

La sécurité dans les réseaux mobiles LTE

Benoit Michau

michau [.] benoit [chez] gmail [.] com

Novembre 2011 (sept. 2012: épurée pour publication)



Agenda

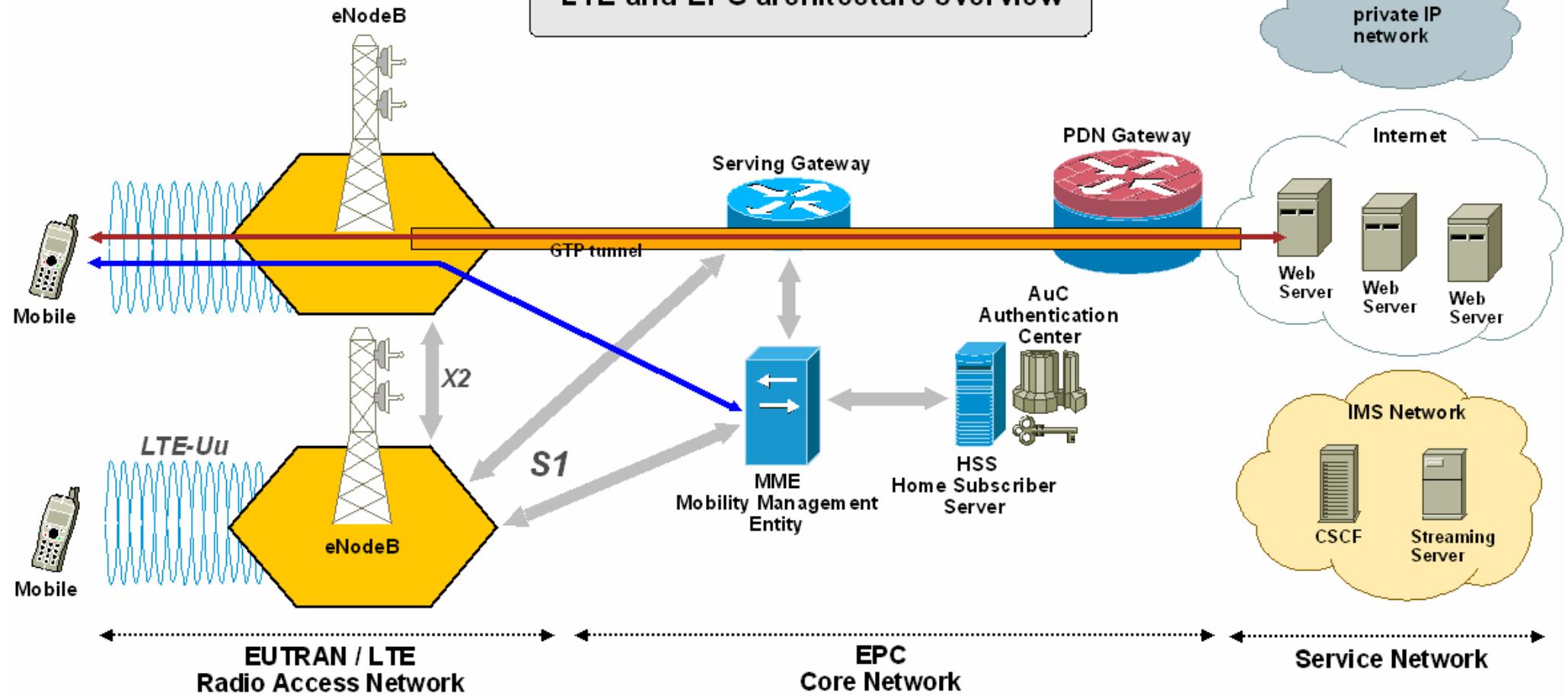
- Architecture du réseau LTE - EPC
- Le modèle de sécurité de LTE - EPC
- Protection des interfaces de l'opérateur
- Evolutions des technologies LTE : femtocells et relais
- Conclusion
- Annexes

Architecture du réseau LTE - EPC

Principes de bases: une architecture générique

- réseau d'accès à plat
 - > plus de contrôleur radio intermédiaire
 - > stations de base eNodeB interconnectées entre elles (X2), et au réseau cœur (S1)
- réseau tout IP
 - > plus de domaine circuit
 - > pas de *service* intégré
 - routage vers des réseaux tiers : IMS, Internet, privés
 - gestion de la mobilité :
transport des sessions abonnés dans des tunnels GTP
- Inter-fonctionnement avec réseaux GSM et UMTS
 - > restriction : carte USIM obligatoire
- Inter-fonctionnement avec réseaux d'accès tiers
 - > WIFI, WiMAX, CDMA2000, ...
 - > gestion de la mobilité avec Mobile IP

