Sécurité des réseaux mobiles

Isabelle KRAEMER – isabelle.kraemer@gmail.com
Janvier 2019

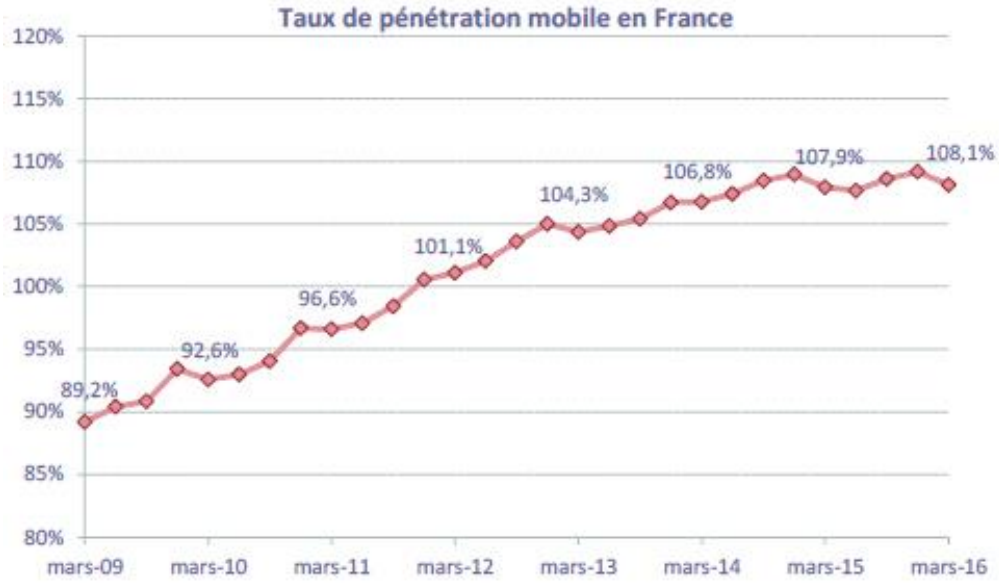
Objectifs du cours

- Plan du cours
  - Considération cryptographiques
  - Réseaux mobiles : principes génériques
  - La 2G
  - La 3G
  - La 4G
  - SS7
  - *Des outils*
  - *Perspectives*

- En particulier, nous n'aborderons pas :
  - La sécurité IMS
  - Des considérations spécifiques à un opérateur particulier

Un peu de contexte

Source : http://www.arcep.fr/index.php?id=13198#c66690



M Économie

ÉCONOMIE | Les données du "Monde" | Économie mondiale | Économie française | Entreprises

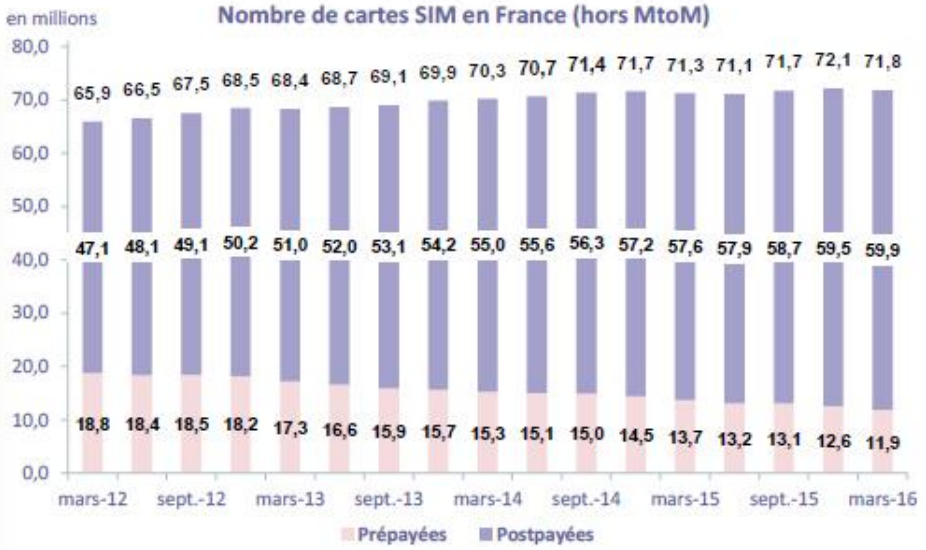
ÉDITION ABONNÉS

Lancement réussi de la 4G pour les trois opérateurs historiques

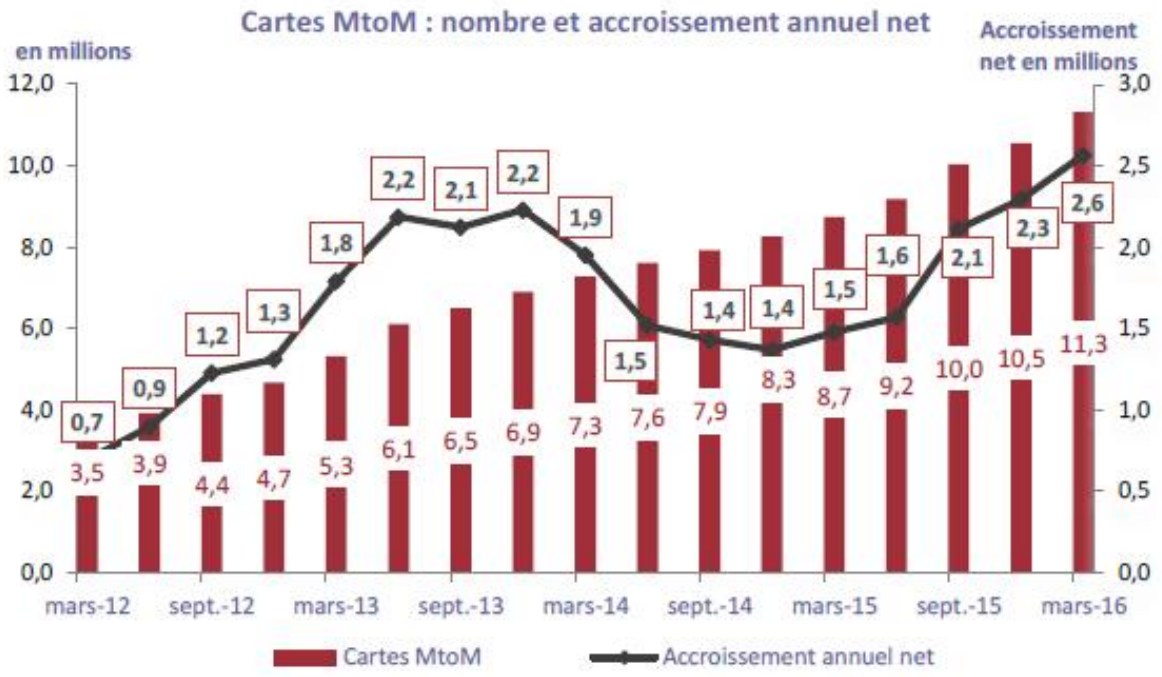
Orange, SFR et Bouygues Telecom ont chacun 1 million d'abonnés au très haut débit mobile.

LE MONDE | 10.01.2014 à 11h41 • Mis à jour le 10.01.2014 à 18h07 |

Par Sarah Belouezzane



Source : http://www.arcep.fr/index.php?id=13198#c66690



(2013) Espionnage de la voie radio par des Etats…

(2016) Interception de communications

… ou pas (2010)

(2015) Vol de secrets techniques

(2005 et 2014) Infiltration chez les opérateurs télécom

Que veut-on protéger ? Quelles propriétés ?

Considérations cryptographiques

La sécurité logique

- Intégrité
  - Le message n'a pas été modifié depuis son émission : il est intègre.
  - ex : « Je vous demande de faire un versement de 10000€ sur le compte numéro 806770 »

- Confidentialité
  - Le message est inintelligible pour toute entité non autorisée (qui n'est pas dans la confidence).
  - ex : « Je vous demande de faire un versement de ¿¾¥‡}®€ sur le compte numéro ‰žèß »

- Disponibilité
  - Le service est utilisable par un client légitime

Notions connexes

- Authentification
  - On est celui (ou celle) que l'on prétend être
    Je suis XXX, voici mon passeport (photo, bande magnétique, papier spécifique, sceau de l'organisme émetteur, empreintes digitales…).
  - ex : « Je vous demande de faire un versement de 1000€ sur le compte numéro 806770 »

- Anti-rejeu
  - Le message (par exemple un ordre) ne peut pas être répété
  - ex : 2x « Je vous demande de faire un versement de 1000€ sur le compte numéro 806770 »

A la base de la cryptographie : les mathématiques

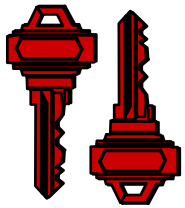
- Des algorithmes aux propriétés mathématiques spécifiques constituent les primitives cryptographiques.

- Par exemple:
  - Fonction non-inversible (ou difficile à inverser)
  - Fonction de chiffrement
  - Générateur pseudo-aléatoire (sortie non prédictible si on ne connaît pas totalement l'état d'initialisation du générateur)

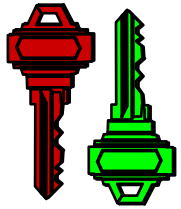
- Les primitives cryptographiques sont à la base des systèmes (ou protocoles) cryptographiques complets.
  - Par exemple : protection TLS, IPsec.

- Les crypto-systèmes servent à assurer la sécurité logique des communications.

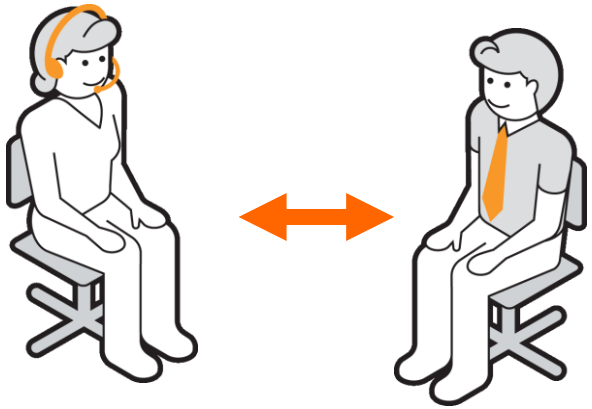
Les 2 grandes familles d'algorithmes cryptographiques



- Les algorithmes symétriques, dits à clés secrètes.
  - L'ensemble des entités impliquées dans une opération cryptographique (chiffrement, authentification…) doivent disposer de la même clé secrète.



- Les algorithmes asymétriques, dits à clés publiques.
  - Chaque entité dispose d'une clé secrète et met à disposition des autres entités une clé publique. La clé publique sert à vérifier / réaliser des opérations cryptographiques (chiffrement, authentification…) pouvant être réalisées / vérifiées uniquement avec la clé secrète.
  - Exemples:



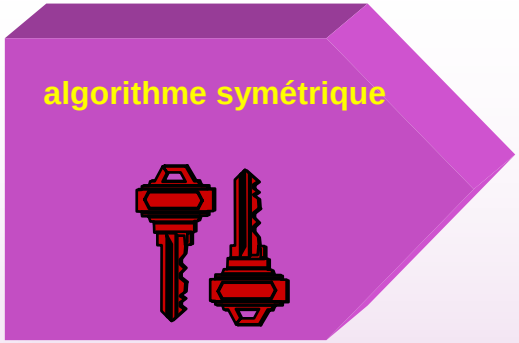
– Pour chiffrer un message et l'envoyer à Bob, Alice utilise la clé publique Pb de Bob. Seul la clé secrète Sb permet de déchiffrer le message.

– Pour signer un message et l'envoyer à Bob, Alice utilise sa clé secrète Sa. Seul la clé publique Pa permet de vérifier la signature du message.

Pourquoi 2 familles d'algorithmes différentes ?

- Les algorithmes symétriques ou asymétriques permettent d'effectuer des fonctions de bases identiques
  - chiffrement, contrôle d'intégrité, authentification
- La principale différence vient de la problématique de l'échange de clés :
  - Pour utiliser un **algorithme symétrique**, il est nécessaire pour Alice et Bob d'avoir préalablement échangé un secret (la clé).
  - Quand on utilise la **cryptographie asymétrique**, on publie les clés publiques des utilisateurs dans un annuaire.
    - Alice n'a donc pas besoin de partager un secret avec Bob, il lui suffit de récupérer la clé publique de Bob pour pouvoir communiquer avec lui.
    - Mais il faut mettre en place une PKI
- En pratique les deux types d'algorithmes cohabitent souvent
  - Les algorithmes asymétriques répondent mieux à la problématique d'échange de clé.
  - Ils sont par contre nettement plus lents que les algorithmes symétriques et demandent plus de ressource lors des calculs cryptographiques.

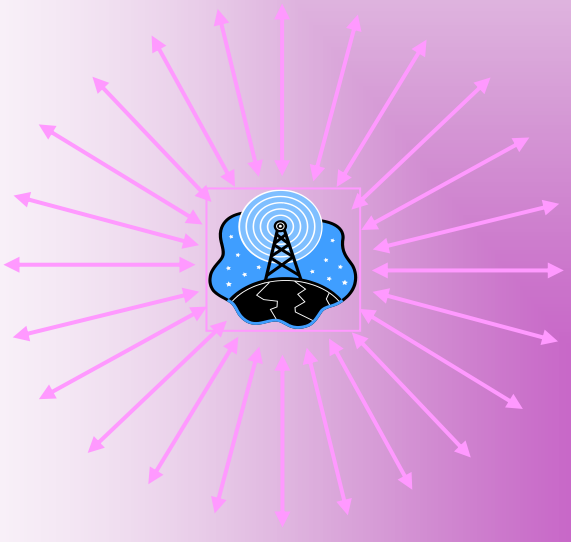
A chaque famille son modèle d'utilisation

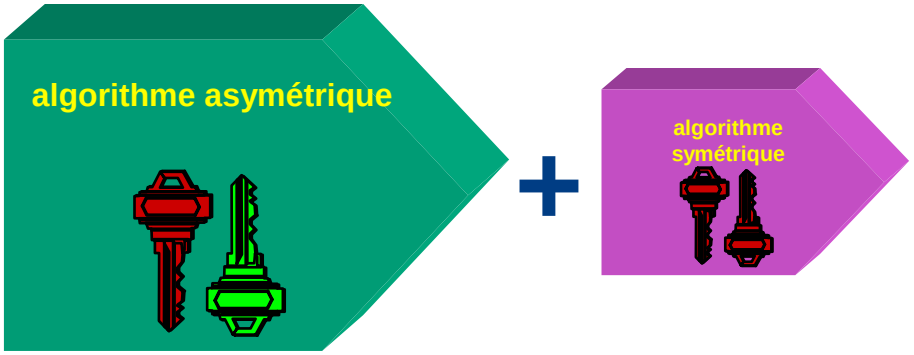


Modèle « fermé »

Relation en « étoile »

Exemple : les réseaux mobiles

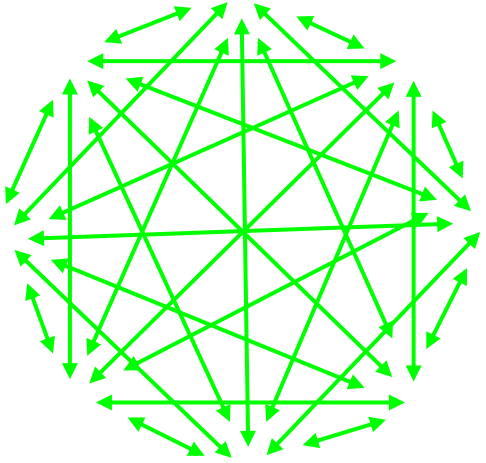




Modèle « ouvert »

Relation « peer to peer »

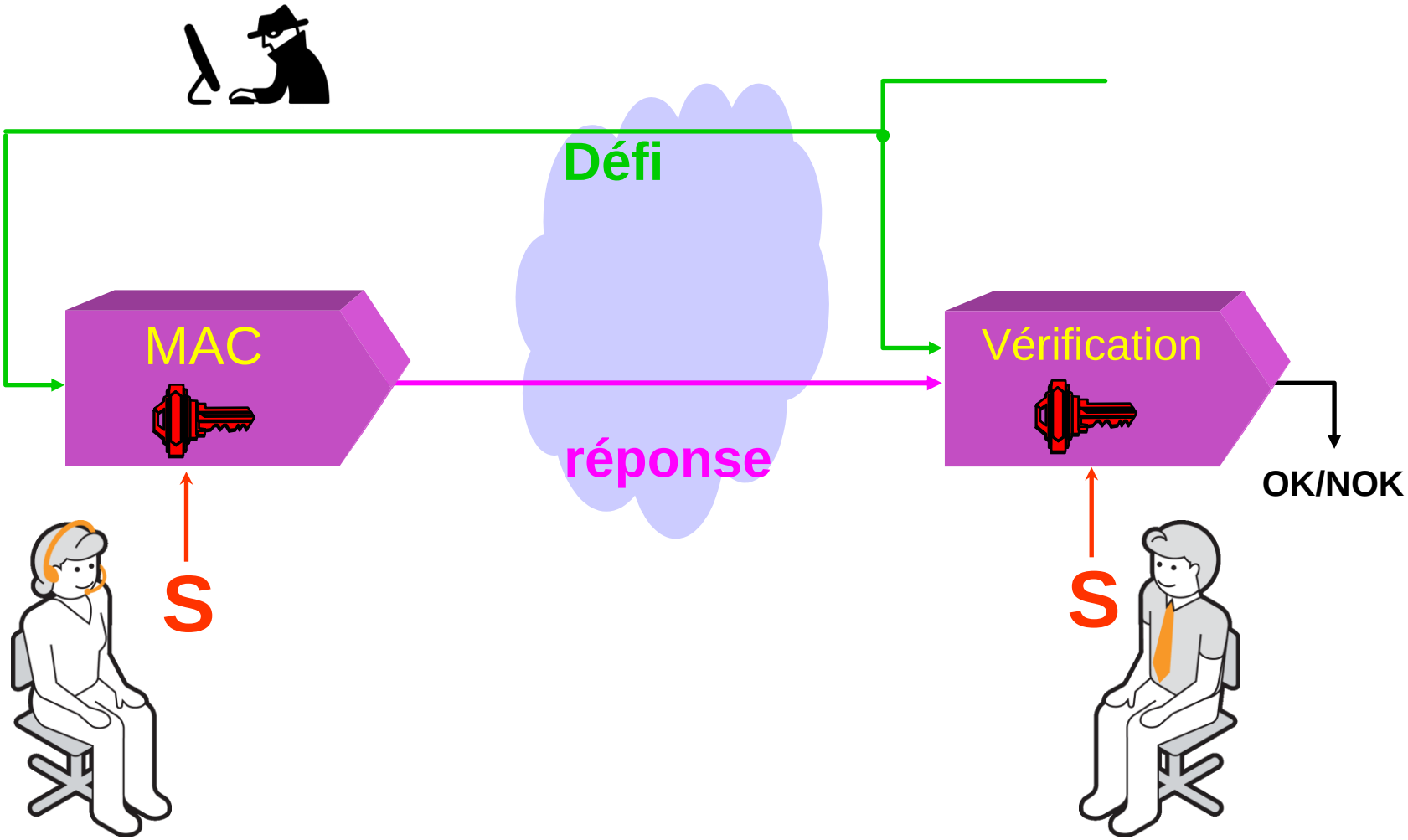
Exemple : Internet



La cryptographie symétrique

Les procédés : l'authentification à clé secrète

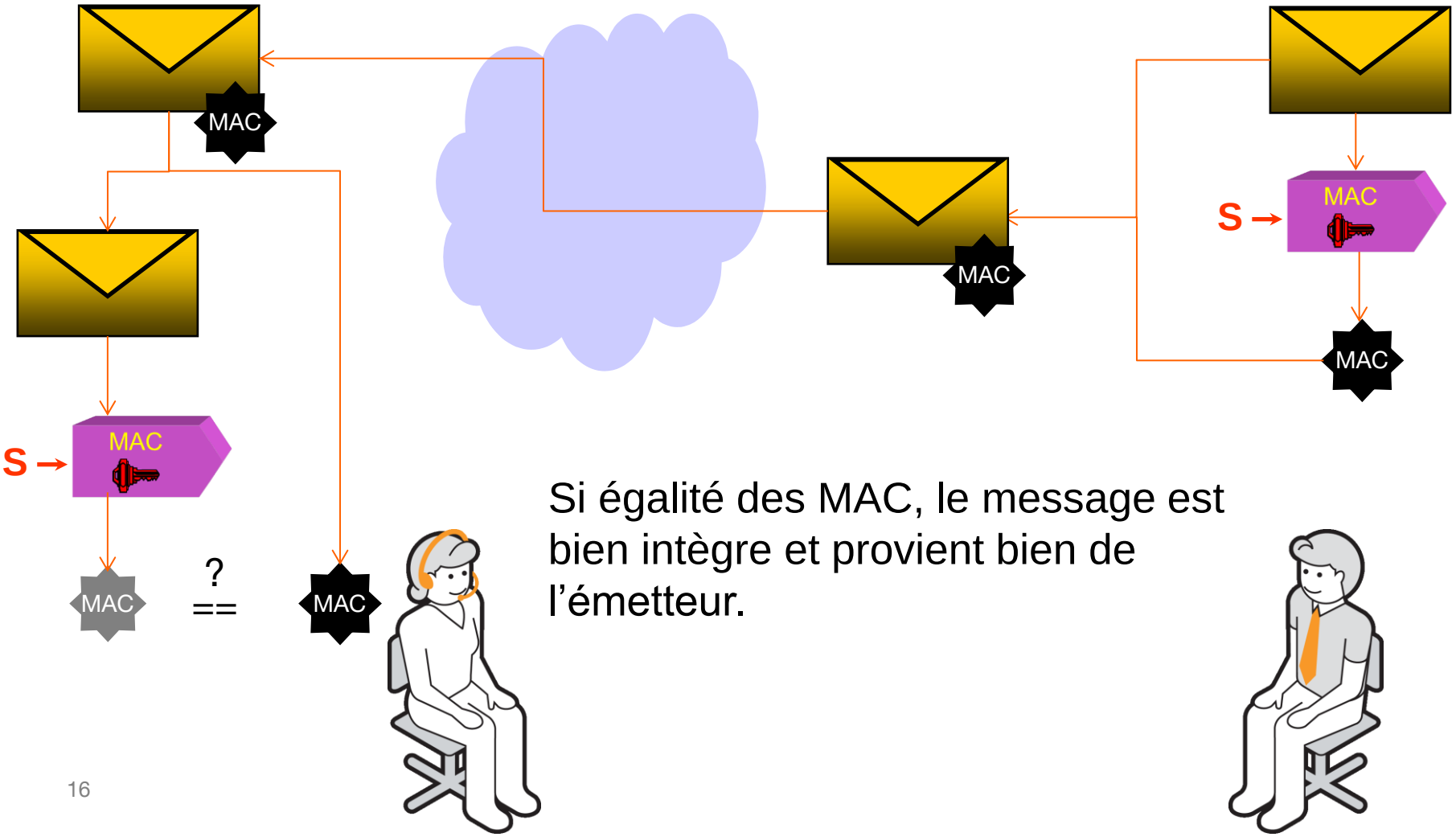
Seul le possesseur du secret **S** peut construire la réponse au défi du serveur. En observant les transactions, Max ne peut répondre à aucun défi car à des défis différents correspondent des réponses différentes.



Les procédés : code d'authentification de message (MAC)

Seul le possesseur du secret **S** peut construire le code d'authentification du message.

⇒ Assure **l'intégrité** du message et **authentifie** son expéditeur

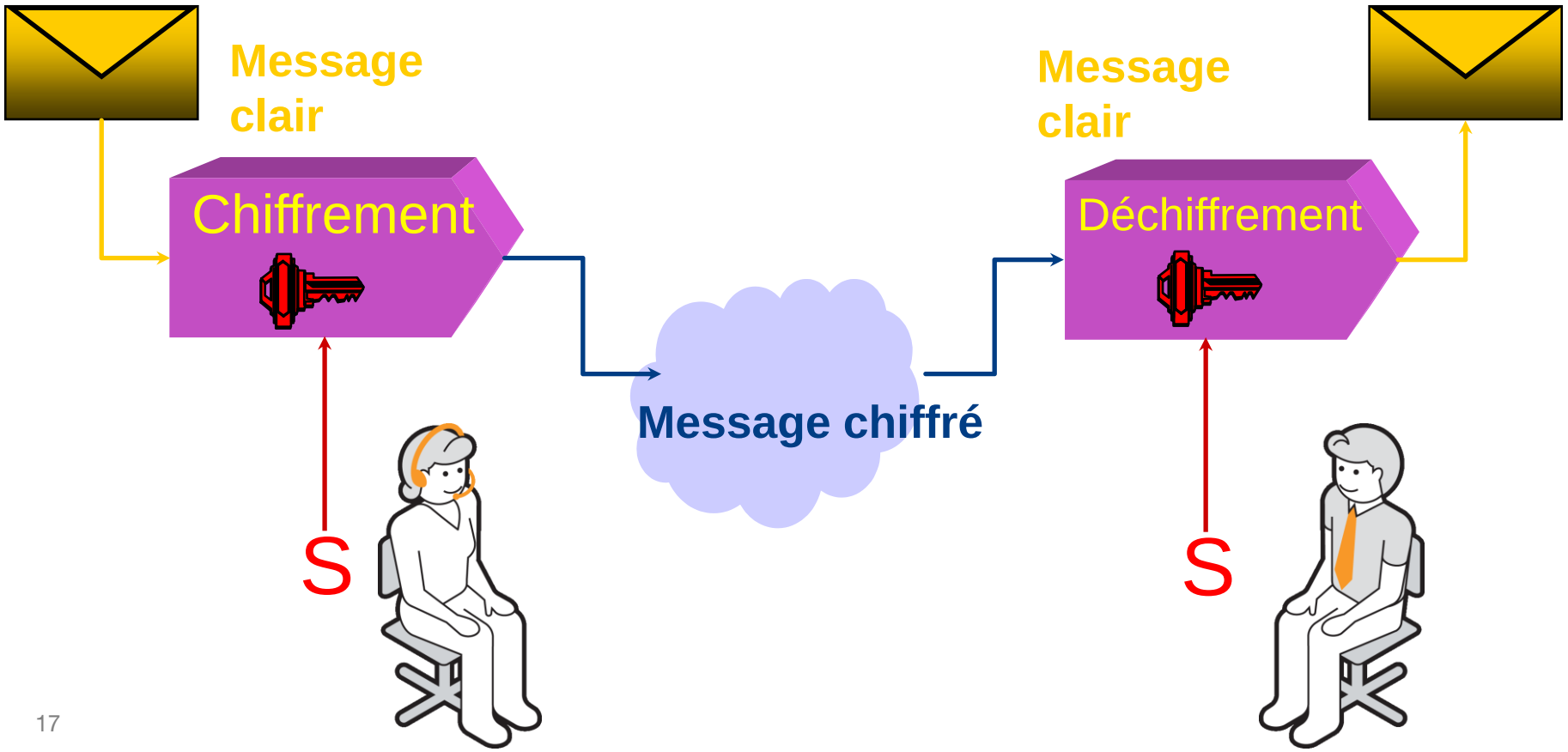


Si égalité des MAC, le message est bien intègre et provient bien de l'émetteur.

Les procédés : le chiffrement (symétrique)

Seul le possesseur du secret **S** peut récupérer le clair du message chiffré par Alice (dont le secret est S).

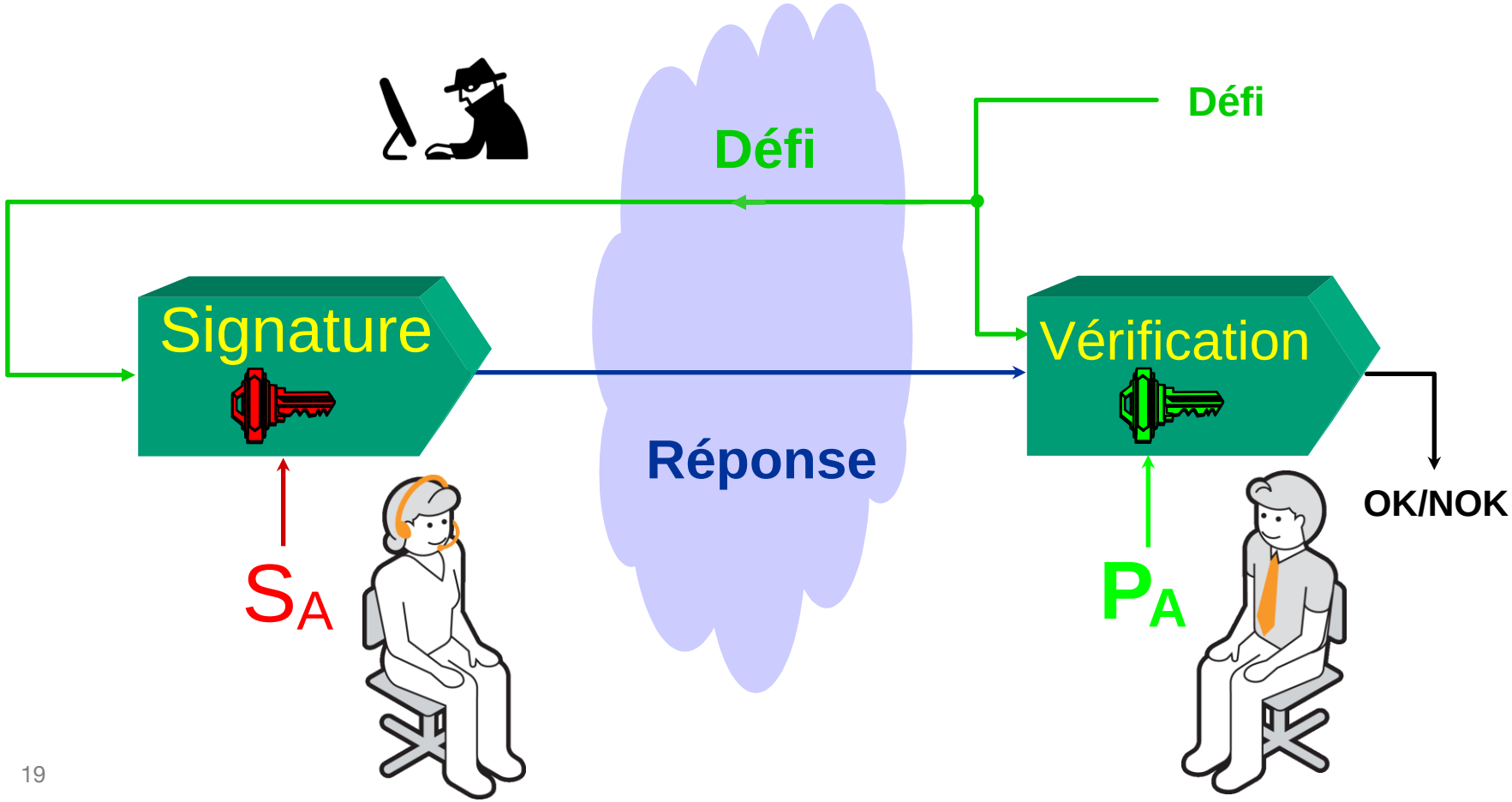
⇒ Assure la **confidentialité** des échanges entre les parties dans la confidence



La cryptographie asymétrique

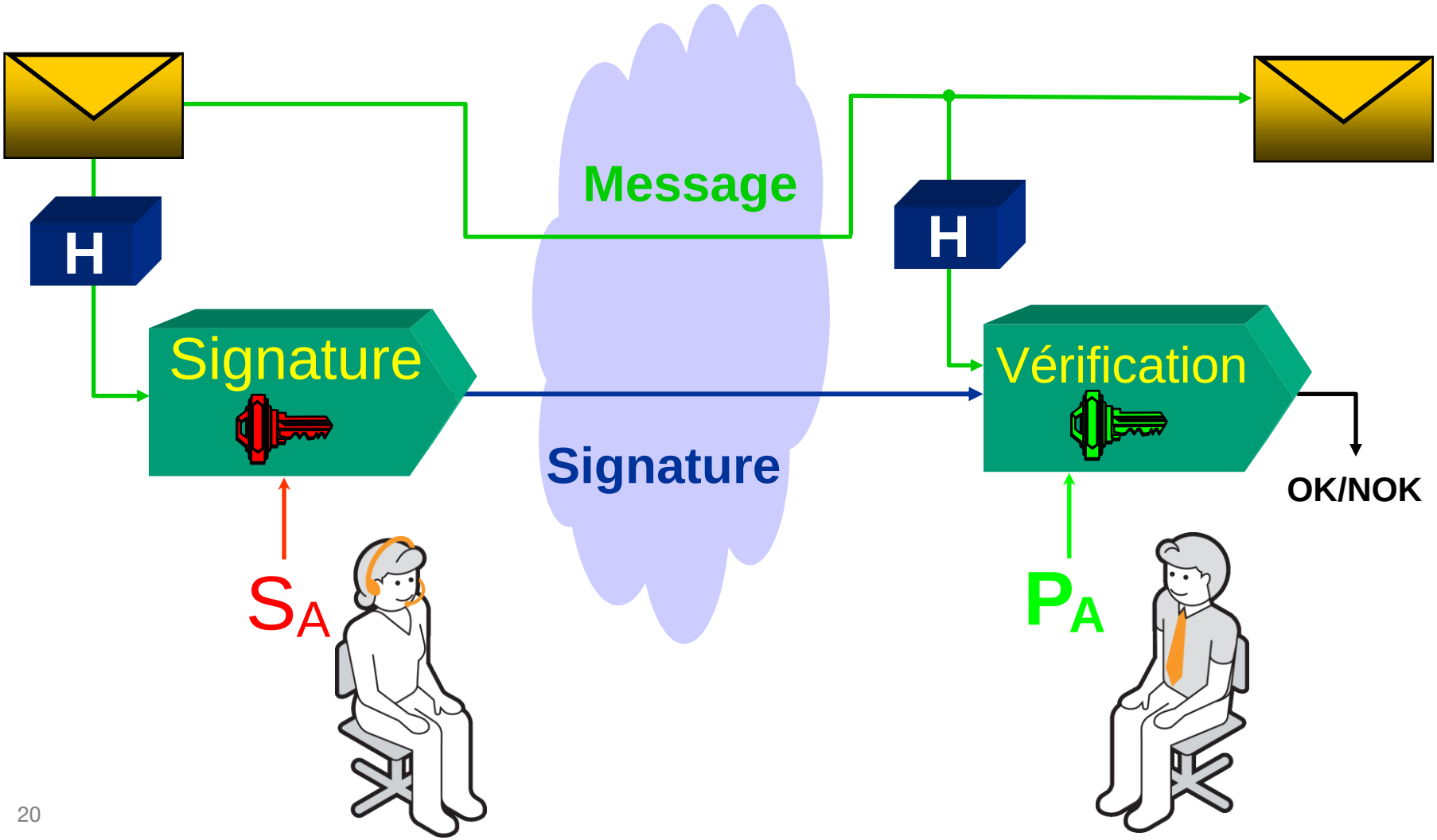
Les procédés : l'authentification

Seul le possesseur du secret S_A (Alice) peut construire la réponse au défi de Bob. En observant les transactions, Max ne peut répondre à aucun défi car à des défis différents correspondent des réponses différentes.

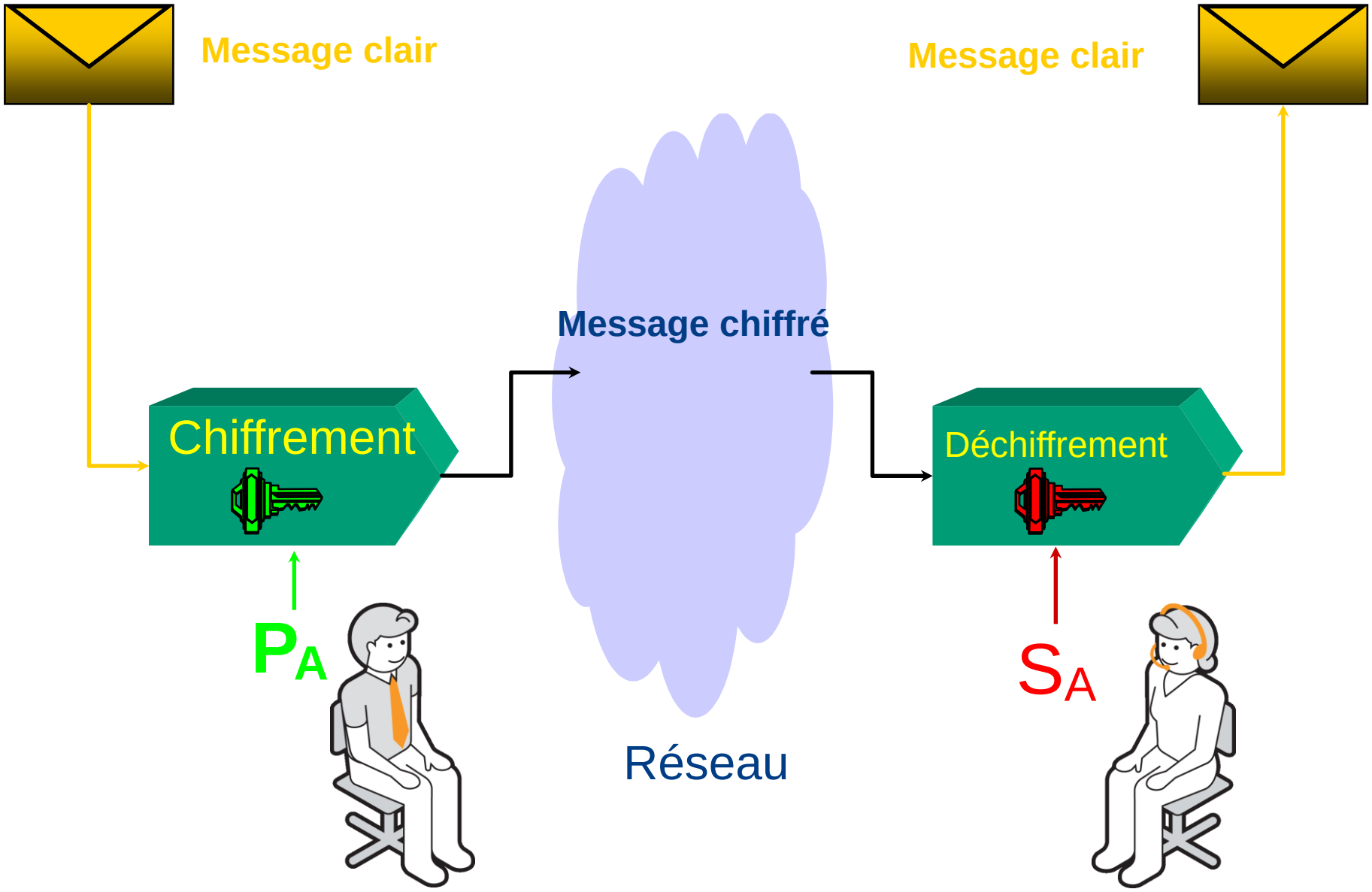


Les procédés : la signature avec condensation

La fonction de condensation (ou *hash function*) **H** permet de signer seulement un condensé (court) du message (qui lui peut être long).



Les procédés : le chiffrement (asymétrique)



Cryptanalyse

La cryptanalyse : quelques exemples d'attaques

- Sur les algorithmes de chiffrement :
  - **Attaque à texte clair choisi** : on choisit les messages clairs et on connait les messages chiffrés, le but est de retrouver la clé.
  - **Attaque à texte clair connu** : on connaît les messages clairs et on connait les messages chiffrés, même but (retrouver la clé).
  - **Attaque sur texte chiffré seul** : on connaît les messages chiffrés, il faut retrouver les messages clairs.
- Sur les algorithmes de *hashage* (utilisé principalement pour les signatures numériques) :
  - On cherche 2 messages qui ont le même *hash* (condensat) pour obtenir une collision.
  - On cherche un message qui donne le même *hash* qu'un message donné.
- De manière générale, on cherche des relations mathématiques sur les algorithmes cryptographiques afin de retrouver des informations de manière moins complexe que par recherche exhaustive
  - complexité = temps de calcul * espace de stockage * information nécessaire

En bref

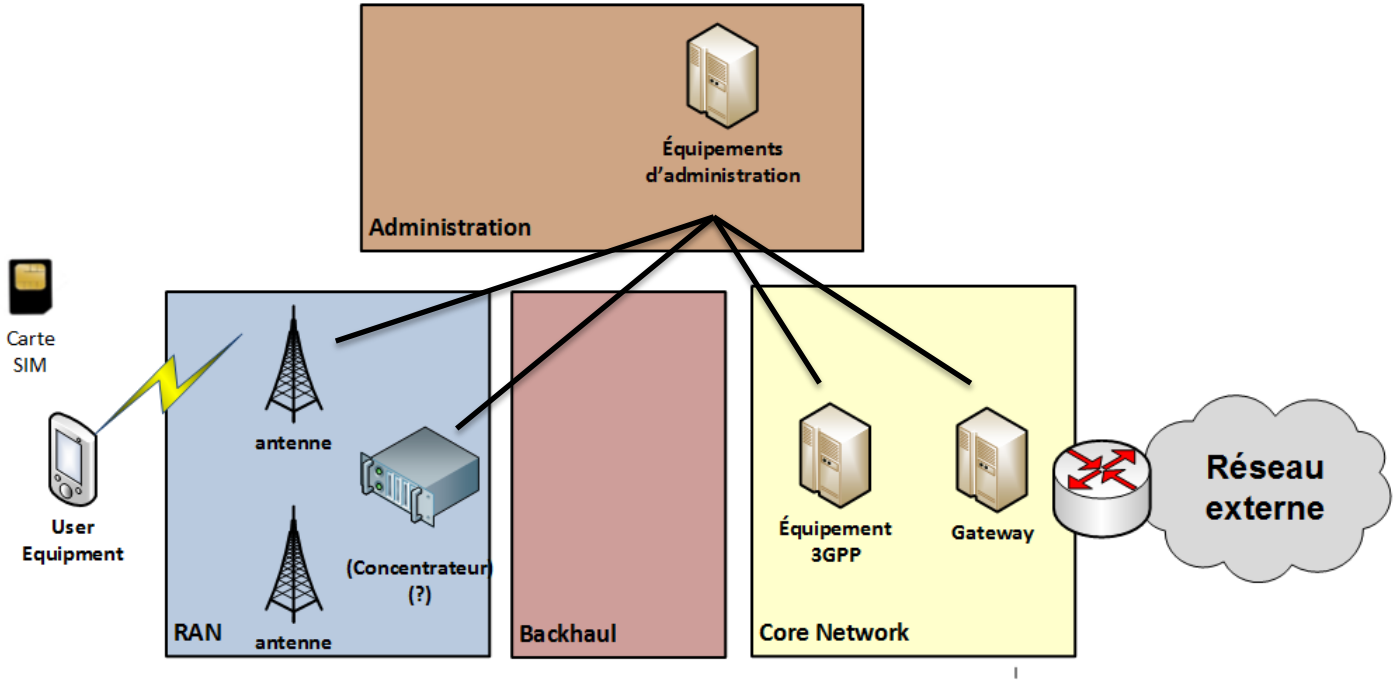
- La sécurité logique des réseaux mobiles (authentification, intégrité, confidentialité, anti-rejeu) repose sur la cryptographie symétrique.

