Role of Crypto in Mobile Communications

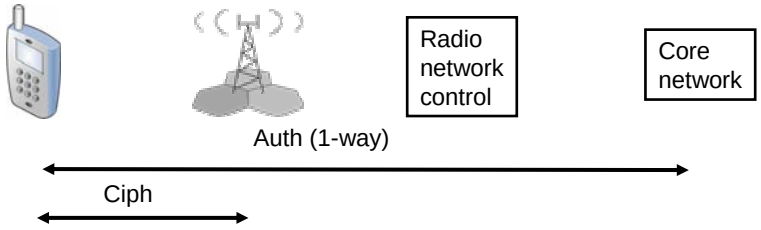
Valtteri Niemi

ECRYPT workshop 27-29 May 2008

Outline

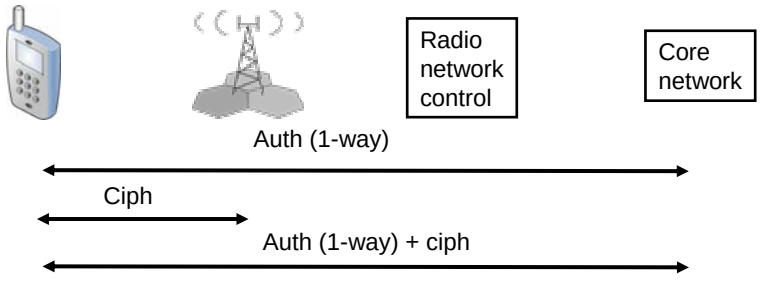
- Some history about:
  - Use of crypto in 1G, 2G, 3G mobile communications
  - 3GPP security specifications
- SAE/LTE security
- Role of crypto in other 3GPP features
  - Network domain security (NDS)
  - IP Multimedia Subsystem (IMS)
  - Interworking with WLAN (I-WLAN)
  - Generic Authentication Architecture (GAA)
  - Multimedia Broadcast/Multicast Service (MBMS)
  - Secure channel between UICC and a (remote) terminal
  - Lawful interception
- Summary

Essential crypto-features in 2G, 3G, SAE/LTE



NOKIA

Essential crypto-features in 2G, 3G, SAE/LTE



NOKIA

Essential crypto-features in 2G, 3G, SAE/LTE

Radio network control

Core network

GSM:

Auth (1-way)

Ciph

GPRS:

Auth (1-way) + ciph

3G:

Auth (2-way)

Ciph + integrity of signalling

NOKIA

Essential crypto-features in 2G, 3G, SAE/LTE

Radio network control

Core network

GSM:

Auth (1-way)

Ciph

GPRS:

Auth (1-way) + ciph

3G:

Auth (2-way)

Ciph + integrity of signalling

SAE/LTE:

Auth (2-way)

Ciph + intg of radio signalling

IPsec

intg of core ntwk signalling

NOKIA

Some history of 3GPP security 1/2

- For 3GPP Release 99, WG SA3 created 14 new specifications, e.g. TS 33.102 “3G security; Security architecture”
  - In addition 5 specifications 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”

NOKIA

Some history of 3GPP security 2/2

- Release 6: SA3 added 17 new specifications, e.g.:
  - TS 33.310 “Network domain security: Authentication Framework”
  - TS 33.234 “I-WLAN security”
  - TS 33.220-222 “Generic Authentication Architecture” specs
  - TS 33.246 “MBMS security
- Release 7: SA3 added 8 new specifications, e.g:
  - 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”
  - In addition, ETSI SAGE created 5 specifications for UEA2 & UIA2 (incl. SNOW 3G spec) (TS 35.215-218, TR 35.919)
- Release 8: Main addition is SAE/LTE security

NOKIA

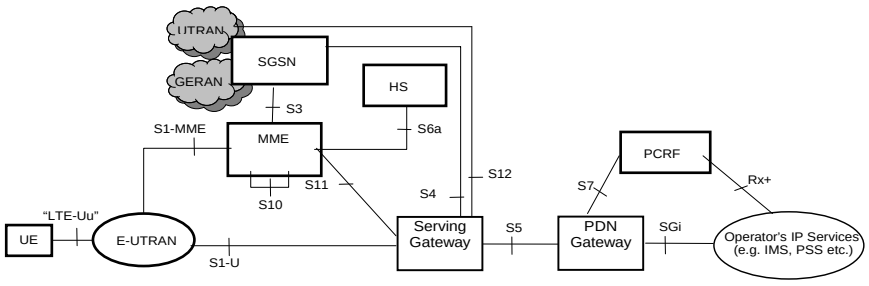
SAE/LTE: What and why?