LTE and EPC architecture overview

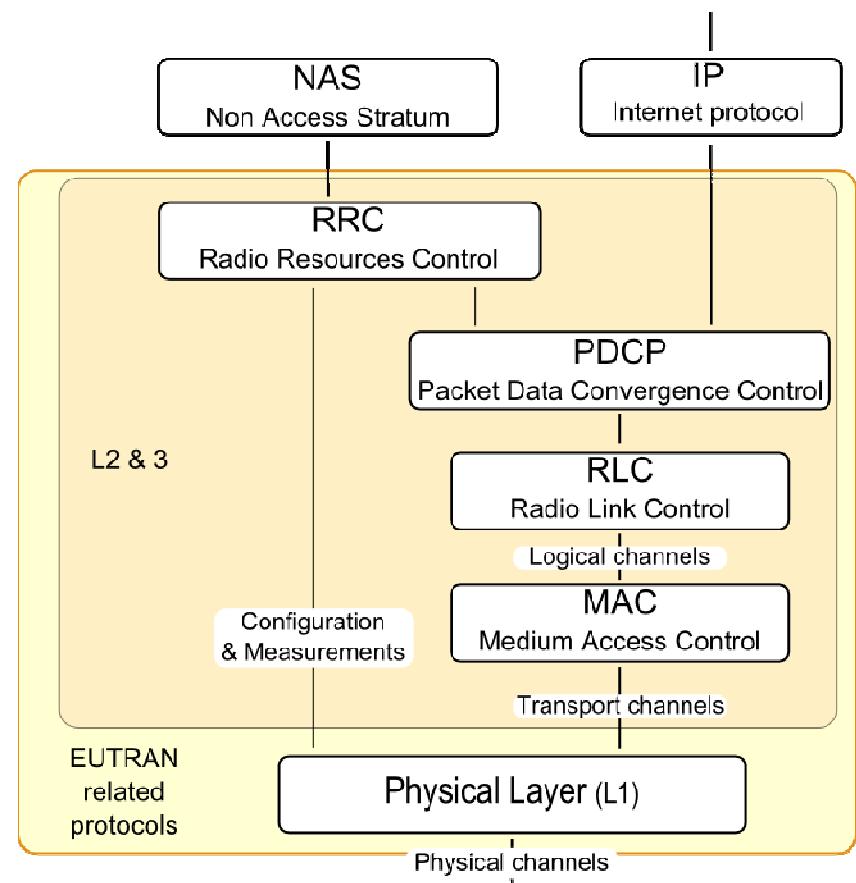


Le modèle de sécurité du LTE / EPC

Une sécurité à plusieurs niveaux

- Réutilisation de l'authentification UMTS
 - > carte USIM dans le mobile
 - > authentification mutuelle avec le réseau (HSS)
 - > production de 2 clés dérivées (C_k , I_k)
- génération d'une clé maîtresse K_{ASME} dédiée au réseau mobile LTE / EPC, à partir de (C_k , I_k)
 - > différentiation de K_{ASME} selon le réseau (MCC / MNC)
- Protection de la signalisation de haut niveau
 - > signalisation NAS : gestion de la mobilité et des sessions
 - > sécurité de bout en bout (mobile <-> MME)
 - > contrôle d'intégrité et chiffrement
- Protection de l'interface radio:
 - > trames PDCP
 - > session utilisateur : chiffrement
 - > signalisation radio (RRC) : contrôle d'intégrité et chiffrement
- Utilisation de HMAC-SHA-256 pour les dérivations de clés successives

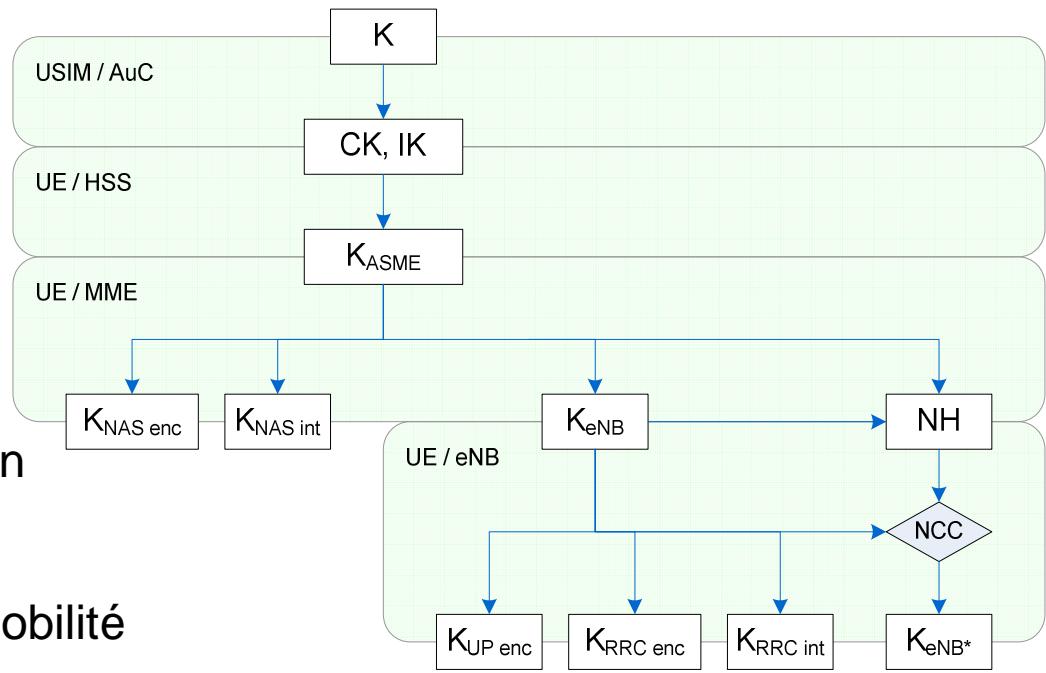
pile protocolaire LTE / EUTRAN
(wikipedia)



