3GPP security hot topics: LTE/SAE and Common IMS

Valtteri Niemi

3GPP SA3 (Security) chairman

Nokia Research Center

Outline

- Some history and background
- Common IMS security
- SAE/LTE security
- Summary

Some history and background

Some history 1/2

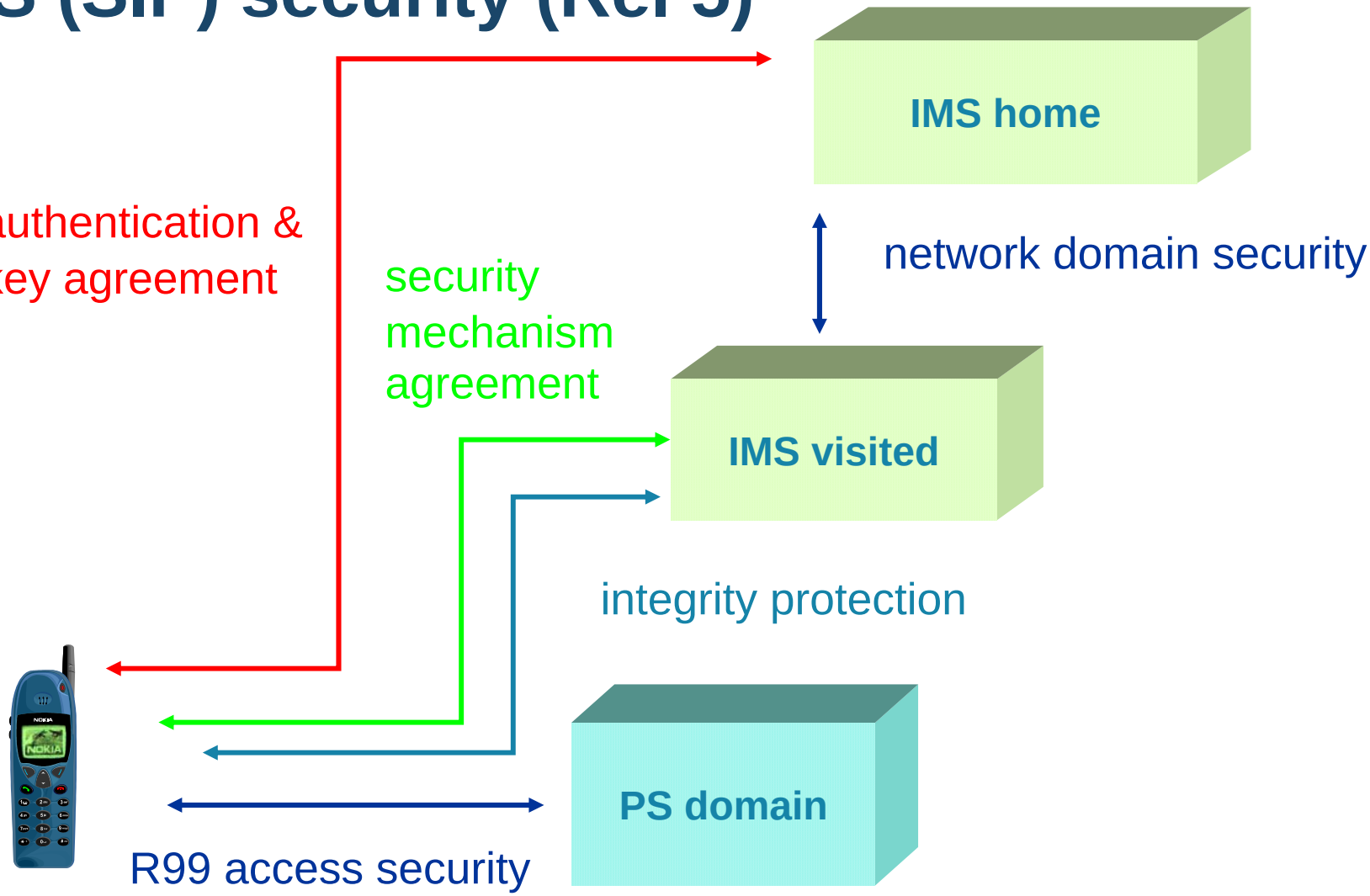
- For 3GPP Release 99, WG SA3 created 19 new specifications, e.g. TS 33.102 “3G security; Security architecture”
  - 5 specifications (out of these 19) originated by ETSI SAGE, e.g. TS 35.202 “KASUMI specification”
- For Release 4, SA3 was kept busy with GERAN security, MAP security (later to be replaced by TCAP security) and various extensions to Rel-99
  - ETSI SAGE originated again 5 new specifications, e.g. TS 35.205-208 “MILENAGE algorithm set”
- 3GPP Release 5: 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: SA3 added 17 new specifications, e.g.:
  - TS 33.310 “Network domain security: Authentication Framework”
  - TR 33.978 “Early IMS security”
- Release 7: SA3 added 8 new specifications:
  - TS 33.110 “Key establishment between a UICC and a terminal”
  - TS 33.259 “Key establishment between a UICC hosting device and a remote device”
  - TS 33.204 “Network Domain Security; Transaction Capabilities Application Part (TCAP) user security”
  - TR 33.918 “HTTPS connection between a UICC and a Network Application Function (NAF)”
  - TR 33.920 “SIM card based GBA”
  - TR 33.803 “Co-existence between TISPAN and 3GPP authentication schemes”
  - TR 33.905 “Trust recommendations for open platforms”
  - TR 33.980 “Liberty Alliance and 3GPP security interworking”
  - In addition, ETSI SAGE created 5 specifications for UEA2 & UIA2 (incl. SNOW 3G spec) (TS 35.215-218, TR 35.919)