Que faut-il pour faire un réseau mobile ?

Réseaux mobiles : principes génériques

Réseaux mobiles : les grands principes

- Les principaux composants
  - Un terminal mobile, équipé d'un carte SIM
  - Un réseau d'accès radio
  - Un cœur de réseau
    - « Circuit » pour les appels / SMS
    - « Paquet » pour la data
  - Une gateway vers des réseaux tiers

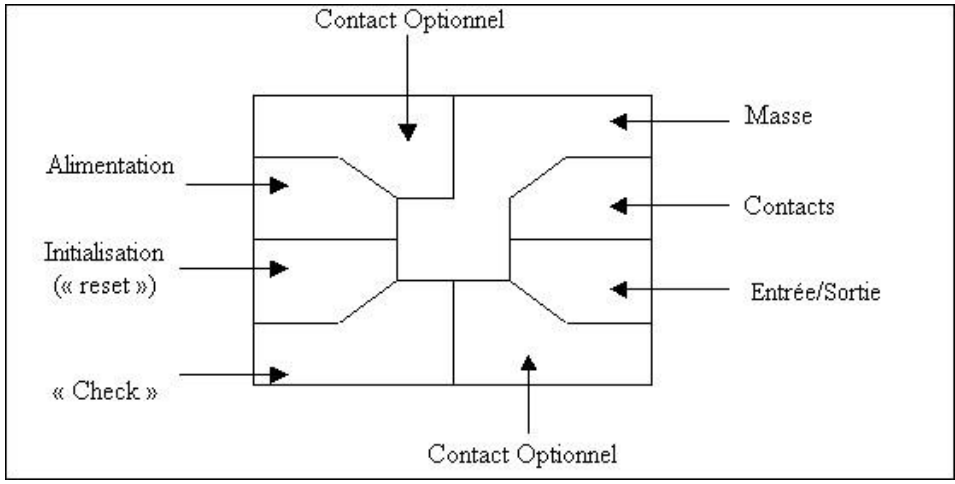


- Où stocker le secret partagé avec le réseau ?

La carte SIM

La carte SIM est une carte à puce

- Une carte à puce, c'est un microcomposant, ne possédant pas d'alimentation propre et permettant de stocker des informations et de faire des calculs.



- Une carte à puce contient
  - un microprocesseur,
  - des mémoires vives pour les calculs,
  - des mémoires réinscriptibles
  - des mémoires non réinscriptibles.

- Utilisation
  - Peut être programmée pour ne faire certaines opérations que si un code de sécurité (« code PIN ») lui est d'abord envoyé.
  - Peut contenir des secrets, des applications spécifiques ou non

La carte SIM est une carte à puce particulière

- Un coffre-fort pour stocker :
  - des données spécifiques de l'abonné (contacts, SMS), alors protégées par le code PIN de l'utilisateur
  - des données spécifiques à l'opérateur, par exemple l'IMSI, qui identifie l'abonné sur le réseau mobile et permet de lui associer son MSISDN.
  - des données sensibles (le secret partagé avec le réseau, les clés de session, etc)

- Une environnement sécurisé
  - Pour exécuter des procédures sensibles (ex : l'authentification de l'utilisateur au réseau).

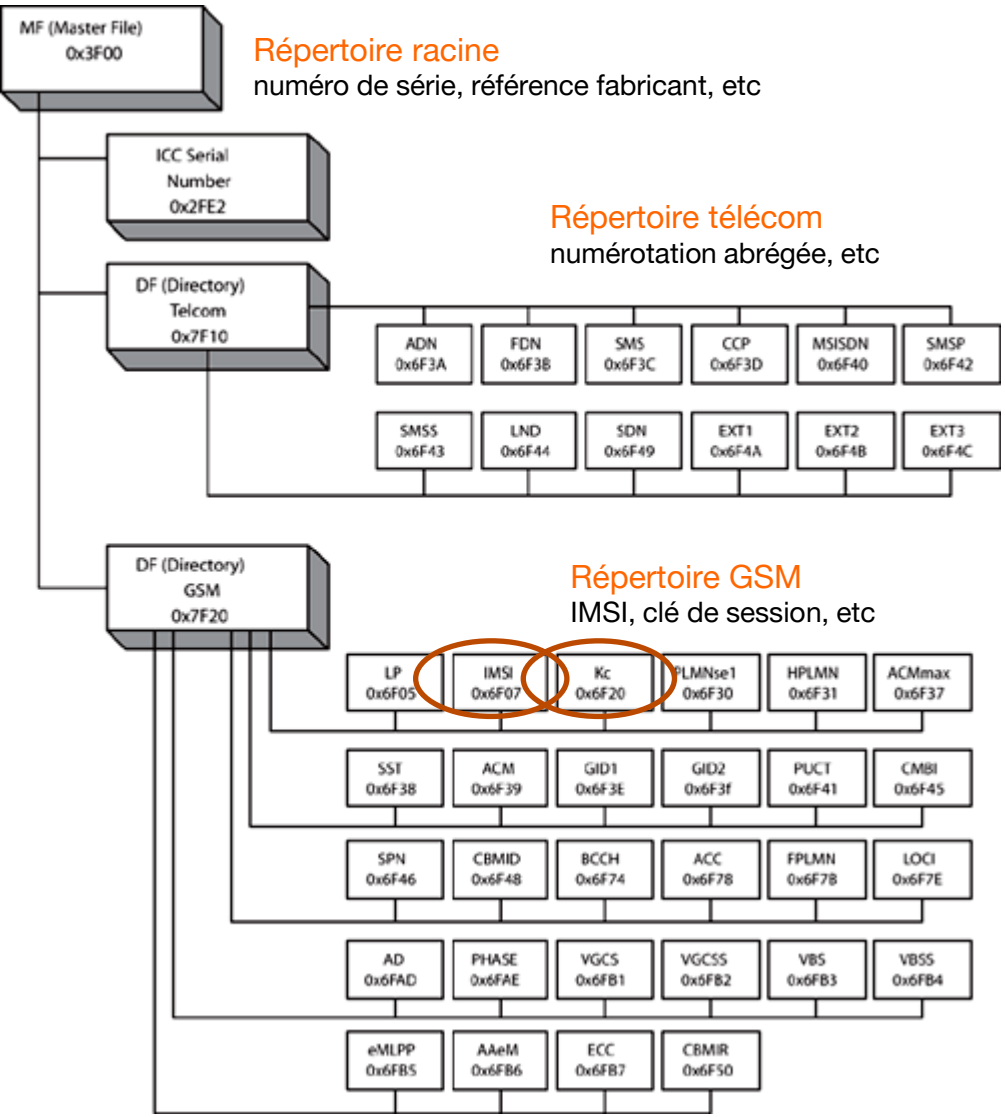
- Des interfaces de communication vers l'extérieur
  - Pour les I/O des fonctions sensibles

- Protégée contre le vol au moyen d'un code PIN vérifié dans la carte

- C'est une carte à puce avec des clés, des paramètres et des algorithmes spécifiques pour les réseaux mobiles

- Un élément de sécurité présent dès les premières spécifications des réseaux GSM (ETSI puis 3GPP TS 11.11)
  - Existence de processus stricts de certification des fonctions embarquées.
  - Ce n'est pas le cas sur les réseaux 3GPP2 (CDMA aux USA) ou la carte est optionnelle, et où les données sensibles sont souvent stockées directement dans le mobile.

La SIM contient un système de fichiers spécifique



- Système hiérarchique avec:
  - un MF : Master File, ou racine du FS
  - des DF : Dedicated File, ou répertoire
  - des EF : Elementary File, ou fichier
- Chaque MF, DF et EF :
  - est protégé ou pas en lecture / écriture selon des droits d'accès (droits ALW / PIN1 / PIN2 / ADM / NEV)

= une politique de sécurité pour l'accès aux données

Source image:
http://etutorials.org/Programming/Pocket+pc+network+programming/Chapter+8.+Pocket+PC+Phone+Edition/SIM+Manager/

La carte à puce : protection ultime?

- Non...
- Des attaques existent sur les cartes à puce, en analysant et/ou agissant sur les conditions extérieures (attaques par canaux auxiliaires):
  - Analyse de la consommation électrique (linéaire, différentielle).
  - Analyse du temps d'exécution de procédures sensibles.
  - Stress de la carte via le signal d'horloge, en température, en rayonnement électromagnétique (pour provoquer des erreurs).
- De plus, la carte ne protège pas contre le design maladroit d'une fonction de sécurité (voir COMP128-1 pour l'authentification au réseau GSM).
- Lorsqu'on veut embarquer une fonction de sécurité dans une carte, il faut:
  - Bien étudier son design, être sûr de sa sécurité intrinsèque.
  - L'implémenter afin d'empêcher toute attaque par canaux auxiliaires.
  - La valider soigneusement.

Attaque de type SPA ou DPA sur les cartes à puces

- Attaque pour retrouver la clé secrète en fonction de la consommation électrique de la carte lors de calculs cryptographiques.

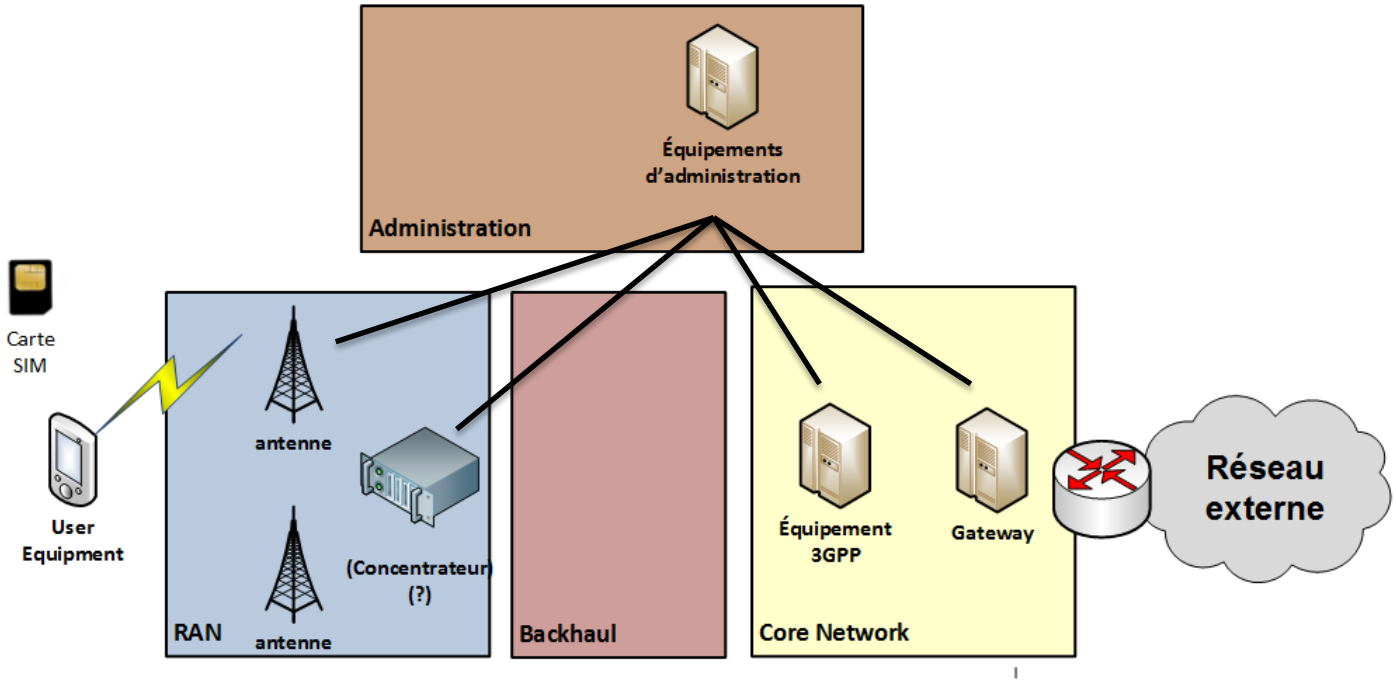
- L'analyse de la consommation électrique donne des informations sur les opérations basiques effectuées : élévation au carré, multiplication, …
  - SPA : Single Power Analysis ; DPA : Differential Power Analysis.
  - Avec un SPA : le profil de consommation électrique de la carte permet de retrouver directement des bits de la clé secrète en fonction des opérations l'impliquant.
  - Avec un DPA : une analyse différentielle et statistique est réalisée sur un nombre important de réalisations d'un même calcul impliquant la clé secrète.

Normes et standards des cartes à puce

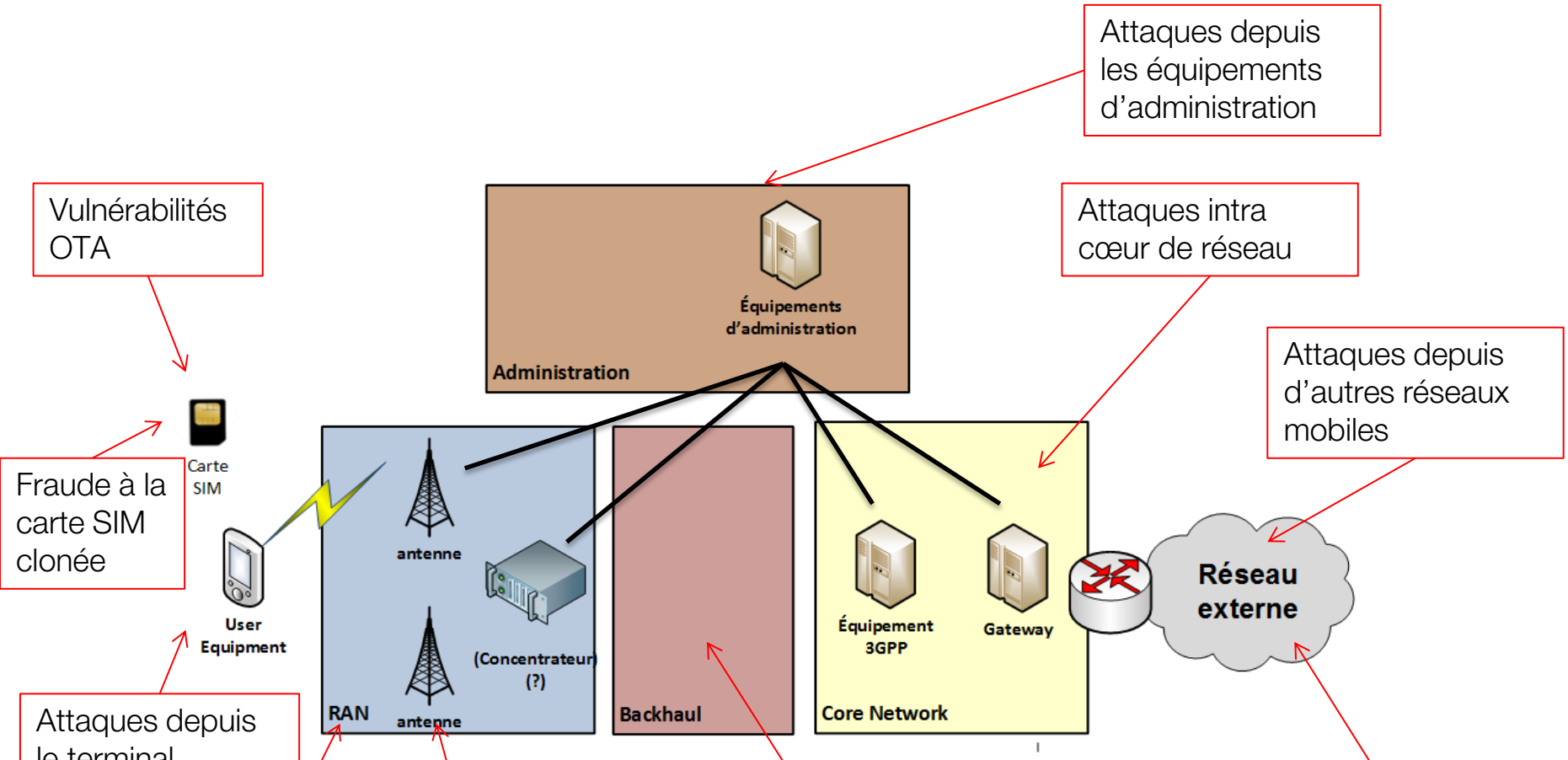
- Interface électrique des cartes à puce
  - ISO 7816 pour les cartes à contact, ISO 14443 et 15693 pour les cartes sans contact.
- Interface entre un terminal de télécommunication et les cartes UICC
  - ETSI TS 102.221 pour les aspects électriques, l'initialisation, les protocoles de transmission, les types de fichiers et de droits d'accès, la gestion des commandes APDU.
  - 3GPP TS 51.011 pour les cartes SIM (GSM / GPRS).
  - 3GPP TS 31.102 (et 31.101) pour les cartes USIM (GSM / GPRS / UMTS / LTE).
  - Les normes 3GPP définissent le système de fichiers (les fichiers, leurs adresses, leurs droits d'accès) et les procédures et commandes spécifiques aux réseaux mobiles.
- … Et dans d'autres domaines (pour les curieux)
  - EMV : norme internationale pour les cartes et terminaux de paiement.
  - PC/SC : PC Smart Card, librairie et API pour parler à une carte à puce avec son PC.
  - JavaCard : norme internationale pour définir des API de programmation et d'interfaces applicatives sur les cartes à puces. S'appuie sur une machine virtuelle JAVA pour carte à puce.

Quelles attaques sur les réseaux mobiles ?

Quelles attaques ?



Quelques exemples d'attaques potentielles

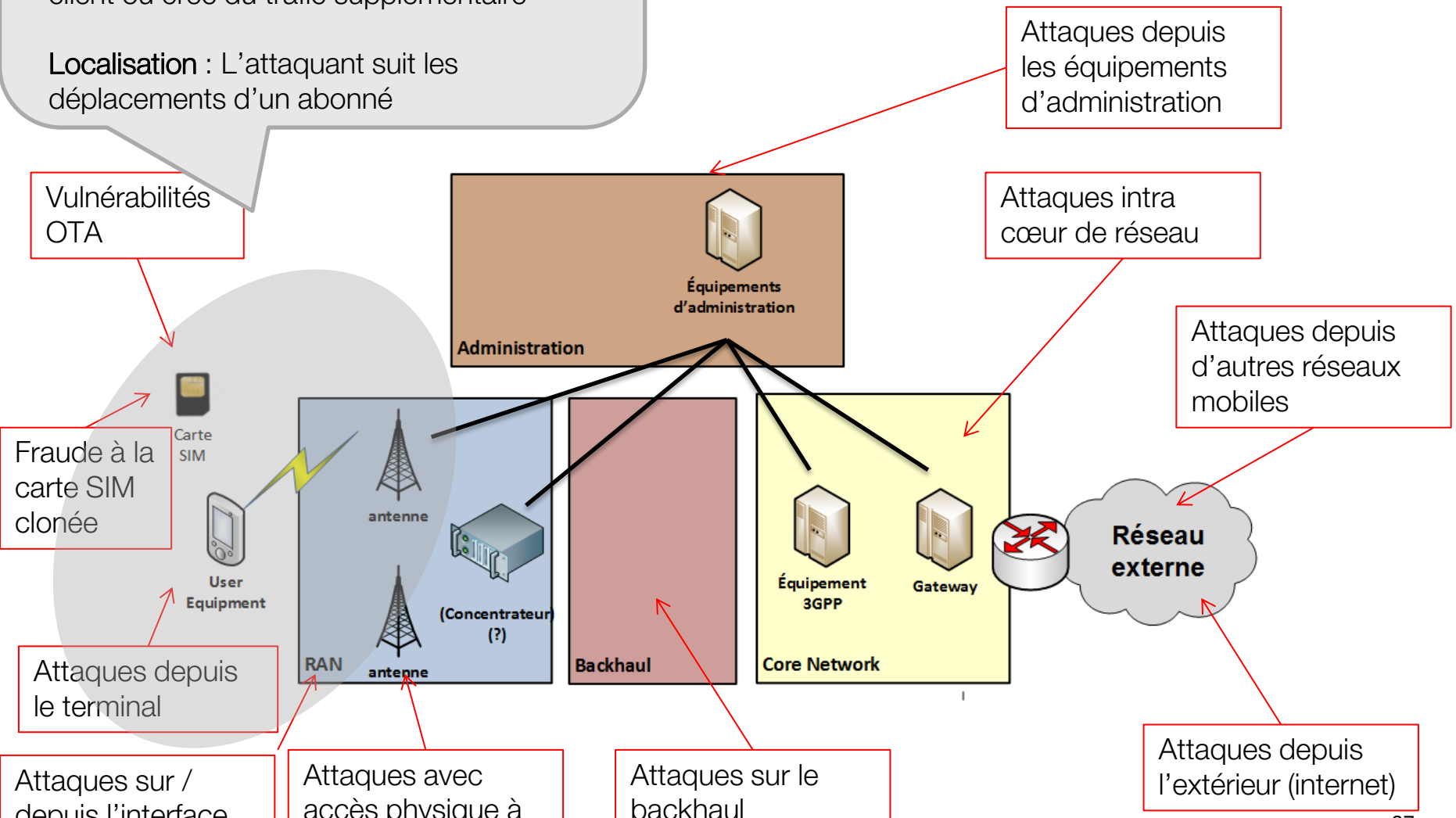


Quelques exemples d'attaques potentielles

Ecoute illégitime : L'attaquant peut lire le contenu des communications émises vers / depuis le client

Détournement de communication : L'attaquant modifie les communications du client ou crée du trafic supplémentaire

Localisation : L'attaquant suit les déplacements d'un abonné



Sécurité de l’accès radio

- La sécurité de l'accès radio : aspect primordial
- La communication radio est ouverte, accessible à tout utilisateur à portée de l'émission.
- La modulation et le codage radio (modulation en fréquence et en phase, multiplexage en temps / en fréquence…) définissent un canal de communication accessible à quiconque en connaît les paramètres (et dispose du matériel nécessaire).
- Nécessité de mise en place de mécanismes de sécurité basés sur des techniques cryptographiques, pour remédier aux problèmes rencontrés.

38

Types de trafic

Plusieurs types de trafic

- Le trafic utilisateur
  - Interprété par l'utilisateur final uniquement
  - Protection de la confidentialité des communications des abonnés
  - Protection de l'intégrité jugée non nécessaire
- Le trafic de signalisation
  - Utilisé pour faire transiter des données sensibles (par exemple, nouvelles identités) et pour le bon fonctionnement du service (handovers, renouvellement des clés…)
    - Nécessité de chiffrer
  - Utilisé pour la négociation d'algorithmes de chiffrement
  - Interprété par les équipements intermédiaires : nécessité de garantir un contenu cohérent
    - Nécessité de garantir l'intégrité des messages
- De manière générale :
  - Chiffrement du trafic utilisateur (optionnel), pour toutes les générations
  - Chiffrement de la signalisation (optionnel)
  - Intégrité de la signalisation assurée depuis la 3G
    - Evolution du modèle de sécurité suite aux attaques constatées sur la 2G

La 2G

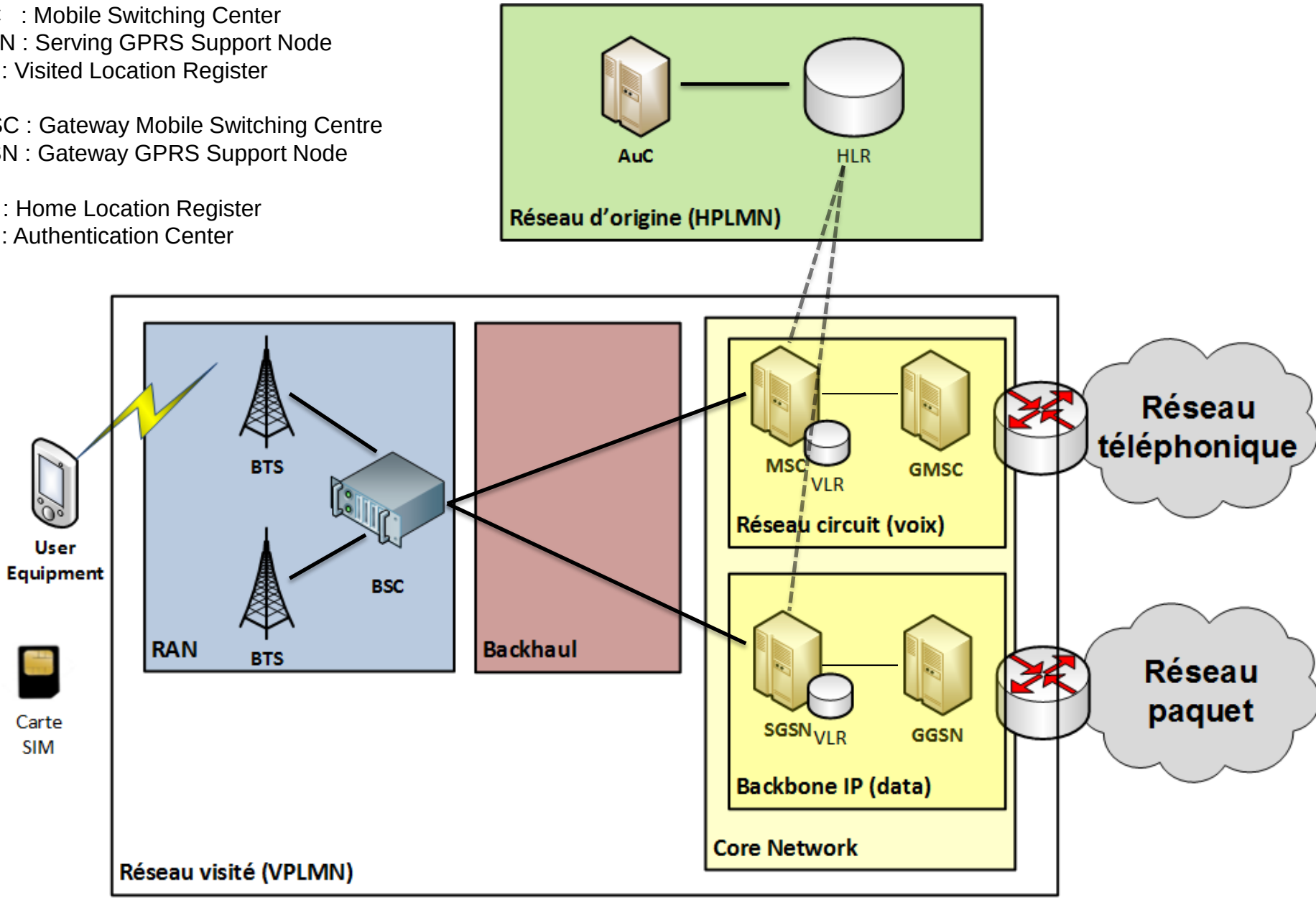
L'architecture GSM - GPRS

SIM : Subscriber Identity Module
BTS: Base Transceiver Station
BSC : Base Station Controller

MSC : Mobile Switching Center
SGSN : Serving GPRS Support Node
VLR : Visited Location Register

GMSC : Gateway Mobile Switching Centre
GGSN : Gateway GPRS Support Node

HLR : Home Location Register
AuC : Authentication Center



Quelles fonctions de sécurité pour la 2G ?

GSM / GPRS : principales fonctions de sécurité

- Utilisation d'identités temporaires – TMSI
  - Protège l'utilisateur contre le repérage passif, la localisation.

- Authentification de l'utilisateur – algo A3/A8
  - Principe : envoi d'un challenge à la carte SIM : la réponse ne peut être juste que si l'on connait Ki
  - Assure le contrôle d'accès au réseau, permet d'éviter la fraude
  - Utilisation d'une carte SIM (clé permanente Ki, algorithme d'authentification et de dérivation de clé de session)

- Chiffrement de la voie radio – algo A5 (GSM) et GEA (GPRS)
  - Assure la protection de l'utilisateur contre les écoutes illicites
  - Protège le réseau de l'opérateur car la signalisation est chiffrée elle aussi

Identification de l'abonné

- MSISDN (Mobile Subscriber ISDN number) :
  - Numéro utilisé par les humains
  - Structure : CC + NDC + SN (ex: 33 6 AB PQ MC DU)

- IMSI (International Mobile Subscriber Identity) :
  - "Identité Privée"
  - Transmise le moins possible sur l'interface radio pour éviter le tracking
  - Structure (15 chiffres) : MCC + MNC + MSIN (ex: 208 01 X1…Xn)
  - MCC : Mobile Country code (3 chiffres)
    - caractérise un pays (exemple : France = 208, Nepal = 429...)
  - MNC : Mobile Network Code (2 or 3 chiffres)
    - caractérise un opérateur (Orange France = 01, SFR = 10, Bouygues = 20)

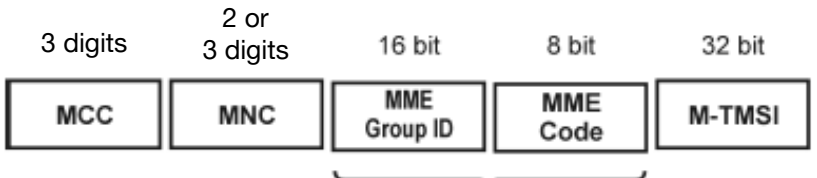
2G / 3G

- TMSI (Temporary Mobile Subscriber Identity)
  - Identitié temporaire allouée par le MSC (à l'abonné pour masquer son IMSI
  - Réallocation régulière de TMSI par le MSC
  - Portée locale à un MSC / VLR

4G

- GUTI (Globally Unique Temporary Identifier)
  - Identité temporaire allouée par le MME (LTE) à l'abonné pour masquer son IMSI
  - Portée globale

GUTI



Source : TS 23.003

GSM : Anonymat

- IMSI = International Mobile Subscriber Identity
  - identité figée
- TMSI = Temporary Mobile Subscriber Identity
  - fréquemment renouvelée
- 1ère communication en arrivant sur un réseau
  - Début de communication : IMSI est transmis en clair.
  - Après passage en mode chiffré : une première valeur de TMSI, choisie par le VLR, est transmise au mobile.
- Communications ultérieures
  - Début de communication : le TMSI est transmis en clair
  - Le TMSI est renouvelé à chaque mise à jour de localisation.
  - Un nouveau TMSI est transféré durant la session chiffrée.

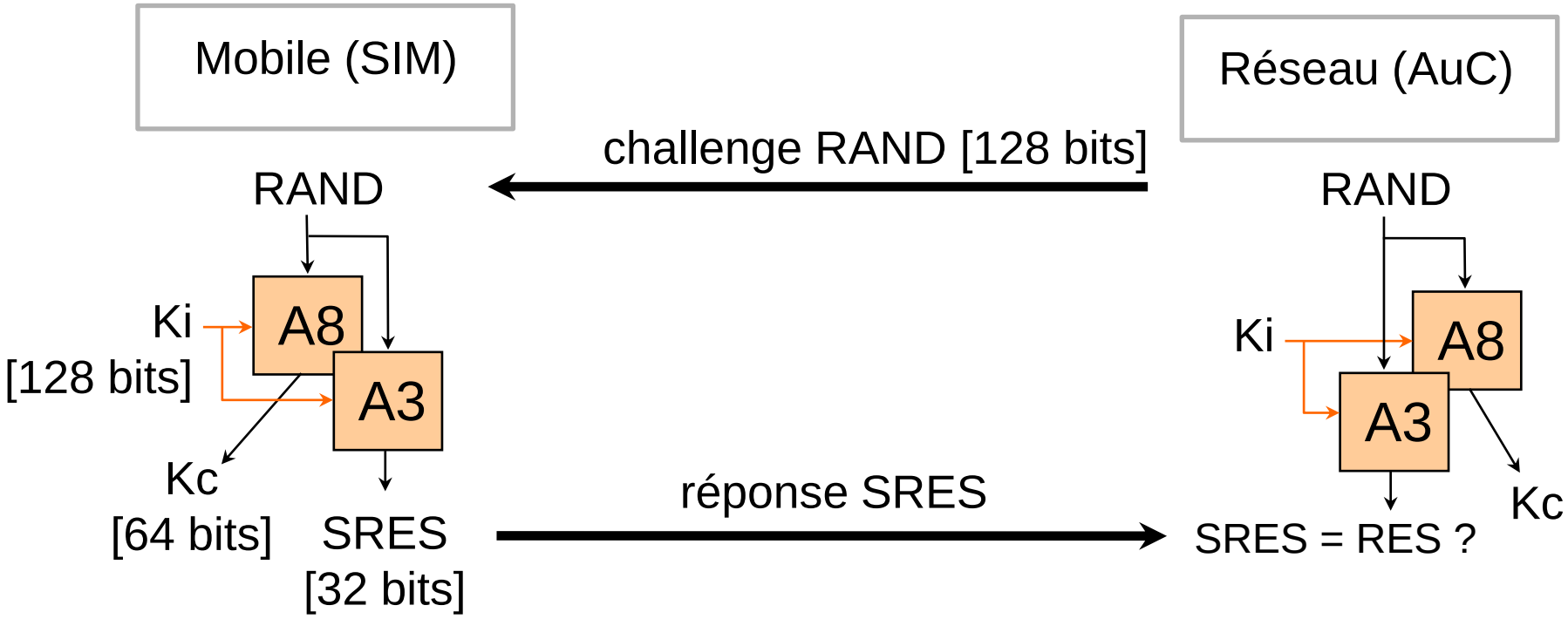
GSM / GPRS : principales fonctions de sécurité

- Utilisation d'identités temporaires – TMSI
  - Protège l'utilisateur contre le repérage passif, la localisation.

- Authentification de l'utilisateur – algorithmes A3/A8
  - Principe : envoi d'un challenge à la carte SIM : la réponse ne peut être juste que si l'on connait Ki
  - Assure le contrôle d'accès au réseau, permet d'éviter la fraude
  - Utilisation d'une carte SIM (clé permanente Ki, algorithme d'authentification et de dérivation de clé de session)

- Chiffrement de la voie radio – algo A5 (GSM) et GEA (GPRS)
  - Assure la protection de l'utilisateur contre les écoutes illicites
  - Protège le réseau de l'opérateur car la signalisation est chiffrée elle aussi

GSM / GPRS : fonctions A3 / A8



GSM / GPRS : principes de l'authentification

- Basée sur le partage d'un secret (clé Ki de 128 bits) entre le mobile (carte SIM) et le réseau (AuC) et des fonctions cryptographiques à clé secrète appelées A3 / A8.

- Le calcul d'authentification permet, à partir de Ki et d'un challenge RAND (128 bits), de générer une réponse RES (32 bits) et une clé de chiffrement Kc (64 bits).
  - RES va être contrôlé par le réseau pour authentifier le mobile.
  - Kc va être utilisée pour chiffrer la communication entre le mobile et le réseau.

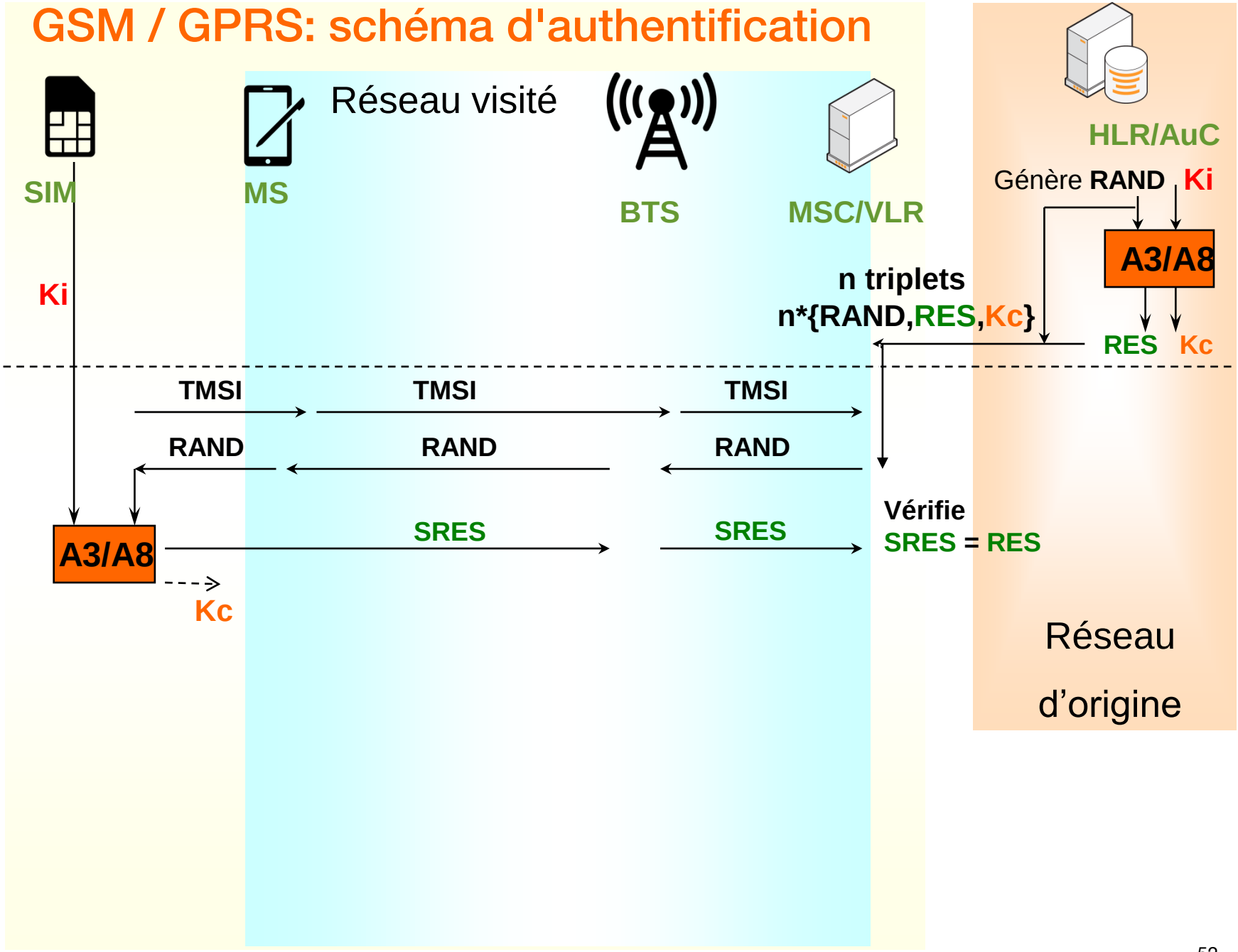
- L'algorithme d'authentification et d'établissement de clé de chiffrement (le cœur de A3 / A8) n'est pas normalisé : il est propre à chaque opérateur, même si des versions conseillées existent.

- Les calculs d'authentification sont réalisés dans l'AuC pour le réseau, et dans la carte SIM pour le terminal. La clé Ki n'est jamais révélée en dehors de ces environnements.

Fonctions A3 / A8 : propriétés requises

- **Non forgeabilité**
  - L'observation de n sorties {Kc, SRES} correspondant à des entrées RAND connues ou choisies ne doit pas permettre de calculer la clé Ki ou de prédire une sortie correspondant à une nouvelle valeur RAND.
  - En particulier, résistance aux méthodes d'attaque connues : cryptanalyse linéaire, cryptanalyse différentielle, attaques par collisions...
- **Séparation cryptographique**
  - La donnée de SRES ne doit fournir aucune information sur Kc (et inversement).
- **L'implémentation sur la carte SIM** doit résister aux attaques par canaux auxiliaires.

GSM / GPRS: schéma d'authentification



GSM / GPRS : l'authentification cassée

- La 1ère version de l'algorithme noyau recommandé pour les fonctions A3 / A8 : COMP128-1, n'était pas suffisamment fiable.
  - Algorithme développé en 1988.
  - Algorithme non normalisé, mais proposé et extrêmement largement adopté.
  - Algorithme non publié, fourni aux opérateurs GSM de manière privée.
  - Reconstruit et publié suite à des "fuites" et de la retro-ingénierie.
  - Cassé : donnant la possibilité de cloner des cartes SIM de manière simpliste (et donc de frauder).
    - Code source disponible ici : http://www.scard.org/gsm/a3a8.txt
    - Permet le clonage de carte SIM : http://mkccybertech4u.yu.tl/files/cardclone.pdf

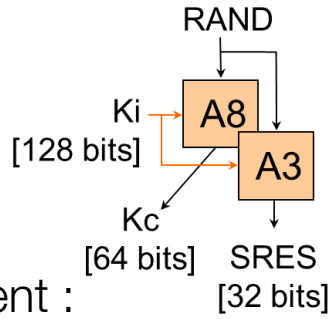
- COMP128-1 génère des collisions.
  - Pour une clé Ki, on peut trouver RAND1 et RAND2 tels que : COMP128-1(Ki, RAND1) = COMP128-1(Ki, RAND2)
  - Cette propriété permet de retrouver la clé Ki en utilisant quelques milliers de challenges RAND
    - 50 000 lors de la 1ère attaque, ~20 000 pour les meilleures attaques aujourd'hui

- COMP128-2 puis 3 ont été ensuite proposés, ainsi que Milenage-2G, adaptation au GSM / GPRS de l'algorithme Milenage défini pour l'UMTS.
  - Malheureusement, COMP128-1 reste utilisé aujourd'hui encore dans certains réseaux GSM.