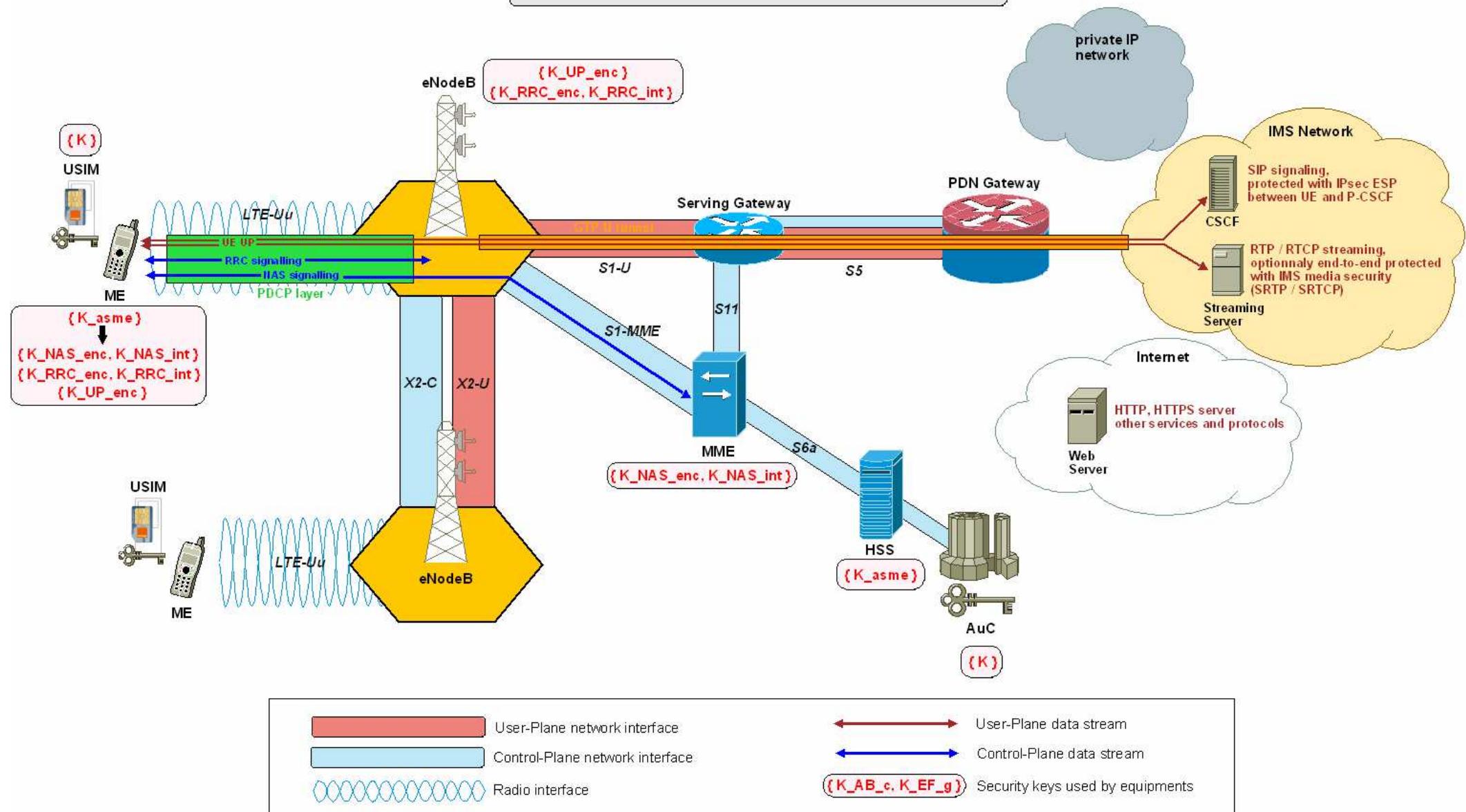
Processus de dérivation de clés

- K: clé d'authentification de l'abonné
 - > durée de vie : 3 à 10 ans
- K_{ASME} : clé maîtresse de session LTE / EPC
 - > durée de vie : quelques heures / jours
- K_{NAS} : clés de sécurité signalisation NAS
 - > durée de vie : identique à K_{ASME}
- K_{RRC} : clés de sécurité signalisation radio RRC
 - > durée de vie : quelques secondes à heures
- K_{UP} : clé de chiffrement des données de session
 - > durée de vie : quelques secondes à heures
- Renouvellement des clés eNodeB à chaque mobilité d'antennes
 - > paramètre de diversification NH maintenu par le MME : même qualité que les clés NAS
 - > recalcul de K_{eNB} et des clés UP et RRC par les eNodeB successifs

Hiérarchie de clés LTE / EPC (3GPP TS 36.300)



LTE and EPC security architecture overview



Algorithmes et niveau de sécurité

- Clé d'authentification K : 128 bits
- K_{ASME} et fonction de dérivation de clé : 256 bits, algorithme publique
 - > *facile* de basculer vers un système complet à 256 bits si nécessaire
- Chiffrement et contrôle d'intégrité : clés de 128 bits, algorithmes publics
 - > algorithmes de chiffrement NAS et PDCP
 - EEA0, EEA1 (SNOW 3G), EEA2 (AES-CTR), EEA3 (ZUC)
 - > algorithmes de contrôle d'intégrité NAS et PDCP
 - EIA1 (SNOW 3G, mode MAC), EIA2 (AES-CMAC), EIA3 (ZUC, mode MAC)
 - > pas d'attaques réalistes connues sur SNOW 3G, AES ni ZUC
 - > les terminaux, eNodeB et MME doivent tous supporter EEA0, SNOW 3G et AES
 - > ZUC récemment introduit pour une utilisation en Chine
- Des failles peuvent demeurer dans certaines procédures et / ou implantations logicielles
 - > acceptation du rejet de vecteurs d'initialisation
 - > vecteur d'initialisation ou clair connus (padding, messages de signalisation)
 - > bugs logiciels et corruption mémoire

Autres fonctions liées à la sécurité

- Interception légale des sessions et de la signalisation dans le cœur de réseau
- Gestion des appels d'urgence
 - >localisation de l'appel
 - >pour les mobiles ne pouvant pas s'authentifier: session sans chiffrement ni contrôle d'intégrité
- Messages d'alertes broadcastés ("tsunami / earthquake alert")

Protection des interfaces de l'opérateur

Sensibilité des interfaces fixes, internes à l'opérateur

- Accessible depuis une antenne
 - > interfaces entre antennes (X2)
 - > interfaces vers le cœur de réseau (S1)
- Accessible depuis d'autres réseaux d'accès
 - > interfaces vers le cœur de réseau en mobilité IP (MIPv4, DSMIPv6, PMIP)
 - > notion d'interface "trusted" / "untrusted"
- Accessible depuis le réseau IP publique
 - > interfaces de roaming (dans de rares cas seulement)
 - messages Diameter (vers HSS)
 - messages de signalisation (vers MME), sessions GTP (vers PDN-gateway)
- Une unique solution:
 - > IPsec ESP
 - > IKEv2:
 - certificats entre équipements réseaux
 - EAP avec carte USIM entre mobiles et équipements réseaux
- Déploiement et usage d'IPsec au choix de(s) l'opérateur(s)