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

NOKIA

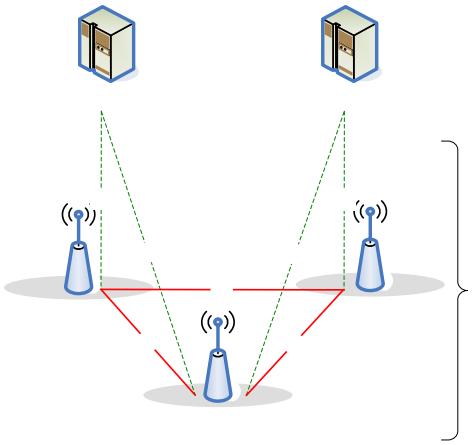
SAE: Non-Roaming Architecture for 3GPP Accesses (TS 23.401)



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

NOKIA

LTE: E-UTRAN architecture (TS 36.300)



NOKIA

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

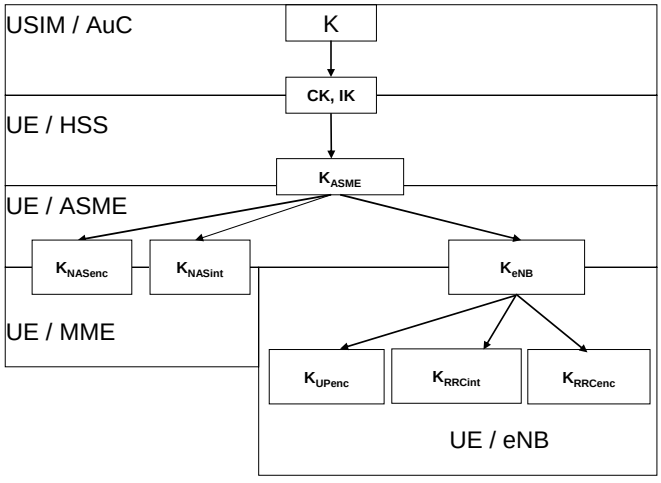
NOKIA

Security functions

- Authentication and key agreement
  - UMTS AKA re-used for SAE
  - SIM access to LTE is explicitly excluded
  - On the other hand, 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