GSM / GPRS : principales fonctions de sécurité

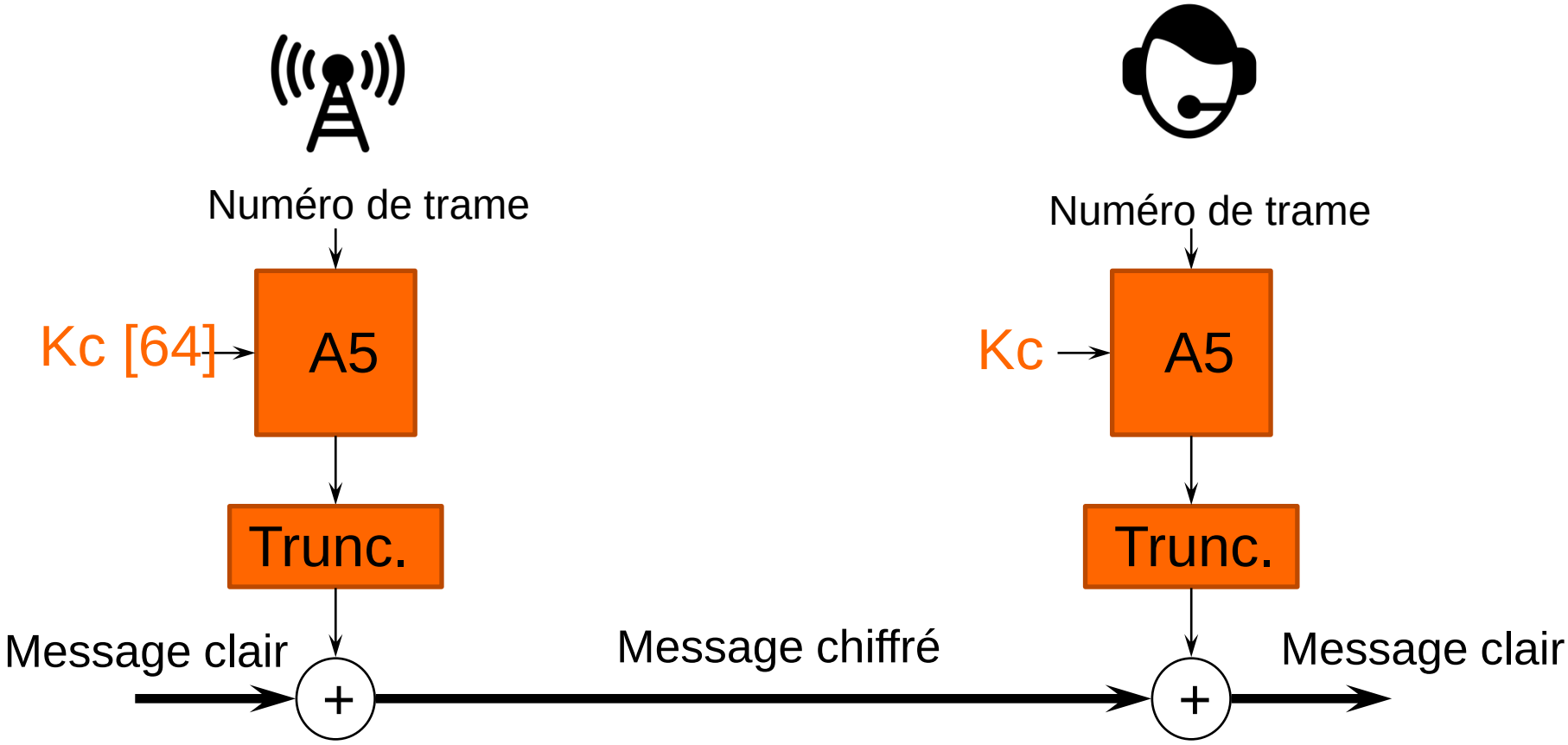
- Utilisation d'identités temporaires – TMSI
  - Protège l'utilisateur contre le repérage passif, la localisation.
- Authentification de l'utilisateur – algo A3/A8
  - Principe : envoi d'un challenge à la carte SIM : la réponse ne peut être juste que si l'on connait Ki
  - Assure le contrôle d'accès au réseau, permet d'éviter la fraude
  - Utilisation d'une carte SIM (clé permanente Ki, algorithme d'authentification et de dérivation de clé de session)
- Chiffrement de la voie radio – algo A5 (GSM) et GEA (GPRS)
  - Assure la protection de l'utilisateur contre les écoutes illicites
  - Protège le réseau de l'opérateur car la signalisation est chiffrée elle aussi

GSM : la confidentialité des communications



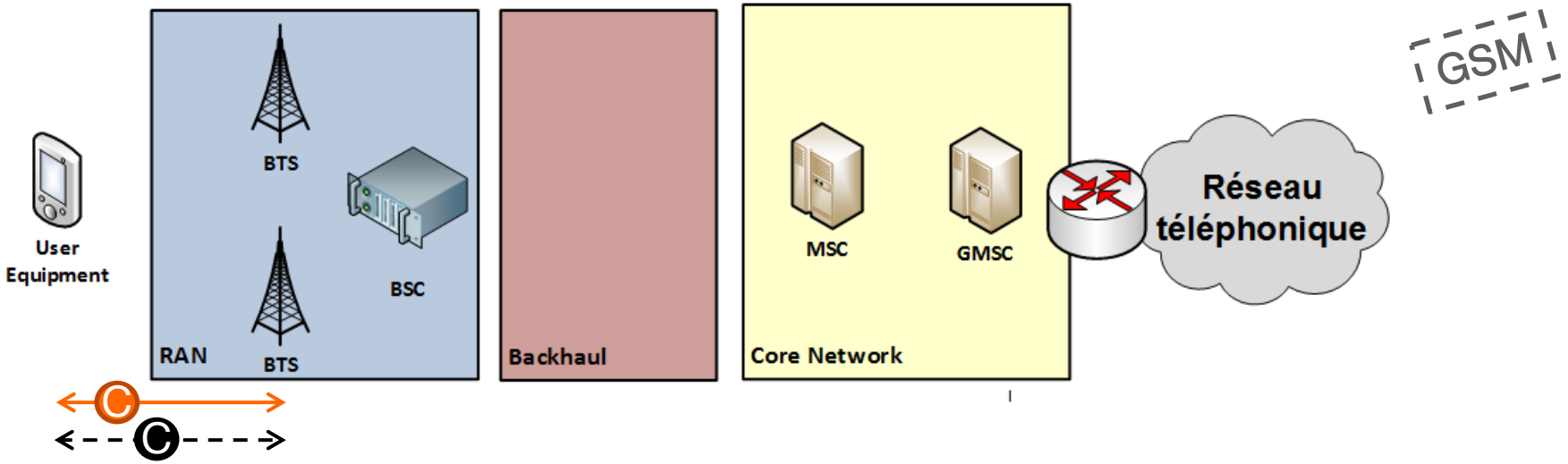
- La confidentialité des communications repose sur le chiffrement :
  - du trafic utilisateur (voix) et de la signalisation;
  - entre le mobile et la BTS.
- Le chiffrement utilise la clé de session Kc de 64 bits établie lors de la procédure d'authentification.
- Il est réalisé par la fonction A5
  - A5/0 : pas de chiffrement.
  - A5/1 : l'algorithme de chiffrement initial du GSM.
  - A5/2 : une version très affaiblie de A5/1, ne donne pas de réelle sécurité.
  - A5/3 : nouvel algorithme défini lors des travaux sur l'UMTS.
  - A5/4 : nouvel algorithme défini lors des travaux sur l'UMTS.
- A5 est une fonction de chiffrement à flot.

Le chiffrement GSM

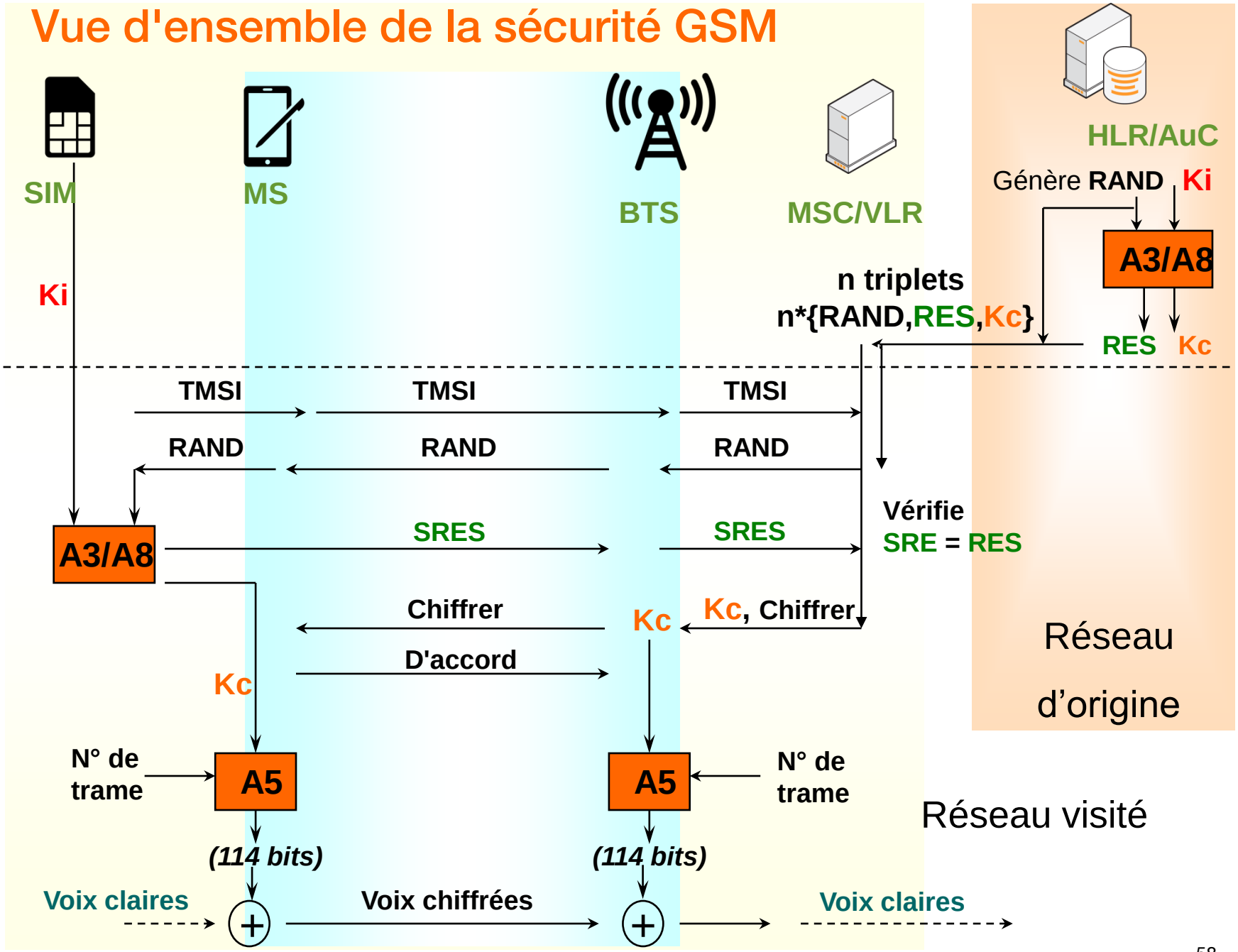


- Le chiffrement s'effectue au niveau 1 : canaux radio **TCH** (Traffic CHannel) et **DCCH** (Dedicated Control CHannel), entre le mobile et la BTS.

GSM : principales fonctions de sécurité



Vue d'ensemble de la sécurité GSM



A5/1 : attaques connues

- A5/1 a été diffusé publiquement en 1999 (1ère fuite en 1994 et retro-ingénierie d'un terminal en 1999). Depuis, un certain nombre d'attaques ont été publiées sur cet algorithme.

- Attaques à "clair connu" :
  - Connaissance de n [~64] bits consécutifs [Golic ; Pornin-Stern] complexité équivalente à 242 systèmes linéaires.
  - Connaissance de N trames [Biryukov-Shamir-Wagner, Biham-Dunkelman].
  - Connaissance statistique des [40] premiers bits de n [~60 000] trames [Ekdahl, Johansson].

- A Crypto '03 une attaque directe sur le chiffré a été publiée [Barkan-Biham-Keller].
  - Elle se base sur l'exploitation de relations linéaires liées au code correcteur d'erreur pour dériver un système linéaire solvable relativement rapidement, et nécessite un pré-calcul important.
  - Egalement, publication de plusieurs attaques actives.

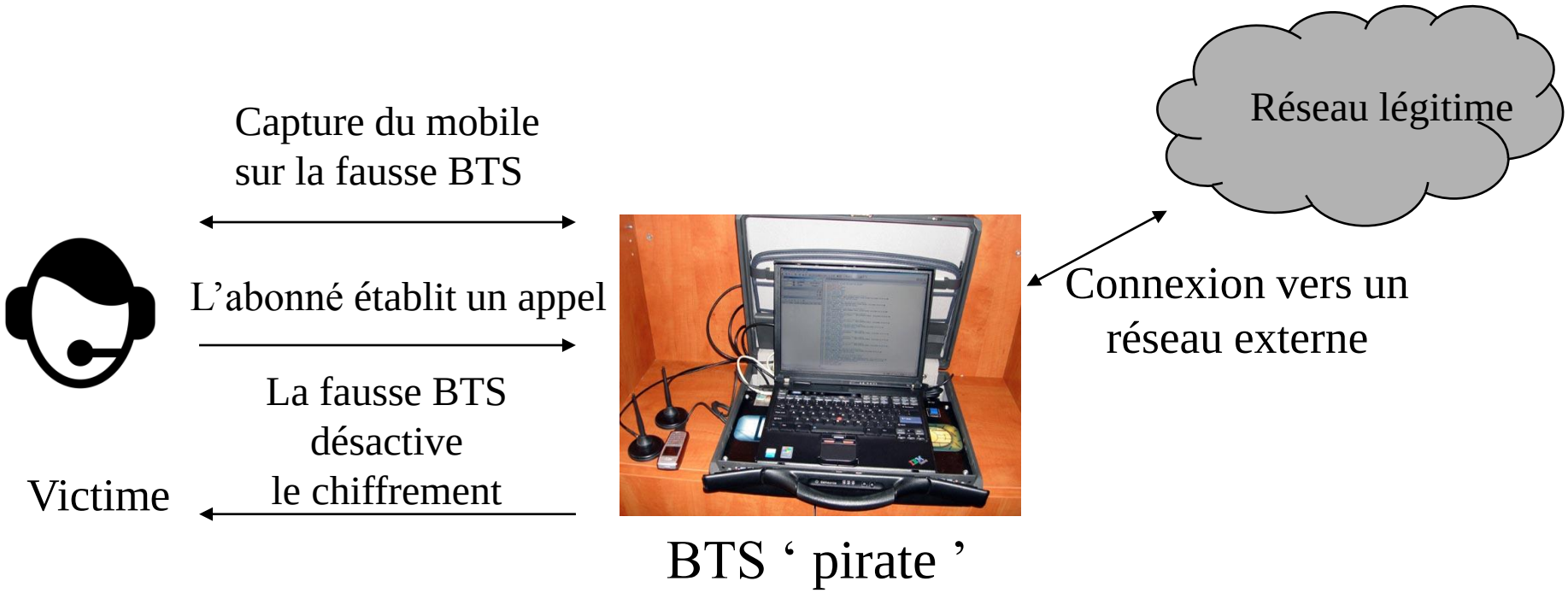
- L'attaque sur le chiffré a inspiré une attaque mise en œuvre avec des tables pré-calculées (2 TO):
  - Annonce fin 2009 de la publication des tables
  - Implémentation pratique depuis 2009 : https://srlabs.de/bites/decrypting-gsm/

- Permet l'écoute passive (et active) des communications chiffrées
- A5/3 et A5/4 sont une solution (partielle) au problème

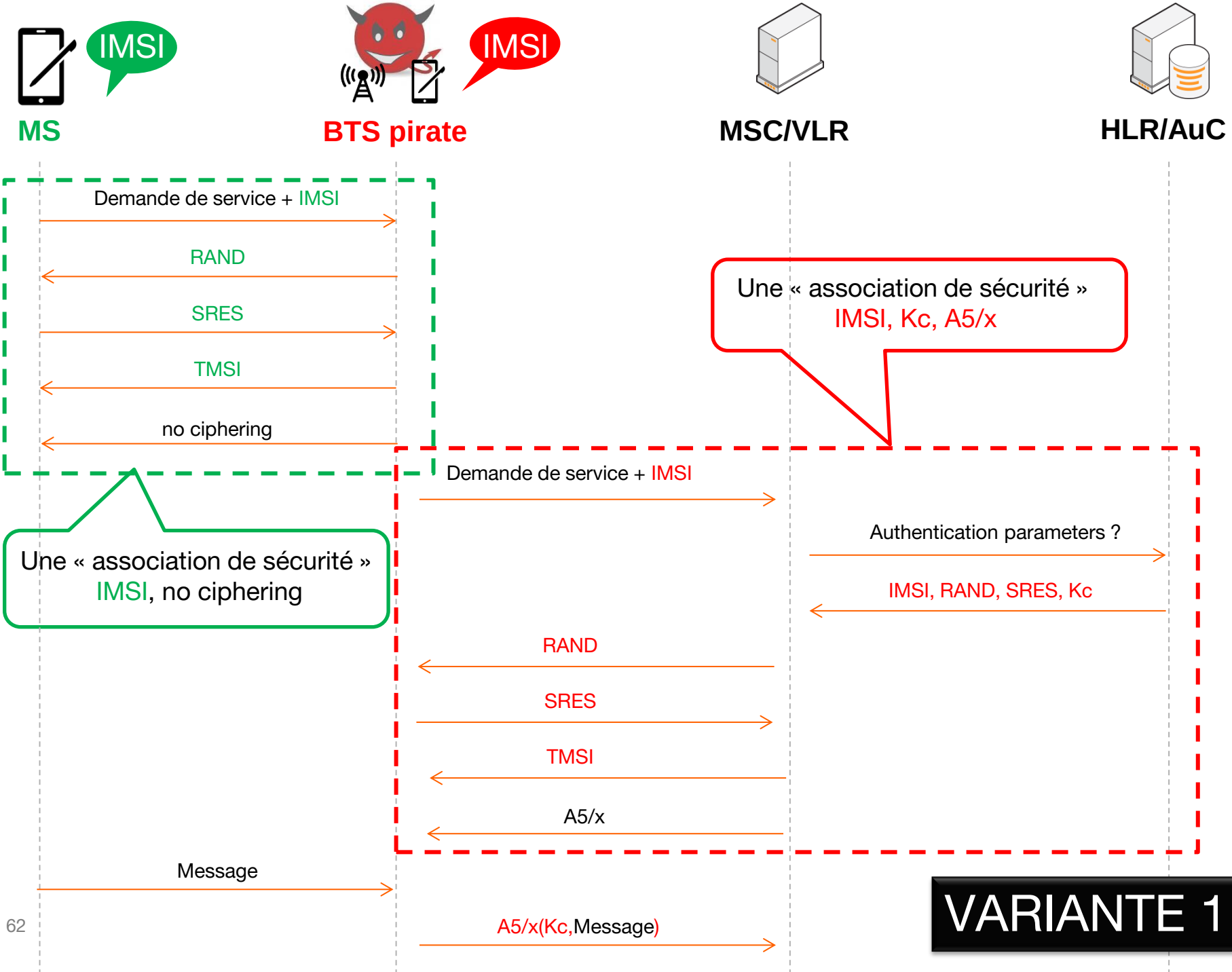
Considération sur les fausses BTS

Source photo: army-technology.com

Interception avec une fausse BTS

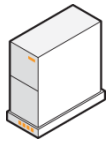


L'attaquant connecte l'appel émis par la victime vers un réseau légitime, ce qui lui permet de se trouver en coupure et d'intercepter les données (attaque dite "man-in-the-middle").


IMSI
IMSI
MS
BTS pirate
MSC/VLR
HLR/AuC
Demande de service + IMSI
RAND
SRES
TMSI
no ciphering
Une « association de sécurité »
IMSI, Kc, A5/x
Une « association de sécurité »
IMSI, no ciphering
Demande de service + IMSI
Authentication parameters ?
IMSI, RAND, SRES, Kc
RAND
SRES
TMSI
A5/x
Message
A5/x(Kc,Message)
VARIANTE 1

MS

BTS pirate



MSC/VLR

HLR/AuC

Demande de service + IMSI

Demande de service + IMSI

Authentication parameters ?

IMSI, RAND, SRES, Kc

RAND

RAND

SRES

SRES

authentification OK

TMSI

TMSI

no ciphering

A5/1

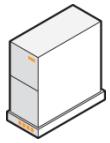
Pas d'intégrité

Message

- A5/1 est cassé => on peut trouver **Kc**
- On chiffre le **Message** avec **Kc**

A5/1(Kc,Message)

VARIANTE 2



MS | BTS pirate | MSC/VLR | HLR/AuC

Demande de service + IMSI

Demande de service + IMSI

Authentication parameters ?

Et si le téléphone n'acceptait pas l'absence de chiffrement ?

Message

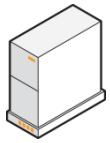
- A5/1 est cassé => on peut trouver **Kc**
- On chiffre le **Message** avec **Kc**

A5/1(Kc,Message)

VARIANTE 2

MS

BTS pirate



MSC/VLR

HLR/AuC

Demande de service + IMSI

[. . .]

A5/1

Une « association de sécurité »
IMSI, **A5/1, Kc**

Une « association de sécurité »
IMSI, **A5/1, Kc**

Demande de service + IMSI

[. . .]

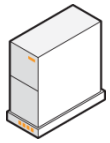
A5/1

A5/1(**Kc**,**Message**)

Cryptanalyse nécessaire :
- A5/1 est cassé => on peut trouver **Kc**
- On déchiffre le **Message**
- On rechiffre le **Message** avec A5/1 et **Kc**

A5/1(**Kc**,**Message**)

VARIANTE 1



MS **BTS pirate** **MSC/VLR** **HLR/AuC**

Demande de service + IMSI

Demande de service + IMSI

Authentication parameters ?

IMSI, RAND, SRES, Kc

RAND

RAND

SRES

SRES

authentification OK

TMSI

TMSI

A5/1

A5/1

A5/1(**Kc**,Message)

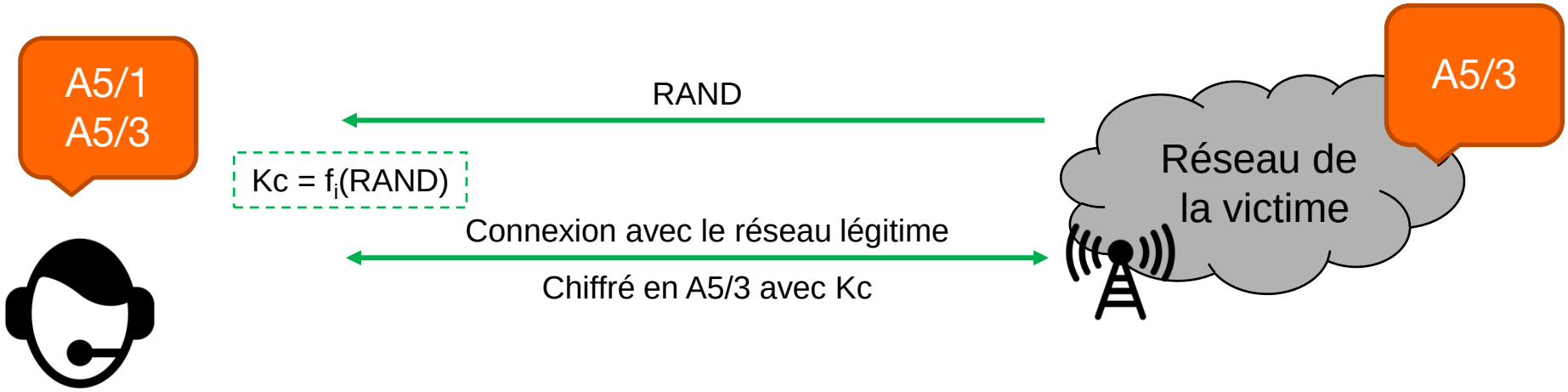
Cryptanalyse nécessaire :
- A5/1 est cassé => on peut trouver **Kc**
- On déchiffre le **Message**
- On rechiffre le **Message** en A5/1 avec **Kc**

A5/1(**Kc**,Message)

VARIANTE 2

Interception transparente avec une fausse BTS

>*Cas où le réseau propose seulement A5/3*



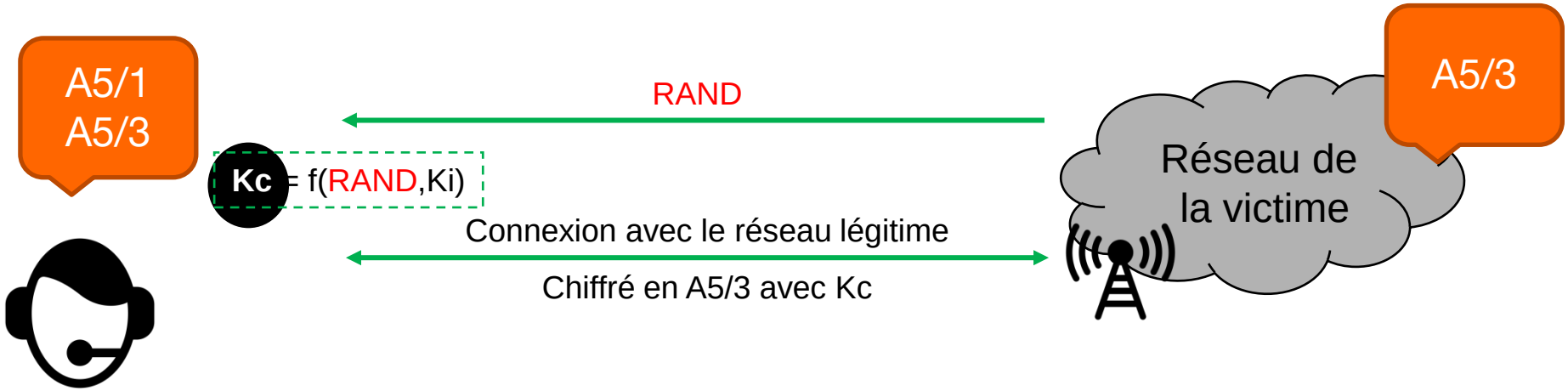
Victime

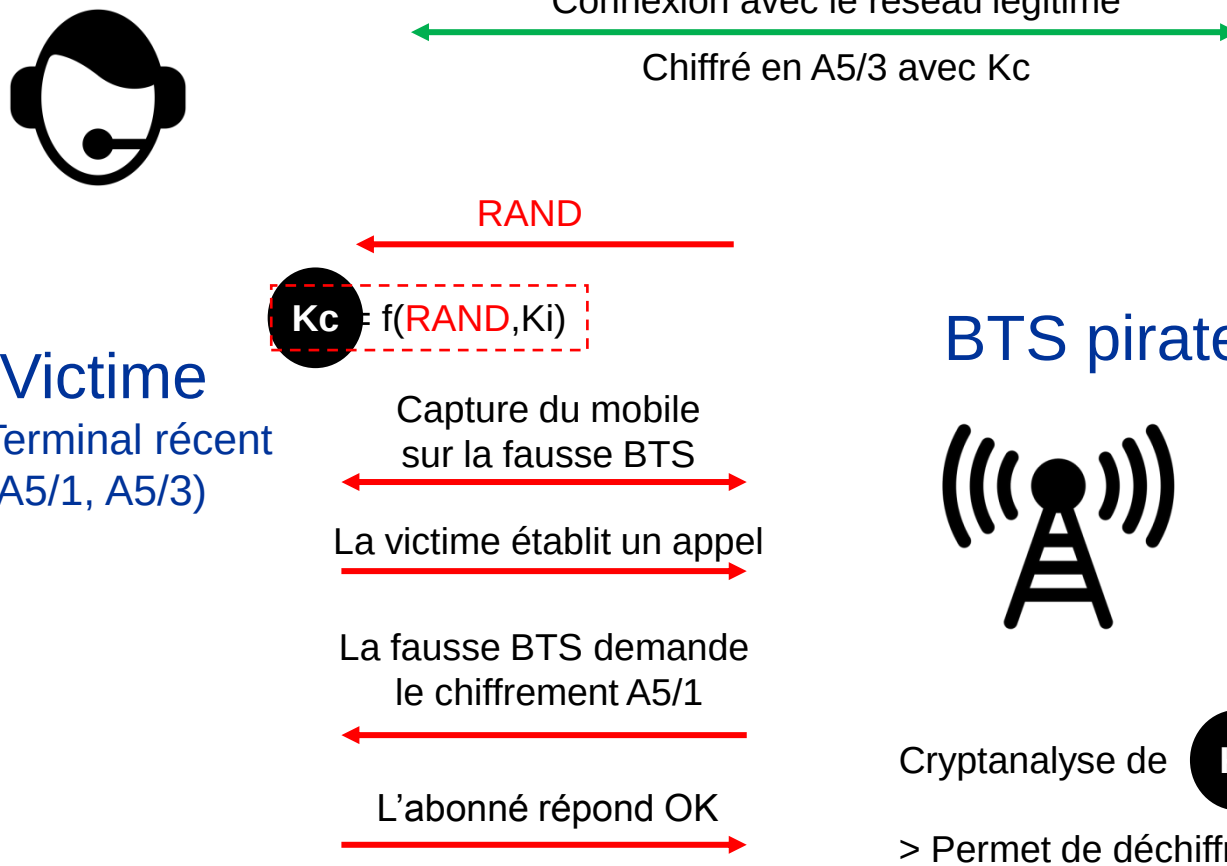
Terminal récent (A5/1, A5/3)

- Si la communication est établie avec un chiffrement A5/3, l'attaquant ne peut pas casser la clé de session Kc car l'algorithme A5/3 a les « bonnes propriétés cryptographiques. »
- Par contre, la clé de session Kc ne dépend pas de l'algorithme de chiffrement ou du temps
  - Avec un même RAND (et la 2G ne protège pas contre ce cas), on aura une même clé de session
  - Les attaques semi actives restent donc possibles.

Interception transparente avec une fausse BTS

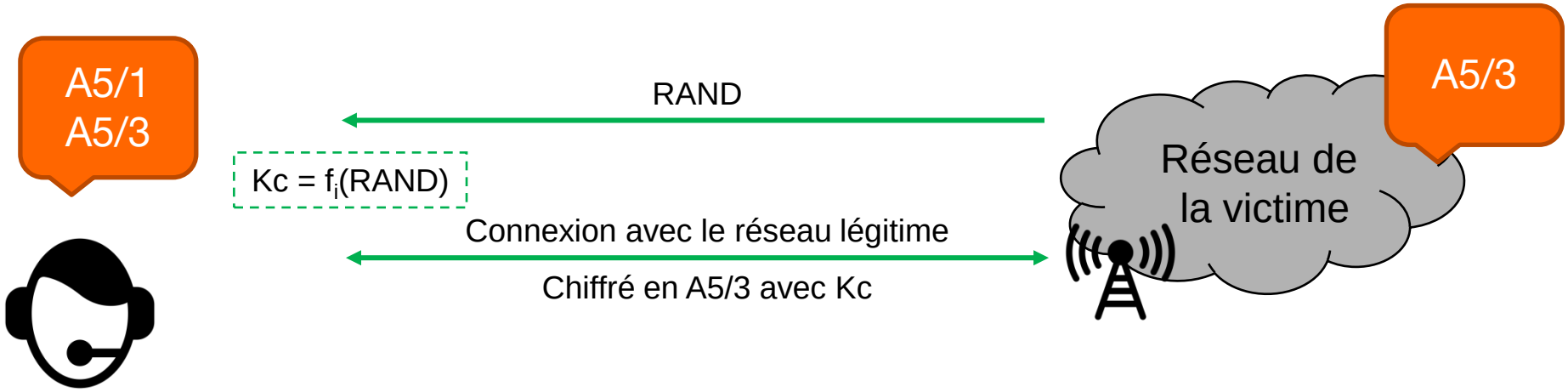
> Cas où le réseau propose seulement A5/3





Interception transparente avec une fausse BTS

> Cas où le réseau propose seulement A5/3



Victime

Terminal récent (A5/1, A5/3)

- Si l'abonné ne supporte qu'A5/3 et mieux, les attaques semi-actives ne sont plus applicables.
- Par contre, l'utilisateur ne pourra pas chiffrer ses communications sur des réseaux qui ne proposent pas A5/3

Fausses BTS : en résumé

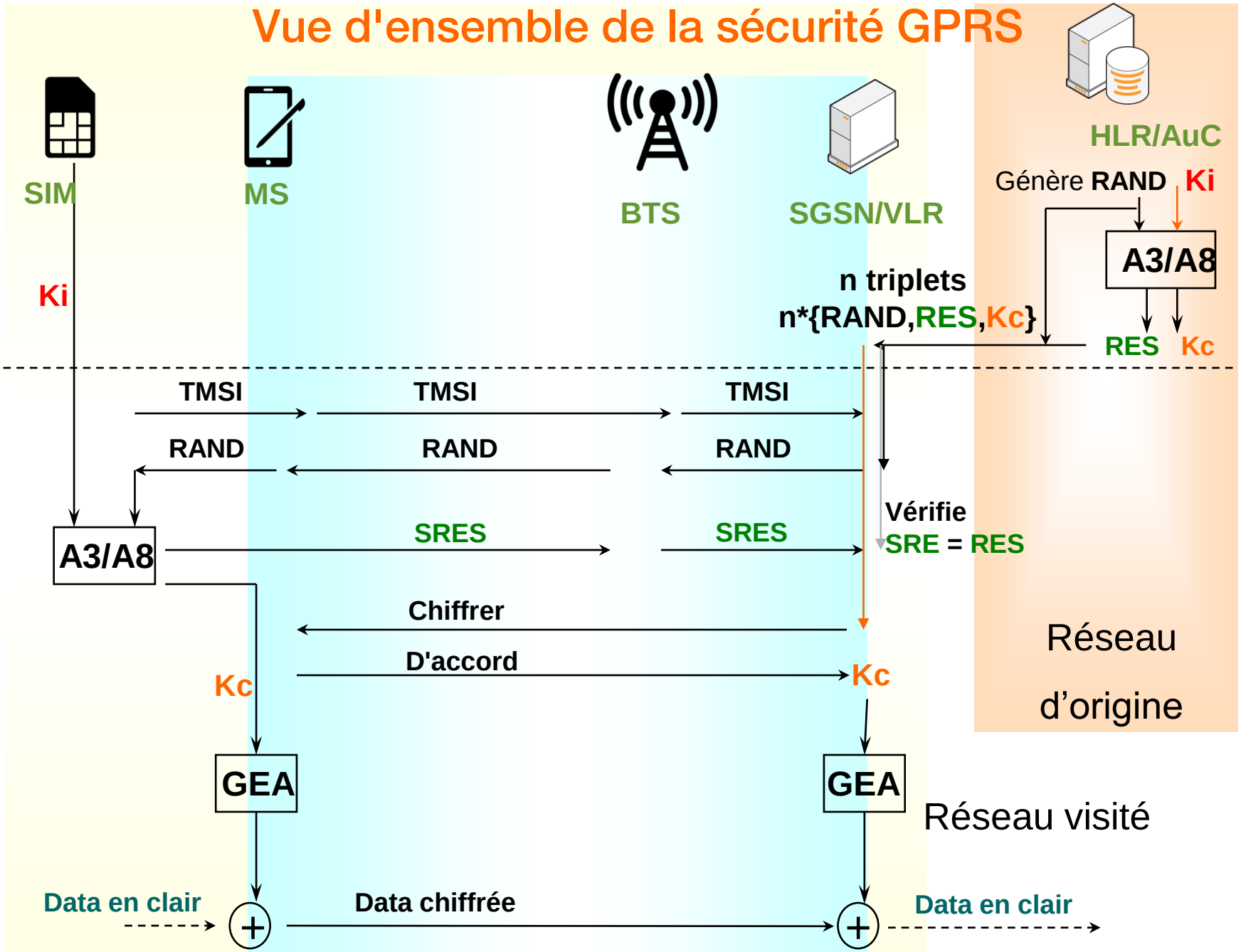
- Des attaques plus ou moins faciles
  - attaques passives
  - attaques actives
  - attaques semi-actives
- Pas contre-mesure efficace à 100% contre les fausses BTS
  - La cryptographie n'est pas une solution parfaite pour les problèmes de design de sécurité de la 2G
- Des outils pour détecter au niveau du terminal les comportements aberrants
  - https://secupwn.github.io/Android-IMSI-Catcher-Detector/
  - https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher

Focus GPRS

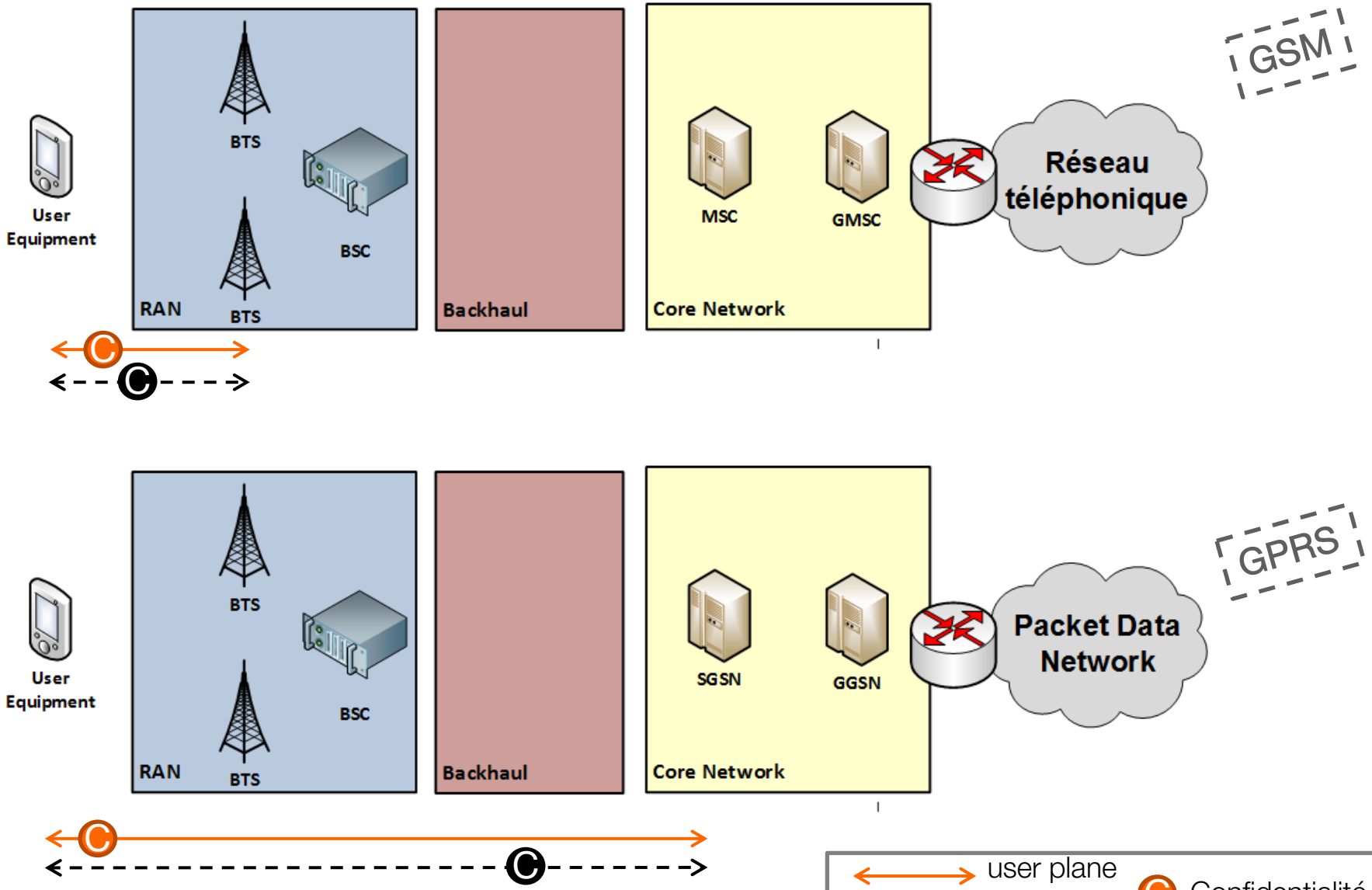
GPRS : la confidentialité des données

- La confidentialité des communications repose sur le chiffrement:
  - du trafic utilisateur (paquet);
  - de la signalisation;
  - entre le mobile et le SGSN.
- Le chiffrement utilise la clé de session GPRS-Kc de 64 bits établie lors de la procédure d'authentification.
- Il est réalisé par la fonction GEA:
  - GEA0 : pas de chiffrement.
  - GEA1 : l'algorithme de chiffrement initiale du GPRS.
  - GEA2 : l'algorithme de "repli" du GPRS (non affaibli, contrairement à A5/2).
  - GEA3 : nouvel algorithme défini lors des travaux sur l'UMTS.
  - GEA4 : nouvel algorithme défini lors des travaux sur l'UMTS.