Evolutions des technologies LTE : femtocells et relais

Femtocells et relais LTE: principe

- Principe de l'eNodeB miniaturisé
 - > traite les sessions de l'utilisateur en clair
 - espionnage
 - > ne peut accéder à la signalisation de haut niveau (NAS)
 - pas de fraudes
 - > accède à la signalisation d'antennes (S1-AP, X2-AP)
 - déni de service
- Femtocells
 - > se connecte au cœur de réseau mobile via l'Internet (accès ADSL)
 - > protection de l'interface filaire avec IPsec
- Relais
 - > se connecte aux eNodeB fixes via une connexion radio LTE large bande
 - > multiplexe les sessions des mobiles dans une unique session
 - > pourra être mobile
- Matériel embarqué et exposé
 - > nécessite de bonnes pratiques (développement logiciel, sécurité système)

Conclusion

Les problématiques de sécurité dans les réseaux mobiles LTE / EPC (1/2)

- Arrêt du chiffrement des sessions utilisateurs dans l'eNodeB
 - > usage d'IPsec entre antennes et cœur de réseau optionnel
 - > femtocells et relais LTE permettant l'interception des sessions de données
- Multiplication des interfaces vers l'extérieur
 - > réseau tout IP
 - > interfaces possibles avec de multiples technologies d'accès (GPRS/3G, CDMA, WiMAX, WIFI...)
 - > interfaces de roaming : plus de 800 MNOs dans plus de 200 pays recensés par la GSMA

Les problématiques de sécurité dans les réseaux mobiles LTE / EPC (2/2)

- Complexité des implantations logicielles
 - > GSM + GPRS + EDGE + UMTS + HSPA + LTE + LTE-Advanced + IMS
 - > des centaines de spécifications techniques
- Convergence des OS d'équipements réseau vers Linux
 - > environnements *connus* (*/bin/bash ...*)
- Convergence des OS applicatifs mobiles (iPhone OS, Android)
 - > failles applicatives : fraudes et espionnage

Le rôle de l'opérateur : normes et audits

- Déployer un réseau mobile fiable intégrant les normes de sécurité
 - > configuration de la politique de sécurité
 - authentification robuste et périodique, limitation de la fraude
 - protection de la confidentialité sur l'interface radio (chiffrement)
 - > sans impact sur le service
 - > inter-fonctionnement avec tous les terminaux de tous les constructeurs et de tous les pays (ou presque)
- Qualifier la sécurité des équipements réseaux et des terminaux
 - > au-delà des standards
 - > prise de conscience des besoins sécurité avec les constructeurs

Le rôle de l'opérateur : avoir du recul

- Assurer un niveau de sécurité global et cohérent
 - > cloisonnement des réseaux selon leur sensibilité et exposition
 - usage d'IPsec sur les interfaces sensibles de l'opérateur
 - filtrage et restrictions d'accès (DMZ)
 - > protocoles IMS pour sécuriser les services de bout en bout
 - > sensibilisation des abonnés
 - mécanismes de sécurité au niveau des sessions des abonnés et opérateurs de services (par exemple, utilisation de TLS)

Annexe 1: normes, acronymes et ressources logicielles

Spécifications

<http://www.3gpp.org/specification-numbering>

- TS 43.020: sécurité GSM et GPRS
- TS 33.102: sécurité UMTS
- TS 33.210 et TS 33.310: sécurité du cœur de réseau
- TS 33.401: sécurité LTE et EPC
- TS 33.402: sécurité des accès non-3GPP à l'EPC
- série TS 33: sécurité
- série TS 35: cryptographie
- série TS 24: signalisation entre mobile et cœur de réseau
- série TS 45: réseau d'accès GSM et GPRS
- série TS 25: réseau d'accès UMTS
- série TS 36: réseau d'accès LTE
- série TS 31: cartes (U)SIM

Acronymes

- GSM [2]: Global System for Mobile telecommunications
- UMTS [2]: Universal Mobile Telecommunications System
- LTE [2]: Long Term Evolution
- EPC [2]: Evolved Packet Core
- GPRS [4]: Global Packet Radio System
- SIM [4]: Subscriber Identity Module
- BTS [4]: Base Transceiver Station
- GEA [4]: GPRS Encryption Algorithm
- SGSN [4]: Serving GPRS Support Node
- USIM [5]: UMTS SIM
- AES [5]: Advanced Encryption Standard
- RRC [5]: Radio Resources Control
- MM [5]: Mobility Management
- CC [5]: Circuit Control
- SMS [5]: Short Message Service
- SM [5]: Session Management
- UIA [5]: UMTS Integrity protection Algorithm
- UEA [5]: UMTS Encryption Algorithm
- RNC [5]: Radio Network Controller
- GTP [7]: GPRS Tunneling Protocol
- HSS [10]: Home Subscriber Server
- MCC [10]: Mobile Country Code
- MNC [10]: Mobile Network Code
- NAS [10]: Non-Access Stratum
- MME [10]: Mobility Management Entity
- PDCP [10]: Packet Data Convergence Protocol
- AuC [11]: Authentication Center
- UP [11]: User-Plane
- NH [11]: Next Hop
- NCC [11]: NH Chaining Count
- EEA [13]: EPS Encryption Algorithm
- EIA [13]: EPS Integrity protection Algorithm
- MIPv4 [16]: Mobile IPv4
- DSMIPv6 [16]: Dual Stack Mobile IPv6
- PMIP [16]: Portable Mobile IP
- ESP [16]: Encapsulating Security Protocol