Common IMS security

IMS (SIP) security (Rel 5)



Authentication in the IMS access domain

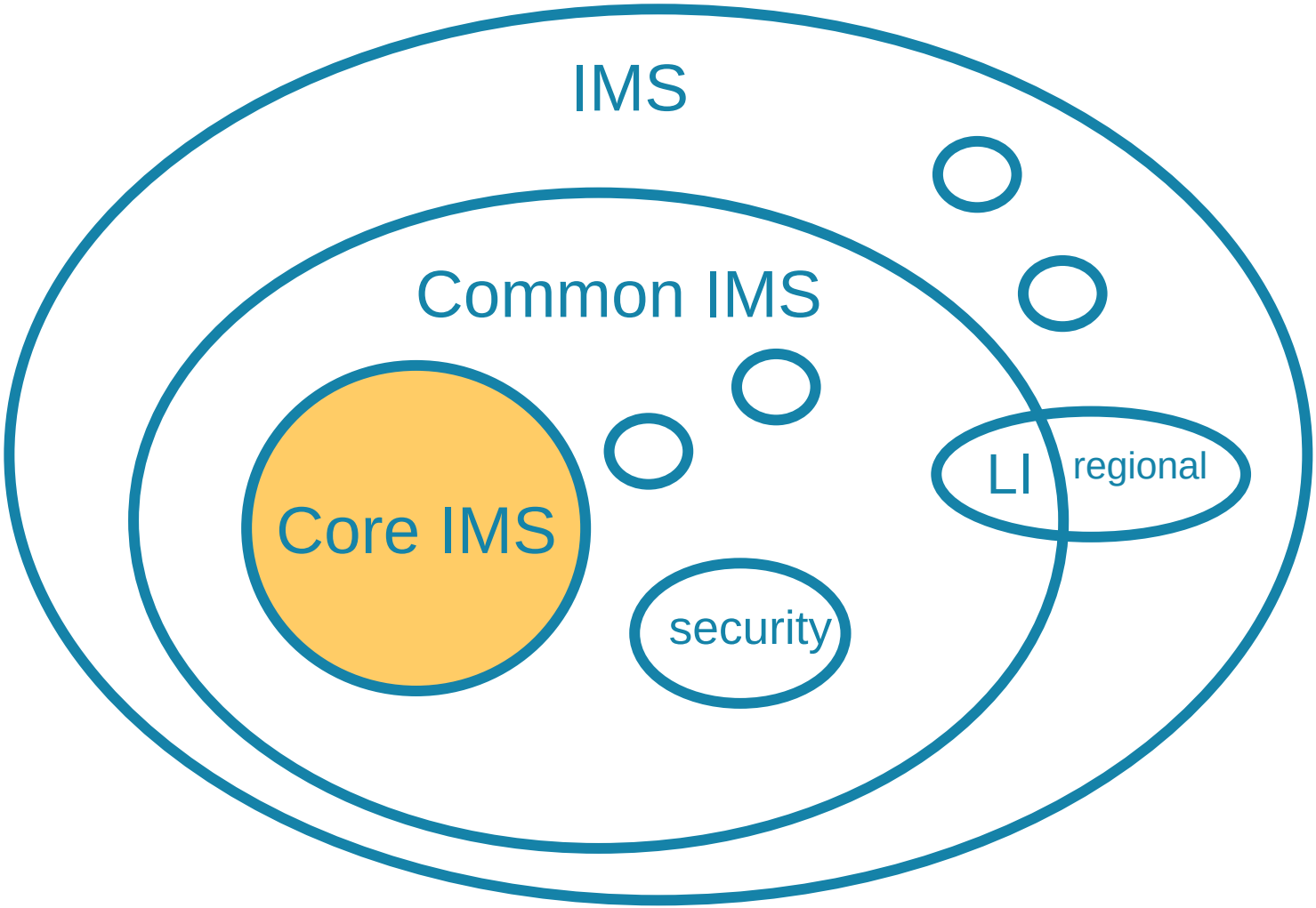
- Strong mutual authentication by re-use of UMTS AKA protocol
  - Based on secret key cryptography
  - Typically implemented on a tamper-resistant UICC (ISIM application)
- UMTS AKA integrated into HTTP Digest
  - According to RFC3310

