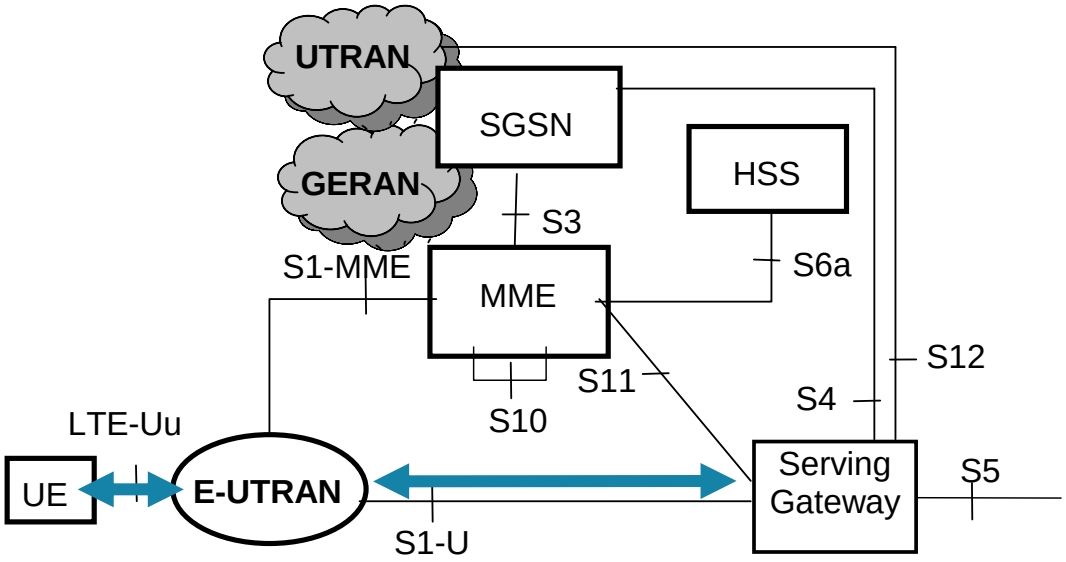
- HSS generates authentication data and provides it to MME
- Challenge-response authentication and key agreement procedure between MME and UE