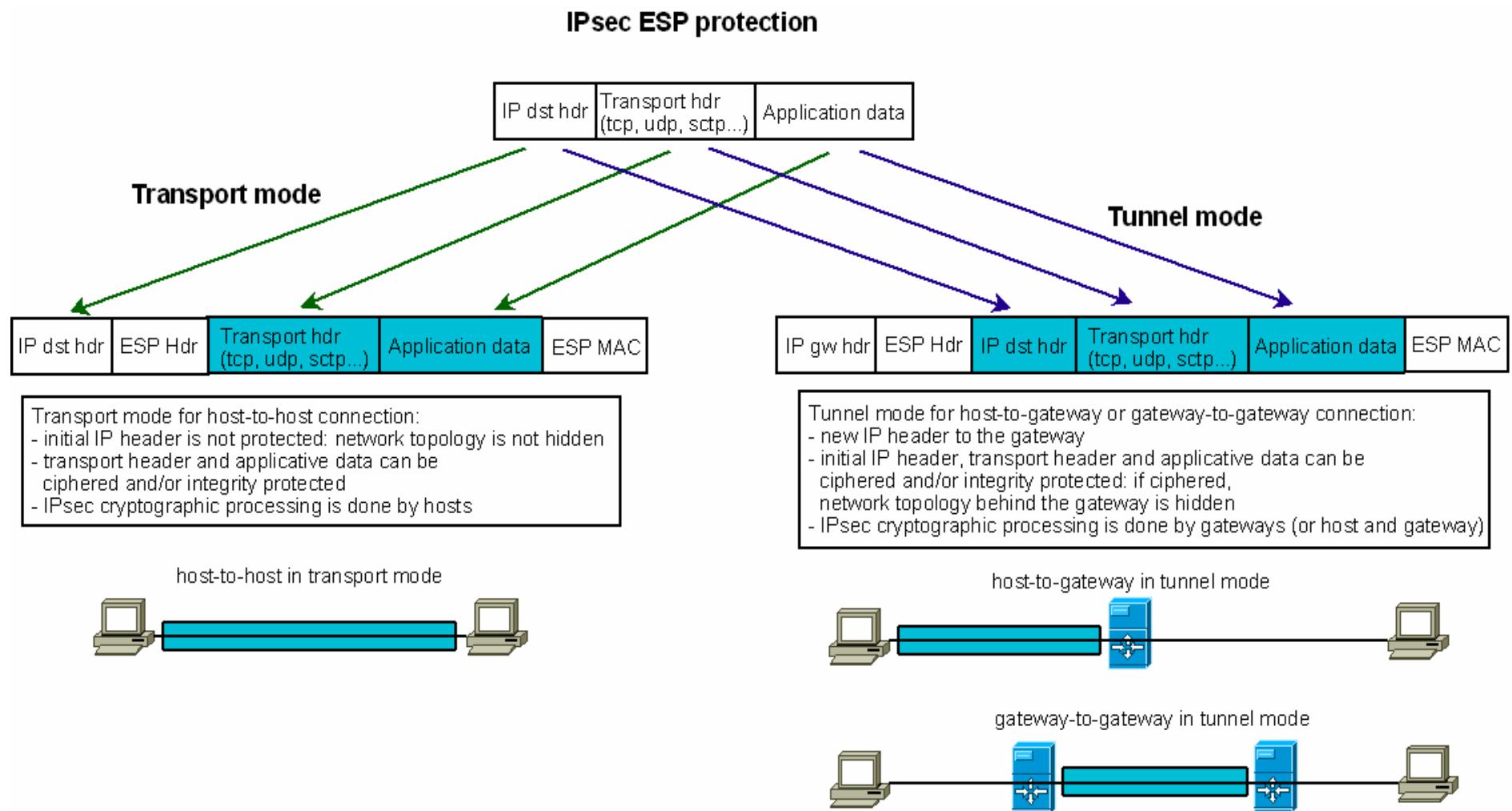
Acronymes

- IKEv2 [16]: Internet Key Exchange version 2
- EAP [16]: Extensible Authentication Protocol
- S1-AP [18]: S1 Application Protocol
- X2-AP [18]: X2 Application Protocol
- MNO [20]: Mobile Network Operator
- GSMA [20]: GSM Association
- IMS [20]: IP Multimedia Subsystem
- OS [20]: Operating System