IMS enhancements in Rel-6 / Rel-7

- Release 6: SIP signalling confidentiality (Rel-5 relies on bearer layer confidentiality)
- Release 7: IMS security TS 33.203 expanded to support NAT traversal for fixed broadband access
- Rel-7: 3GPP TR 33.803 created to show how different authentication mechanisms may co-exist in one single IMS system (with several different access systems)
  - IMS access with UICC (3GPP)
  - “Early” IMS access with SIM (3GPP)
  - NASS-bundled authentication (TISPAN)
  - HTTP Digest as defined by TISPAN

Rel-8: Introduction of “Common IMS”

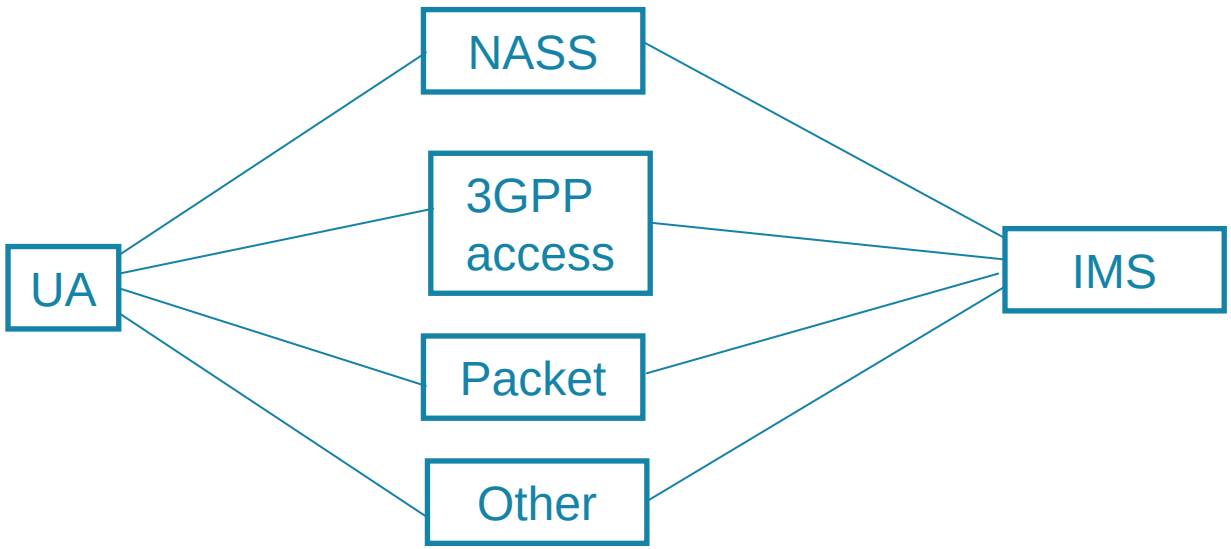
- During Rel-7 timeframe several industries had adopted IMS:
  - Fixed broadband (specs by ETSI TISPAN)
  - Packet cable (delta specs by CableLabs)
  - CDMA networks (specs by 3GPP2)
- Each had defined their own extensions/modifications → danger of unnecessary divergence (e.g. in security)
- For release 8, it was agreed that 3GPP maintains and develops exclusively specs for *both* Core IMS functionality *and* selected additional IMS related functionality, including security