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

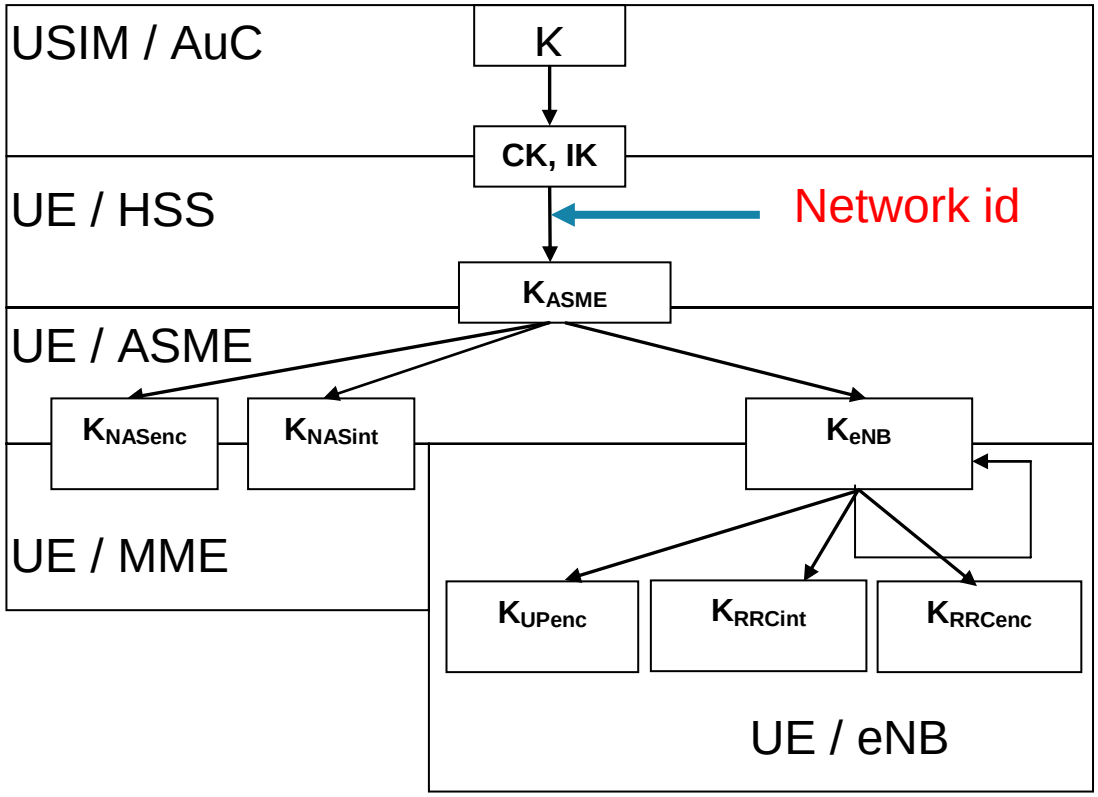


- S1-U protection is not UE-specific
  - (Enhanced) network domain security mechanisms (based on IPsec)
  - Optional to use
- Integrity is not protected for various reasons, e.g.:
  - performance
  - limited protection for application layer

Crypto-Algortitms

- Two sets of algorithms
  - 128-EEA1 and 128-EIA1 (identical to UEA2 and UIA2 for UMTS)
  - AES and SNOW 3G chosen as basis
    - Principle: should be as different from each other as possible
- Rel-99 USIM is sufficient
  - Key length 128 bits
    - included possibility to add 256-bit keys
  - Deeper key hierarchy than UMTS
  - (one-way) key derivation function needed
- Public and open
  - Can be downloaded to look at
  - Available from ETSI web site and GSMA web site