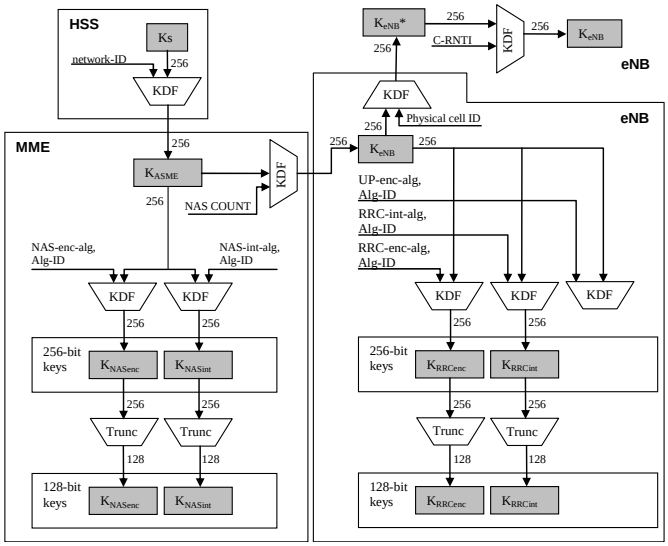
NOKIA

SAE key hierarchy



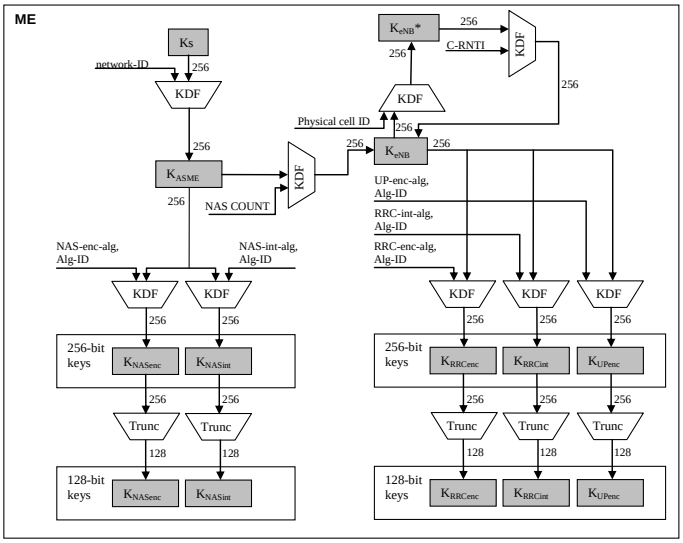
NOKIA

Key derivation and distribution, network side



NOKIA

Key derivations, terminal side



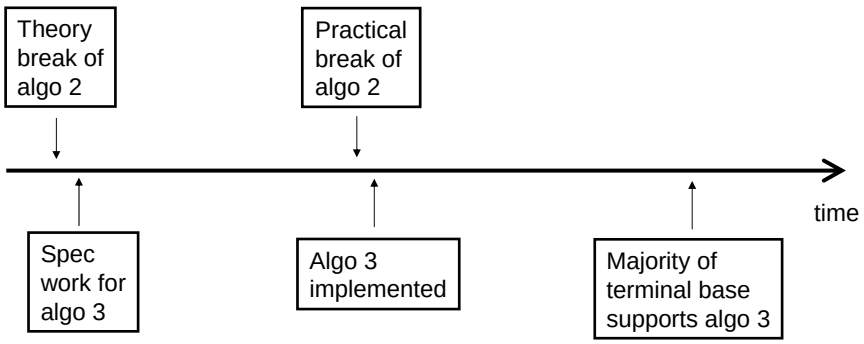
NOKIA

Crypto-algorithms

- Two sets of algorithms from Day One
  - If one breaks, we still have one standing
  - 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
  - HMAC-SHA-256 chosen as basis

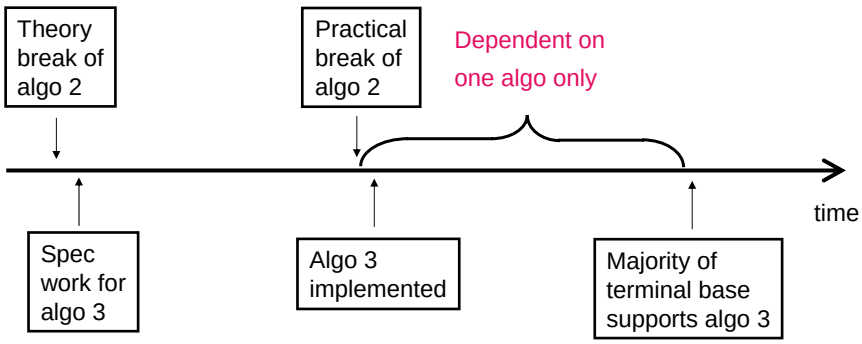
NOKIA

Need for algorithm agility: example



NOKIA

Need for algorithm agility: example



NOKIA

Caveat: Security of algorithm capability negotiation

- Algorithm capabilities exchanged first without protection
- Re-exchanged and verified once integrity protection is turned on

  → all integrity algorithms should resist real-time attacks in the beginning of the connection

- If this is not the case anymore, broken algorithm has to be withdrawn completely from the system
  - In the same way as A5/2 is withdrawn from GSM

NOKIA

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

NOKIA

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 untrusted by the operator (of SAE network)

NOKIA

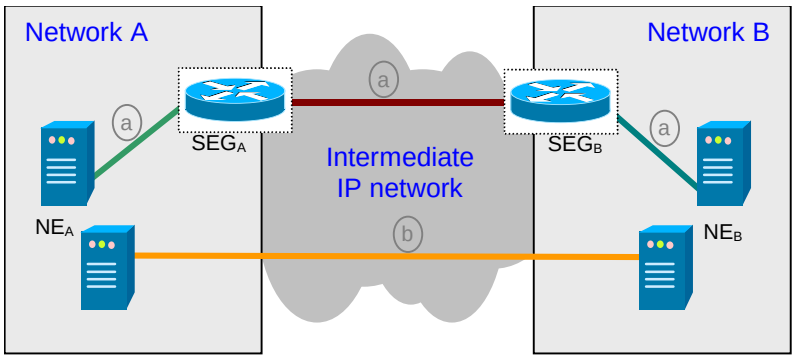
SAE/LTE: SA3 specifications

- TS 33.401: SAE security architecture
- TS 33.402: Security with non-3GPP accesses