IMS
Common IMS
Core IMS
security
LI
regional

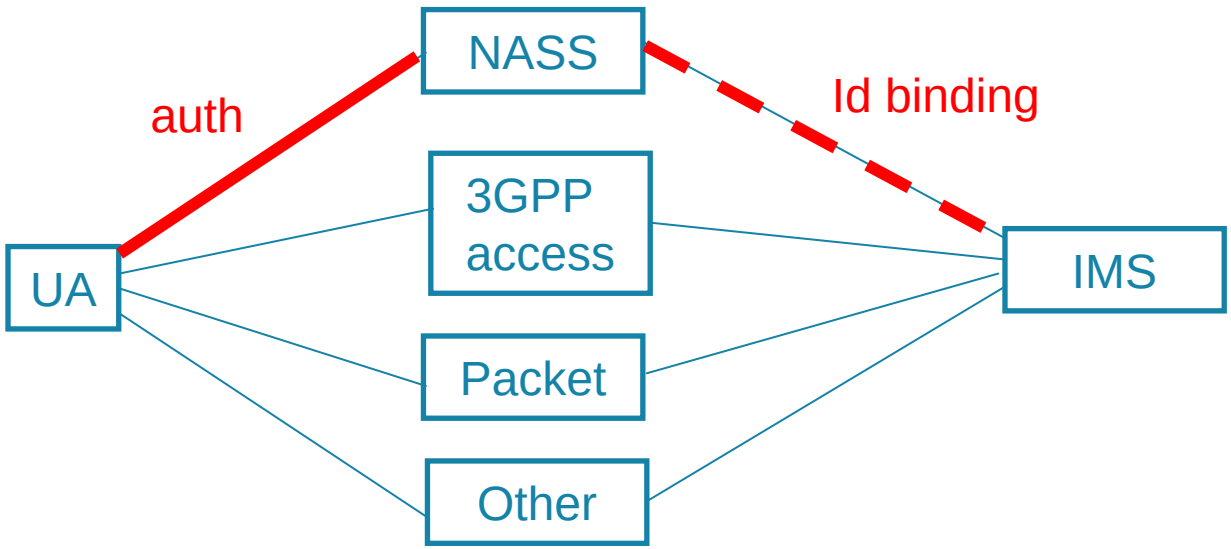
Common IMS security enhancements

- Several new normative annexes to TS 33.203 (Rel-8)
  - NASS-IMS bundled authentication
  - SIP Digest - based authentication
  - Access security with TLS
  - Co-existence of authentication schemes (replaces TR 33.803)
- Early IMS security TR 33.978 promoted to TS in Rel-8
- Media security
  - Access-independent protection mechanisms
  - TR 33.828 work in progress: draft requirements exist
  - Coordinated with IETF

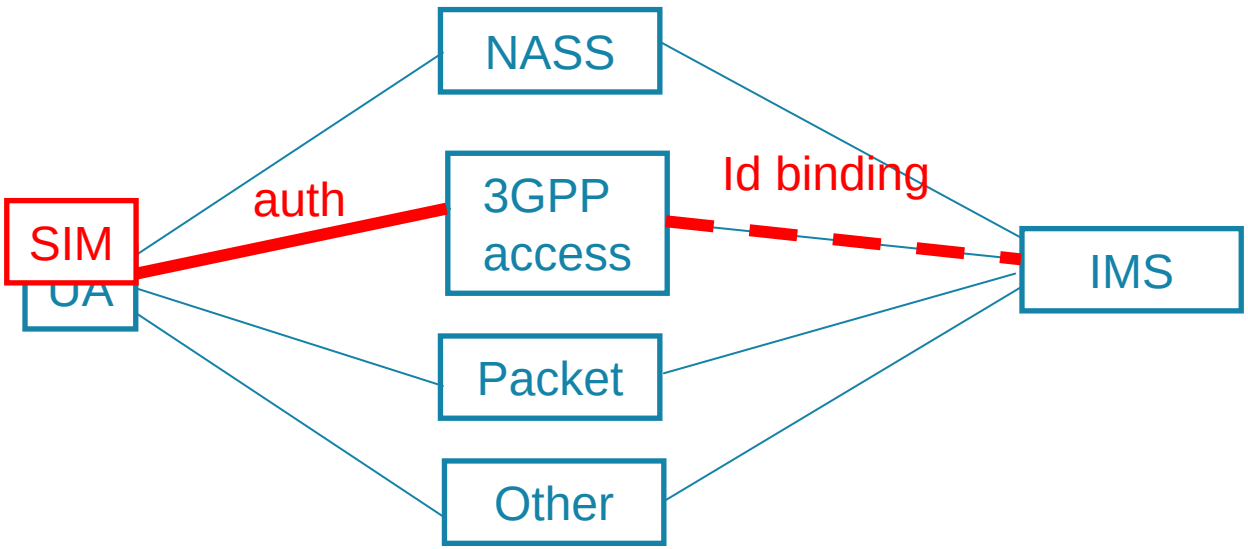
Different IMS authentication schemes 1/5