Key hierarchy in LTE/SAE



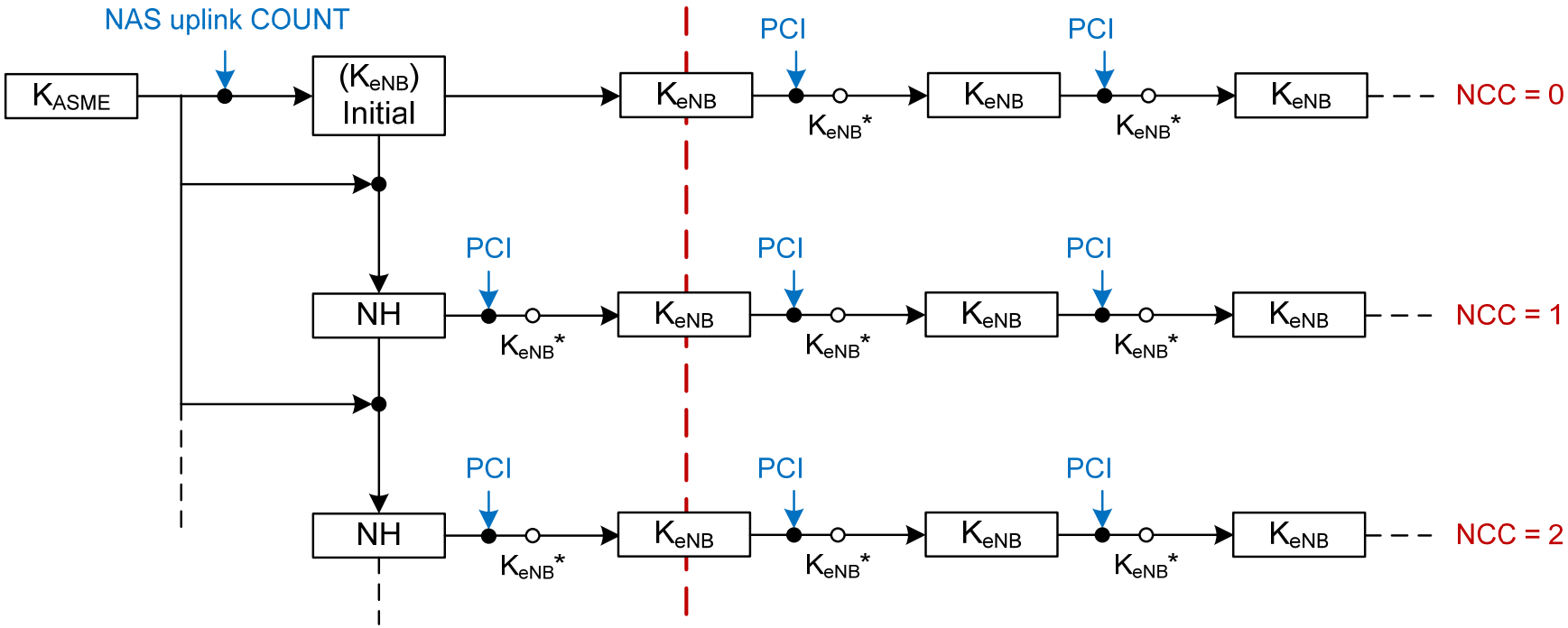
Cryptographic network separation

- 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)
  - → EAP-AKA' created in IETF

Handovers without MME involvement

- 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*

  native content (keys created earlier in the *target* system)

  and

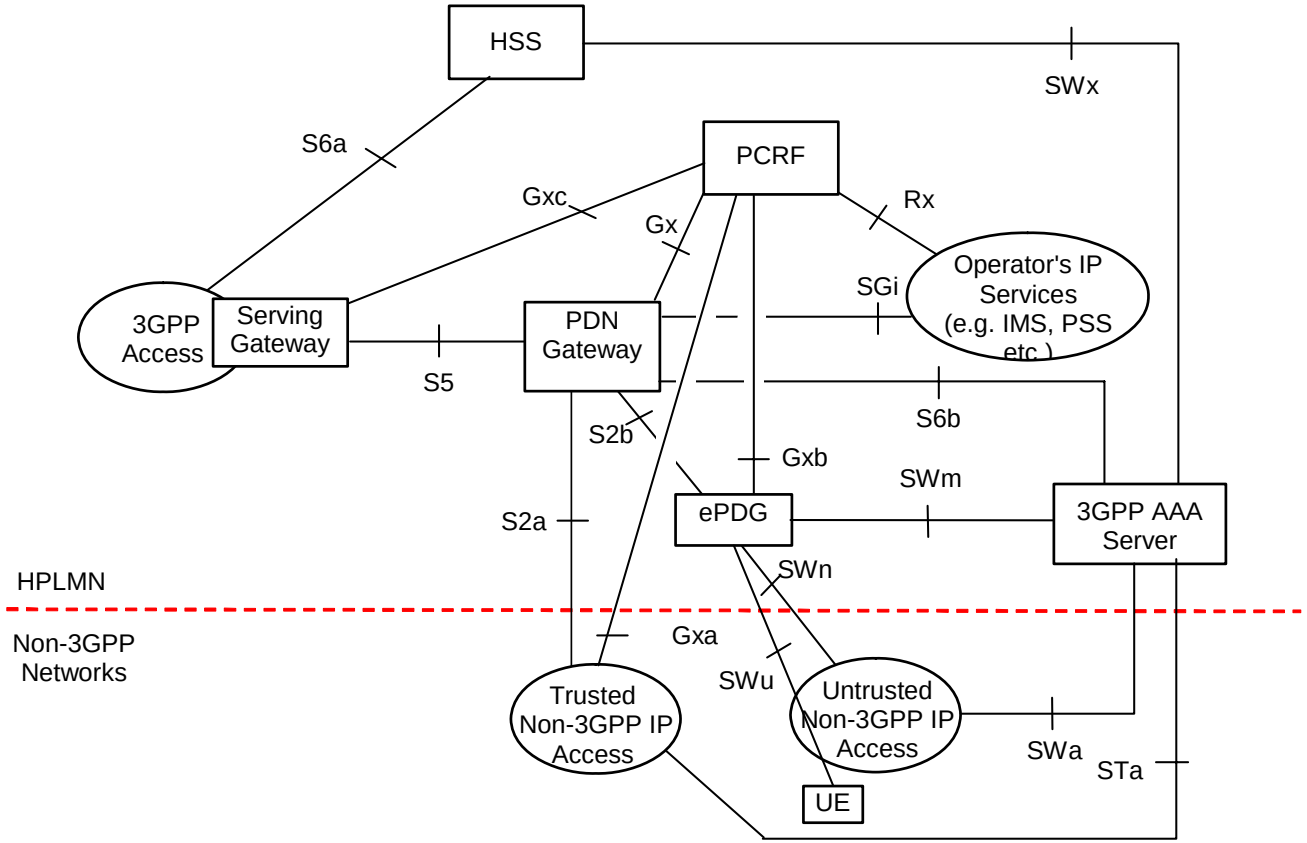
  mapped content (converted from the keys in the *source* system)