Sécurité LTE / EPC: quelques ressources publiques

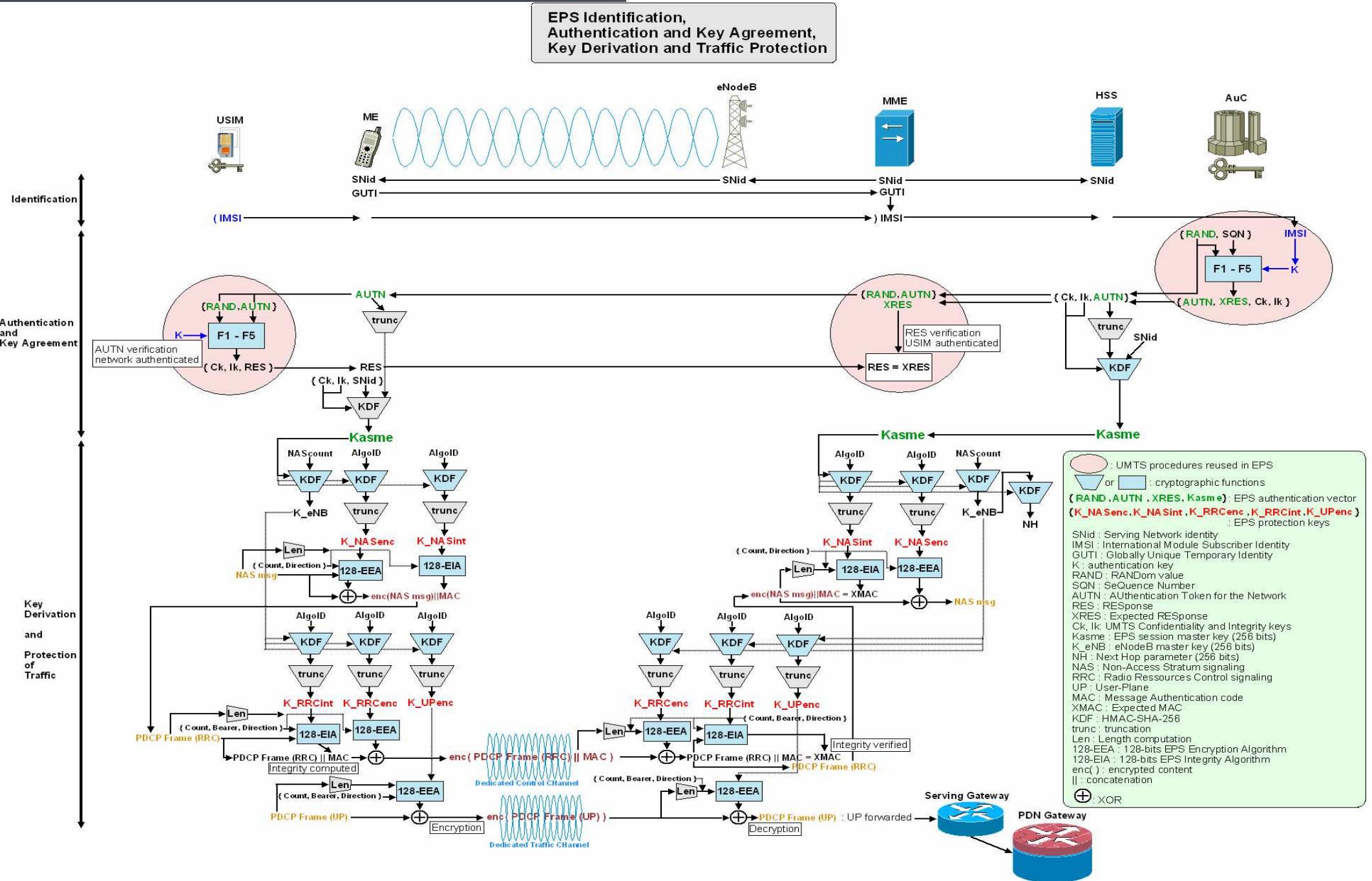
- Des ressources Internet nombreuses (pour les protocoles cœur):
 - > <http://www.kernel.org/>: Linux, implémente nativement SCTP et IPsec.
 - > <http://freeradius.org/>: un serveur AAA open-source.
 - > <http://www.wireshark.org/>: analyseur protocolaire "ultime"
- Peu de ressources publiques concernant la partie radio:
 - > <http://www.openairinterface.org/>
 - > http://www.constantwave.com/lte_source_code.aspx
- Radio logicielle ("Software Defined Radio"):
 - > <http://gnuradio.org/redmine/projects/gnuradio/wiki>
 - > <http://www.ettus.com/>
 - > <http://www.funcubedongle.com/>

Annexe 2: IPsec ESP



Annexe 3: détails sur la sécurité LTE et les procédures de mobilité (anglais)

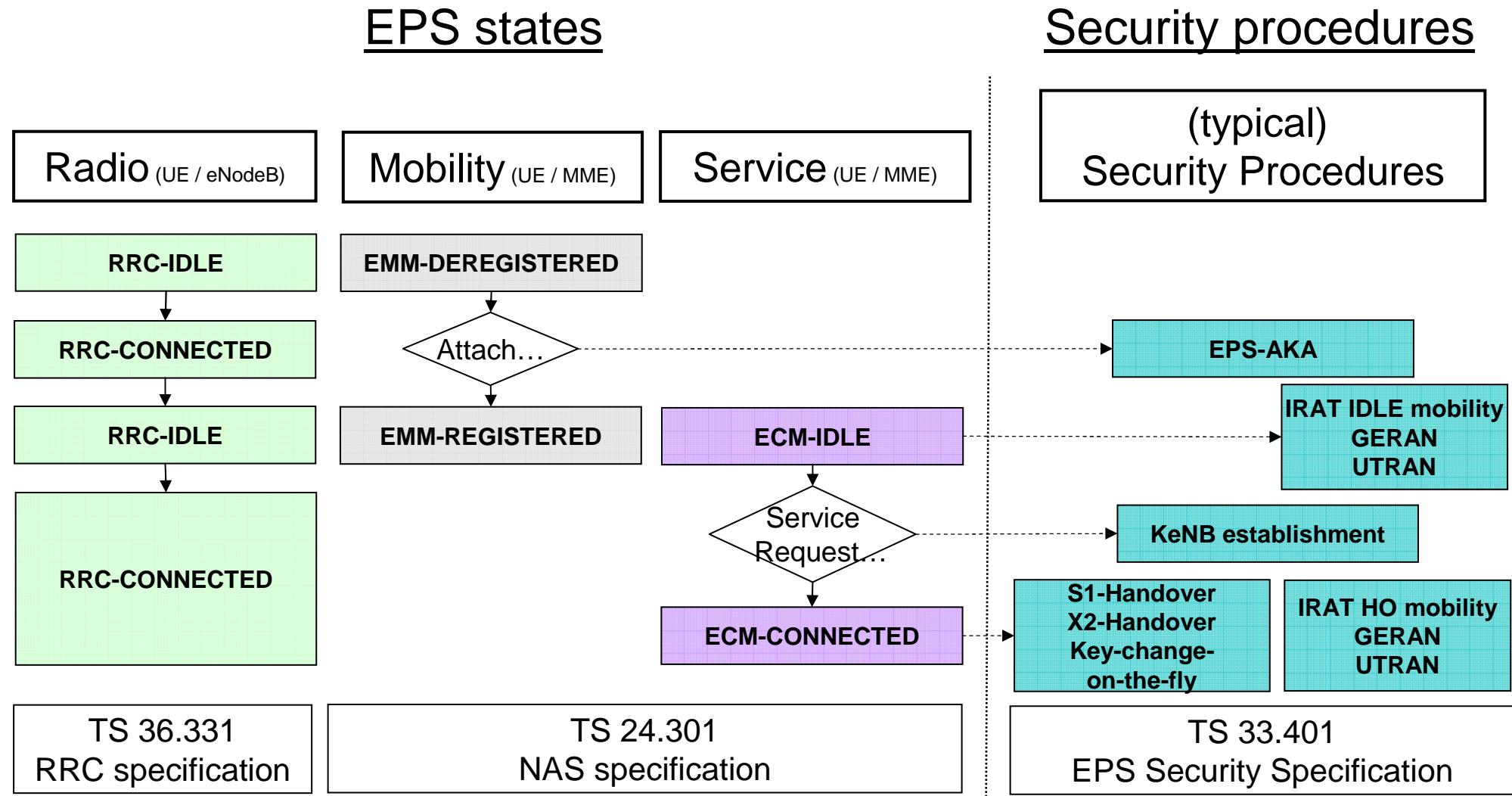
Layered security model (Radio / NAS)