Vue d'ensemble de la sécurité GPRS



GSM / GPRS : principales fonctions de sécurité



GEA/1 et GEA/2 : attaques connues

- Security by obscurity
  - Pas de fuites jusqu'à maintenant
- Cryptanalyse de GEA1
  - résultats publiés en 2011
  - réflexion pour supprimer GEA/1 de la liste des algo supportés côté réseau
- Attaque par tables arc-en-ciel pour GEA1 et GEA2
  - seulement si IV constant
- Contremesures
  - client : surcouche de chiffrement
  - réseau : utiliser des méthodes de chiffrement plus robustes et mieux implémentées – passer à GEA3 voire GEA4

Bilan

GSM / GPRS : failles de sécurité intrinsèques

- Algo de chiffrement (et d'authentification) cassés

- Absence d'authentification du réseau
  - Possible de soumettre n'importe quel challenge RAND à la carte SIM pour tenter de déduire la clé d'authentification.
  - Possible d'utiliser une fausse station de base et se faire passer pour le réseau pour intercepter des communications.

- Réutilisation possible des triplets d'authentification {RAND, RES, Kc}
  - Si un attaquant récupère un triplet valide, il peut le réutiliser indéfiniment.
  - Interception d'une communication chiffrée (dont le RAND lors de l'authentification) : avec un accès à posteriori sur la carte SIM, on peut rejouer RAND pour obtenir Kc et alors déchiffrer la communication.

- Pas de protection de l'intégrité de la signalisation
  - un attaquant peut manipuler les messages de signalisation (la plupart des messages restent chiffrés).

- Le chiffrement s'arrête au niveau de la station de base pour la partie circuit (voix, SMS).

- La clé de session ne dépend pas de l'algorithme de chiffrement utilisé

- Des messages prédictibles sont envoyés chiffrés
  - Contre-mesure réseau : randomisation du padding

Conclusions sur la 2G

Fonctions de sécurité	GSM
Identités temporaires	
Authentification de l'utilisateur	
Authentification du réseau	
Protection contre le rejeu	
Chiffrement radio	
Contrôle d'intégrité signalisation (MAC)	
Clés de session liées au serving network	

En **gras** : les objectifs de sécurité de la 2G

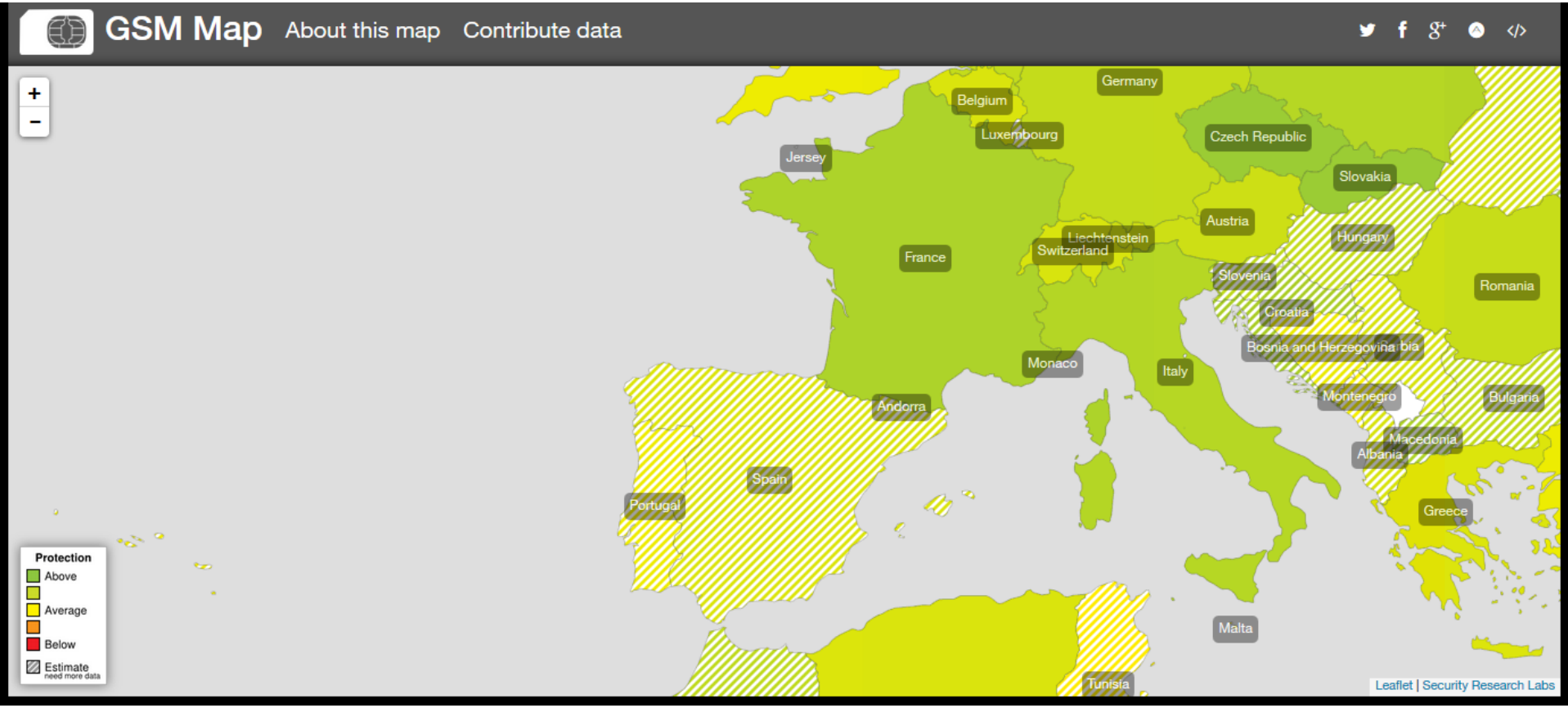
Algorithmes : récapitulatif

	GSM	GPRS
Authentification+ génération de clé	GSM-AKA = A3 + A8 *- COMP128-1 (cassé)* *- COMP128-2* *- COMP128-3* *- Milenage2G*	
Chiffrement	A5 *-A5/0 (nul)* ***-A5/1 (cassé)*** *-A5/2 (cassé)* *-A5/3* *-A5/4*	GEA *- GEA/0* ***- GEA/1 (cassé)*** *-GEA/2* *-GEA/3*
Intégrité	Aucune	Aucune

Sécurité GSM / GPRS: quelques ressources

- Le maintien des normes GSM / GPRS sont prises en charge par le 3GPP
  - TS 43.020 : sécurité GSM et GPRS.
  - http://www.3gpp.org/ftp/Specs/html-info/43020.htm
- Diverses ressources Internet
  - http://www.gsma.com/ (site GSMA)
  - http://cryptome.org/0001/gsm-a5-files.htm (référence les attaques sur le GSM)
  - http://events.ccc.de/camp/2011/Fahrplan/attachments/1868_110810.SRLabs-Camp-GRPS_Intercept.pdf (attaques sur le GPRS)
- Outils
  - https://svn.berlin.ccc.de/projects/airprobe (sniffer GSM)
  - http://openbts.sourceforge.net/ (BTS open-source)
  - http://openbsc.osmocom.org/trac/ (BSC et composants cœur open-source)
  - http://bb.osmocom.org/trac/ (base-band TI Calypso open-source)

https://gsmmap.org/



La 3G (UMTS)

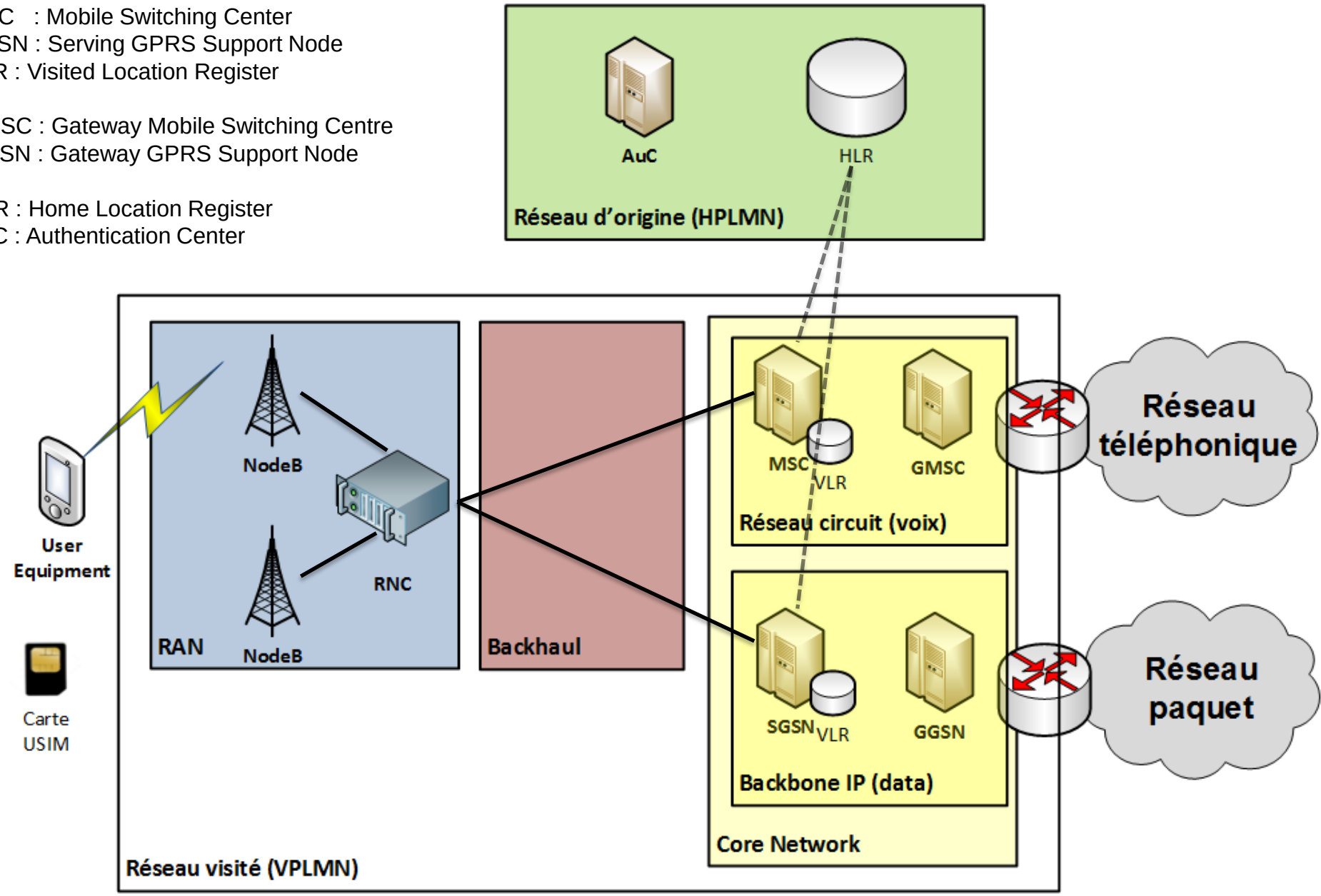
Architecture UMTS

USIM : UMTS Subs. Ident. Module
BTS -> NodeB
BSC -> **RNC : Radio Node Controller**

MSC : Mobile Switching Center
SGSN : Serving GPRS Support Node
VLR : Visited Location Register

GMSC : Gateway Mobile Switching Centre
GGSN : Gateway GPRS Support Node

HLR : Home Location Register
AuC : Authentication Center



GSM / GPRS : failles de sécurité intrinsèques

- Algo de chiffrement (et d'authentification) cassés
  - En 3G : Nouveaux algorithmes de chiffrement (et d'authentification)
- Absence d'authentification du réseau
  - En 3G : Authentification du réseau par la carte USIM.
- Réutilisation possible des triplets d'authentification {RAND, RES, Kc}
  - En 3G : Mécanisme anti-rejeu des valeurs d'authentification.
- Pas de protection de l'intégrité de la signalisation
  - En 3G : Contrôle d'intégrité obligatoire des messages de signalisation.
- Le chiffrement s'arrête au niveau de l'antenne pour la partie circuit (voix, SMS).
  - En 3G : NodeB transparents, le chiffrement des communications (voix et données) va jusqu'au cœur du sous-système radio (RNC).
- La clé de session ne dépend pas de l'algorithme de chiffrement utilisé
  - En 3G : toujours vrai, mais les autres mesures de sécurité rendent le risque moins important

Les améliorations de sécurité envisagées

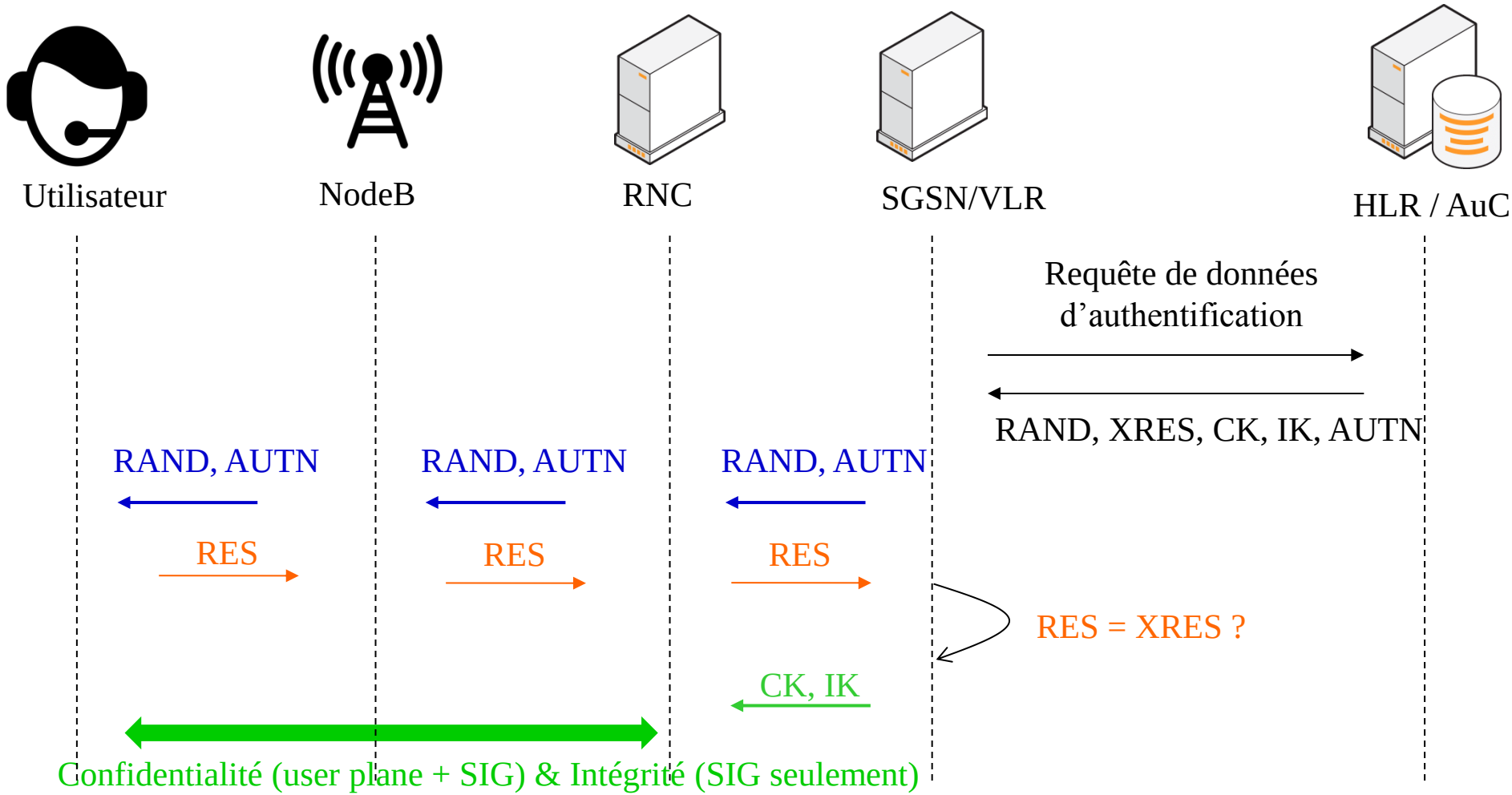
- Authentification du réseau par la carte USIM.
- Mécanisme anti-rejeu des valeurs d'authentification.
- Nouveaux algorithmes de chiffrement.
- Node-B transparents, le chiffrement des communications (voix et données) va jusqu'au cœur du sous-système radio (RNC).
- Contrôle d'intégrité obligatoire des messages de signalisation.

Quelles fonctions de sécurité pour la 3G ?

Améliorations sécurité UMTS

- Nouveau mécanisme d'authentification : UMTS-AKA (Authentication and Key Agreement).
  - Un nouveau mécanisme d'authentification a été développé ; il fournit des fonctions de sécurité additionnelles au mécanisme d'authentification du système GSM.
- Nouvel algorithme de chiffrement : Kasumi.
  - Un nouvel algorithme de chiffrement a été développé pour le système UMTS. Cet algorithme procure une sécurité solide, et ce pour une période de temps a priori relativement longue.
- Contrôle d'intégrité de la signalisation sur la voie radio.
  - L'intégrité des messages de signalisation sur l'interface radio est assurée, ce qui empêche la modification ou l'insertion malveillante de messages sur cette interface.

UMTS : schéma d'authentification

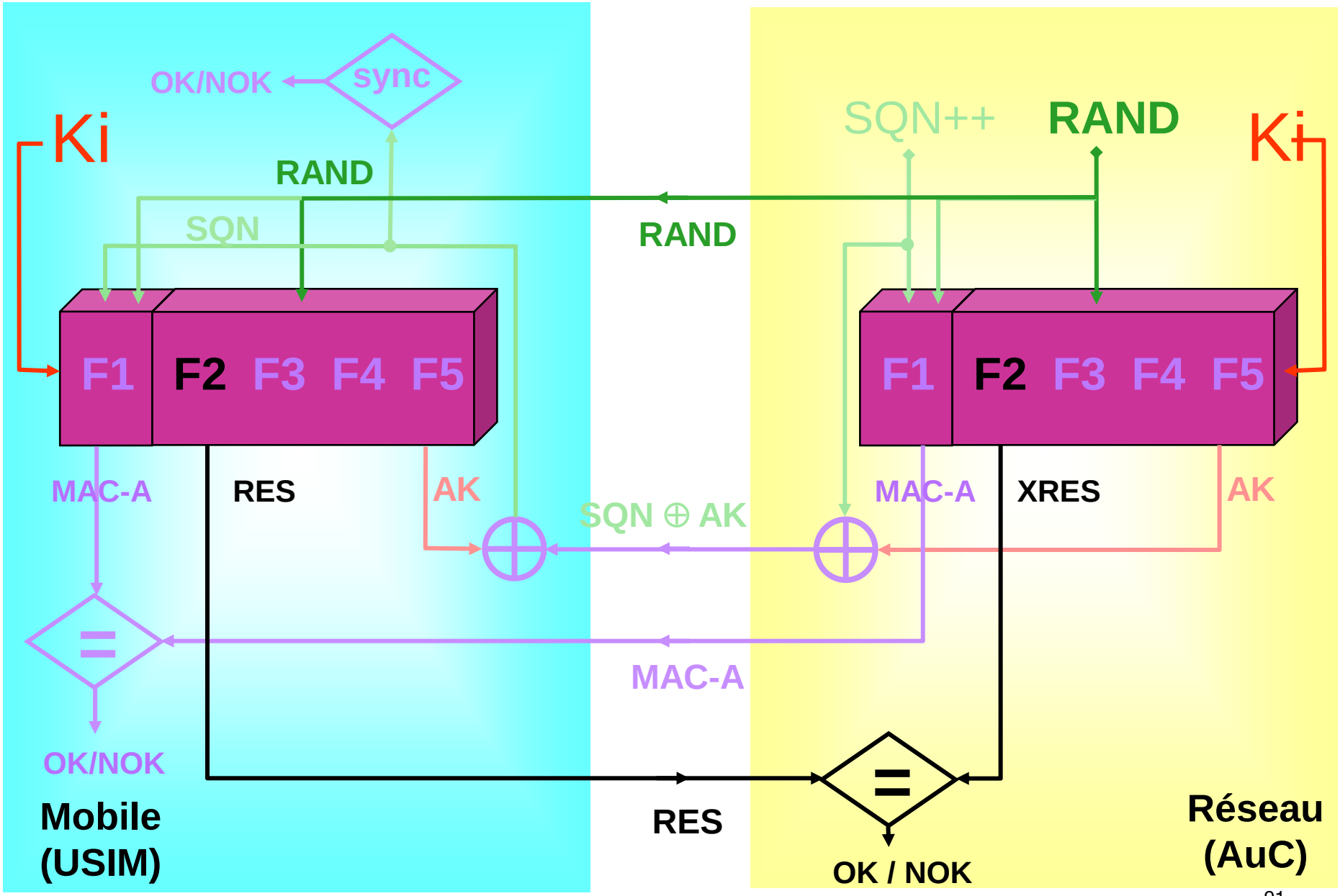


>>> Les procédures d'authentification à la partie UMTS - voix (MSC / VLR) et UMTS - paquets (SGSN) sont indépendantes, et identiques en fonctionnement.

Fonctions réalisées par le mécanisme UMTS-AKA

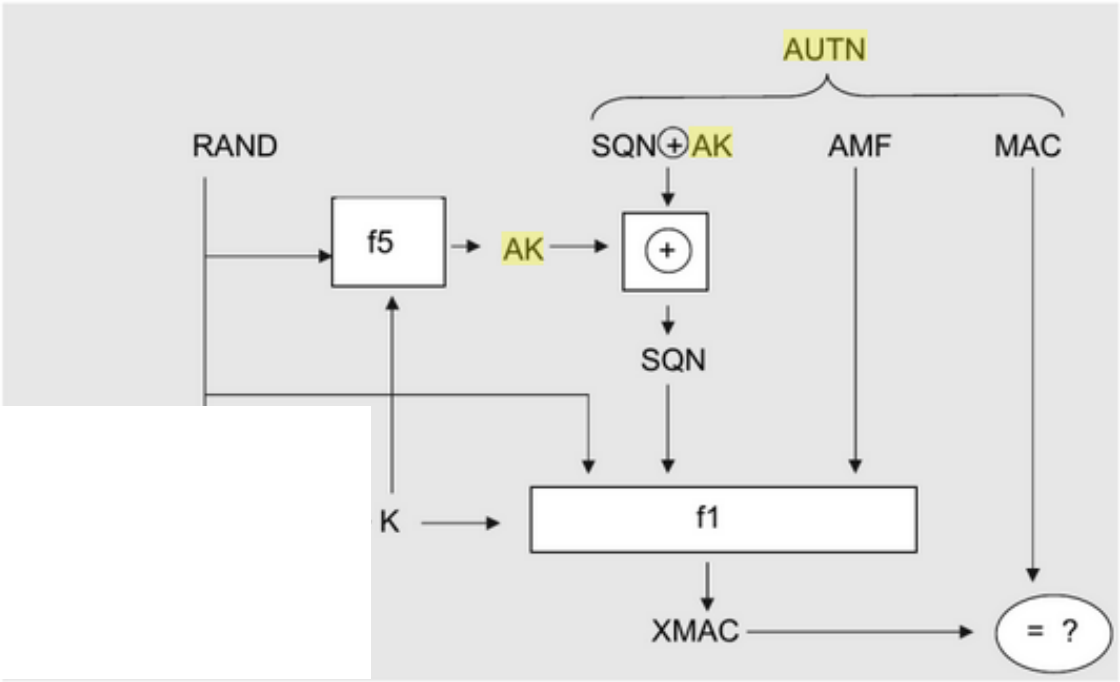
- Authentification de l'utilisateur par le réseau (comme en GSM).
- Génération de clés de chiffrement CK (comme en GSM) et d'intégrité IK entre le réseau et le terminal mobile.
- Authentification du réseau par le terminal mobile:
  - le jeton AUTN est signé à l'aide de la clé d'authentification de l'abonné;
  - il est construit à partir de la valeur RAND, qui ne peut donc pas être modifiée par un tiers (seul le réseau légitime permet de faire réaliser une procédure d'authentification complète par la carte USIM).
- Protection contre la réutilisation du vecteur d'authentification:
  - le jeton AUTN contient un numéro de séquence;
  - une procédure de resynchronisation est définie.
- Authentification déclenchée par le réseau lors de différentes procédures (selon la politique de l'opérateur).

Authentification du mobile par le réseau



Source: UMTS Security, Par Valtteri Niemi,Kaisa Nyberg. Edition Wiley.

$$AUTN[128] = SQN \oplus AK \,||\, AMF \,||\, MAC\text{-}A$$



1- MAC = atteste de l'authenticité de SQN

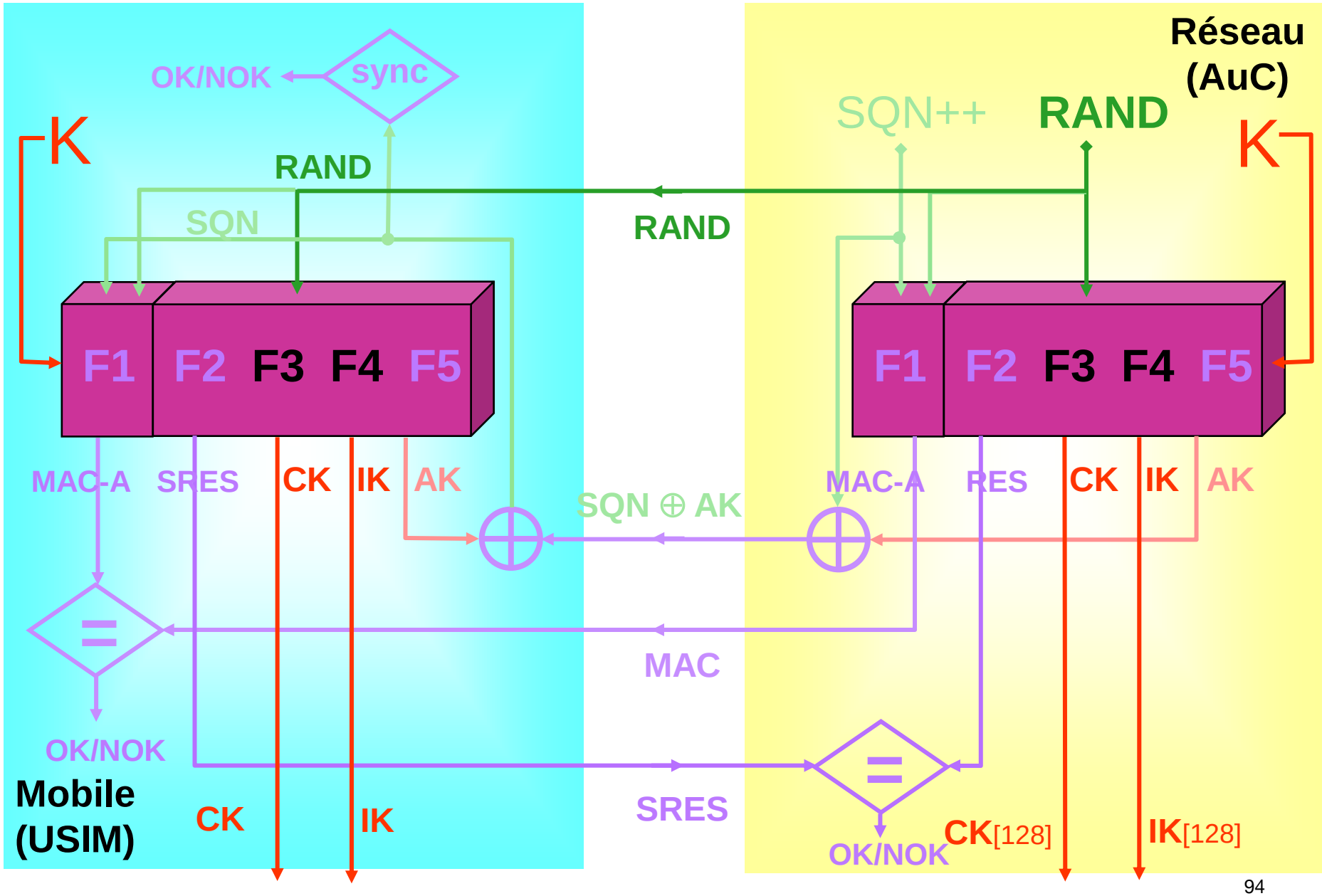
2- SQN = numéro de séquence utilisé pour vérifier que le challenge est « frais »

Figure 2.4 Authentication handling in USIM

AUTN = authentication token; RAND = random number; SQN = sequence number; AK = Anonymity Key; AMF = Authentication Management Field; MAC = Message Authenication Code; RES = user response; CK = Cipher Key; IK = Integrity Key; XMAC = expected MAC

- Si l'attaquant envoie un challenge aléatoire : le MAC sera en échec. Seul le réseau peut calculer un MAC correct et donc générer un challenge acceptable.
- Si le challenge a déjà été utilisé (ou est périmé) : la vérification de SQN côté mobile entrainera la fin de la procédure (en échec), même si le MAC est valide (puis resynchronisation)

Génération des clés : chiffrement – intégrité



Améliorations sécurité UMTS

- Nouveau mécanisme d'authentification : UMTS-AKA (Authentication and Key Agreement).
  - Un nouveau mécanisme d'authentification a été développé ; il fournit des fonctions de sécurité additionnelles au mécanisme d'authentification du système GSM.
- Nouvel algorithme de chiffrement : Kasumi.
  - Un nouvel algorithme de chiffrement a été développé pour le système UMTS. Cet algorithme procure une sécurité solide, et ce pour une période de temps a priori relativement longue.
- Contrôle d'intégrité de la signalisation sur la voie radio.
  - L'intégrité des messages de signalisation sur l'interface radio est assurée, ce qui empêche la modification ou l'insertion malveillante de messages sur cette interface.

Chiffrement et intégrité de l'accès radio UMTS

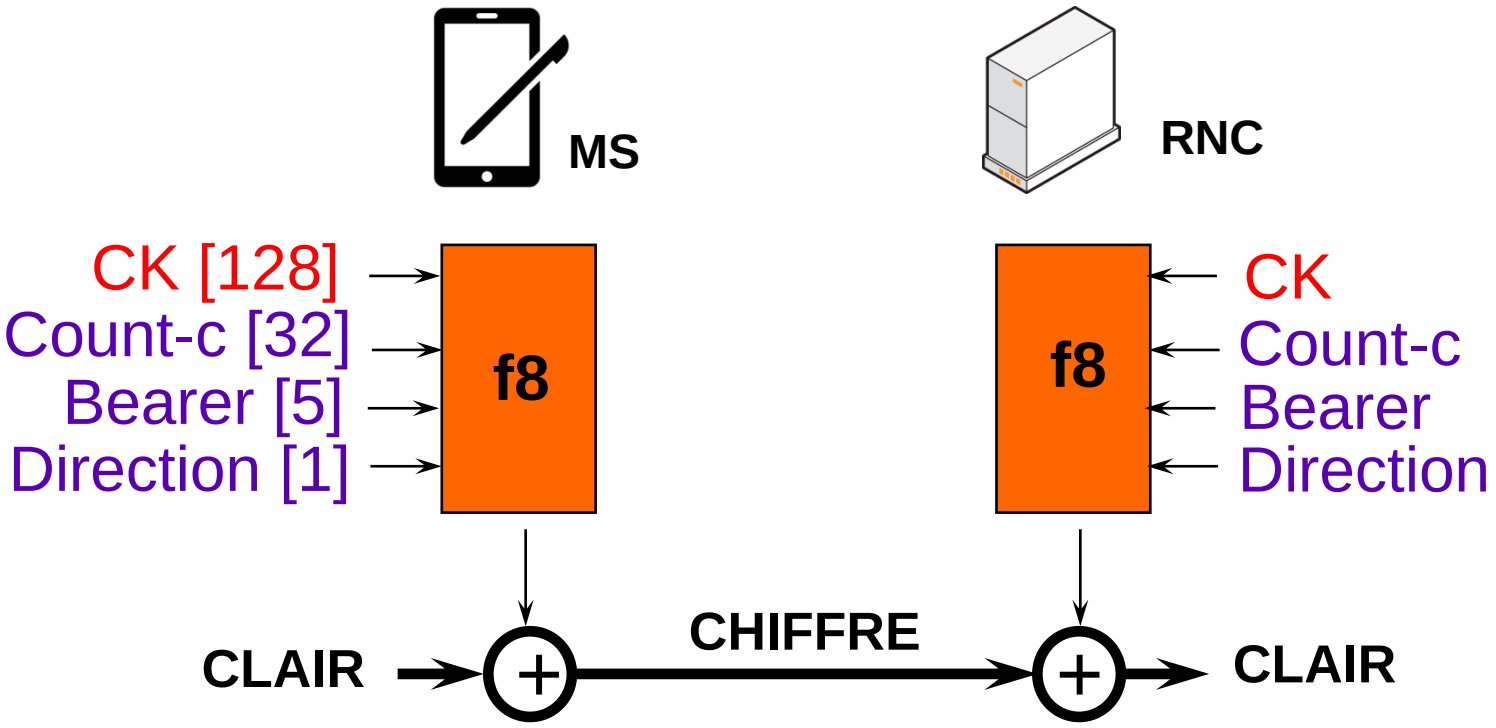
- Chiffrement et contrôle d'intégrité sont réalisés grâce aux fonctions F8 et F9. Ils s'appuient sur un algorithme cryptographique cœur, utilisé selon différents modes d'opérations.
- En UMTS Rel.99, un nouvel algorithme cryptographique, Kasumi, a été développé à partir d'un algorithme de Mitsubishi, Misty.
  - Misty est un algorithme de chiffrement par bloc de taille 64 bits utilisant des clés de 128 bits, ce qui assure une sécurité forte pour une période assez longue.
- Snow-3G a été défini comme 2nd algorithme de sécurité de l'UMTS, en Rel.7, développé à partir de l'algorithme Snow.
  - SNOW-3G est un algorithme de chiffrement à flot utilisant des clés de 128 bits.
- La solidité du chiffrement et du contrôle d'intégrité est impérative pour éviter le détournement d'appels une fois l'authentification réalisée
- Le chiffrement et le contrôle d'intégrité s'effectuent entre le terminal mobile et le RNC, ce qui assure la protection du lien NodeB - RNC (lien BTS - BSC non protégé en GSM).

Caractéristiques du chiffrement UMTS

- Il assure la confidentialité des communications.
- Le chiffrement est appliqué sur le trafic utilisateur et la signalisation, de manière optionnelle.
- Il est appliqué entre le terminal et le RNC.
- L'algorithme à utiliser est choisi parmi :
  - UEA-0 : pas de chiffrement,
  - UEA-1 : Kasumi,
  - UEA-2 : SNOW-3G.
- Il est négocié entre le terminal et le RNC
  - *Security Mode Command*
  - Signalisation protégée en intégrité afin qu'un attaquant ne puisse pas activement changer l'algorithme à utiliser (vers un algorithme plus faible).
- Il utilise la clé CK produite lors de l'authentification.

Chiffrement UMTS (fonction F8) (stream cipher)

Count-c : paramètre dépendant du temps
Bearer : identité du canal utilisé
Direction : uplink ou downlink



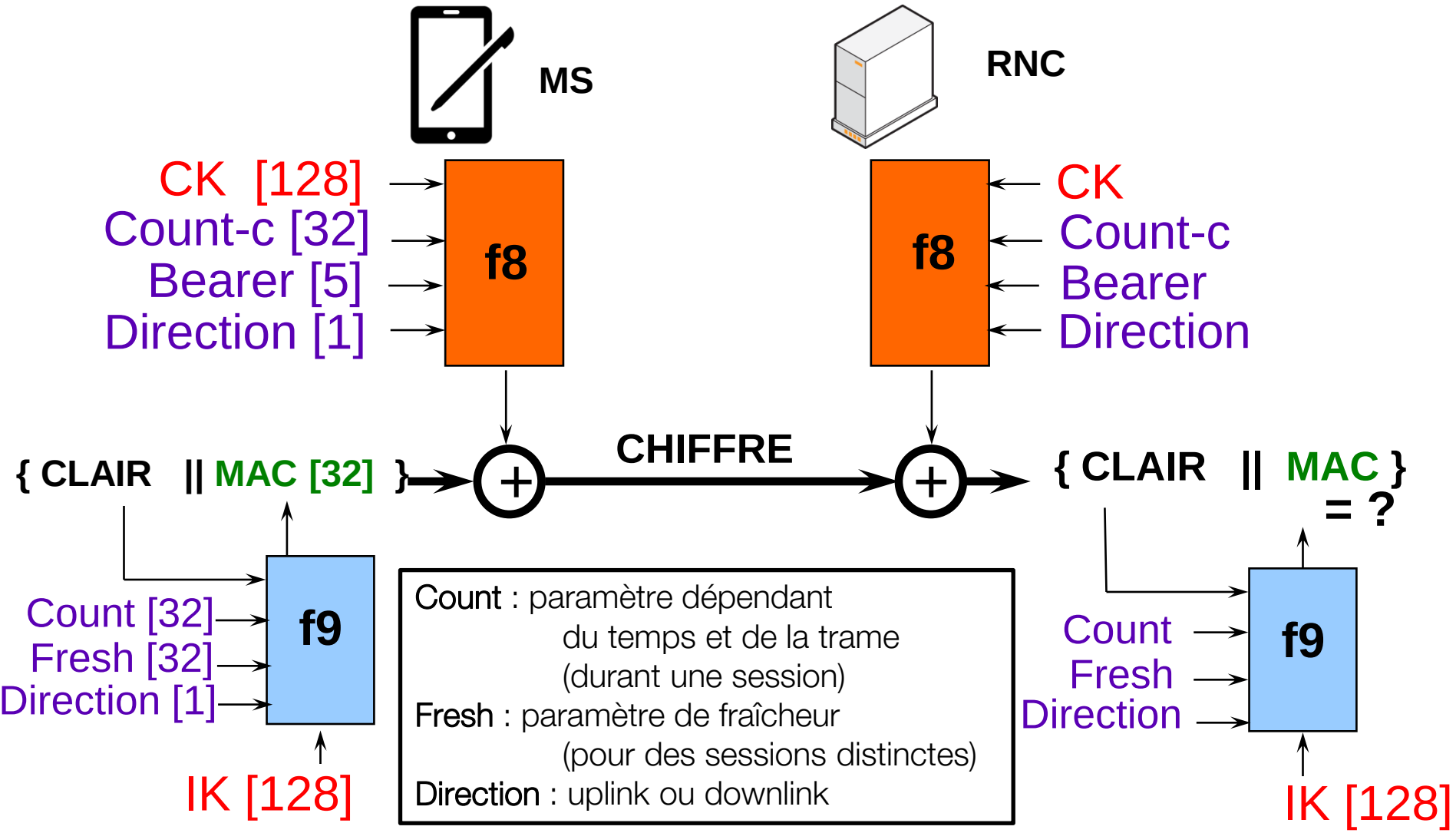
Améliorations sécurité UMTS

- Nouveau mécanisme d'authentification : UMTS-AKA (Authentication and Key Agreement).
  - Un nouveau mécanisme d'authentification a été développé ; il fournit des fonctions de sécurité additionnelles au mécanisme d'authentification du système GSM.
- Nouvel algorithme de chiffrement : Kasumi.
  - Un nouvel algorithme de chiffrement a été développé pour le système UMTS. Cet algorithme procure une sécurité solide, et ce pour une période de temps a priori relativement longue.
- Contrôle d'intégrité de la signalisation sur la voie radio.
  - L'intégrité des messages de signalisation sur l'interface radio est assurée, ce qui empêche la modification ou l'insertion malveillante de messages sur cette interface.

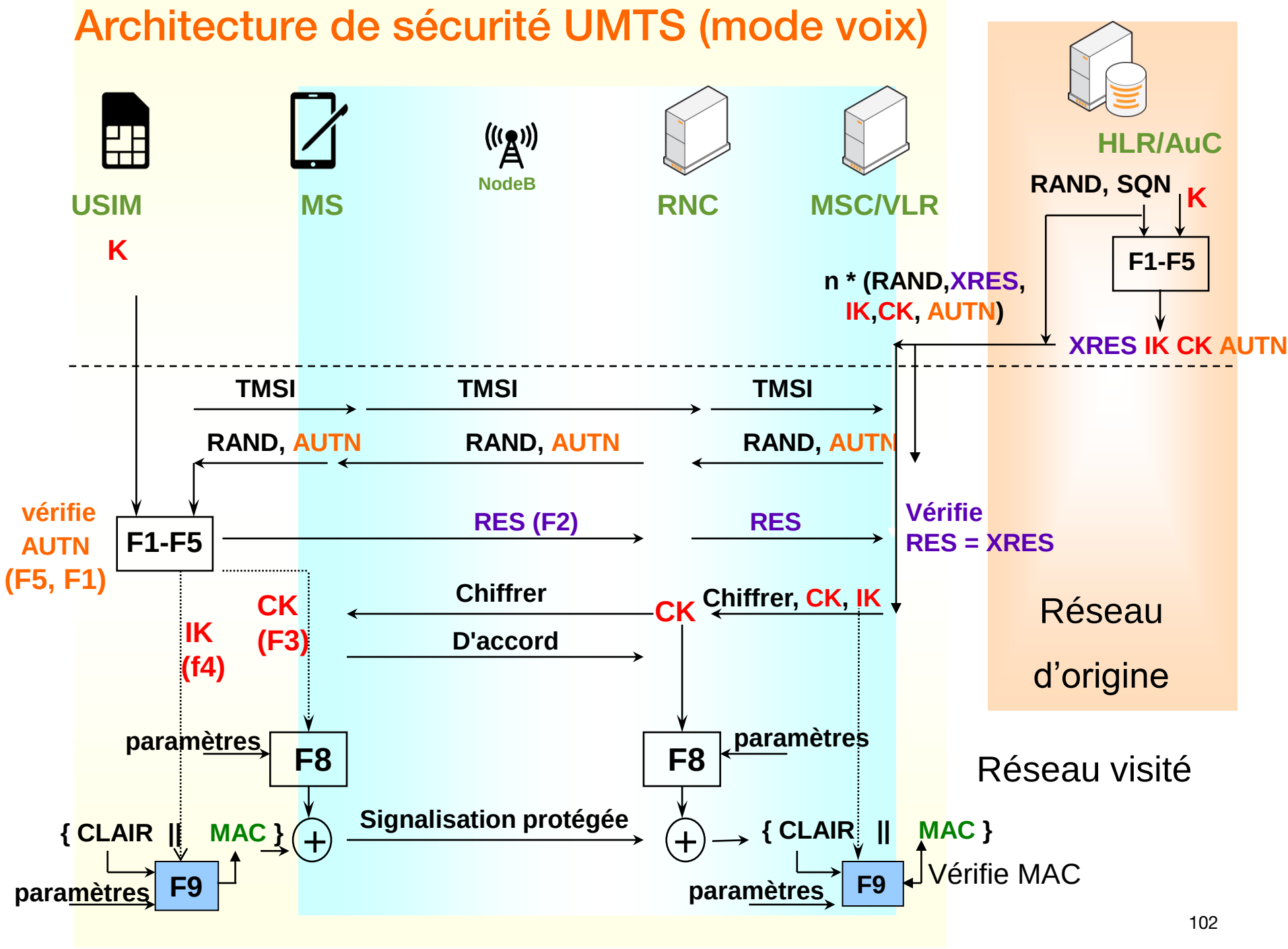
Caractéristiques du contrôle d'intégrité UMTS

- Il assure que les communications ne sont pas modifiées durant leur transport.
- Il s'agit d'une fonction MAC (*Message Authentication Code*).
- Le contrôle d'intégrité est appliqué sur la signalisation, de manière obligatoire (sauf lors d'appels d'urgence non authentifiés, sans USIM).
- Il est appliqué entre le terminal et le RNC.
- L'algorithme à utiliser est choisi parmi :
  - UIA-0 : pas de contrôle d'intégrité,
  - UIA-1 : Kasumi,
  - UIA-2 : SNOW-3G.
- Il est négocié entre le terminal et le RNC
  - *Security Mode Command*
  - Signalisation protégée en intégrité afin qu'un attaquant ne puisse pas activement changer l'algorithme à utiliser (vers un algorithme plus faible).
- Il utilise la clé IK produite lors de l'authentification.