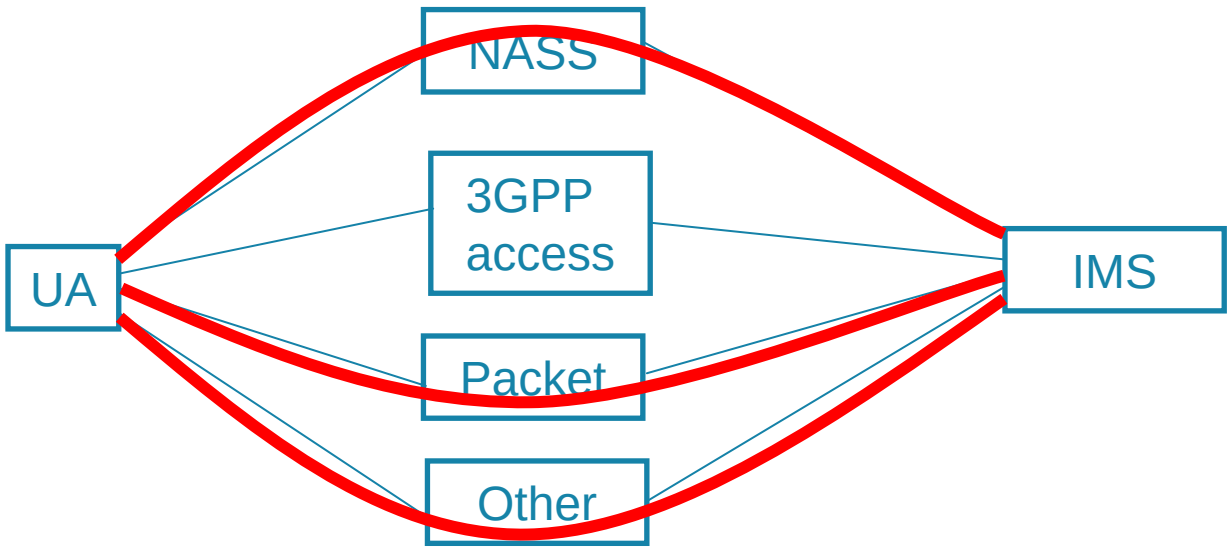
Different IMS authentication schemes 2/5: NBA



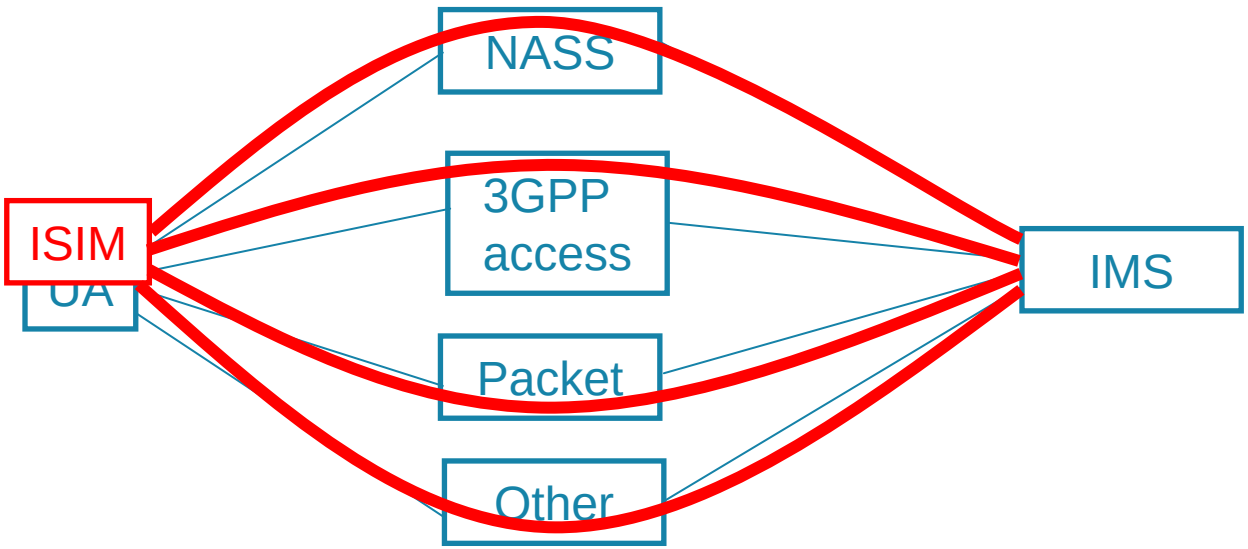
Different IMS authentication schemes 3/5: Early IMS security