Radio security versatility

- Each time an active UE moves to a new LTE cell: new K_{eNB} and $\{K_{RRCenc/int}, K_{UPenc}\}$ are computed and taken into use
 - > A compromised eNodeB has (almost) no security impact on the communication:
 - that was established with previous eNodeBs (backward security)
 - that will be establish with forthcoming eNodeBs (forward security)
- 2 types of K_{eNB} recomputation:
 - > Depending of hand-over types (S1, X2) and fresh data received by source eNodeB from serving MME
- Additional procedures allowing renewal of radio keys:
 - > Intra-eNodeB hand-over
 - > Intra-cell hand-over
 - > To take into use new K_{eNB} computed by the serving eNodeB thanks to fresh data coming from the serving MME

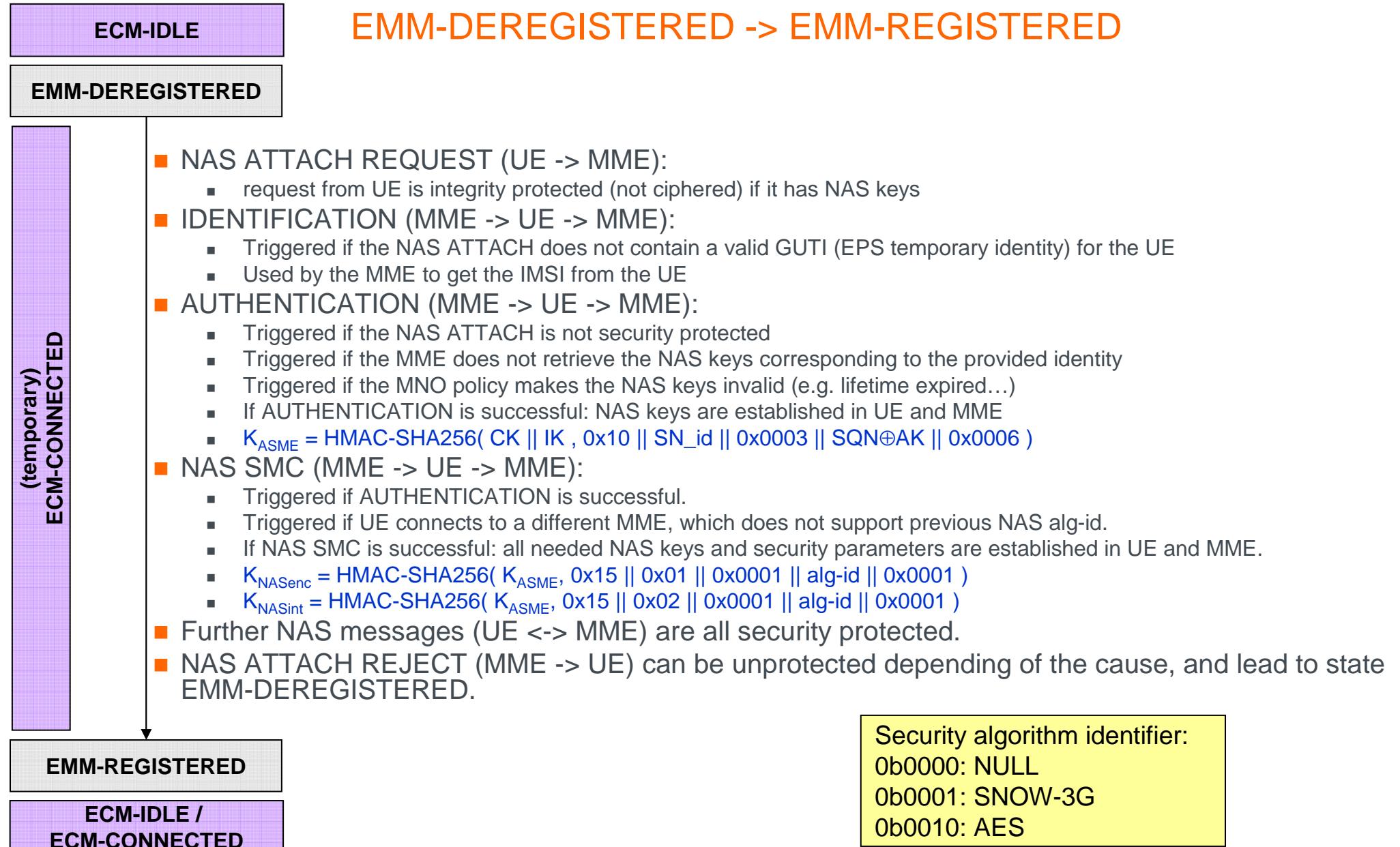
EPS (over) simplified state machine



Effective activation of the security

- SECURITY MODE COMMAND procedure
 - Launched after authentication
 - Allows to select and activate ciphering and integrity protection algorithms
- SMC at NAS layer
 - MME -> UE SMC request message:
 - Replays UE security capabilities, initially transmitted unprotected by UE to network
 - Provides algorithms chosen by the MME to be used
 - Is integrity-protected with K_{NASint}
 - UE -> MME SMC response message:
 - Is ciphered and integrity-protected with $K_{\text{NASenc/int}}$
 - Activate the protection of further NAS communication between UE and MME
- SMC at AS / radio layer (embedded in RRConnectionReconfiguration)
 - eNodeB -> UE request message:
 - Provides algorithms chosen by the eNodeB to be used
 - Is integrity-protected with K_{RRCint}
 - UE -> eNodeB response message:
 - Is ciphered and integrity-protected with $K_{\text{RRCenc/int}}$
 - Activate the protection of further radio communication (over DRBs and SRB1/2)