NOKIA

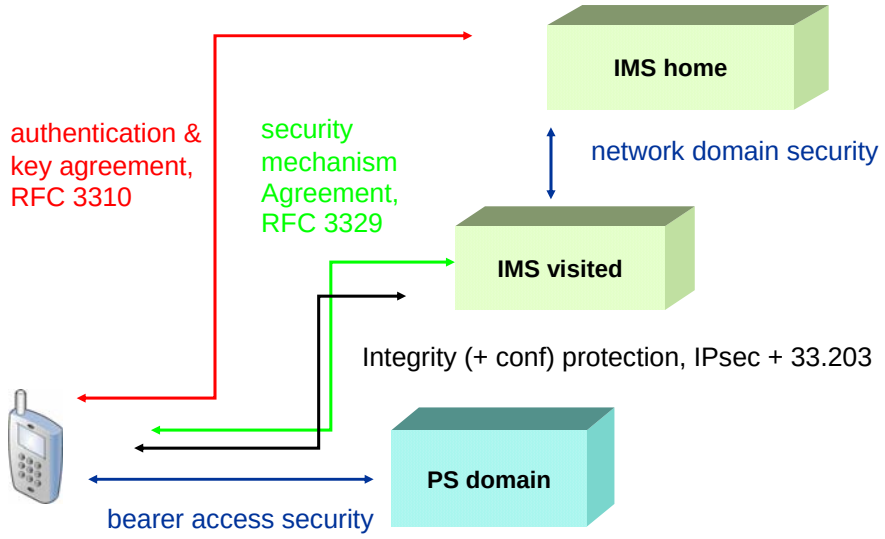
Network domain security using IPsec

- Inter-operator signaling is done via security gateways (a)
- End-to-end security (b) can be added using key management with PKI, see TS 33.310
- 3GPP has also created TCAPsec (analogous to IPsec), see TS 33.204



NOKIA

IMS (SIP) security



NOKIA

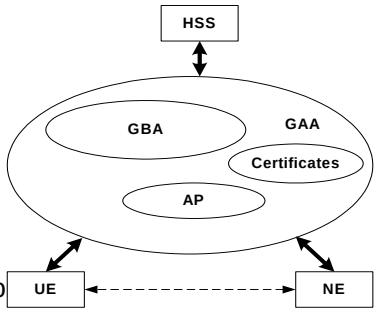
WLAN interworking in 3GPP

- WLAN access zone can be connected to cellular core network
- Shared subscriber database & charging & authentication (WLAN Direct IP access)
  - Authentication between WLAN-UE and 3GPP AAA server
  - based on EAP (RFC3748)
  - EAP-SIM: based on GSM AKA and network authentication (RFC4186)
  - EAP-AKA: based on UMTS AKA (RFC4187)
- Shared services (WLAN 3GPP IP Access), e.g. access to IMS
  - Security is provided by IPsec tunnel between UE and PDG
  - WLAN-UE uses IKEv2 for tunnel establishment
  - EAP messages carried over IKEv2 terminate in AAA server.
- Service continuity is the next step

NOKIA

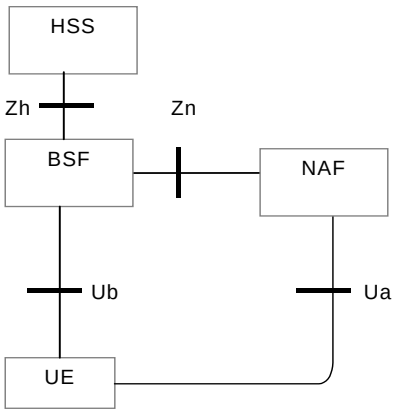
Generic Authentication Architecture (GAA)

- GAA consists of three parts (Rel-6):
- *TS 33.220 Generic Bootstrapping Architecture* (GBA) offers generic authentication capability for various applications based on shared secret. Subscriber authentication in GBA is based on HTTP Digest AKA [RFC 3310].
- *TS 33.221 Support of subscriber certificates:* PKI Portal issues subscriber certificates for UEs and delivers an operato CA certificates. The issuing procedure is secured by using shared keys from GBA.
- *TS 33.222 Access to Network Application Function using HTTPS* is also based on GBA.