  may exist
  - Note: native 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 *native* keys are used (depending on the identity used in *Routing Area Update Request*)
  - From UTRAN to E-UTRAN: *native* 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 *native* 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)

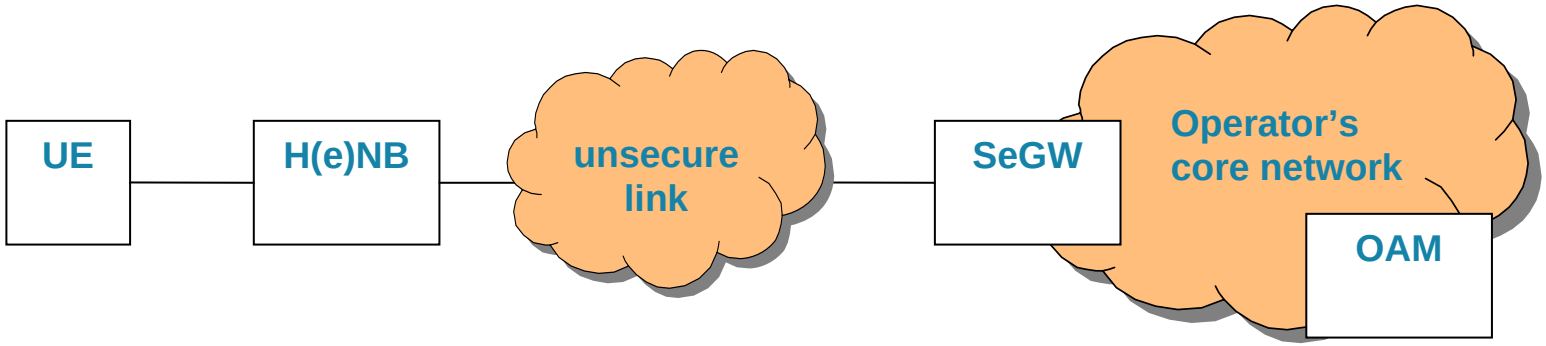
- Three options for mobility between 3GPP and non-3GPP networks:
  - Proxy Mobile IP: no user-specific security associations between the Proxy and Home Agent
  - Client MIPv4: tailor-made security mechanisms are used
  - Dual Stack MIPv6: IPsec with IKEv2 is used between UE and HA
- IPsec tunnel (with 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