EPS state transition and security activation



Radio keys handling at hand-over (1/2)

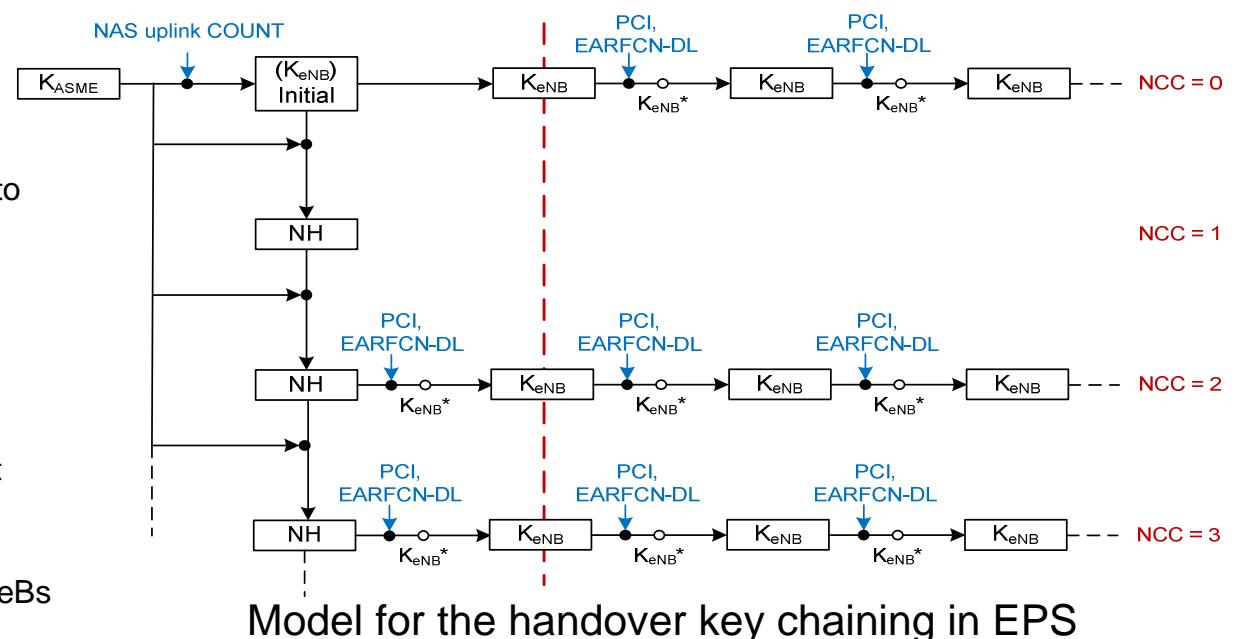
- Entering ECM-Connected mode: $\{K_{eNB}, NH, NCC\}$ established in MME and UE
- At Initial-Context-Setup: K_{eNB} used by initial serving eNodeB and UE to build the AS security context (with RRC and UP keys)
- Then, depending of types of mobility (S1, X2), content of S1 commands and available data in eNodeBs, 2 types of radio keys renewal happen

■ horizontal key derivation:

- current K_{eNB} is further derived with target eNodeB parameters in source eNodeB and UE
- K_{eNB}^* is transmitted to the target eNodeB and used to reconfigure the radio security at hand-over
- Backward security is achieved at eNodeBs level

■ vertical key derivation:

- a fresh $\{NH, NCC\}$ is derived by the UE and MME,
- MME transmits it to the target eNodeB
- NH is further derived by UE and eNodeB with target eNodeB parameters to produce a new K_{eNB} used to reconfigure the radio security
- Backward and forward security is achieved at eNodeBs level.



Radio keys handling at hand-over (2/2)

- For X2 hand-over:
 - When unused {NH, NCC} available in the source eNodeB, a vertical key derivation is triggered
 - When no fresh {NH, NCC} available, an horizontal key derivation is triggered
 - If the serving eNodeB receives a fresh {NH, NCC} after a horizontal key derivation, an intra-cell hand-over can be triggered to make use of it and achieve forward security
- For S1 hand-over:
 - A fresh {NH, NCC} is always used, as hand-over is managed by the serving MME
 - Always vertical key derivation
- The UE behaviour is the same regardless the type of derivation:
 - UE is instructed by the network
 - NCC is always transmitted to the UE in hand-over commands
 - If NCC is not incremented: horizontal key derivation
 - If NCC is incremented: vertical key derivation
 - It's possible for UE and MME to pre-compute all {NH, NCC} from the start of an active connection

Inter-operability with 2G and 3G

- MME and SGSN have to inter-operate
 - > In IDLE mobility from LTE to 2G / 3G:
 - An existing 3G security context (e.g. kept in UE cache) can be reused between UE and SGSN
 - EPS security context can be mapped to a 3G one and passed to SGSN
 - Full 3G-AKA
 - > In IDLE mobility from 2G / 3G to LTE:
 - An existing EPS security context (e.g. kept in UE cache) can be reused between UE and MME
 - 3G security context can be passed to target MME and mapped to an EPS security context
 - Full EPS-AKA
 - > In active mobility between 2G / 3G and LTE:
 - Procedures to map 3G and EPS security context
 - When mapping a 3G security context to an EPS one
 - strong recommendation to run an EPS-AKA and
 - take new "native" EPS security context into use quickly (e.g. with an LTE intra-cell HO)
- MME and MSC have to inter-operate for SRVCC (Single Radio Voice Call Continuity)
 - > In active mobility from LTE (PS domain) to 2G / 3G (CS domain):
 - EPS security context is mapped to a 3G CS one and passed to MSC server