Contrôle d'intégrité UMTS (fonction F9)



Architecture de sécurité UMTS (mode voix)

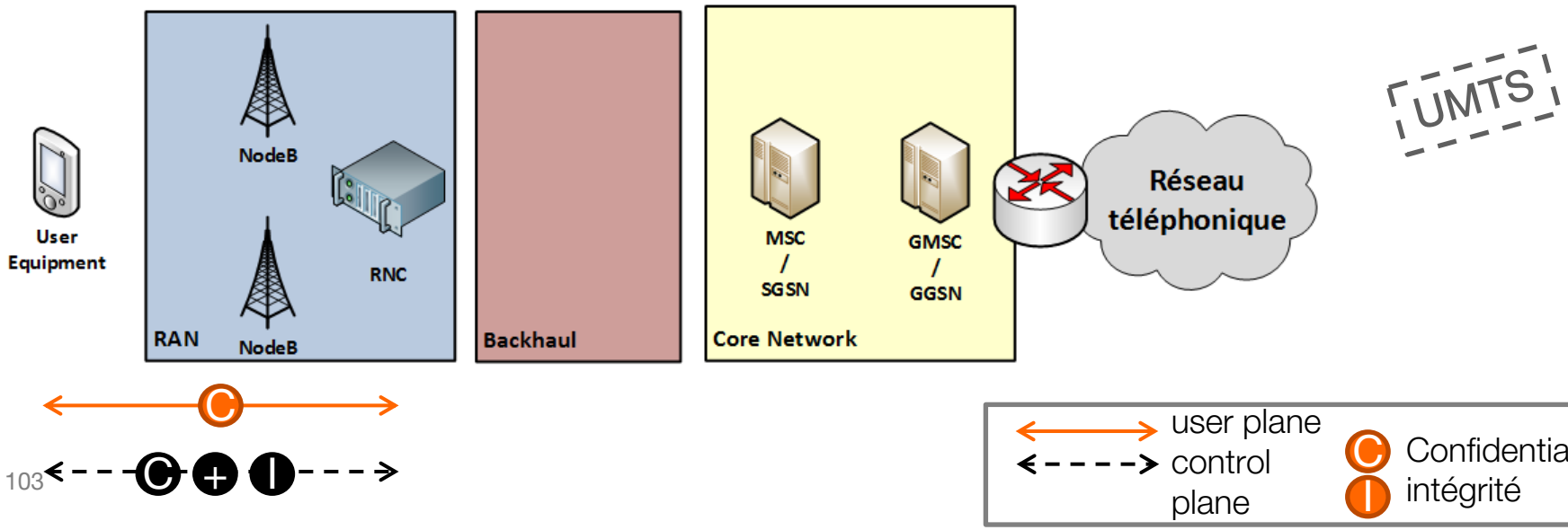


Les améliorations de sécurité

- Authentification
  - Authentification de l'utilisateur avec des algorithmes résistants
  - Authentification du réseau par la carte USIM.
  - Mécanisme anti-rejeu des vecteurs d'authentification.

- Chiffrement
  - Nouveaux algorithmes de chiffrement.
  - Antennes (= Node-B) transparents, le chiffrement des communications (voix et données) va jusqu'au cœur du sous-système radio (RNC).

- Intégrité
  - Contrôle d'intégrité obligatoire des messages de signalisation.



Comparaison GSM - UMTS

Fonctions de sécurité	GSM	UMTS
Identités temporaires		
Authentification de l'utilisateur		
Authentification du réseau		
Protection contre le rejeu		
Chiffrement radio		
Contrôle d'intégrité signalisation (MAC)		
Clés de session liées au serving network		

UMTS : attaques possibles

- Brouiller les fréquences UMTS pour basculer en GSM / GPRS.
  - Toutes les attaques GSM / GPRS peuvent être réalisées sur les terminaux compatibles (dual mode).
- L'accès UMTS peut se faire avec une SIM GSM (dont certaines peuvent être clonées).
  - Pas d'authentification du réseau : les failles du GSM sont alors applicables à l'UMTS.
- Réutilisation possible des quintuplets d'authentification UMTS légitimes.
  - Possible et/ou limitée selon la politique de l'opérateur sur la durée de vie des contextes de sécurité (plus particulièrement de CK, IK et des identités temporaires TMSI).
- En particulier
  - Pas d'attaque cryptographique applicable sur les algorithmes utilisés
- Le design et les fonctions de la sécurité UMTS sont complets et efficaces.

Algorithmes : récapitulatif

	GSM	GPRS	UMTS
Authentification+ génération de clé	GSM-AKA = A3 + A8 *-COMP128-1 (cassé)* *-COMP128-2* *-COMP128-3* *-Milenage2G*		UMTS-AKA = (f1,f2)+(f3,f4) *-Milenage*
Chiffrement	A5 *-A5/0 (nul)* *-A5/1 (cassé)* *-A5/2 (cassé)* *-A5/3* *-A5/4*	GEA *-GEA/0* *-GEA/1 (cassé)* *-GEA/2* *-GEA/3*	f8 *-UEA0 (nul)* *-UEA1 (Kasumi)* *-UEA2 (snow3G)*
Intégrité	Aucune	Aucune	f9 *-UIA0 (nul)* *-UIA1 (snow3G)* *-UIA2 (aes)*

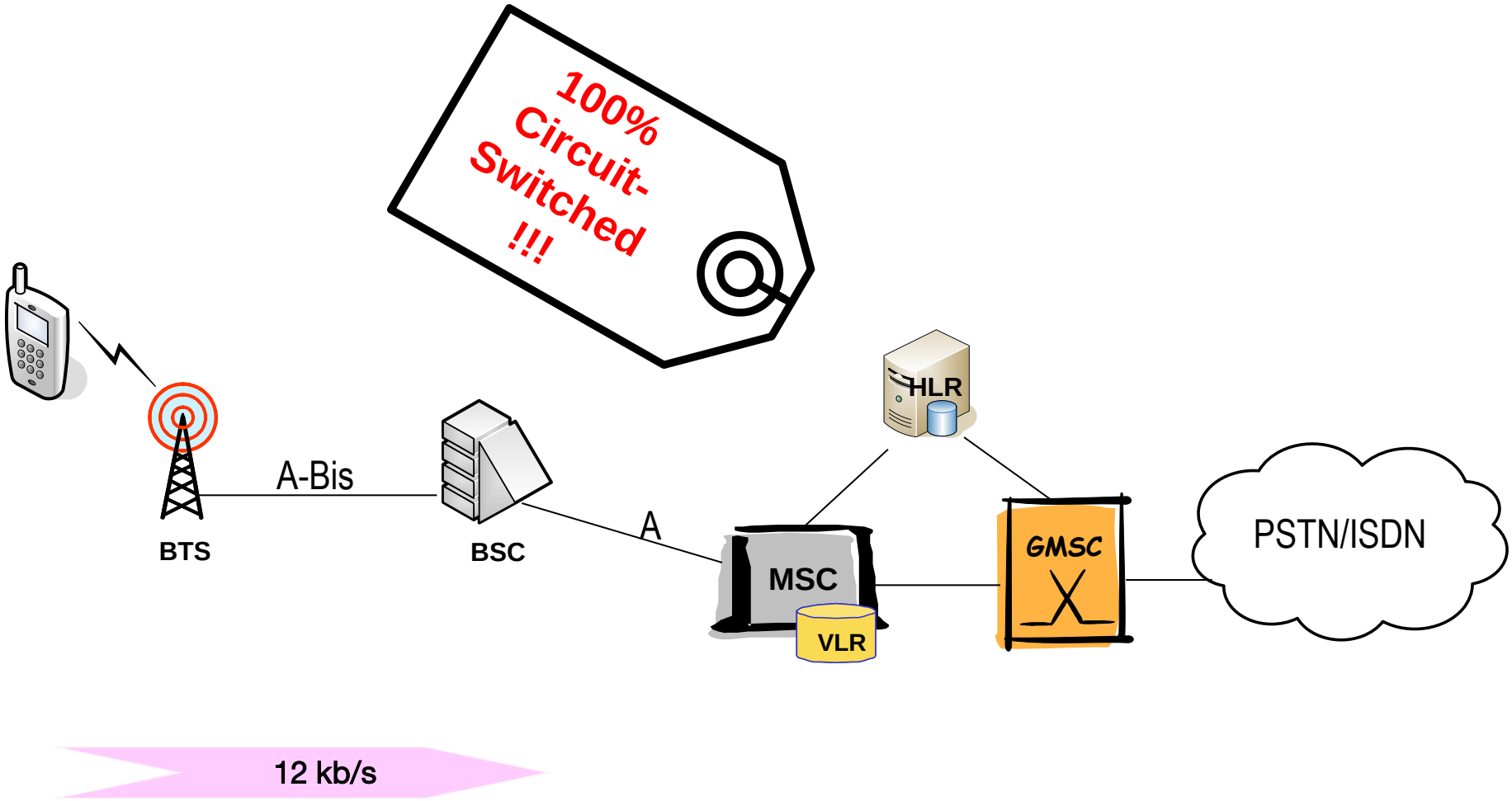
Sécurité UMTS: quelques ressources

- La spécification de l'UMTS est réalisée par le 3GPP
  - TS 33.102 : sécurité UMTS.
  - http://www.3gpp.org/ftp/Specs/html-info/33102.htm
  - Série TS 35 : algorithmes cryptographiques UMTS.

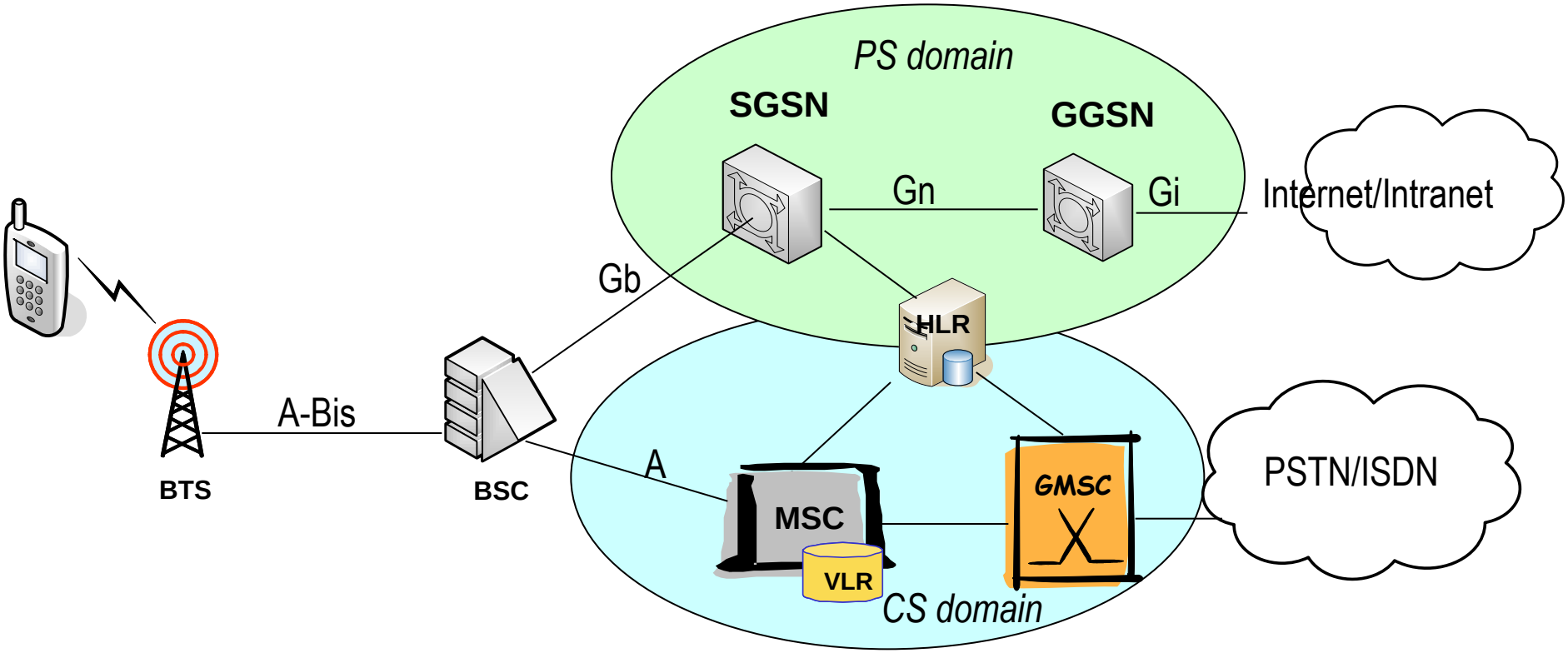
La 4G

…du GSM au LTE…

D'abord, le GSM…



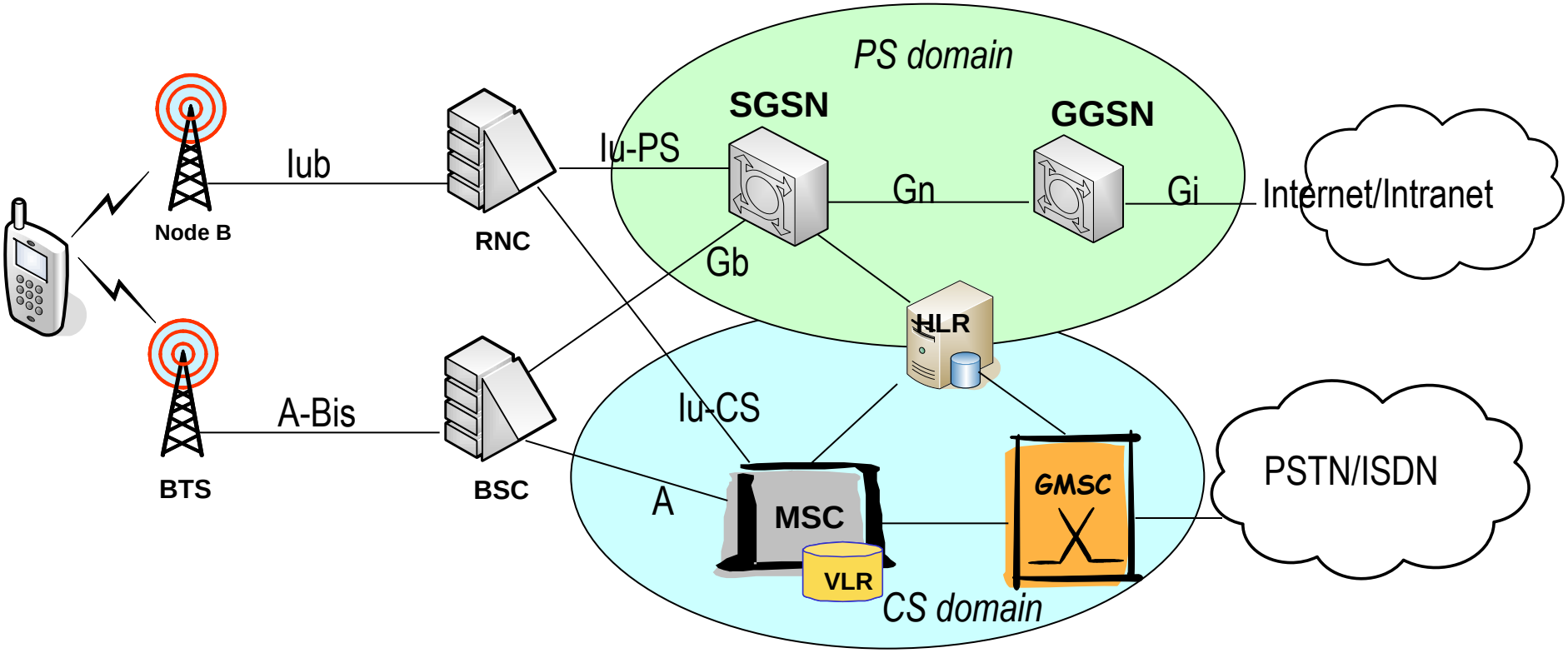
…puis le GPRS…



12 kb/s

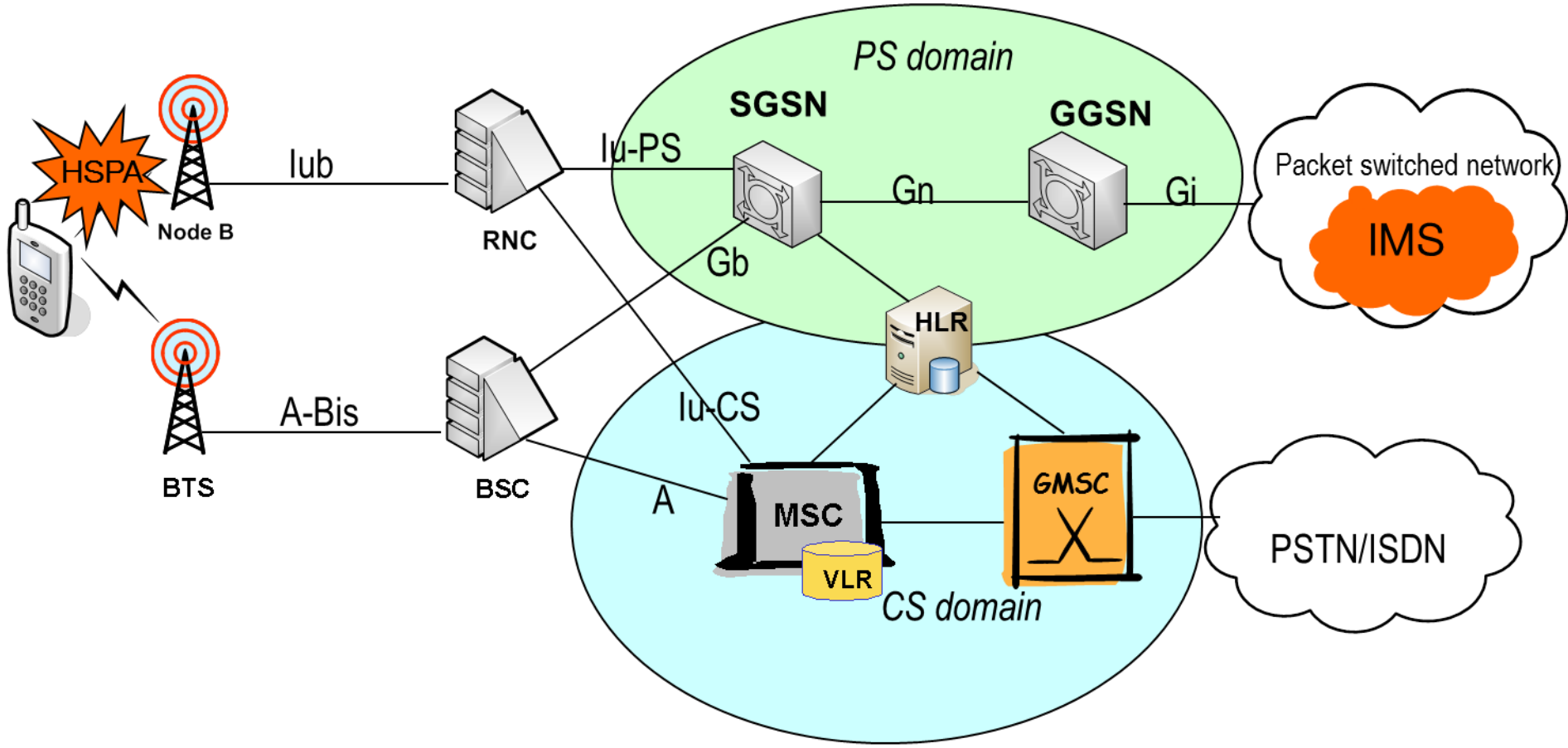
170 kb/s

…et l'UMTS



12 kb/s → 170 kb/s → 384 kb/s

R5, R6, R7: optimisation de la radio et ajout d'IMS…

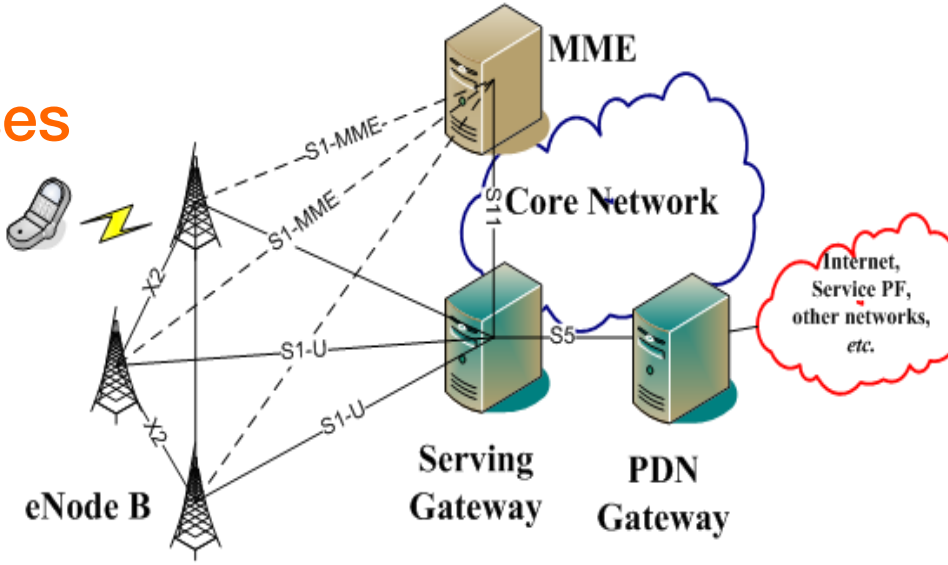


12 kb/s | 170 kb/s | 384 kb/s | ↓42 Mb/s ↑11 Mb/s

Le cahier des charges fonctionnel

- Performance
  - Haut débit
  - Peu de latence
- Low cost (OPEX & CAPEX)
  - il faut réduire le nombre de noeuds
- QoS : à gérer soigneusement
  - technologie radio…
- Passage à l'échelle et flexibilité
- Universalité : une technologie globale, simple
- Réseaux d'accès variés

LTE : les principes de bases

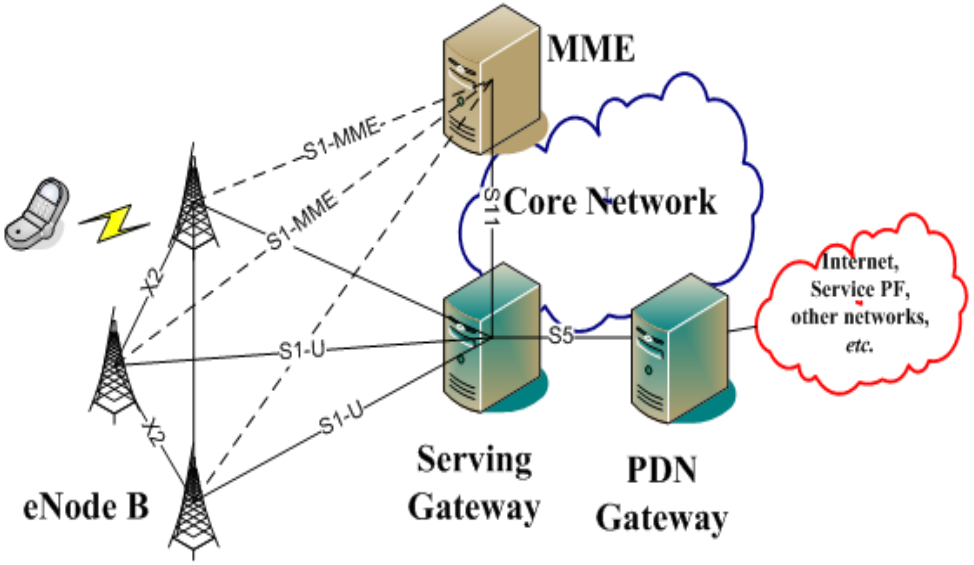


- Refonte des technologies d'accès radio et de l'architecture de l'accès
  - Réutilisation des bandes de fréquences GSM, GPRS, UMTS.
  - Suppression des contrôleurs radio (BSC / RNC) : les stations radio eNodeB embarquent l'intelligence nécessaire à la gestion complète de leurs ressources
    - impacte fortement l'architecture de sécurité

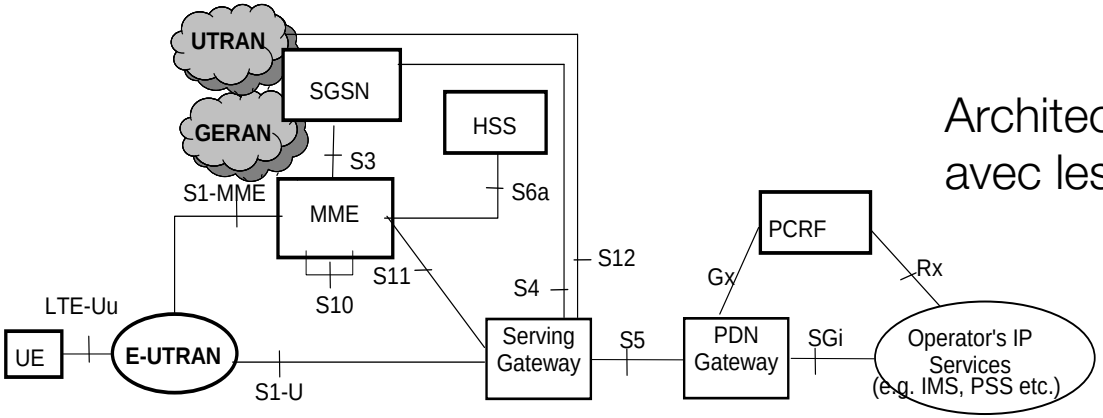
- Refonte de l'architecture du cœur
  - plus de mode circuit
  - mode paquet uniquement, pas de service spécifique intégré (s'appuie sur l'IMS)
  - interconnexions avec réseaux 3GPP (GSM, GPRS, UMTS) et non-3GPP (3GPP2, WIMAX, Wi-Fi…).

- L'ensemble des communications entre les éléments du réseau sont sur IP.
  - Signalisation principalement basée sur SCTP/IP, GTP-C (TCP) et Diameter (TCP ou SCTP).
  - Flux utilisateurs basés sur GTP/UDP/IP.
  - Support prévu également de protocoles de mobilité IP (Mobile IP, MIPv4, MIPv6, DSMIP, PMIP).

L'architecture de base de LTE



Architecture standard LTE



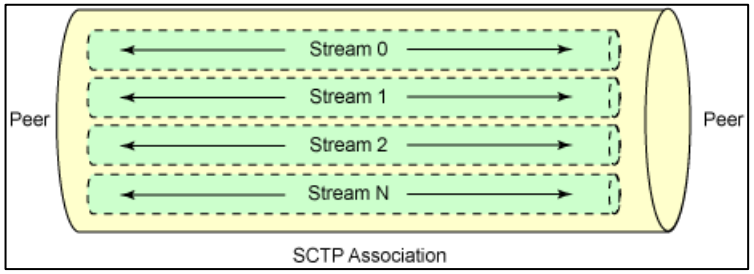
Architecture standard LTE
avec les interfaces GSM / GPRS / UMTS

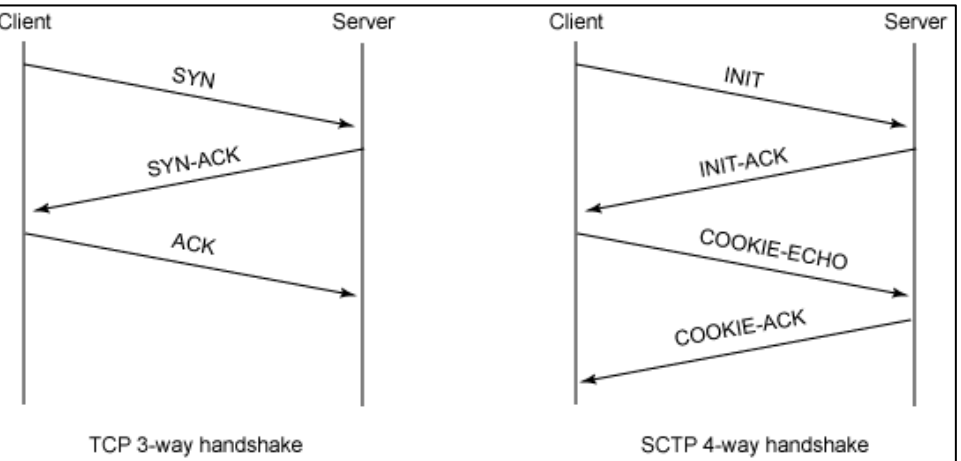
Focus SCTP

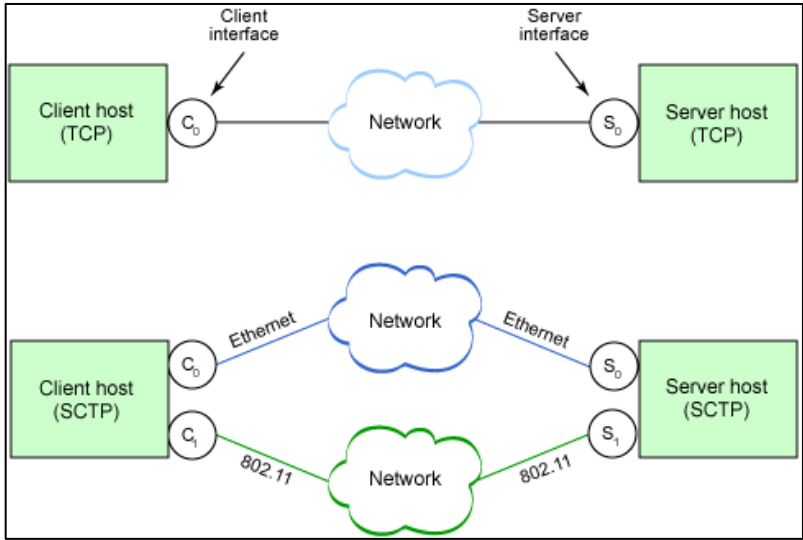
Focus SCTP

- Protocole de niveau 4 (comme UDP, TCP, etc) normalisé par l'IETF
  - RFC 2960 (et beaucoup d'autres)
  - Evolution de la couche transport pour répondre aux besoins telco

- Principales fonctionnalités SCTP
  - Protocole orienté session (association SCTP), exclusivement unicast
  - Remise ordonnée (ou pas) des paquets
  - Détection et retransmission des paquets perdus ou altérés
  - Gestion de plusieurs interfaces réseau (multi-homing)
  - Gestion de plusieurs flux au sein d'une association (multi-streaming)
  - Initialisation sécurisé de l'association (anti-spoofing)







Focus SCTP

- Sous Linux
  - https://github.com/borkmann/lksctp-tools/tree/master/src/withsctp

README

```
This is a package to let you use SCTP with your existing TCP-based binaries.

usage:

$ withsctp xinetd       # Start xinetd stream services on SCTP.
$ withsctp telnet localhost     # Make a telnet over SCTP/IP connection.
```

Sécurité LTE

Les concepts de base de la sécurité LTE

- Réutilisation des fonctions de sécurité UMTS, qui jusqu'ici sont efficaces
  - mécanisme d'authentification quasiment identique
  - utilisation d'identités temporaires (appelées GUTI, et non plus TMSI et P-TMSI)
  - négociation des algorithmes de sécurité
  - chiffrement et contrôle d'intégrité (pour la signalisation) de la communication radio
  - réutilisation de l'algorithme cryptographique SNOW-3G

- Renforcement de la sécurité
  - USIM obligatoire pour accéder au LTE (pas possible avec une SIM) : authentification mutuelle obligatoire
  - définition d'une hiérarchie de clés pour protéger le canal logique entre terminal et MME, en plus du canal radio entre terminal et eNode-B
  - Clés dérivées liées avec l'identité du réseau accédé
  - utilisation de l'algorithme cryptographique AES-128 en plus de SNOW-3G.

L'authentification entre EPS et USIM

- Procédure identique à l'UMTS
  - Réutilisation des USIM et des AuC, avec une clé d'authentification K de 128 bits.
  - Réutilisation de l'AKA et de Milenage.
- Unique modification: spécification de 1 bit du champ AMF, qui permet au terminal et à la carte USIM de distinguer authentification à l'UMTS ou à l'EPS.
- Une fois réseau et USIM mutuellement authentifiés, des dérivations de clés à partir de {CK, IK} sont réalisées pour l'EPS.
  - Ceci explique la nécessité de distinction par le bit AMF.
  - On parle ici d'EPS-AKA (*EPS Authentication and Key Agreement*).
  - Production de K_ASME et de l'ensemble des clés de sécurité nécessaires à l'EPS à partir de {CK, IK}.

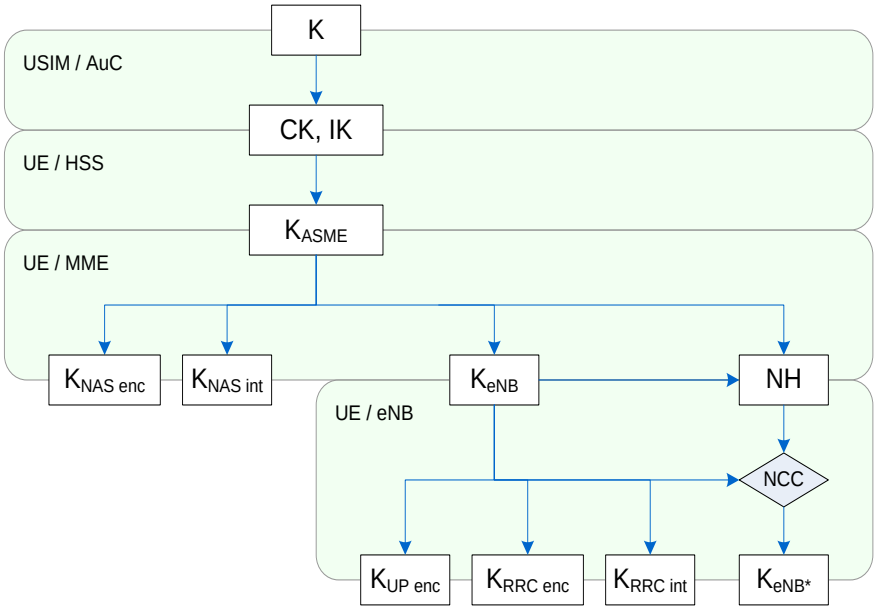
Répartition de la sécurité dans l'EPS

- Plus de contrôleurs radio pour prendre en charge la sécurité des communications, comme en UMTS.
  - La sécurité radio LTE s'arrête dans les stations de base eNodeB.
  - Les eNodeB ne se situent pas forcément dans des zones sous le contrôle physique de l'opérateur.

- Modifications de l'architecture de sécurité par rapport à l'UMTS : il est nécessaire de protéger certaines parties des communications au-delà des eNodeB.
  - Les messages de signalisation de haut niveau (ou messages NAS : *Non-Access Stratum*) échangés entre terminal et MME sont protégés de bout en bout. Les eNodeB ne peuvent pas accéder à leur contenu, et ne font que les transmettre.
  - 5 clés de sécurité sont définies pour un fonctionnement nominal:
    - K_UP_enc : clé pour la confidentialité des données utilisateurs sur la voie radio
    - K_RRC_enc et K_RRC_int : clés pour la confidentialité et le contrôle d'intégrité des messages de signalisation RRC (*Radio Ressources Control*) sur la voie radio.
    - K_NAS_enc et K_NAS_int : clés pour la confidentialité et le contrôle d'intégrité des messages de signalisation NAS.

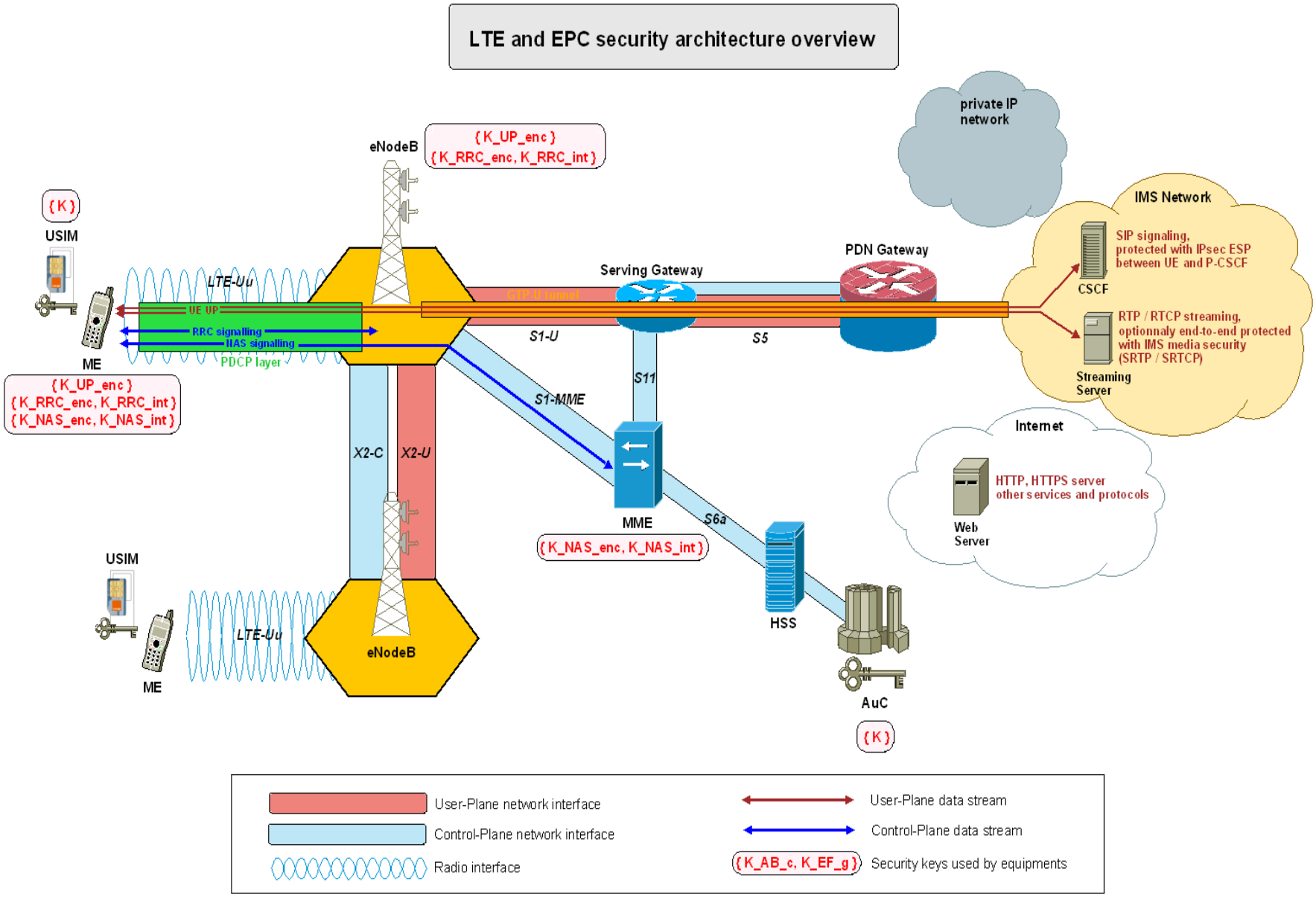
La hiérarchie des clés EPS

- K : clé d'authentification et {CK, IK} clés de sécurité issues de l'authentification UMTS.
- HSS : Home Subscriber Server, remplace le HLR et en assure les fonctions.
- K_ASME (*Access Security Management Entity*) : clé maîtresse pour une session EPS, générée à partir de {CK, IK}.
- 5 clés de sécurité générées à partir de K_ASME :
  - pour le MME ;
  - Pour le eNodeB.
- Un paramètre : NH, généré à partir de K_ASME, et utilisé pour diversifier les clés RRC et UP lors des mobilités.