Different IMS authentication schemes 4/5: SIP Digest + TLS (+ IP addr binding)



Different IMS authentication schemes 5/5: Full IMS (TS 33.203 main body)



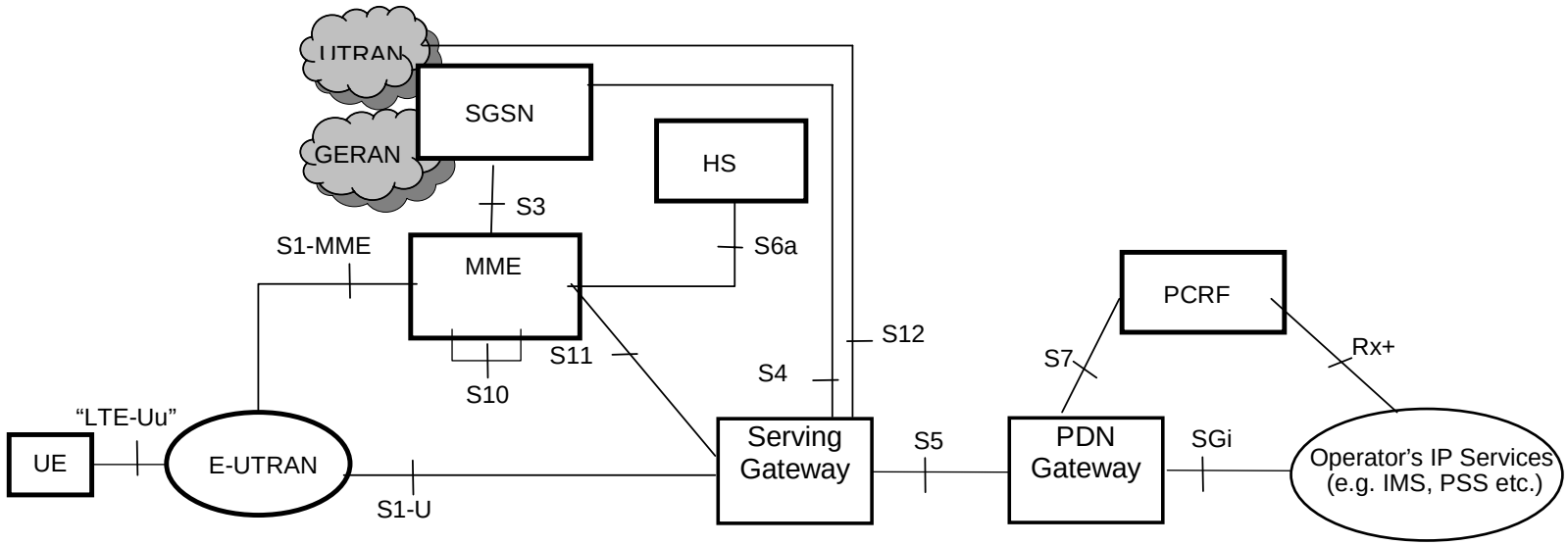
SAE/LTE security

SAE/LTE: What and why?

SAE = System Architecture Evolution
LTE = Long Term Evolution (of radio networks)