NOKIA

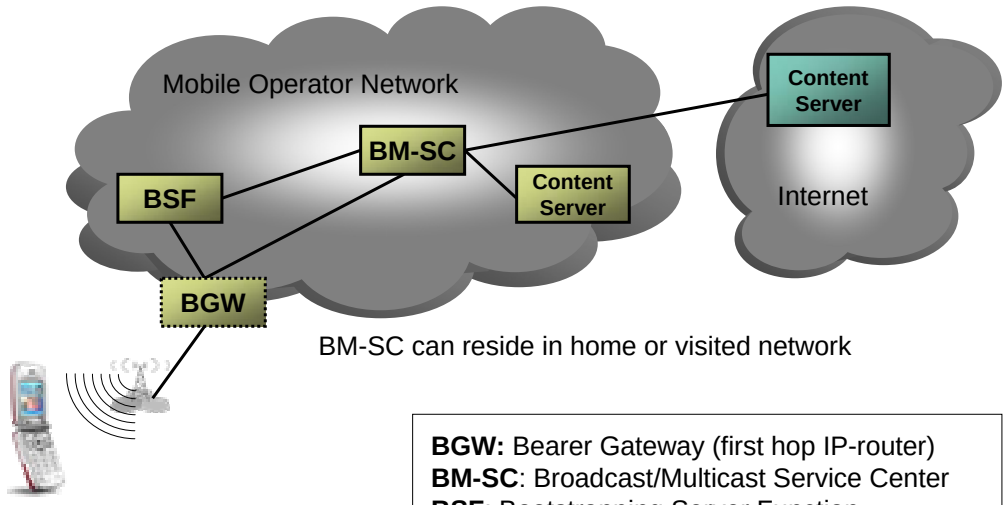
GBA: Generic Bootstrapping



- Bootstrapping Server Function (BSF) and the UE run AKA protocol, and agreed session keys are later used between UE and Network Application Function (NAF).
- After the bootstrapping, the UE and NAF can run some application-specific protocol where security is based on derived session keys

NOKIA

MBMS Security Architecture (node layout)



BM-SC can reside in home or visited network

BGW: Bearer Gateway (first hop IP-router)
BM-SC: Broadcast/Multicast Service Center
BSF: Bootstrapping Server Function

NOKIA

Summary of MBMS Security

- Service protection, not content protection in DRM-sense
- Application layer solution which is bearer agnostic
- Based on IETF and OMA protocols
  - MIKEY for key delivery
  - SRTP for streaming protection
  - DCF for download protection
- GBA used for mutual authentication and distribution of shared secret
- Three-level key hierarchy for data protection
- Specified in TS 33.246

NOKIA

Secure channel between UICC and terminal

- Background: security elements emerge in terminals, e.g. TPM in laptops, MTM in mobile phones
- It makes sense to secure the (local) interface between UICC and terminal, esp. for scenarios where the user may be the enemy, e.g. broadcast
- Secure transport specified by ETSI SCP group
- Key management specified in TS 33.110
  - Based on GBA
- “Sister” spec TS 33.259 provides key management between UICC-hosting device and a (remote) terminal

NOKIA

Lawful interception

- 3GPP specifies required lawful interception mechanisms for all features
- Call/message content and related data provided from certain network elements to the law enforcement side
  - Assumes typically that the content appears in clear in the network element
  - End-to-end encryption is still possible if keys are provided
- No weak algorithms introduced for LI purposes
  - All 3GPP algorithms are publicly known
- National variations exist
- Specified in TSs 33.106-108

NOKIA

Summary

- Number of cryptographic solutions still growing in mobile communications
- 3GPP has provided 6 releases of security specifications
- SAE/LTE security
  - User plane security terminates in base station site
  - Extended key hierarchy
  - Covers interworking with non-3GPP networks
  - Cryptoalgorithms based on AES and SNOW 3G
- Other 3GPP features
  - 3GPP has specified several emerging standards that rely heavily on crypto
  - Lawful interception is **not** provided using weak algorithms but it puts constraints on end-to-end security