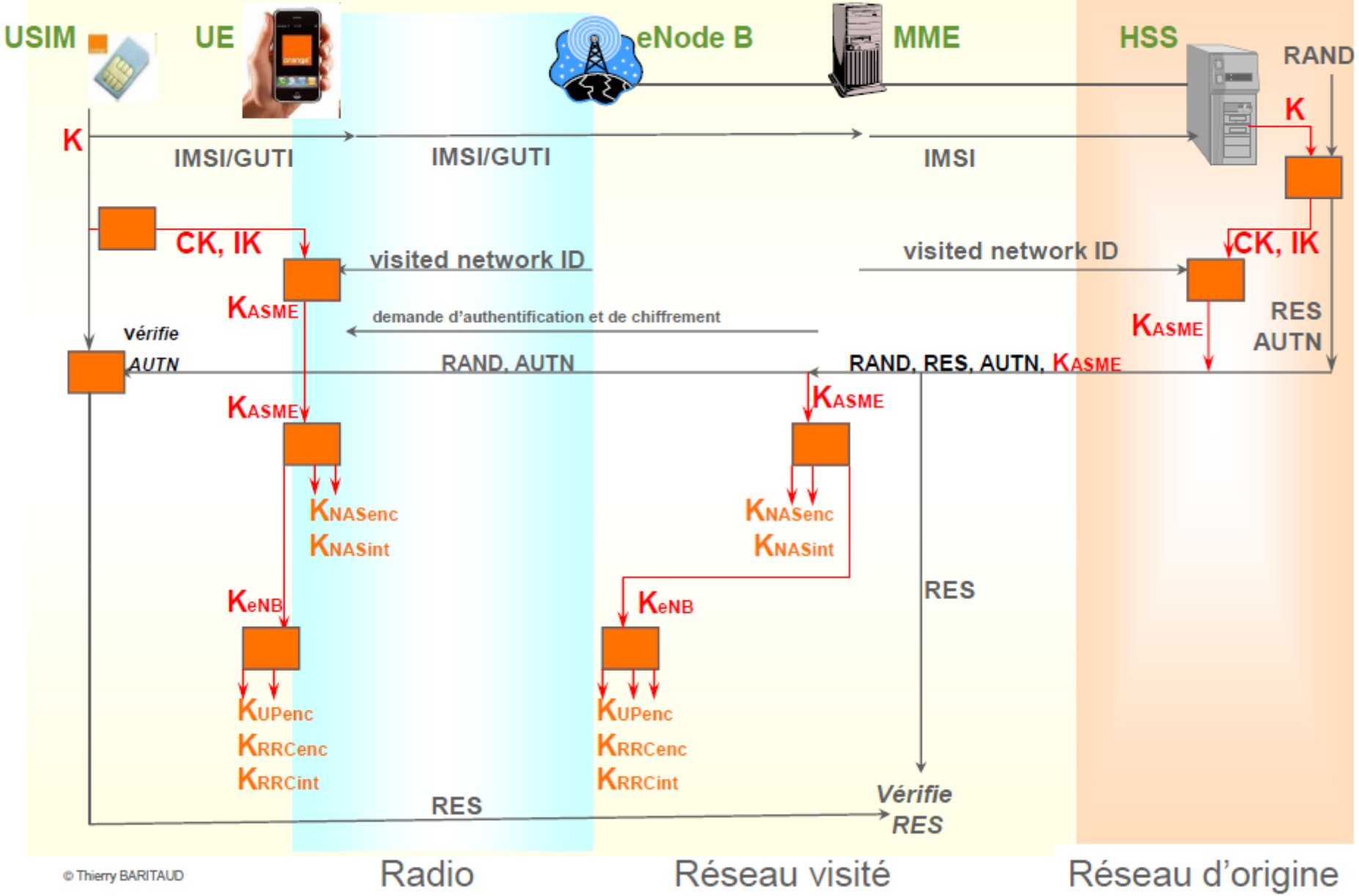


Hiérarchie des clés EPS

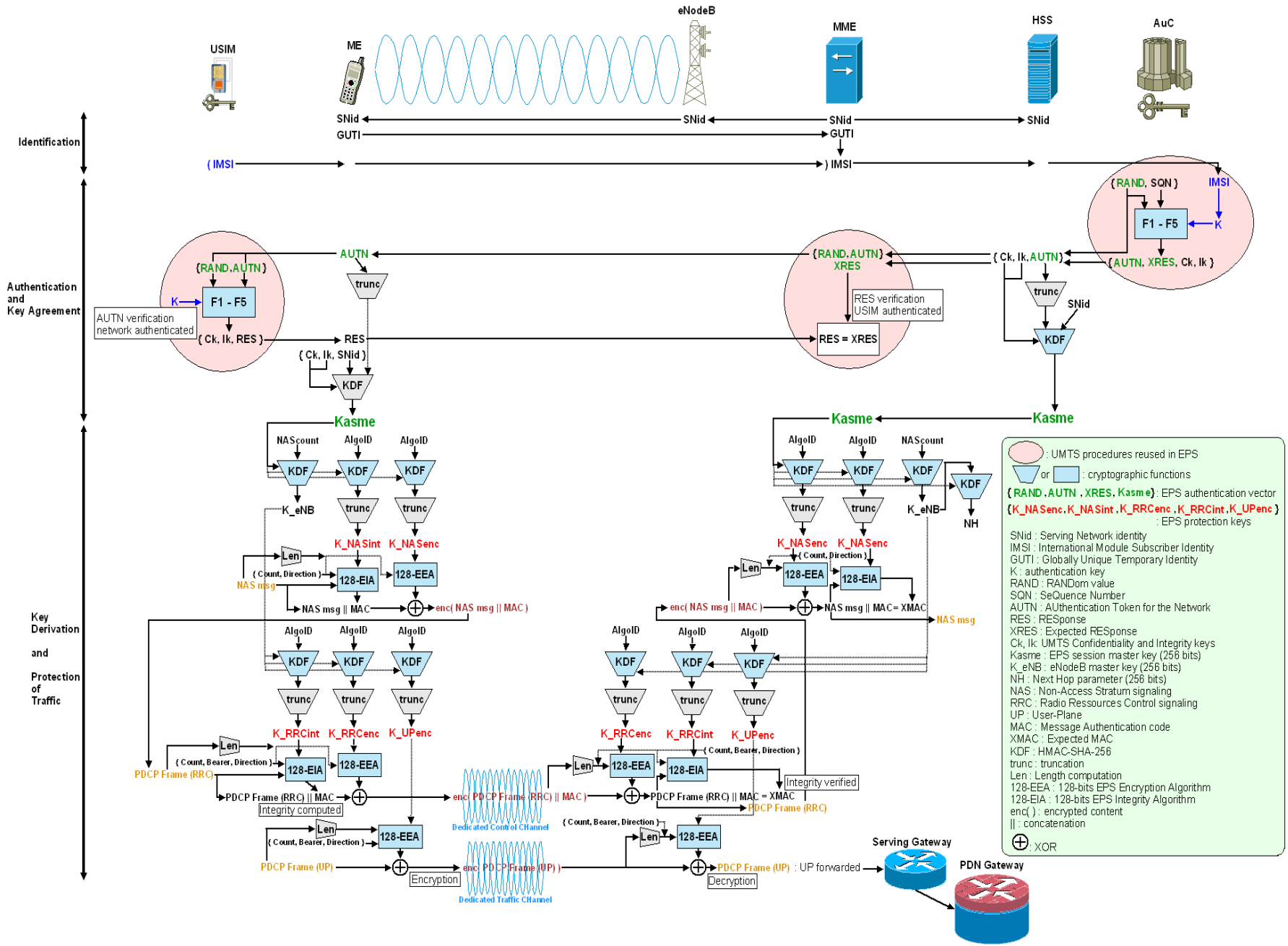
Vue d'ensemble de la sécurité EPS



ARCHITECTURE DE SECURITE LTE



EPS Identification, Authentication and Key Agreement, Key Derivation and Traffic Protection



Les algorithmes de chiffrement et de contrôle d'intégrité

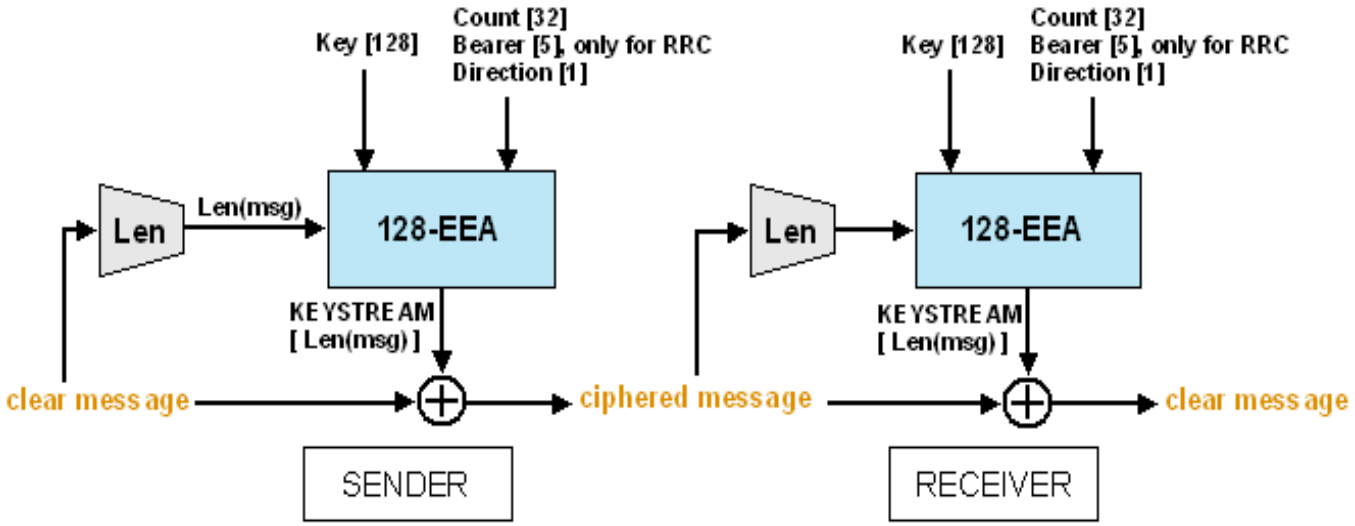
- 3 algorithmes de chiffrement disponibles :
  - EEA0 : NULL, pas de chiffrement (appel d'urgence, ou simplement opérateurs peu scrupuleux quant à la confidentialité des communications de ses abonnés…).
  - 128-EEA1: SNOW-3G, fonctionnement identique à la spécification UMTS (UEA2).
  - 128-EEA2 : AES, mode CTR, clé de 128 bits.
  - 128-EEA3 : ZUC, algorithme poussé par les opérateurs chinois pour remplir ses exigences cryptographiques
  - L'activation du chiffrement, et la priorité sur les algorithmes à utiliser, sont paramétrées par l'opérateur et imposées par le réseau.

- 3 algorithmes de contrôle d'intégrité disponibles :
  - EIA0 : NULL, pas de contrôle d'intégrité (appel d'urgence non authentifié).
  - 128-EIA1 : SNOW-3G, fonctionnement identique à la spécification UMTS (UIA2).
  - 128-EIA2 : AES, mode CMAC, clé de 128 bits.
  - 128-EIA3 : ZUC, algorithme poussé par les opérateurs chinois
  - Le contrôle d'intégrité est obligatoire, réalisé uniquement sur la signalisation. La priorité sur les algorithmes à utiliser est paramétrée par l'opérateur et imposée par le réseau.

Les algorithmes de chiffrement et de contrôle d'intégrité

- SNOW-3G
  - algorithme de chiffrement à flot, produisant un suite de mots de 32 bits, à partir d'une clé de 128 bits, et d'un vecteur d'initialisation de 128 bits.
- AES
  - algorithme de chiffrement par blocs de 128 bits en entrée et sortie, utilisant des clés de 128, 192 ou 256 bits.
- ZUC
  - algorithme de chiffrement à flot, produisant un suite de mots de 32 bits, à partir d'une clé de 128 bits, et d'un vecteur d'initialisation de 128 bits.
  - accepté au 3GPP en 2011
  - pas de failles évidentes mises en évidence jusqu'à aujourd'hui…
- Les algorithmes cryptographiques utilisés (SNOW-3G, AES, SHA256) sont publics:
  - Analysés de près par de nombreuses équipes (moins pour SNOW-3G que pour AES et SHA).
  - Réputés robustes et sûrs.
  - Sauf ZUC (trop récent)

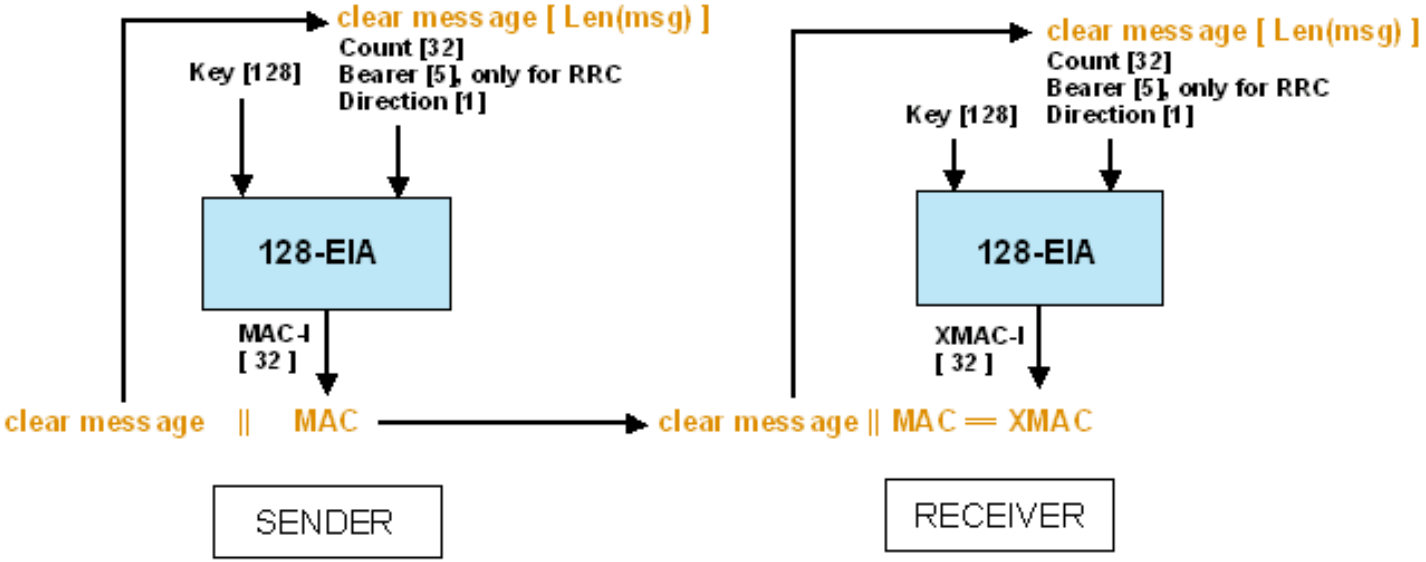
EEA : fonction de chiffrement, orientée chiffrement à flot



Principe de fonctionnement de 128-EEA

- Utilisé pour chiffrer les trames PDCP UP (trafic utilisateur), PDCP RRC (sig) et les messages NAS (sig).
- Pour les messages NAS, pas de paramètres d'entrée bearer.
- L'algorithme sert àproduire une suite chiffrante (KEYSTREAM) de la taille du message à chiffrer / déchiffrer.
- Le message clair / chiffré est XORé avec la suite chiffrante.
- Production du KEYSTREAM possible avant de connaître le contenu du message.

EIA: fonction de MAC (Message Authentication Code)



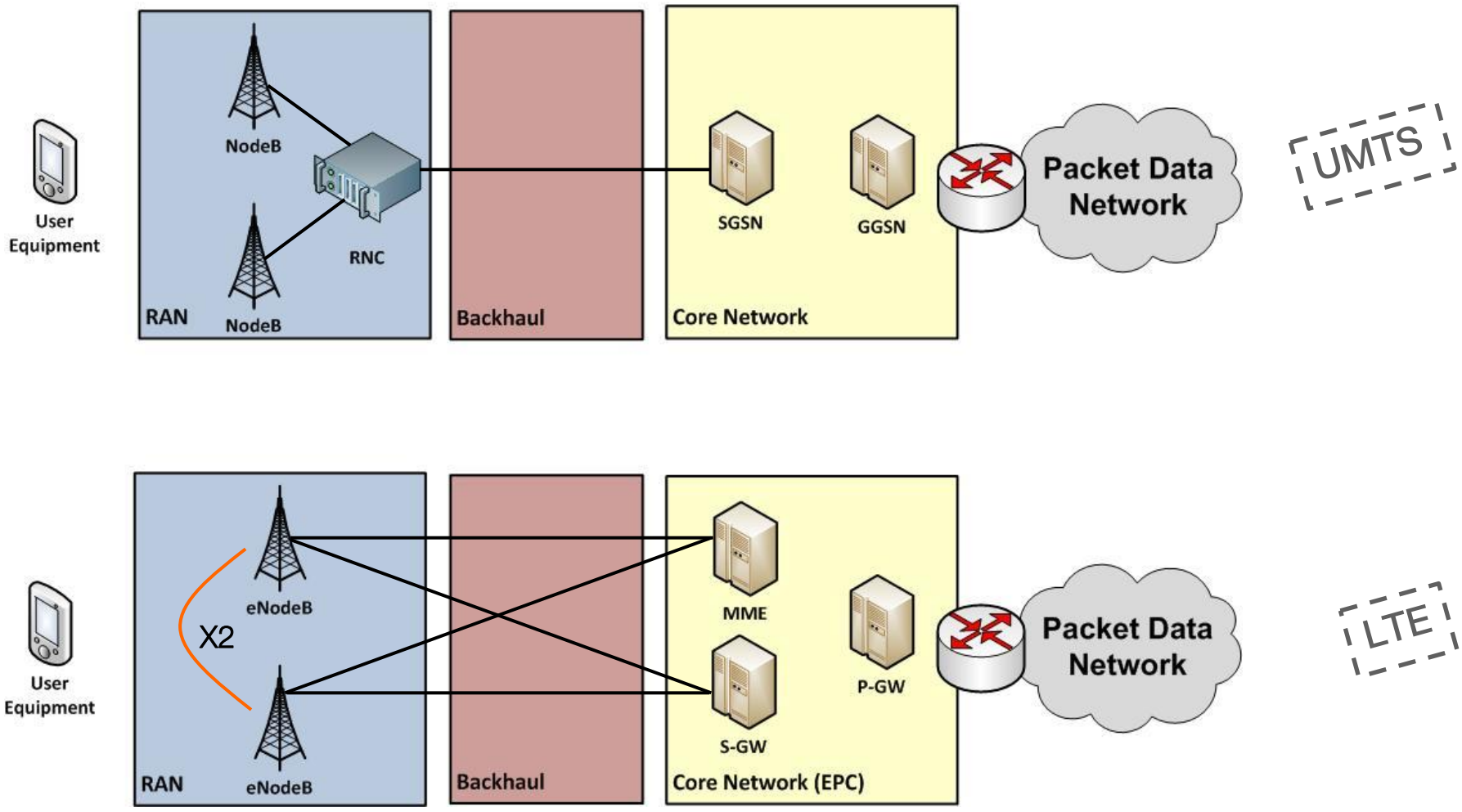
Principe de fonctionnement de 128-EIA

- Utilisé pour les trames PDCP RRC et les messages NAS.
- Pour les messages NAS, pas de paramètres d'entrée *bearer*.
- MAC fait systématiquement 32 bits.
- L'algorithme sert à produire un code d'authentification de la commande de signalisation

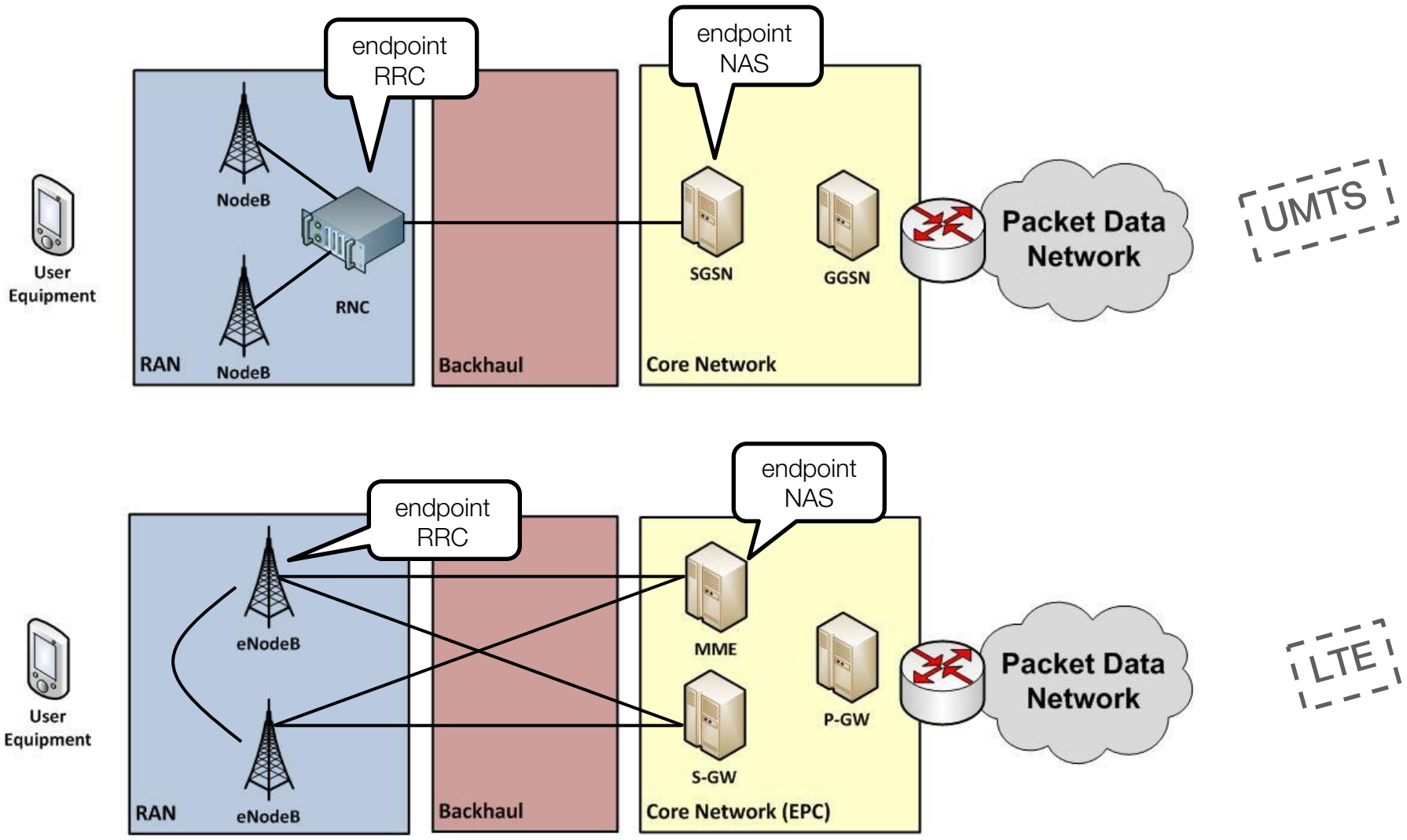
De la 3G au LTE : évolutions de l'architecture

> une architecture à plat…

> …avec un lien direct antre les antennes (X2)

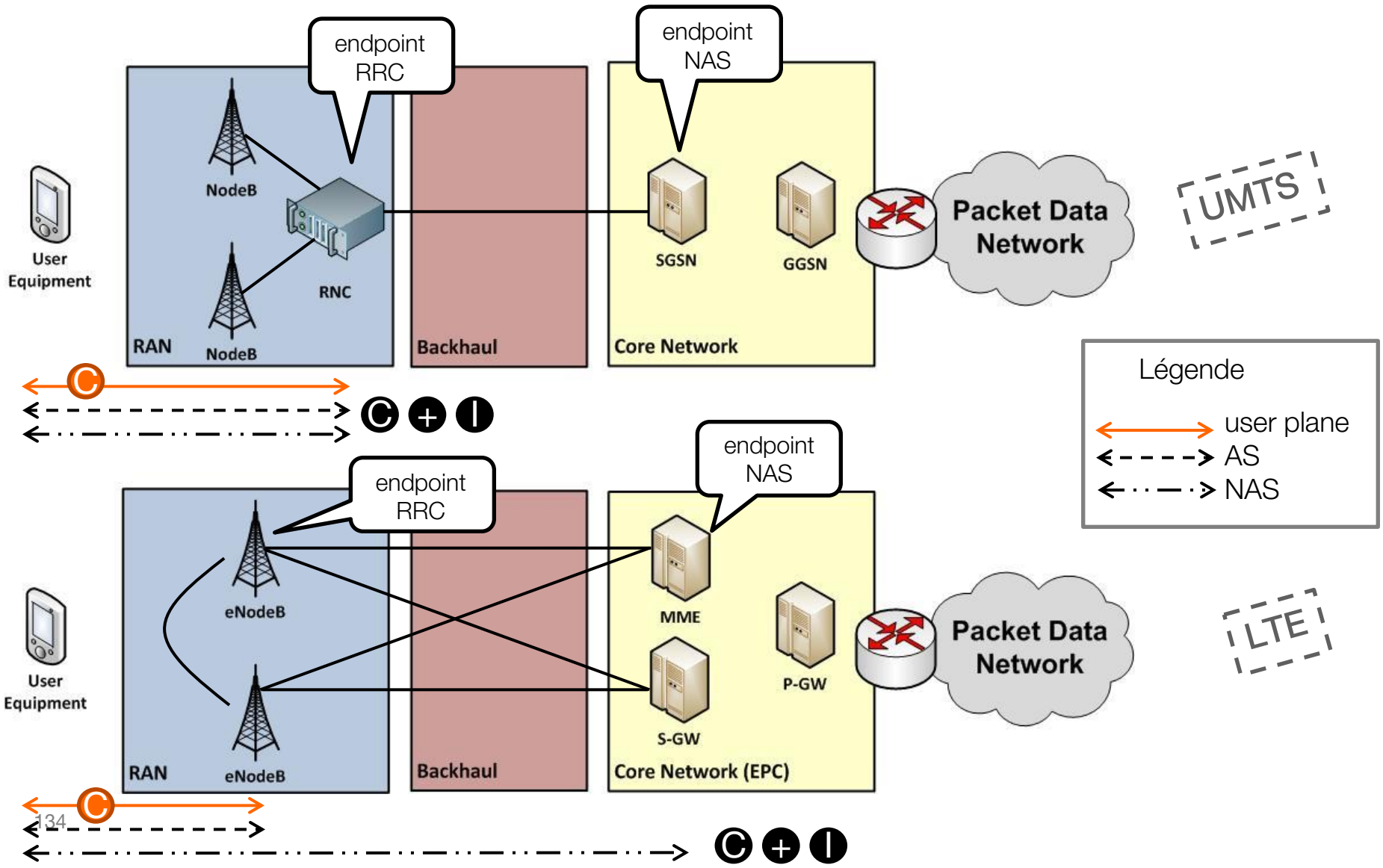


De la 3G au LTE :



De la 3G au LTE :

> control plane sécurisé de bout-en-bout



Quelques antennes

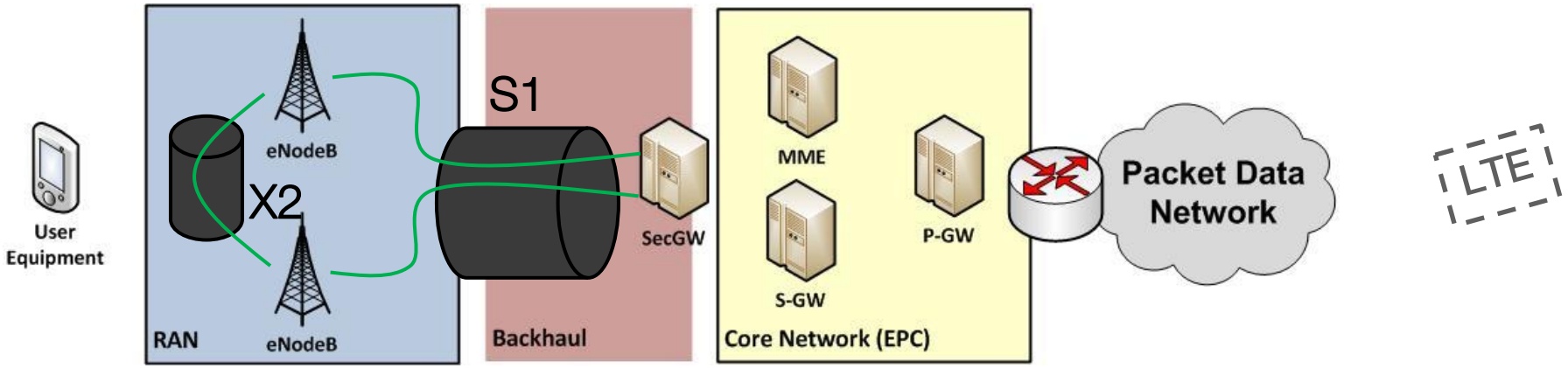
Le réseau de transport LTE : routage tout IP

- Le réseau de transport du LTE supporte les interfaces X2 (inter eNodeB) et S1 (entre eNodeB et EPC).
  - Tous les messages de signalisation sont transportés sur SCTP / IP (protocoles S1-AP et X2-AP, spécifiés par le 3GPP).
  - Les flux utilisateurs sont transportés sur GTP-U / UDP / IP (GTP spécifié par le 3GPP).
  - Aucun de ces protocoles n'intègre de fonction de sécurité.

- Selon le niveau de contrôle d'accès aux eNodeB, il convient de réaliser une éventuelle protection cryptographique des flux.
  - Sans protection, un attaquant accédant à l'environnement physique d'un eNodeB peut injecter des messages de signalisation vers d'autres eNodeB, ou vers les MME, et espionner les communications utilisateurs.
  - Utilisation d'IPsec ESP, entre les eNodeB, et avec une passerelle à l'entrée de l'EPC, pour la signalisation.
  - Utilisation d'une sécurité applicative pour les flux utilisateurs (*IMS media plane security*, utilisation de TLS pour les plateformes de service…).

Le réseau de transport LTE : routage tout IP et tunnel IPsec

- Recommandation pour le trafic entre eNB et entre les eNB et le cœur de réseau :
  - Encapsulation du user plane et du control plane dans des tunnels IPsec
  - interfaces appelée « X2 » and « S1 »

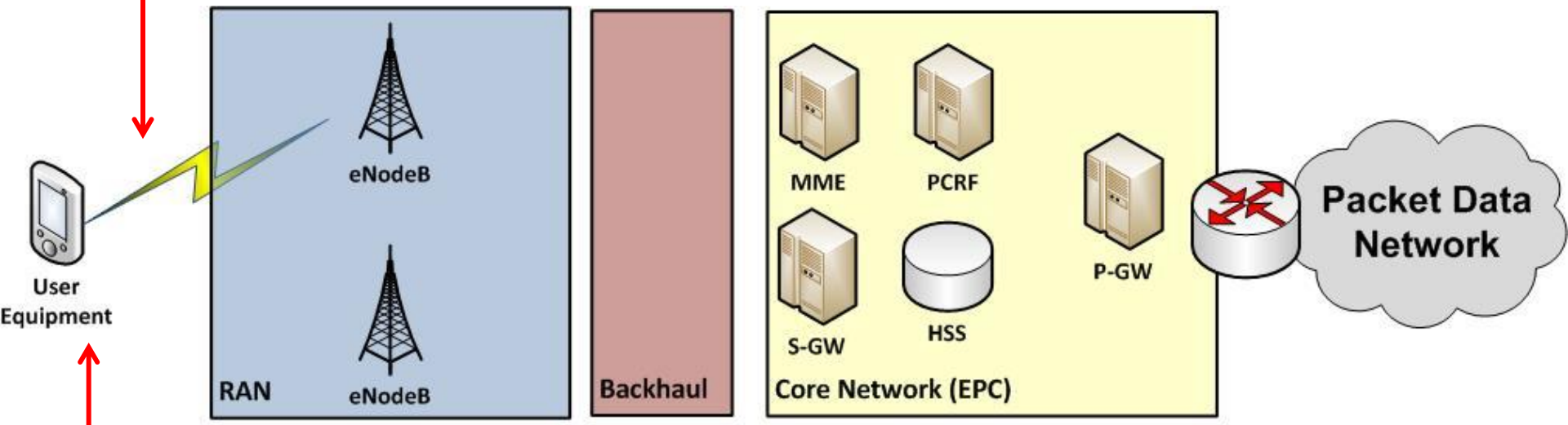


Risques résiduels sur le LTE

Comment se prémunir des attaques ?

- **Chiffrement et intégrité** obligatoires sur le canal radio
- **Renouvellement** régulier du TMSI (ou équivalent)
- **Ré authentification** régulière des utilisateurs

Attaques sur le lien radio



Attaques IP depuis l'UE

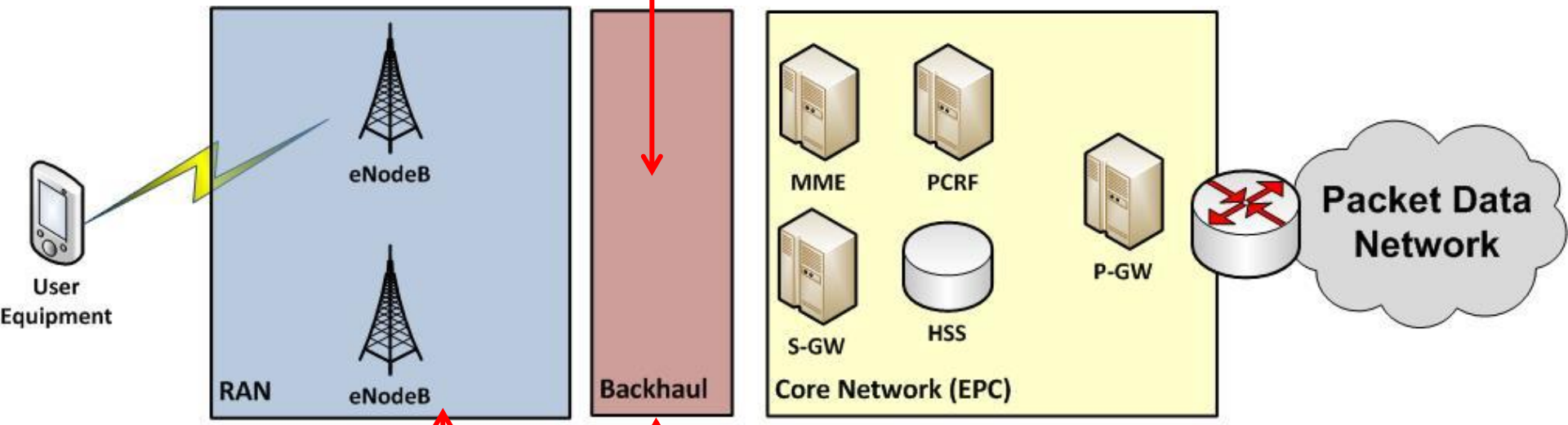
- **Sécurité en profondeur** / bonnes pratiques
  - ségrégation des réseaux, fermeture des services non utilisés, mots de passe par défaut changés, IDS / IPS / SIEM…
- Les **contre-mesures traditionnelles des réseaux IP** s'appliquent
- Veille sur les **malwares & botnets mobiles**

Other mobile network / GRX

Comment se prémunir des attaques ?

Sécuriser **l'accès logique et physique** aux antennes et au backhaul

Attaques par un accès physique au réseau de collecte



tunnel IPsec entre eNB (**X2**) et entre les eNB et le backhaul (**S1**), **pour la signalisation et les communications**

Attaques physiques sur l'antenne

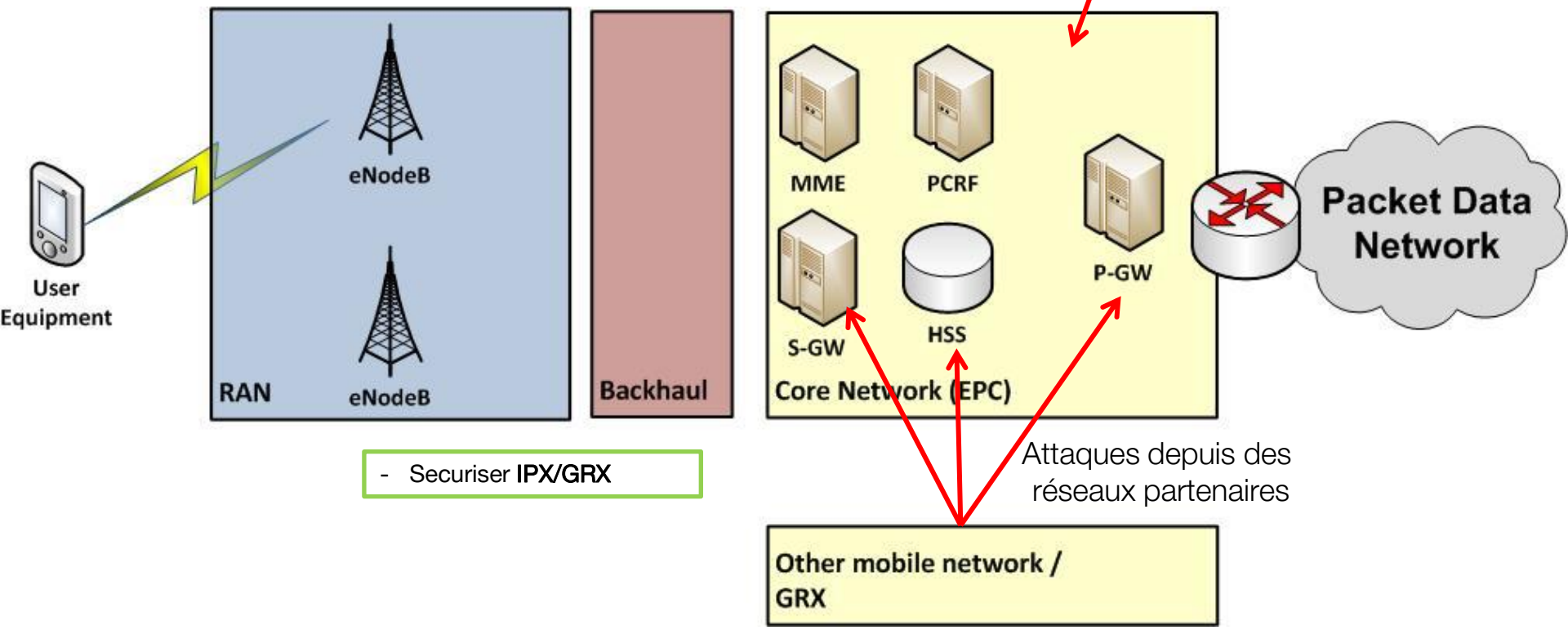
Attaques L2/L3 sur la collecte

Other mobile network / GRX

Comment se prémunir des attaques ?

Bonnes pratiques (définir de rôles avec le plus petit ensemble de privilèges possible, logguer les actions, etc)

Attaques depuis le cœur de réseau

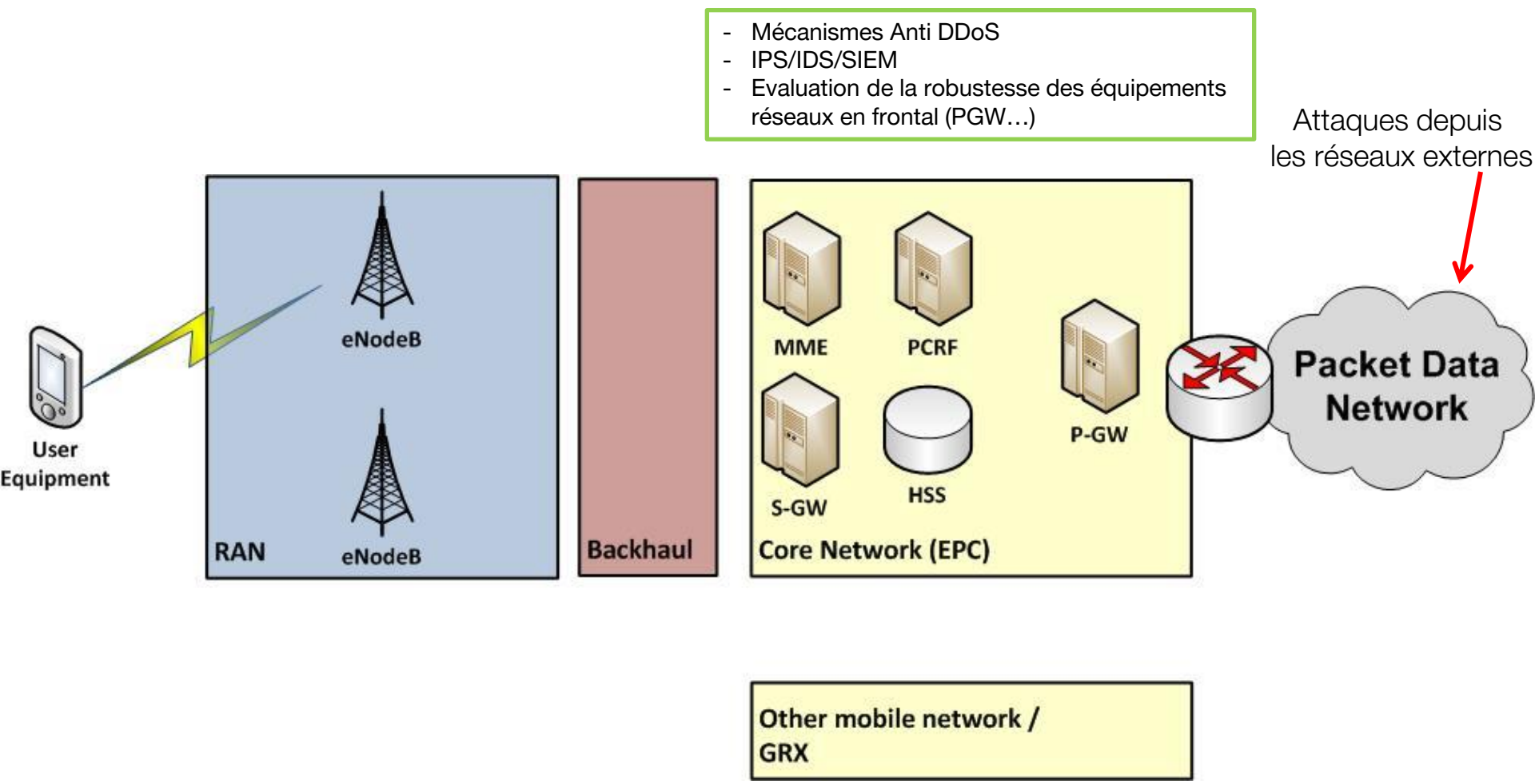


- Securiser **IPX/GRX**

Attaques depuis des réseaux partenaires

Comment se prémunir des attaques ?