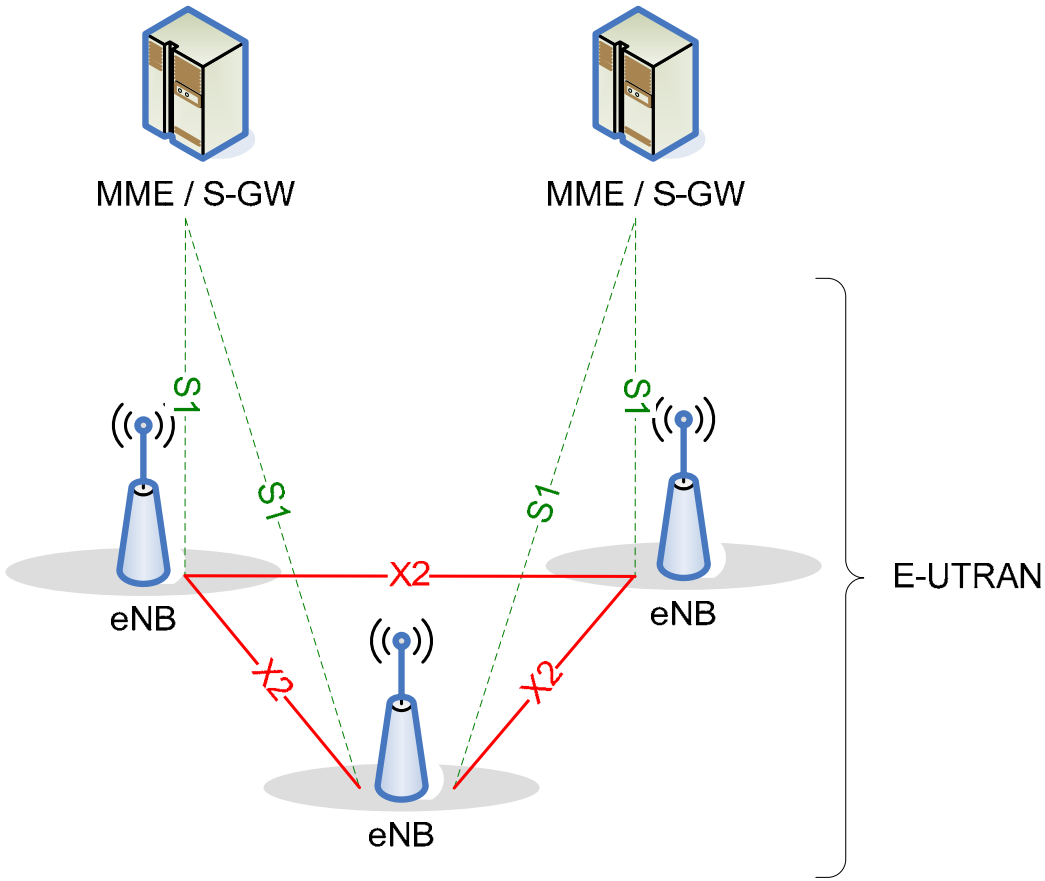
- LTE offers higher data rates, up to 100 Mb/sec
  - Multi-antenna technologies
  - New transmission schema based on OFDM
  - Signaling/scheduling optimizations
- SAE offers optimized IP-based architecture
  - Packet-based
  - Flat architecture: 2 network nodes for user plane
  - Simplified protocol stack
  - Optimized inter-working with legacy cellular, incl. CDMA
  - Inter-working with non-3GPP accesses, incl. WiMAX

SAE: Non-Roaming Architecture for 3GPP Accesses (TS 23.401)



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

LTE: E-UTRAN architecture (TS 36.300)