H(e)NB Security specification work

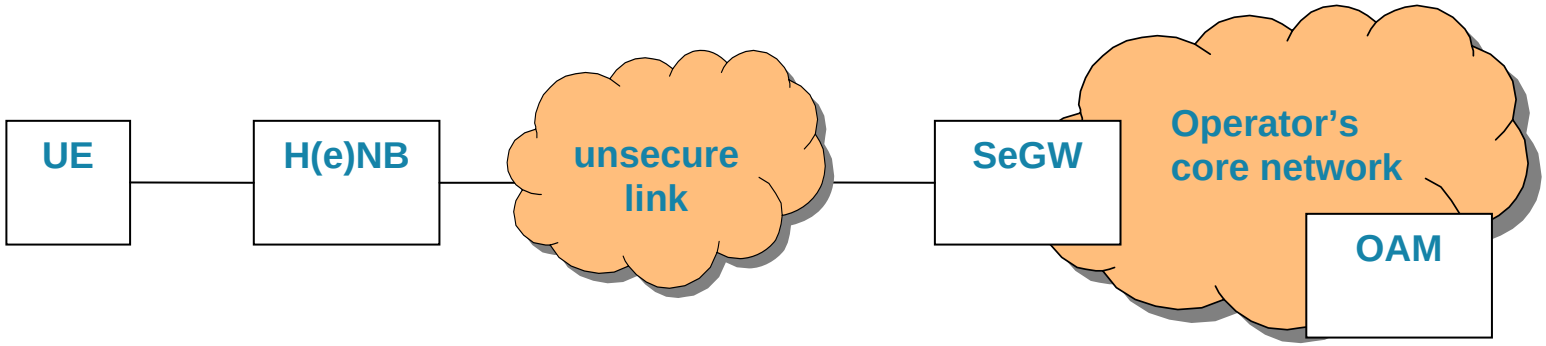
- TR 33.820
  - Technical Report (informative)
  - Approved in March 2009
  - Study on Security of Home (e) Node B
- TS 33.xyz
  - Technical Specification (normative)
  - Currently under development
  - 3GPP Security Aspects of Home NodeB and Home eNodeB

Home (e)NB Security architecture (1/2)



- CSG (Closed Subscriber Group)
  - group of subscribers permitted to access one or more cells of the PLMN with restricted access ("CSG cells")
- Hosting party
  - party hosting H(e)NB and having contract with PLMN operator
- Hosting Party Module (HPM)
  - module holding credentials for authentication of hosting party
- Security Gateway
  - element at the edge of the core network terminating security association(s) for backhaul link between H(e)NB and core network
- Trusted Environment (TrE)
  - logically separate entity and set of functions/resources within H(e)NB
  - trustworthy environment to executesoftware and store sensitive data (e.g. PS keys)

Home (e)NB Security architecture (2/2)



- Air interface between UE and H(e)NB backwards compatible with UTRAN
- H(e)NB access operator's core network via a Security Gateway (SeGW)
  - Backhaul between H(e)NB and SeGW may be unsecure
- SeGW represents operator's core network
  - To perform mutual authentication with H(e)NB
  - Mutual authentication may need support of authentication server or PKI
- Security tunnel established between H(e)NB and SeGW
  - to protect information transmitted in backhaul link
- Secure communication required for OAM

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

All threats addressed by countermeasures in Technical Report 33.820

Authentication

Consists of:

- H(e)NB identity authentication
- Trusted Environment (TrE) identity authentication
- H(e)NB device identity and TrE identity binding
- The H(e)NB integrity verification

Two separate concepts of authentication:

- Mutual authentication of H(e)NB and operator's network (mandatory)
  - H(e)NB Identity authenticated by network
    - credentials stored in TrE in H(e)NB
  - identity of operator's network authenticated by H(e)NB
- Authentication of hosting party by operator's network (optional)
  - credentials contained in a separate Hosting Party Module (HPM) in H(e)NB
  - bundled with the device authentication (one step)
- Authentication either by certificates or EAP-AKA
  - Protocol used: IKEv2

Other security mechanisms

- Device Integrity Check
- Location Locking
  - Location identification (UE reporting/Surrounding Cell or Local)
  - Location authentication and authorization
  - Solutions
    - IP address based
    - Macro-cell/UE reporting based
    - (A)GPS based
    - Combination of the above
- Access Control Mechanism
  - ACL for Pre-R8 UE accessing HNB
  - CSG for H(e)NB
- OAM
  - Hop-by-hop
  - End-to-end
- Clock Synchronization
  - Based on backhaul link between H(e)NB and SeGW
  - Based on security protocol of clock synchronization protocol

Summary and Conclusions

Summary and Conclusions

- 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
  - Device Authentication
    - Solutions based on either EAP-AKA or Certificates adequate for pre-R8 deployments
    - Certificate-based solution, coupled with TrE, is mandatory part of Release 9
  - HPM Authentication
    - Optional to implement and EAP-AKA based
  - Authentication Protocol
    - IKEv2

Thank you!

For more information:

www.etsi.org

www.3gpp.org