- Mécanismes Anti DDoS
- IPS/IDS/SIEM
- Evaluation de la robustesse des équipements réseaux en frontal (PGW…)



Conclusion sur la sécurité du LTE et de l'EPC

- L'architecture de sécurité est poussée plus loin, vis-à-vis de l'UMTS, pour répondre aux changements d'architectures.
  - Design plus complexe, mais bien adapté.

- La complexité des multiples architectures, interfaces, protocoles, procédures de mobilité… rend plus difficile la perception et la garantie de sécurité et de maîtrise du réseau pour les opérateurs.

Fonctions de sécurité	GSM	UMTS	LTE
Identités temporaires			
Authentification de l'utilisateur			
Authentification du réseau			
Protection contre le rejeu			
Chiffrement radio			
Contrôle d'intégrité signalisation (MAC)			
Clés de session liées au serving network			

Algorithmes : récapitulatif

	GSM	GPRS	UMTS	LTE
Authentification + génération de clé	GSM-AKA = A3 + A8 *-COMP128-1 (cassé)* *-COMP128-2* *-COMP128-3* *-Milenage2G*		UMTS-AKA = (f1,f2)+(f3,f4) *-Milenage*	EPS-AKA = (f1,f2)+(f3,f4) + dérivations de la hiérarchie de clés
Chiffrement	A5 *-A5/0 (nul)* *-A5/1 (cassé)* *-A5/2 (cassé)* *-A5/3* *-A5/4*	GEA *-GEA/0* *-GEA/1 (cassé)* *-GEA/2* *-GEA/3*	f8 *-UEA0 (nul)* *-UEA1 (Kasumi)* *-UEA2 (snow3G)*	f8 *-EEA0 (nul)* *-EEA1 (snow3G)* *-EEA2 (aes)* *-EEA3 (zuc)*
Intégrité	Aucune	Aucune	f9 *-UIA0 (nul)* *-UIA1 (snow3G)* *-UIA2 (aes)*	f9 *-EIA0 (nul)* *-EIA1 (snow3G)* *-EIA2 (aes)* *-EIA3 (zuc)*

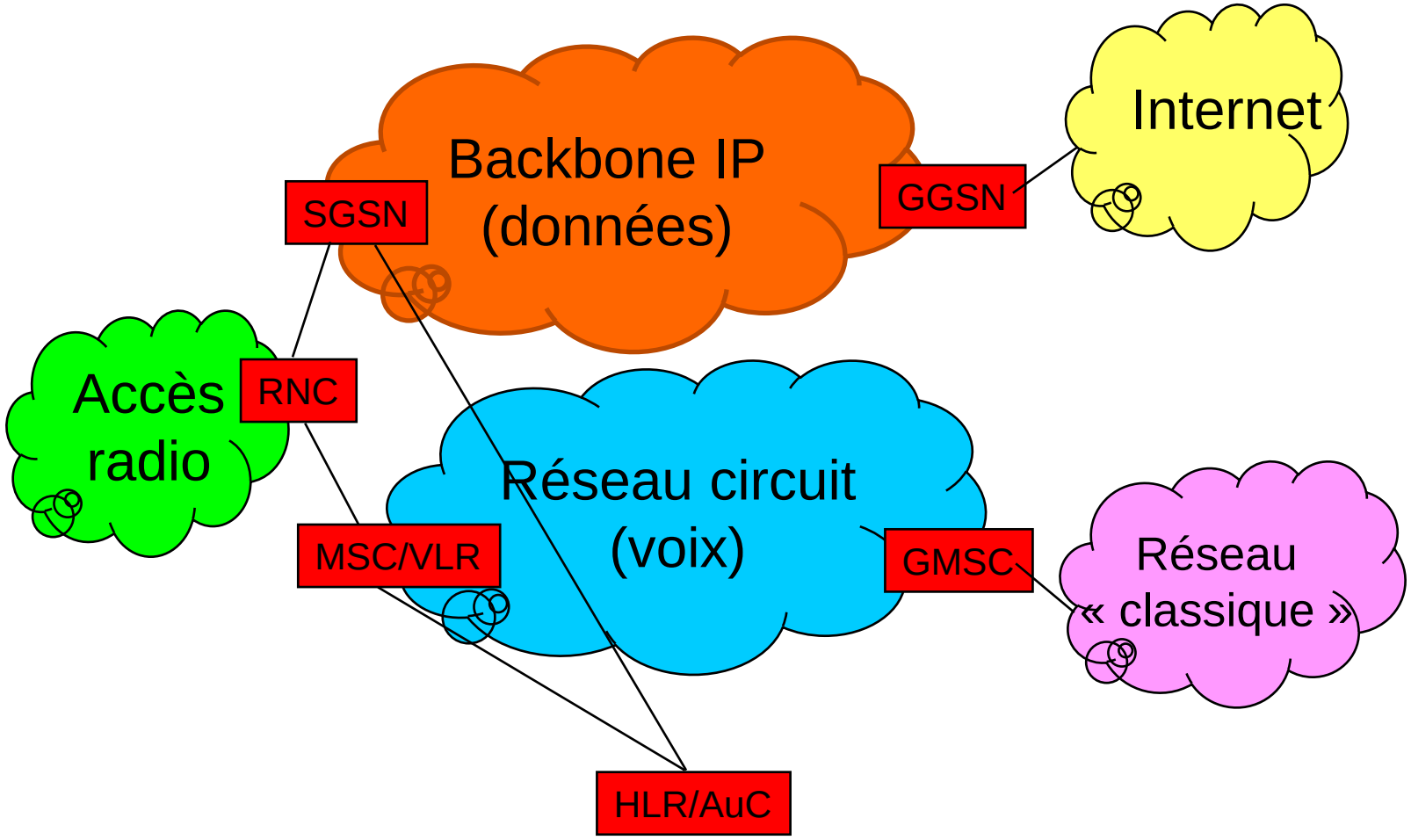
Sécurité de l'EPS : quelques ressources

- La spécification de la sécurité LTE et EPC est réalisée par le 3GPP
  - TS 33.401 et TS 33.402 : architecture du réseau EPS.
  - http://www.3gpp.org/ftp/Specs/html-info/33401.htm (sécurité LTE - EPC)
  - http://www.3gpp.org/ftp/Specs/html-info/33402.htm (sécurité des interfaces non-3GPP)

- Des ressources Internet nombreuses (pour les protocoles cœur)
  - http://www.kernel.org/ : Linux, implémente nativement SCTP.
  - http://code.google.com/p/s11interface/ : simulation d'un MME et d'un SGW LTE et des messages GTPv2 qu'ils échangent
  - http://bellard.org/lte/
    - Pas de codes publics concernant la partie radio.

La sécurité dans le réseau cœur mobile (GSM – GPRS – UMTS)

Structure du réseau cœur UMTS et GSM – GPRS



Evolution du réseau cœur mobile et nouveaux risques

- Les réseaux cœurs commutés des opérateurs télécoms reposent actuellement en grande partie sur des liaisons privées dédiées et s'appuyant sur des technologies de type X25 ou ATM.

- Les réseaux de transport évoluent rapidement vers des technologies basées sur le protocole IP. Les réseaux mobiles convergent vers le monde Internet afin de permettre à un particulier d'accéder à Internet en mobilité.
  - Depuis la mise en place du cœur GPRS, et avec l'impulsion de l'UMTS, le cœur de réseau paquet se développe largement.

- Cette évolution va forcer le réseau cœur paquet à s'ouvrir davantage vers des réseaux extérieurs, en utilisant des techniques ouvertes et répandues.
  - Cela entraîne de nouvelles menaces pour le réseau de l'opérateur.

Principales menaces sur le réseau cœur

- Déni de service
  - les attaques de déni de service consistent à empêcher le bon fonctionnement d'un système : elles impactent la disponibilité du système
  - Ce sont des attaques souvent simples (type *flooding* d'un serveur web), mais elles peuvent aussi utiliser les systèmes de signalisation pour impacter un grand nombre de machines.

- Interceptions illégales
  - l'écoute du trafic dans les réseaux cœurs peut permettre d'intercepter le trafic d'un utilisateur,
  - ou bien de recupérer les données d'authentification envoyées du HLR au VLR / SGSN (ces données contiennent les clés de session utilisées sur la voie radio).

- Fraudes diverses
  - l'interception de données d'authentification peut mener à certains scénarios de fraudes (se faire passer pour un autre abonné, accéder à des services sans en avoir le droit, générer du trafic vers des numéros premium…).
  - L'accès à des interfaces sensibles (HLR, VLR, SGSN) peut permettre de transmettre des commandes de signalisations menant à des scénarios de fraudes (usurpation de MSISDN, modification d'abonnement…).

Un réseau cœur et transport basé sur IP

- La mise en place d'un réseau cœur basé sur des technologies de type IP introduit une plus grande incertitude sur la sécurité.
  - Cœur paquet basé par défaut sur IP.
  - Signalisation SS7 en migration vers SIGTRAN pour être routée sur IP (à la place d'ATM).
  - Réseau de transport UMTS (supportant les connexions entre sous-système radio et réseau cœur) en migration vers IP.
  - Protocoles IP davantage maîtrisés par les hackers et l'ensemble des utilisateurs Internet.
- Il est donc nécessaire de mettre en œuvre des mécanismes pour assurer la sécurité du réseau de transport IP et le bon fonctionnement du système
  - Mise en place de filtrages en bordure de réseau (firewalls…).
  - Développement de la sécurisation des transactions entre machines, en particulier au niveau de la signalisation.
  - Utilisation d'IPsec.

La sécurisation d'IP avec les protocoles IPsec

- Le terme IPsec recouvre un ensemble de mécanismes de sécurité qui permettent d'assurer la sécurité du transport de données basé sur le protocole IP.

- IPsec est un système de sécurité qui s'applique sur la couche réseau et sécurise l'ensemble des données routées / de routage, à l'opposé de la sécurité applicative qui peut être plus sélective.

- IPsec est composé de deux protocoles
  - AH (Authentication Header) : mode qui assure l'intégrité et l'authentification des paquets IP (en-tête IP y compris).
  - ESP (Encapsulated Security Payload) : mode qui assure le chiffrement et/ou l'authentification des données routées sur IP.

- IPsec s'appuie sur deux modes distincts
  - Transport : utilisé pour une sécurité de bout en bout.
  - Tunnel: utilisé pour une sécurité entre un terminal et une passerelle, ou entre deux passerelles.

Modes d'utilisation d'IPsec

- Passerelle à passerelle

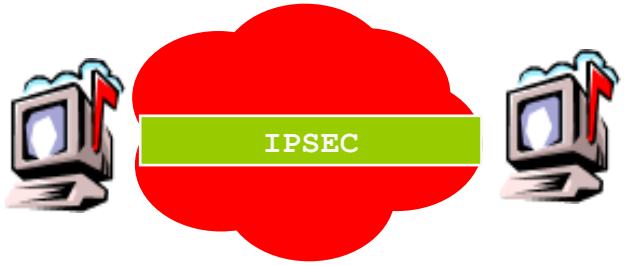
-> mode tunnel

- Machine à passerelle

-> mode tunnel

- Machine à machine

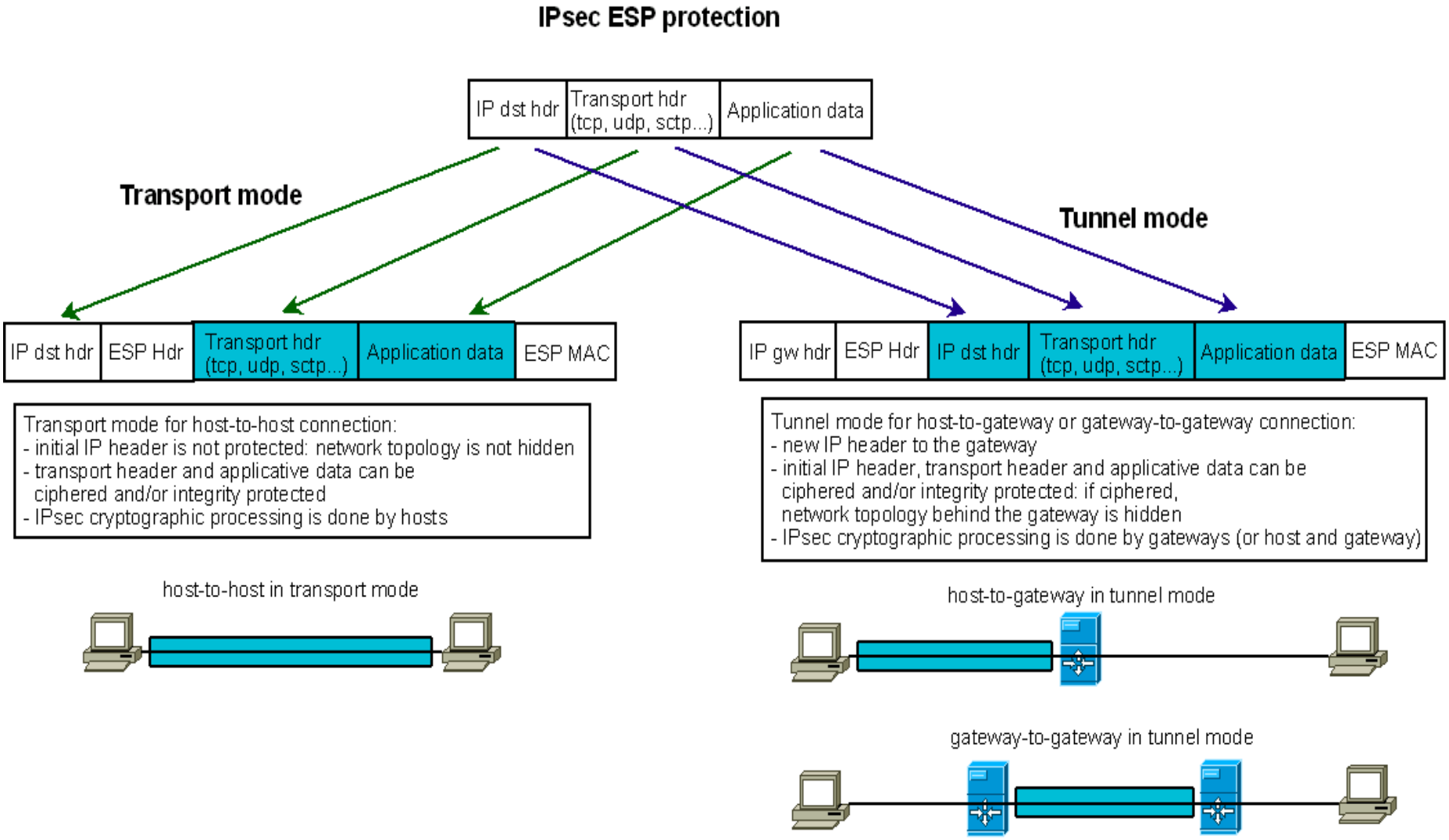
-> mode transport



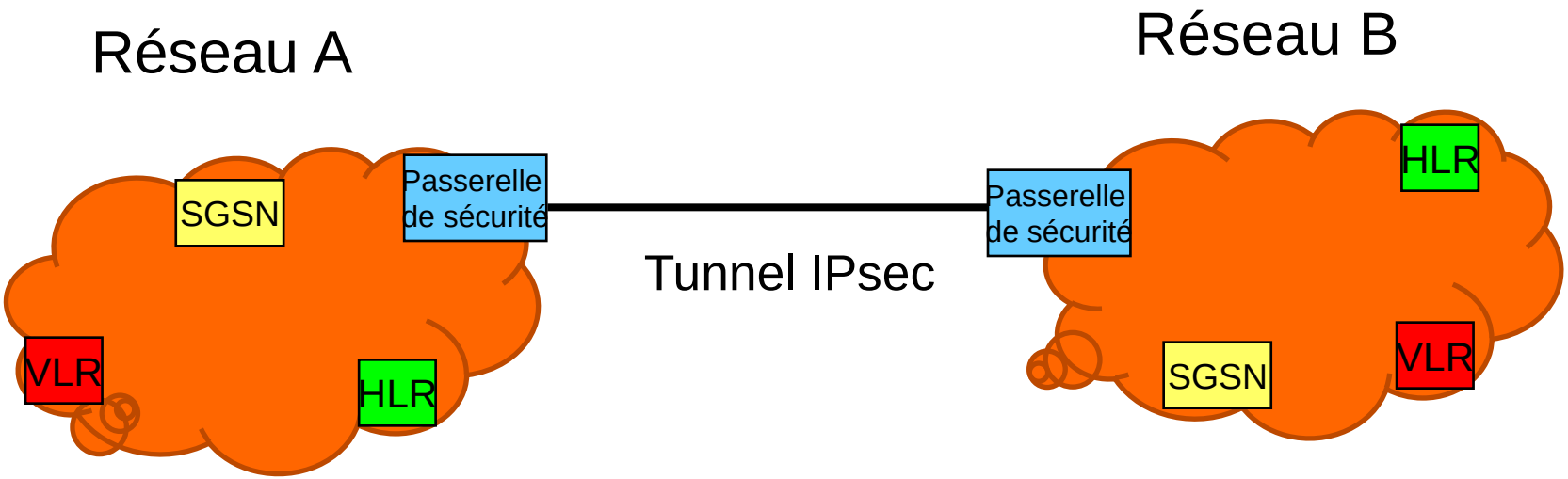
Les modes d'utilisation d'IPsec dans le cœur mobile

- Le système IPsec est spécifié dans la RFC 4301.
- Le protocole AH est peu adapté
  - ne fournit pas de confidentialité;
  - ne permet pas de passer les NAT (fonction parfois réalisée par des firewalls) : AH effectue un contrôle d'intégrité sur l'en-tête IP (sauf certains champs : TTL par exemple) ;
  - IPsec AH est spécifié dans la RFC 4302.
- Le protocole ESP est mieux adapté:
  - fournit au choix : intégrité / chiffrement / chiffrement et intégrité ;
  - N'impacte pas les informations de routage de l'en-tête IP ;
  - IPsec ESP est spécifié dans la RFC 4303.
- Le mode transport est peu adapté
  - impose aux équipements télécoms de prendre en charge IPsec ESP et les ressources nécessaires aux calculs cryptographiques.
- Le mode tunnel est mieux adapté
  - Permet de déléguer la prise en charge d'IPsec dans un équipement dédié : une passerelle, qui peut aussi réaliser d'autres fonctions de sécurité (filtrage…).

IPsec ESP: principes d'encapsulation transport / tunnel



Architectures d'interconnexions des réseaux cœurs



Architectures d'interconnexions des réseaux cœurs (2)

- Création dynamique de SA via IKE/ISAKMP (*Internet Key Exchange*)

- La sécurité du réseau cœur d'un opérateur est sa propre responsabilité, et l'ensemble de ce réseau est considéré comme un domaine de sécurité unique.
  - L'utilisation d'IPsec à l'intérieur du réseau cœur de l'opérateur est une option afin d'augmenter le niveau de sécurité interne en réalisant plusieurs domaines de sécurité distincts.

- Les différents réseaux cœurs sont reliés entre eux au travers de passerelles de sécurité qui sont des points de passage obligés (par exemple, les zones GRX).
  - IPsec peut être utilisé pour protéger les données échangées entre deux opérateurs différents (ou entre deux domaines de sécurité au sein du réseau d'un même opérateur) sur les liens IP.

Limitation à l'utilisation d'IPsec et IKE

- Protocoles et API complexes.
- Impact d'IPsec sur les performances : IPsec étant un protocole de couche basse, le chiffrement est peu sélectif et nécessite donc une puissance de calcul importante, ce qui dégrade les performances des équipements.
- Gestion des clés d'authentification pour IKE :
  - Les opérateurs négocient de façon bilatérale des accords de coopération, ce qui permettrait d'échanger des secrets pour une configuration automatique. Cependant, le nombre important d'opérateurs dans le monde (860 opérateurs répartis dans 219 pays) rend cette pratique difficile à gérer d'un point de vue opérationnel.
  - La mise en place d'une infrastructure à clé publique (pour déployer des certificats) pose de nombreux problèmes juridiques et politiques pour les opérateurs. De fait, malgré l'utilité qu'aurait une PKI inter-opérateurs pour différentes applications, celle-ci n'existe pas à ce jour.

Les services paquets de plus en plus nombreux et prisés (avec également les déploiements IMS), et l'arrivée du réseau LTE / EPC entièrement basé sur IP, vont pousser à l'utilisation de la sécurité IP et d'IPsec.

Sécurité du réseau cœur: quelques ressources

- La spécification d'interface cœur mobile sécurisés est réalisée par le 3GPP
  - TS 33.210 et TS 33.310 : sécurité des domaines réseaux.
  - http://www.3gpp.org/ftp/Specs/html-info/33210.htm (usage d'IPsec)
  - http://www.3gpp.org/ftp/Specs/html-info/33310.htm (architecture d'authentification)

- Des ressources Internet très nombreuses (le monde IP…)
  - http://www.strongswan.org/: Strongswan, daemon IKEv1 et IKEv2 pour Linux.
  - http://www.kernel.org/: Linux, implémente nativement IPsec (implémentation KLIPS en 2.4 et NETKEY en 2.6) avec interfaces *pfkey* et *xfrm*.
  - http://www.freebsd.org/: FreeBSD, implémente nativement IPsec (implémentation KAME).
  - http://www.openss7.org/ : implémentation (un peu obscure) de SIGTRAN pour UNIX.
  - http://sourceforge.net/projects/ggsn/: implémentation open-source (minimaliste) d'un client SGSN et serveur GGSN pour le protocole GTP.

SS7

Qu'est-ce que SS7 ?
Signalling System #7

- Un ensemble de protocoles utilisé par tous les opérateurs téléphoniques
- Standardisés dans les années '80
- A l'époque, peu d'opérateurs, et ce sont
  - de grands groupes
  - des organismes contrôlés par l'Etat
- Approche de type « walled garden » :
  - on fait confiance,
  - on n'a pas besoin d'authentification

Qu'est-ce que SS7 ?
Signalling System #7

- De nouveaux protocoles sont ajoutés dans les années '90 et 2000 (ETSI, 3GPP) pour proposer des services plus modernes (roaming, SMS, data)

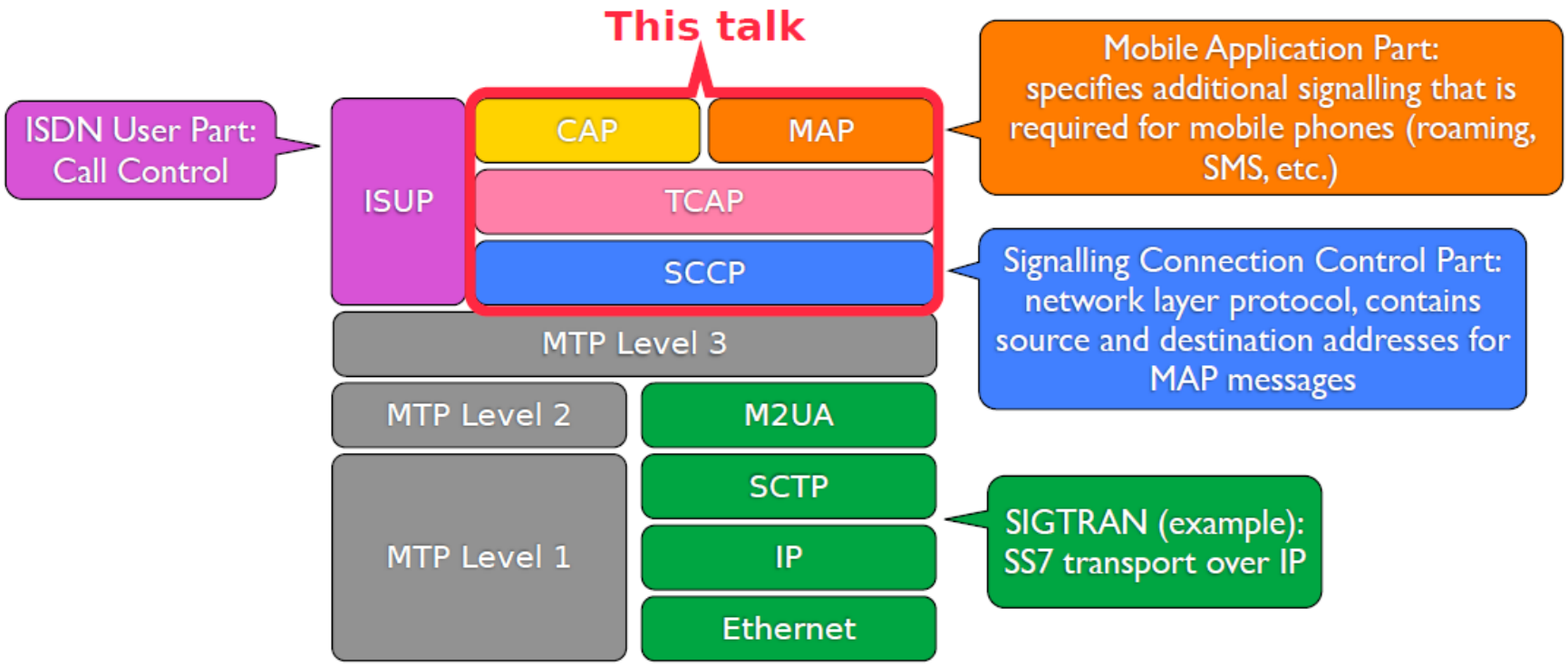
- Mobile Application Part (MAP)
  - Pour les services qui ne sont pas de la voix (ex : roaming, SMS, etc)

- CAMEL Application Part (CAP)
  - Pour des usages avancés

- Toujours pas d'authentification

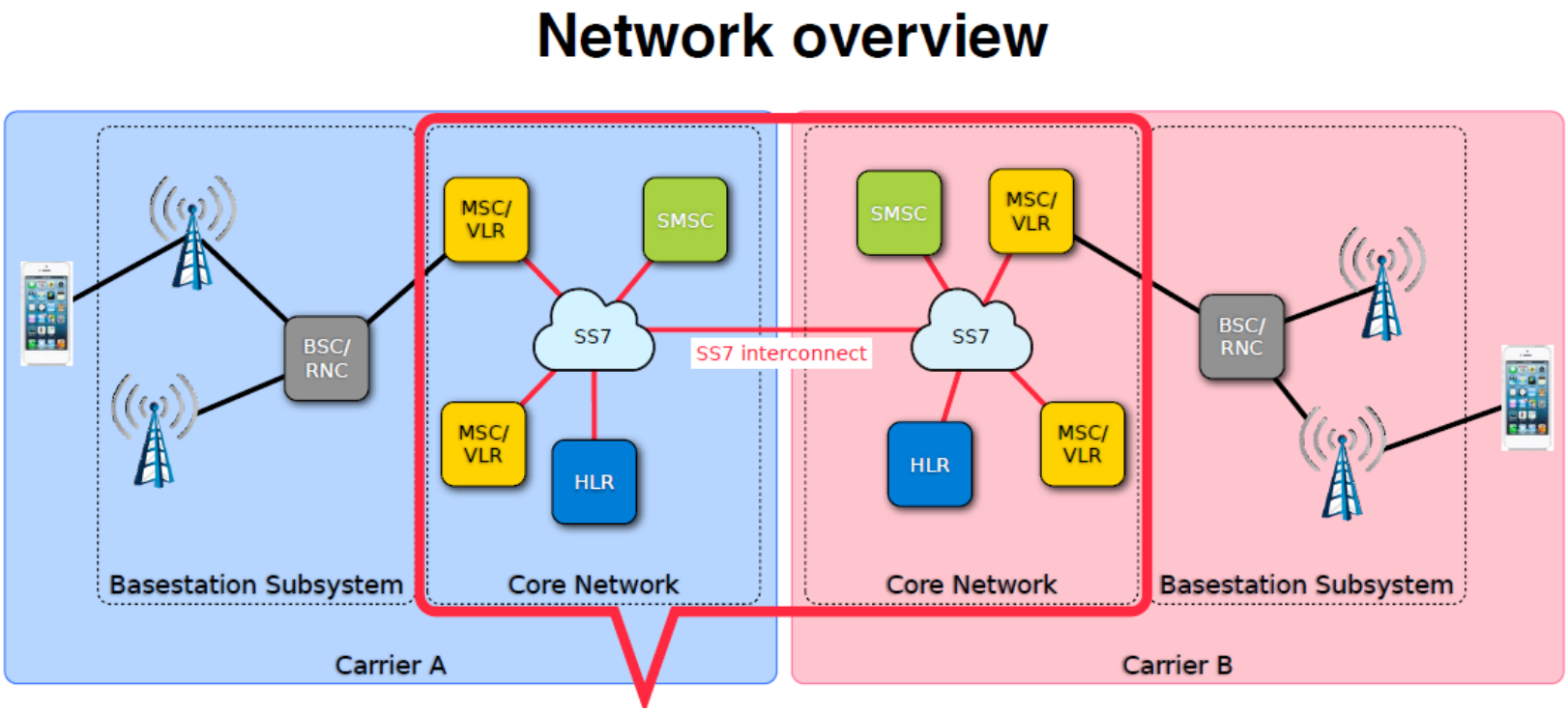
source : « SS7: Locate. Track. Manipulate. », 31C3, 28/12/2014, Tobias Engel

Comment ça marche ?
La stack protocolaire



source : « SS7: Locate. Track. Manipulate. », 31C3, 28/12/2014, Tobias Engel

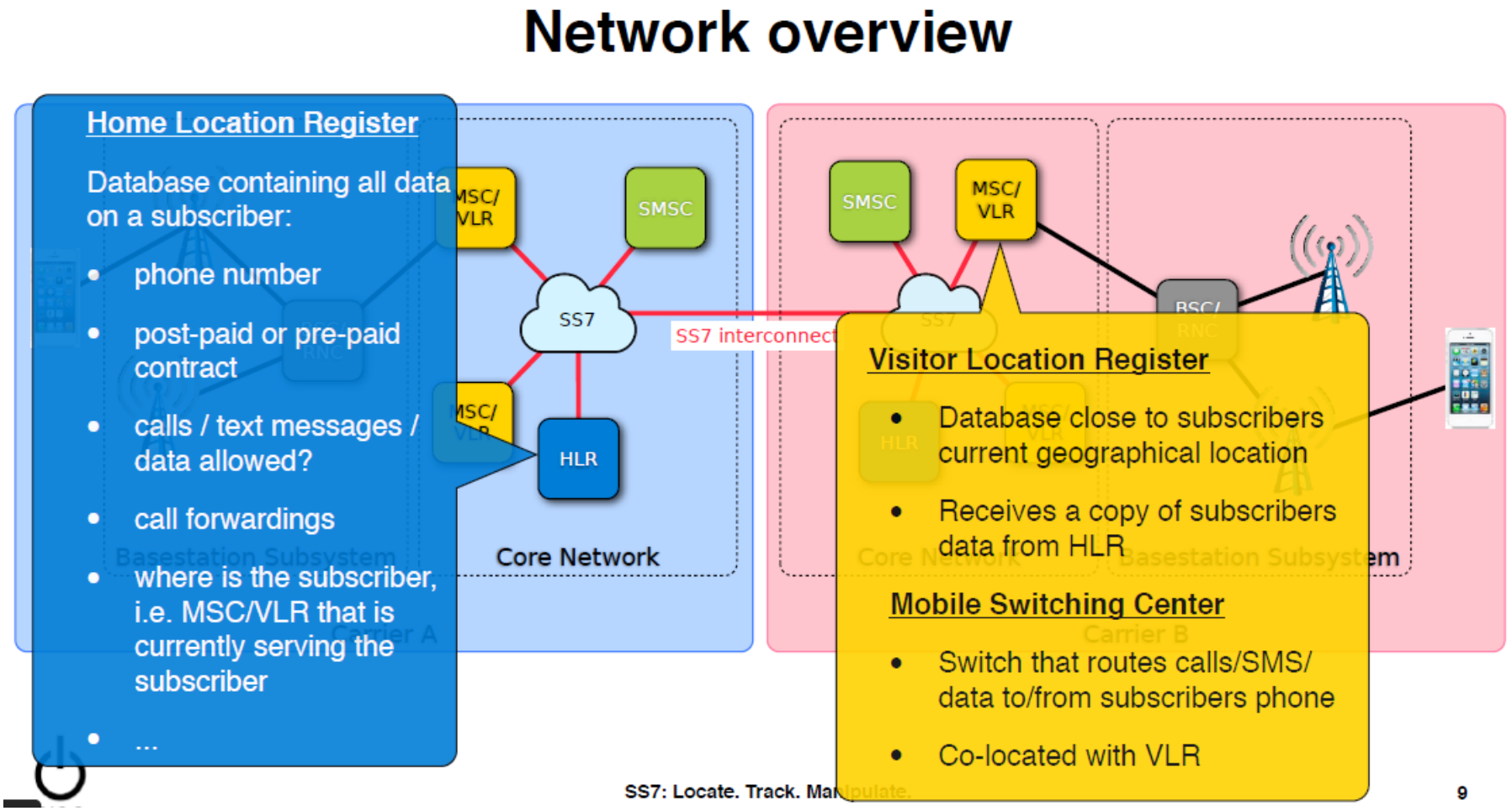
Comment ça marche ?
Vue réseau



Focus

source : « SS7: Locate. Track. Manipulate. », 31C3, 28/12/2014, Tobias Engel

Comment ça marche ?
Vue réseau

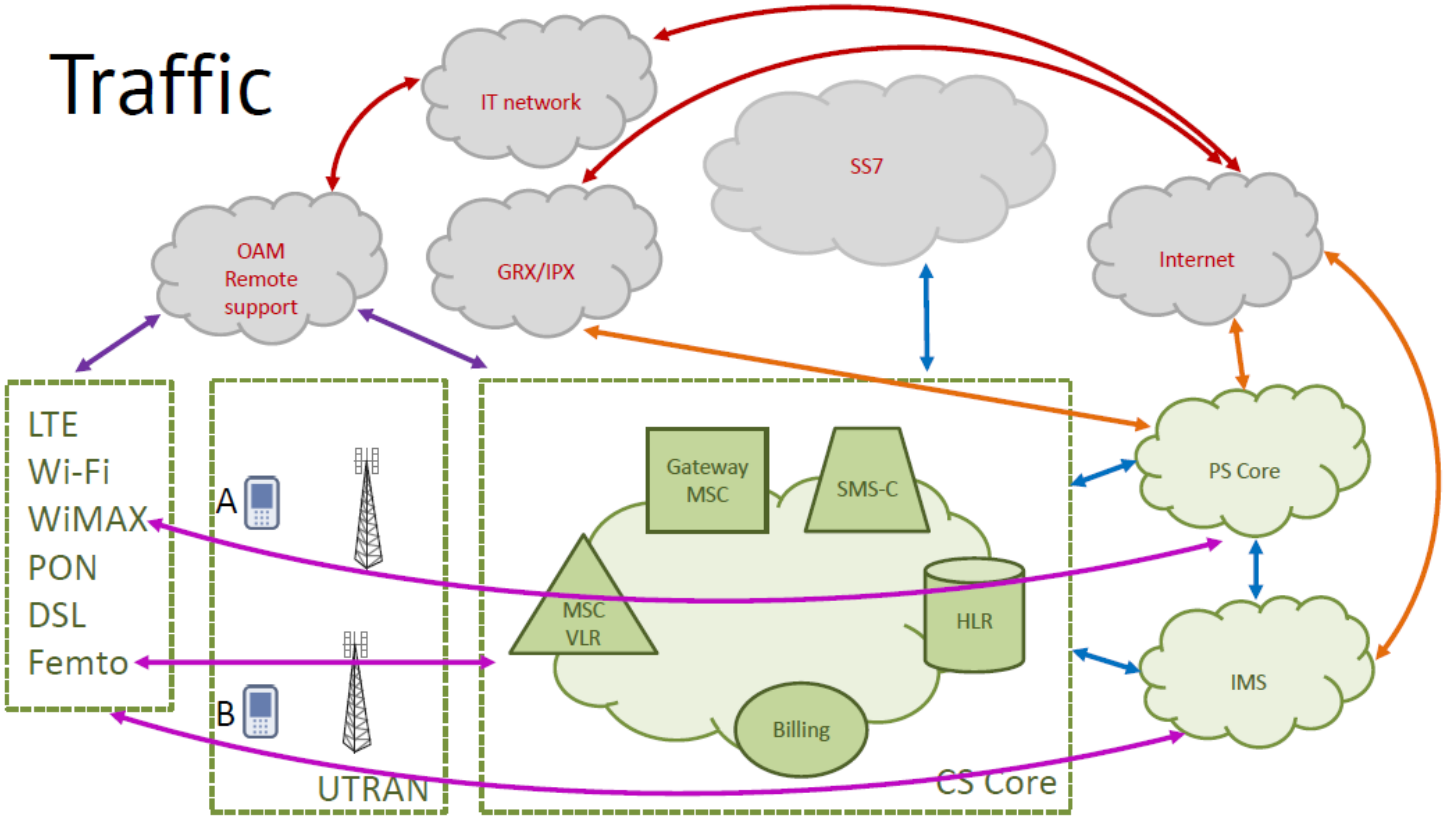


source : « Attacks on Telecom Operators and Mobile Subscribers via SS7 », Syscan 2015, PT

Comment accéder à ce réseau ?

- L'attaquant…
  - …achète l'accès auprès de telcos
  - …abuse d'un équipement du réseau auquel il a accès
  - …compromet un équipement télécom

- Un réseau très interconnecté



Quels risques ?