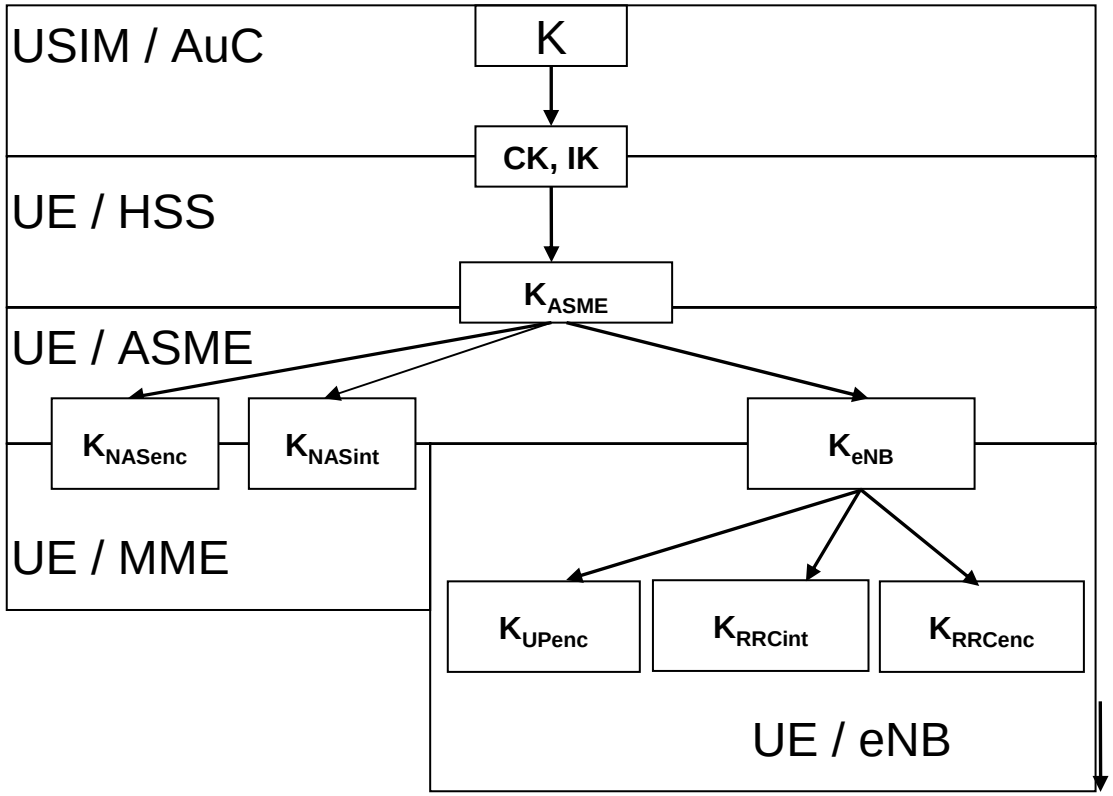
Implications on security

- Flat architecture → user plane security terminates in eNodeB
  - Deeper key hierarchy
  - Implementation security for eNodeB
- Many different access technologies → different kind of networks participate → trust models more complex
  - Extended key hierarchy
  - Weaknesses in one network not to affect others
  - Many inter-working cases to be covered

Security functions

- Authentication and key agreement
  - UMTS AKA re-used for SAE
  - SIM access to LTE is explicitly excluded
  - Rel-99 USIM is sufficient
- Signalling protection
  - For core network (NAS) signalling, integrity and confidentiality protection terminate in MME
  - For radio network (RRC) signalling, integrity and confidentiality protection terminate in eNodeB
- User plane protection
  - Encryption terminates in eNodeB
  - Separate protection in network interfaces
- Network domain security used for network internal interfaces

SAE key hierarchy



Crypto-algorithms

- Two sets of algorithms from Day One
  - If one breaks, we still have one
  - Should be as different from each other as possible
  - AES and SNOW 3G chosen as basis → ETSI SAGE to specify modes
- Rel-99 USIM is sufficient → master key 128 bits
  - All keys used for crypto-algorithms are 128 bits but included possibility to add 256-bit keys later (if needed)
- Deeper key hierarchy → (one-way) key derivation function needed
- Not yet confirmed all input parameters to encryption and integrity algorithms

eNodeB implementation security

- Requirements included in 3GPP specs
- Detailed mechanisms probably out of scope of 3GPP specs, technologies from e.g. TCG may be used
- Special attention to “Home eNodeB deployments”; study ongoing in SA3

Security for handovers

- Extended key hierarchy allows fast key refreshing for intra-LTE handovers
- Security context transferred in handovers with GERAN/UTRAN
  - After completion of HO, possibility for key renewal
- Possibility to refresh keys also during long sessions with no handovers

Inter-working with non-3GPP networks

- Two options for mobility between 3GPP and non-3GPP networks:
  - Proxy Mobile IP: no user-specific security associations between the Proxy and Home Agent
  - Client Mobile IP: for Dual Stack MIPv6, IPsec with IKEv2 is used
- IPsec tunnel (with evolved Packet Data Gateway) used in case the non-3GPP network is un-trusted by the operator (of SAE network)
- Several open issues still

SAE/LTE: SA3 specifications

- TR 33.821: Rationale and tracking of decisions
- TR 33.922: Security aspects of 3GPP-non-3GPP mobility
- TS 33.abc: SAE security architecture
- TS 33.xyz: Security with non-3GPP accesses

Summary

Summary

- Common IMS security
  - Coherent set of specs in 3GPP Release 8
  - Several alternative authentication schemes which may co-exist in one IMS system
  - Several ways to provide integrity of SIP signalling
  - (Access-independent) Media security: work in progress
- SAE/LTE security
  - New architecture and business environment require enhancements to 3G security
  - User plane security terminates in base station site
  - Extended key hierarchy
  - SIM access prohibited
  - Covers inter-working with non-3GPP networks
  - Crypto-algorithms based on AES and SNOW 3G

For more information:

www.3gpp.org