- Localisation
  - Localiser un abonné et le suivre
- DoS
  - Rendre le service inaccessible pour un abonné ciblé, ou pour tous les abonnés d'un opérateur
- Interception
  - Ecouter le trafic de l'utilisateur (appels, SMS, data). En particulier :
    - OTP (banques, etc)
    - Procédure de récupération de mots de passe oublié (emails, réseaux sociaux…)
- Détournement de trafic
  - Re-router le trafic de la victime (par exemple pour frauder)

Contrairement aux manipulations sur la voie radio, l'attaquant n'a pas besoin d'être à portée d'émission

The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH | SCIENCE

Security

SS7 spookery on the cheap allows hackers to impersonate mobile chat subscribers

WhatsApp, Telegram secure - but the transport isn't

(2016) Interception de communications

Real-World SS7 Attack — Hackers Are Stealing Money From Bank Accounts

Wednesday, May 03, 2017 Swati Khandelwal

Tweet Share Share 44 Share 1.2k Share Share

Security researchers have been warning for years about critical security holes in the Signaling System 7 (SS7) that could allow hackers to listen in private phone calls and read text messages on a potentially vast scale,

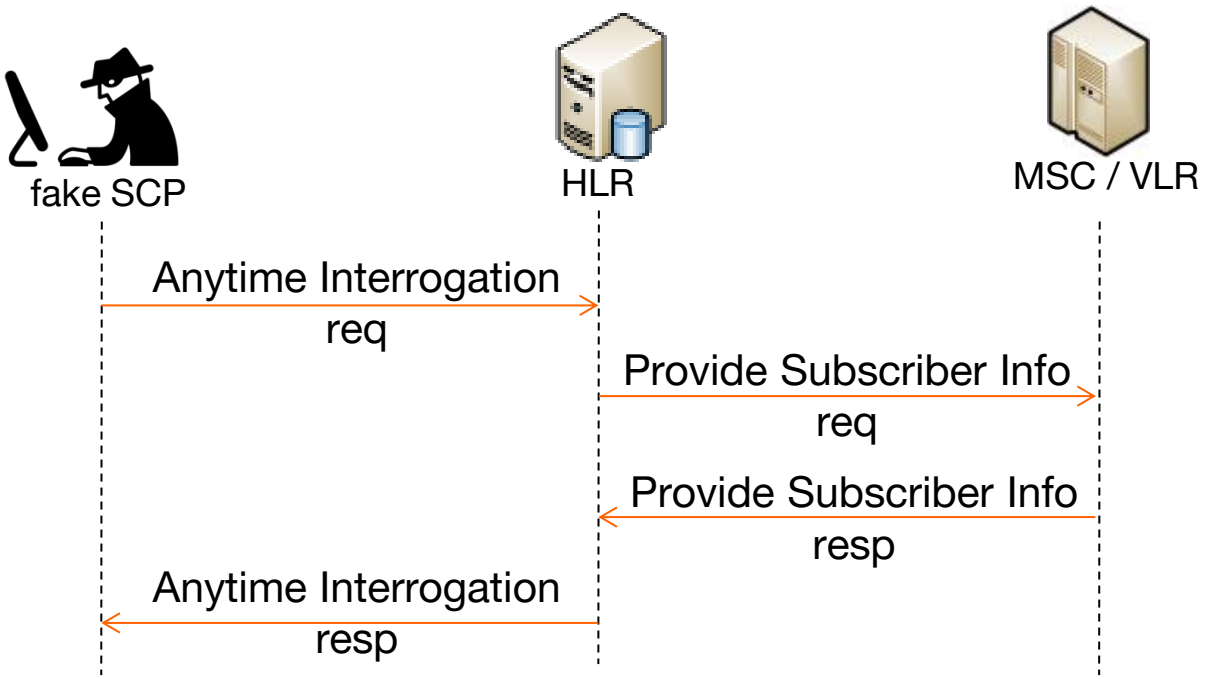
(2017)

Quelques scénarios

> fuite de données

Quelques exemples de scénarios
> MAP Any Time Interrogation

- message utilisé pour connaitre la localisation de l'abonné (location area, cell-ID), pour lui proposer des services à valeur ajoutée (par exemple, des zones à tarif préférentiel)
- conçu pour être utilisé seulement à l'intérieur du HPLMN

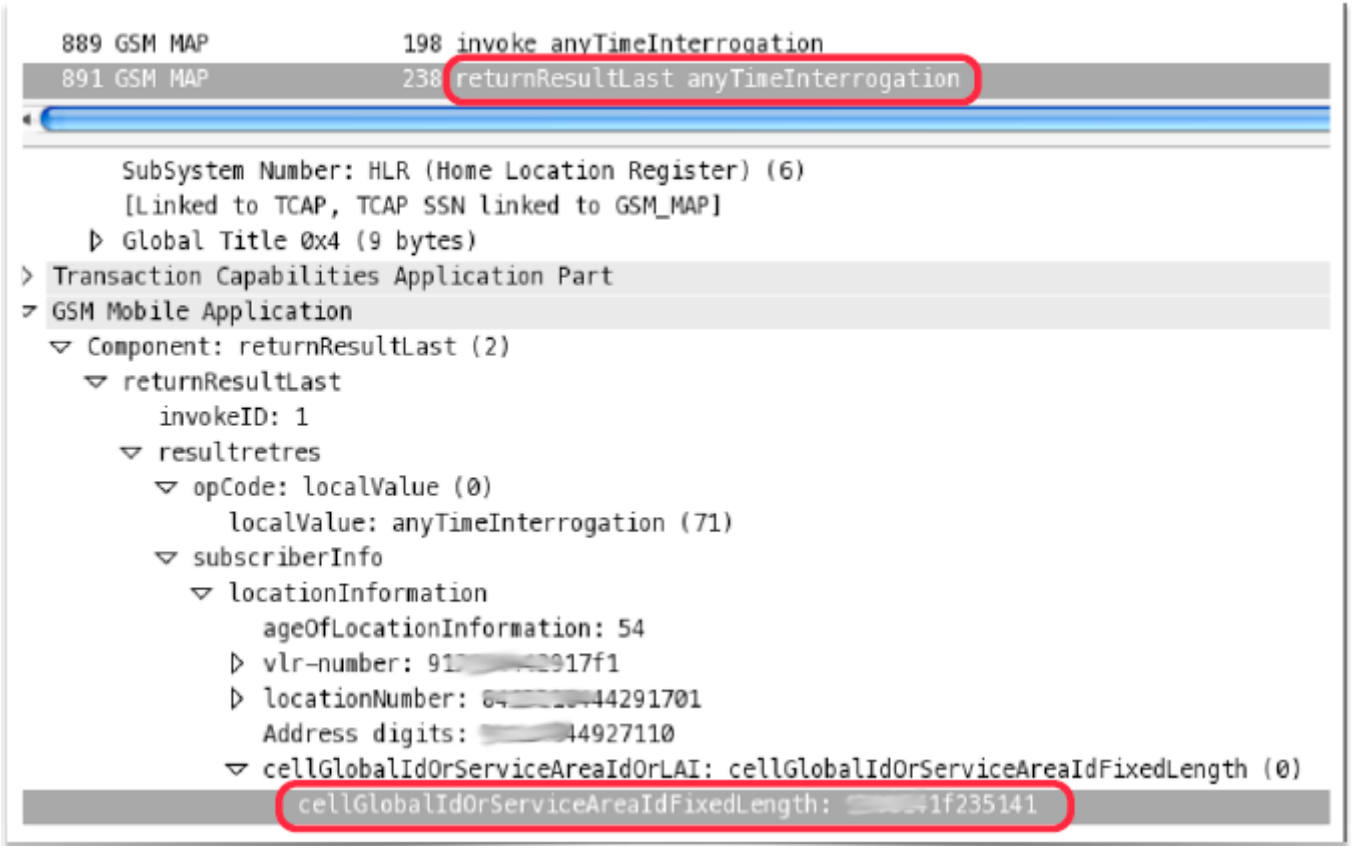


Résultat : fuite de la localisation de l'utilisateur

source : « SS7: Locate. Track. Manipulate. », 31C3, 28/12/2014, Tobias Engel

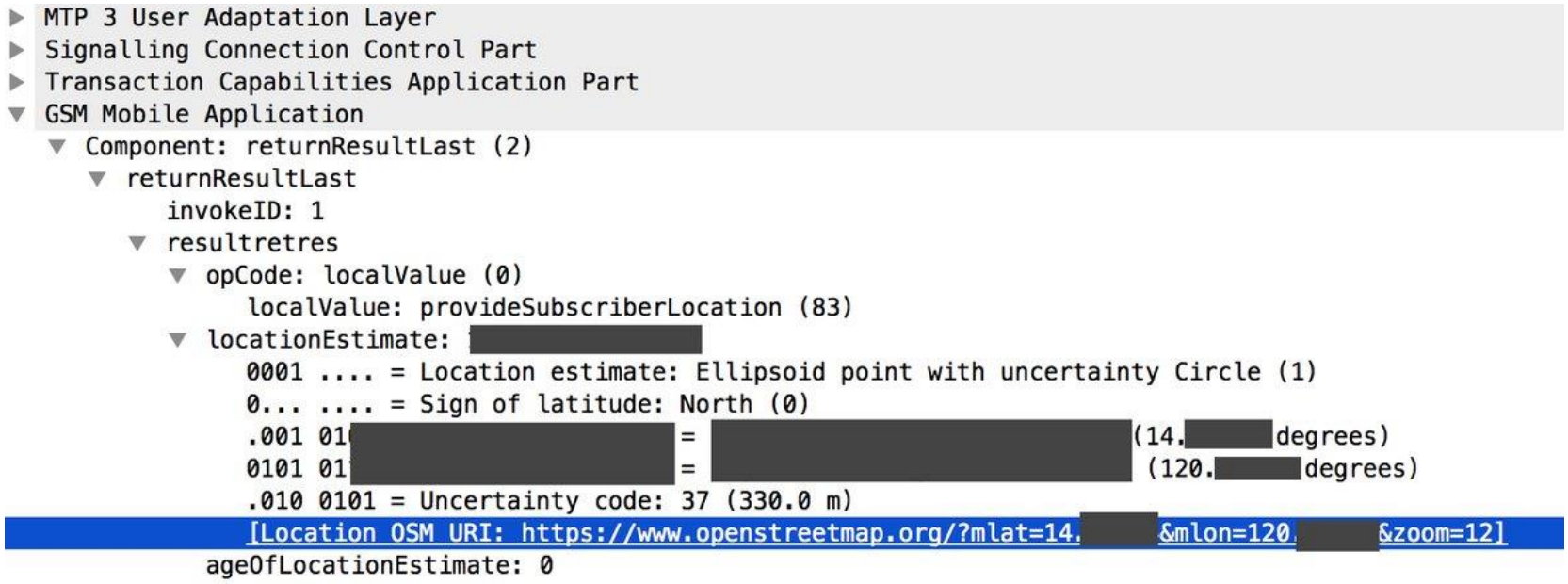
Quelques exemples de scénarios

> MAP Any Time Interrogation



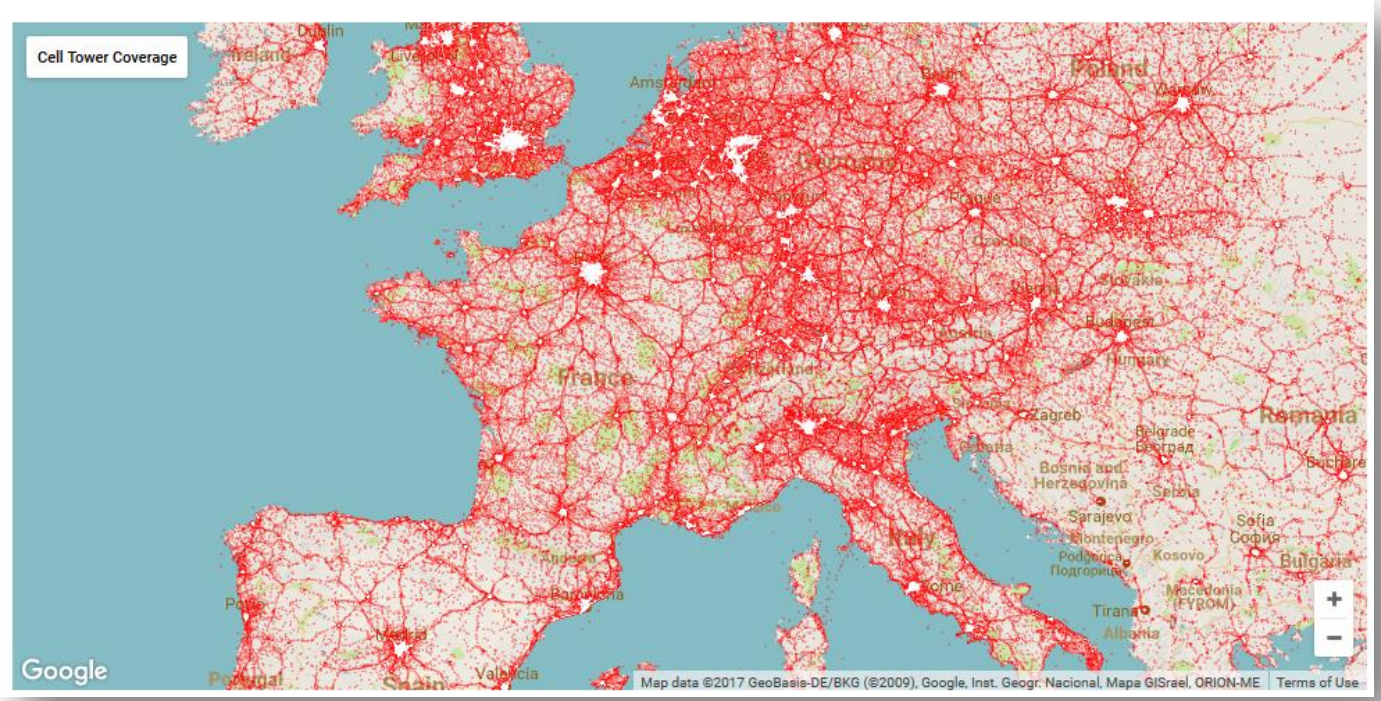
Quelques exemples de scénarios
> MAP Any Time Interrogation

- openstreetmap



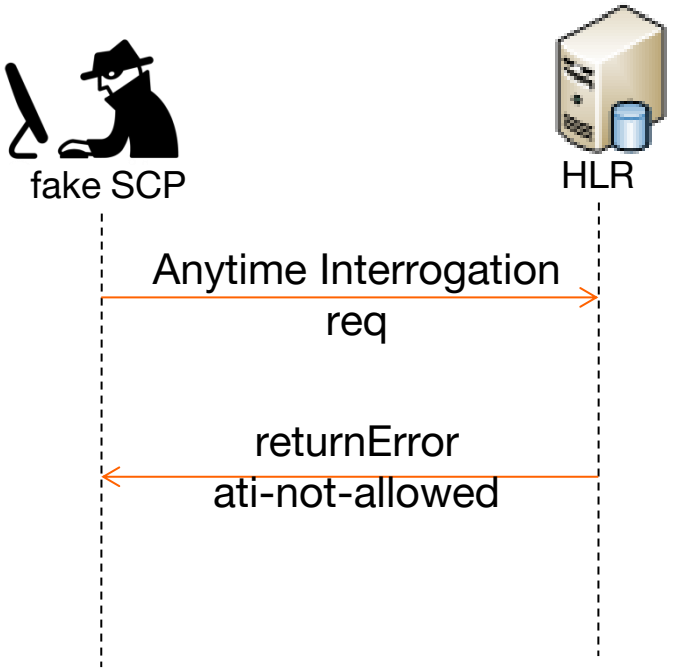
Quelques exemples de scénarios
> MAP Any Time Interrogation

- opencellid



Quelques exemples de scénarios
> MAP Any Time Interrogation – contre mesure

- message utilisé pour connaitre la localisation de l'abonné (location area, cell-ID), pour lui proposer des services à valeur ajoutée (par exemple, des zones à tarif préférentiel)
- conçu pour être utilisé seulement à l'intérieur du HPLMN

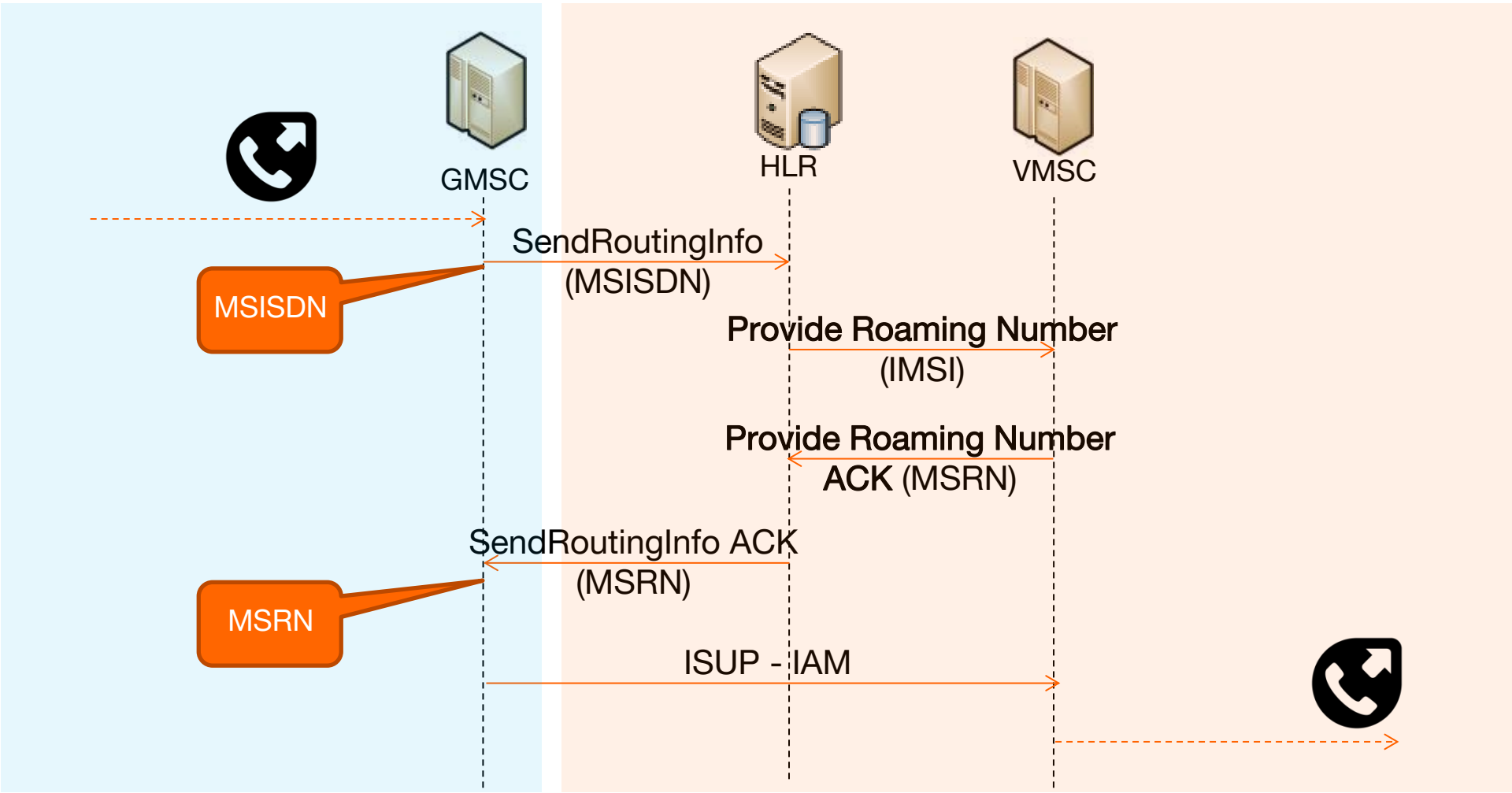


Bloqué, chez certains opérateurs

Quelques scénarios

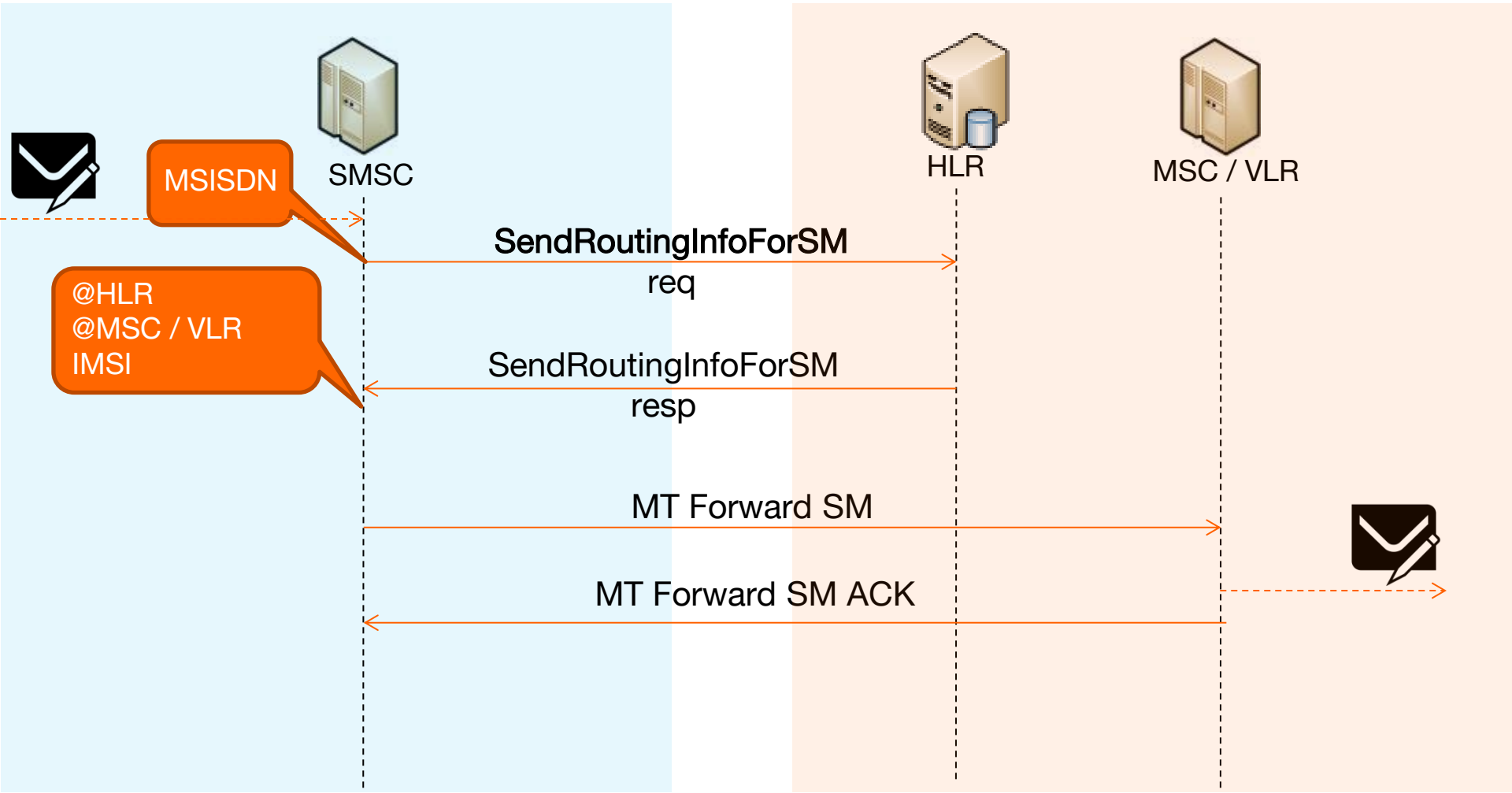
> DoS

Quelques exemples de scénarios
> PRN (Provide Roaming Number)



Utilisé pour acheminer un appel

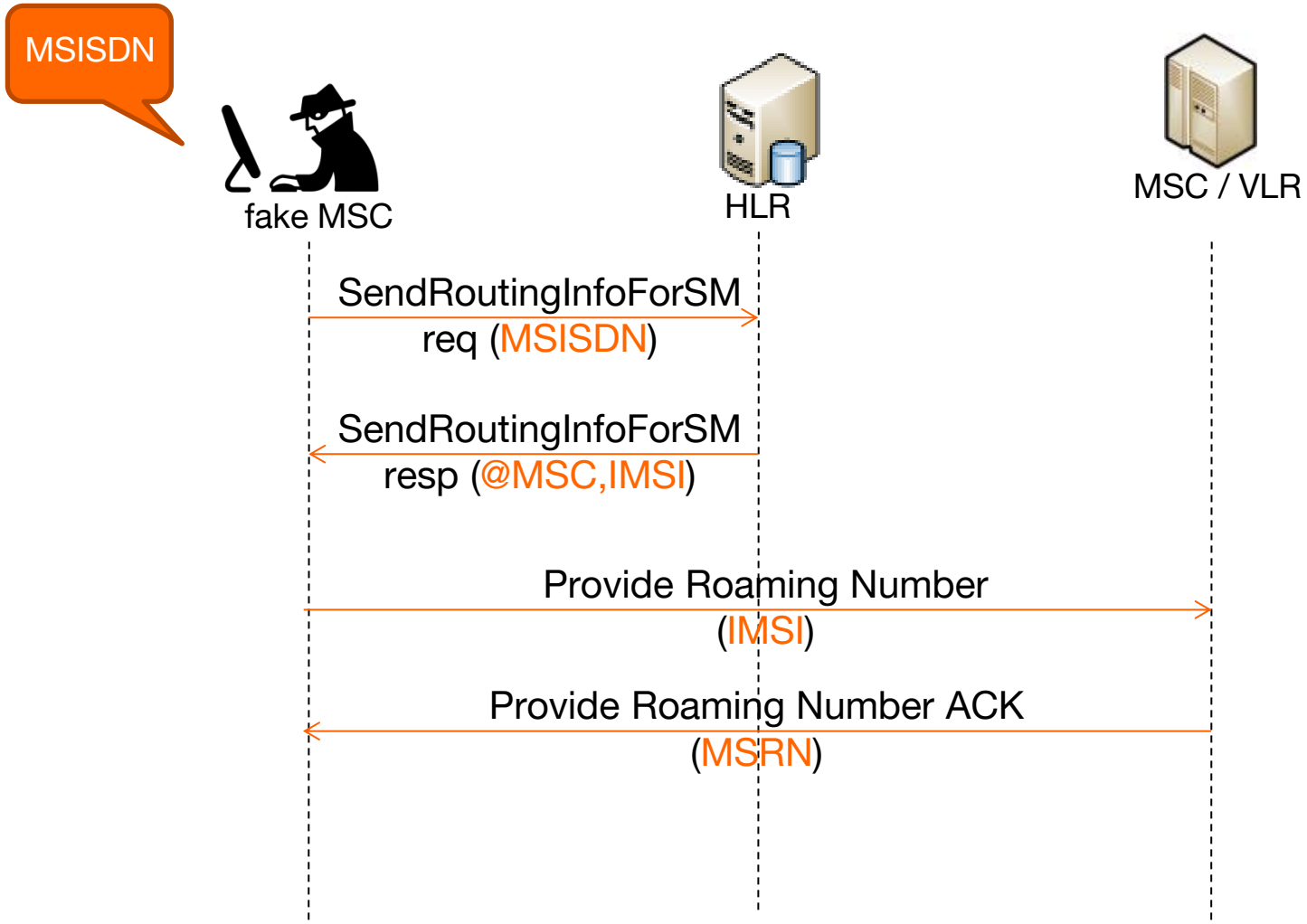
Quelques exemples de scénarios
> SRI4SM (Send Routing Information For Short Messages)



Utilisé pour délivrer un SMS

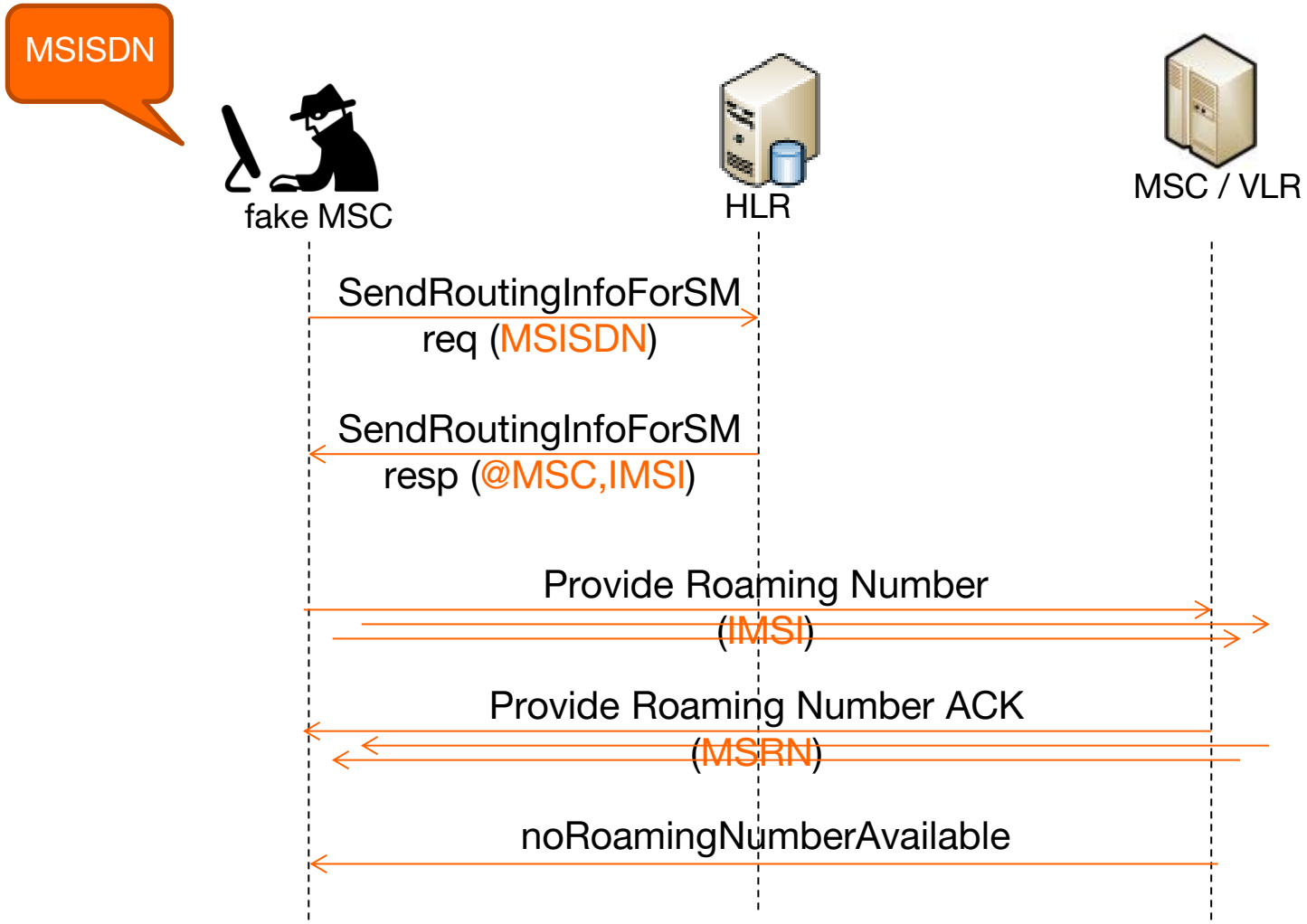
Quelques exemples de scénarios

>



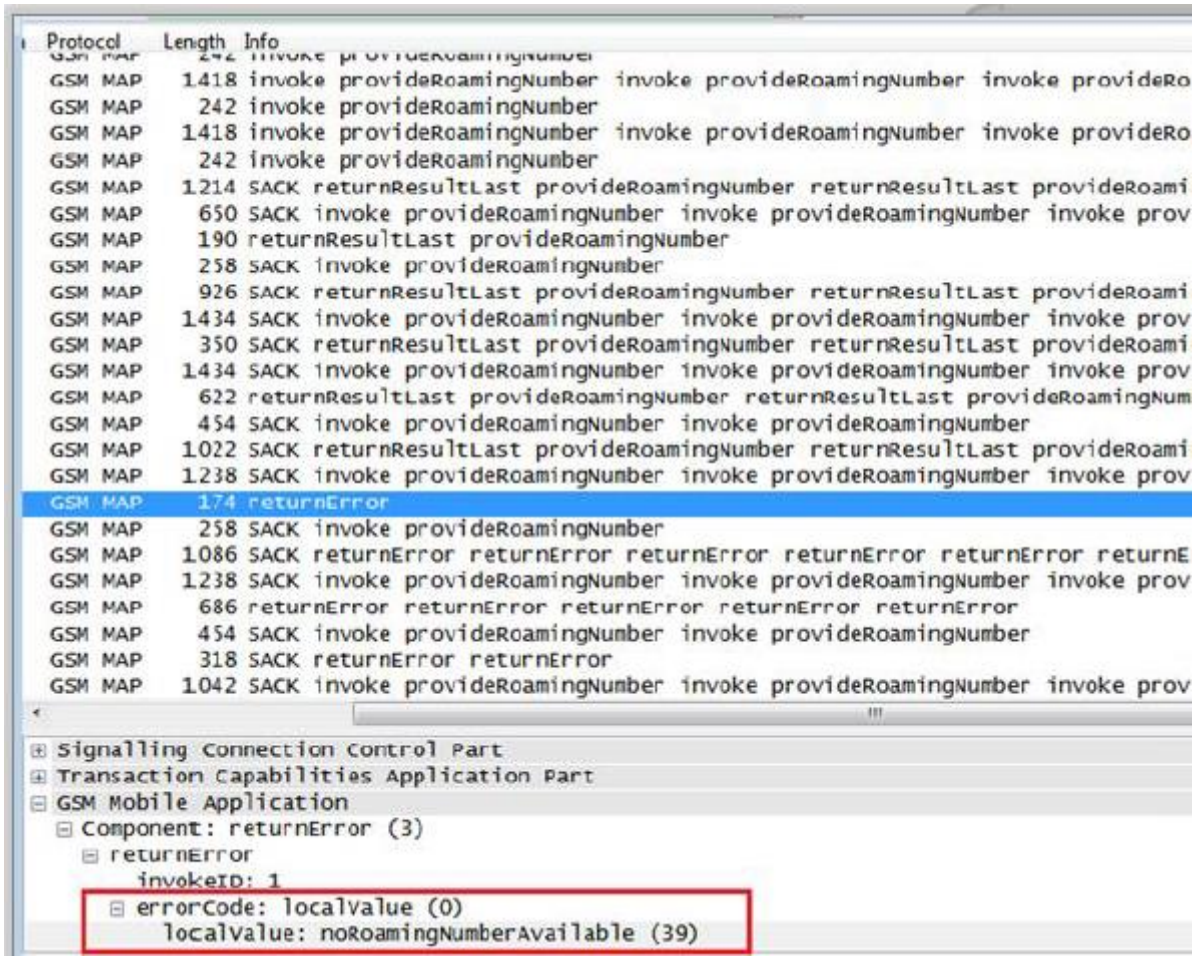
Quelques exemples de scénarios

>



Résultat : DoS sur le MSC de l'opérateur

source : « Attacks on Telecom Operators and Mobile Subscribers via SS7 », Syscan 2015, PT



Et en 4G ?

- Passage de SS7 à Diameter…
- …qui reprend les mêmes fonctionnalités…
- …et les mêmes vulnérabilités…
- …et donc aussi, les mêmes contre-mesures

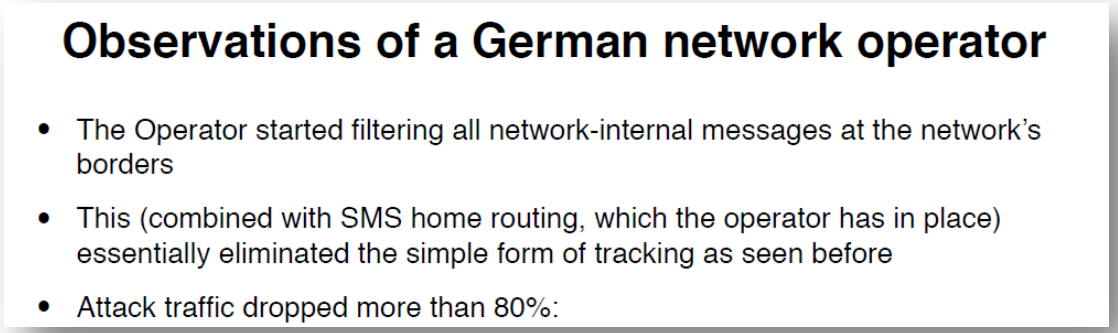
- « Detach me not, DoS attacks against 4G cellular users worldwide from your desk”, Black Hat Europe 2016

Contre-mesures

Quelles contre-mesures ?

- Bloquer ce qui ne doit pas venir des interfaces de roaming
  - cf AnyTimeInterrogation

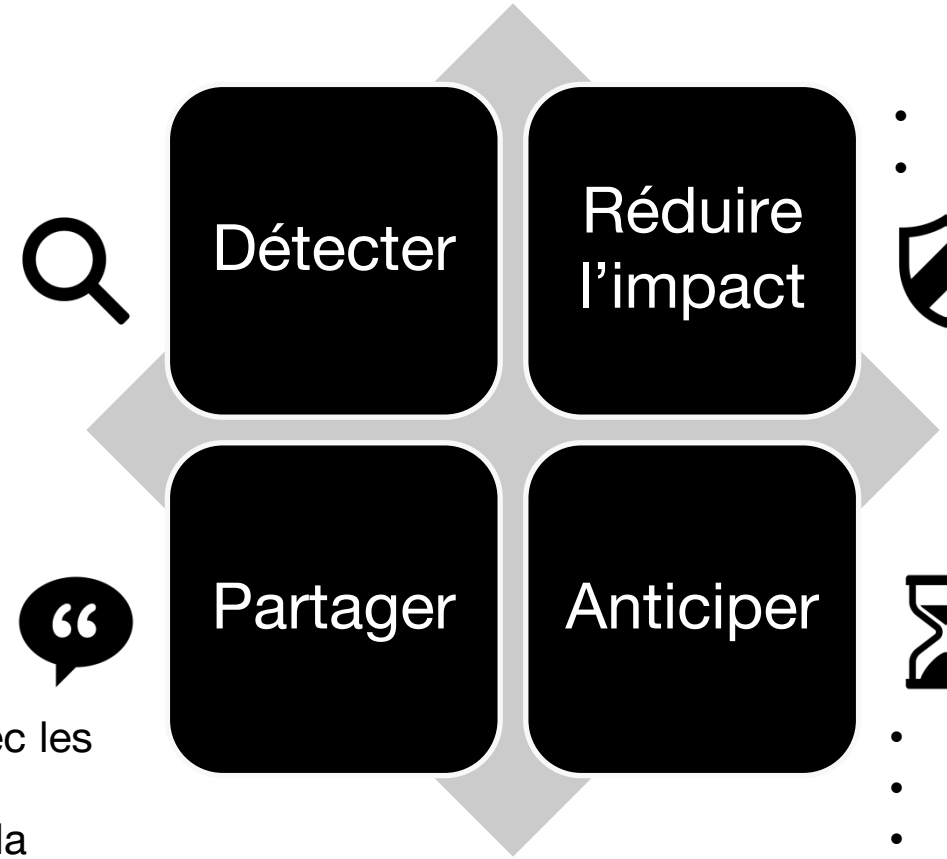
source : « SS7: Locate. Track. Manipulate. », 31C3, 28/12/2014, Tobias Engel



- Corréler les éléments techniques pour vérifier la cohérence des requêtes
  - par exemple : l'utilisateur est-il en roaming ? est-ce au moins plausible ?
  - par exemple : corréler la cohérence des paquets SS7

Contre-mesures

- Monitoring



- Filtrage
- IPsec là où c'est possible

- Coopération avec les législateurs
- Echanges dans la communauté

- Aspects juridiques
- Hardening
- Investigations des cas suspects

Des tests

Des outils

Des outils : Ressources documentaires

- Les normes / Les livres
  - 3GPP : Accès libre et gratuit, en constante évolution
  - Plusieurs étapes
    - « stage 1 » : spécifications de services,
    - « stage 2 » : architectures implémentant ces services
    - « stage 3 » : l'implémentation technique (format de messages bit par bit, piles protocolaires …) de ces architectures.
  - Ce que les normes ne décrivent pas (responsabilité de l'opérateur)
    - représentation des équipements fonctionnels seulement, abstraction des réseaux de collecte, routeurs, load balancers, firewalls, IDS / IPS, etc.
    - ne s'intéresse qu'à l'interfonctionnement et donc ne couvre pas l'implémentation de ces fonctions
    - la segmentation et le cloisonnement intra cœur de réseau et inter opérateurs abordée dans des normes spécifiques : les TS 33.210 et TS 33.310.
  - L'opérateur est responsable de la mise en œuvre d'une ingénierie IP fonctionnelle, de la pérennité des mesures de sécurité déployées, du maintien en conditions opérationnelles, de la qualité des équipements sourcés, du maintien et de l'évolution des normes (3GPP, IETF, etc)

3GPP : spécifications

http://www.3gpp.org/specifications/specification-numbering

An automated list of Specification numbers - with the Title and details of the Specification Group responsible.

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
General information (long defunct)			00 series
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series	48 series	08 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series	49 series	09 series
Programme management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
UE and (U)SIM test specifications	34 series	(2)	11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA) and LTE-Advanced radio technology	36 series	-	-
Multiple radio access technology aspects	37 series	-	-

3GPP : participants au 3GPP SA3

- Principalement
  - MNO / équipementiers / device / SIM
- Les délégués sont obligés de s'enregistrer
  - Les listes de participants sont publiques
  - http://webapp.etsi.org/3GPPRegistration//fViewPart.asp?mid=31386

LIST OF REGISTERED ATTENDEES

View Listing | View Badges | CSV delim

56 registered participants / 0 attended

Name	Role	Organization	Organization Represented
Adrangi, Farid	Delegate	Intel Corporation (UK) Ltd (ETSI)	Intel Corporation (UK) Ltd (ETSI)
Aldén, Magnus	Delegate	TeliaSonera AB (ETSI)	TeliaSonera AB (ETSI)
Alfano, Nicholas	Delegate	BlackBerry UK Limited (ETSI)	BlackBerry UK Limited (ETSI)
Allen, Andrew	Delegate	BlackBerry UK Limited (ETSI)	Research in Motion Japan Ltd. (ARIB)

- Contributions et compte-rendu de meeting publics
  - http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

Outils : Manipulation de cartes SIM

- https://github.com/mitshell/card

- Pré-requis logiciels :
  - python 2.6 (may work with older version: not tested), a smartcard reader (USB or RS-232),
  - pcsc-lite driver and daemon under Linux (or the Windows' native smartcard service),
  - the smartcard pcsc python binding (called pyscard): http://pyscard.sourceforge.net/.

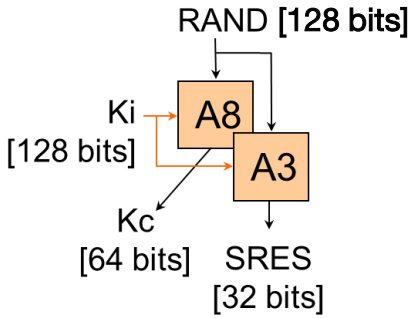
- Packages / outils nécessaires
  - pscsd, swig, pcsc-tools, libpcsclite-dev, python2.7-dev, pyscard

- sudo python setup.py install
- ipython

Outils : Manipulation de cartes SIM

- Matériel nécessaire : lecteur de carte à puce
- Librairie utilisée : mitshell / card
  - Manipulation de cartes SIM (2G) ou USIM (3G, 4G)
  - Exemple : désactivation du PIN
  - Exemple : envoi d'un challenge 2G et écoute de la réponse
- Application
  - permet de se familiariser avec le comportement d'une carte SIM
  - Notamment sur la notion de challenge / réponse
- Attention
  - Les API exposées par la carte ne sont pas directement accessible depuis le réseau. Elle sont accédées par le terminal mobile.

Outils : Manipulation de cartes SIM



- ### a SIM card session ###
- >>> from card.SIM import *
- >>> s = SIM()
- >>> s.disable_pin('0123')

- >>> s.run_gsm_alg(RAND = 16*[0xEE])
  [[186, 6, 7, 233], [27, 138, 6, 159, 176, 99, 36, 76]]

SRES Kc

rejouable à l'infini ! (exercice laissé au lecteur)

- >>> s.disconnect()

- ### a USIM card session ###
- >>> from card.USIM import *

- >>> u.authenticate(RAND=16*[0xAA], ctx='2G')

[[73, 153, 135, 97], [204, 140, 250, 128, 34, 50, 232, 224]]

>>> u.disconnect()

Des outils : manipulation des couches radio

- Pré-requis
  - Matériel : à des prix accessibles
    - Pour l'acquisition / l'émission du signal radio
  - Logiciel : nombreux SDR open source
    - Gnuradio (traitement du signal)
    - OpenBTS (implémentation open-source de l'interface radio GSM)
    - OsmocomBB (implémentation open source d'un baseband GSM)
    - OpenLTE (4G)
- Détails
  - Faiblesses qui concernent principalement les réseaux 2G
  - Outillage principalement disponible pour la 2G
- De nombreux tutoriels
- Attention
  - L'émission de signaux radio dans les bandes de fréquences GSM/UMTS/LTE est régulée et soumise à la détention de licences en France et dans de nombreux pays. Chaque utilisateur de ce genre d'outils engage donc sa responsabilité sur ces points.

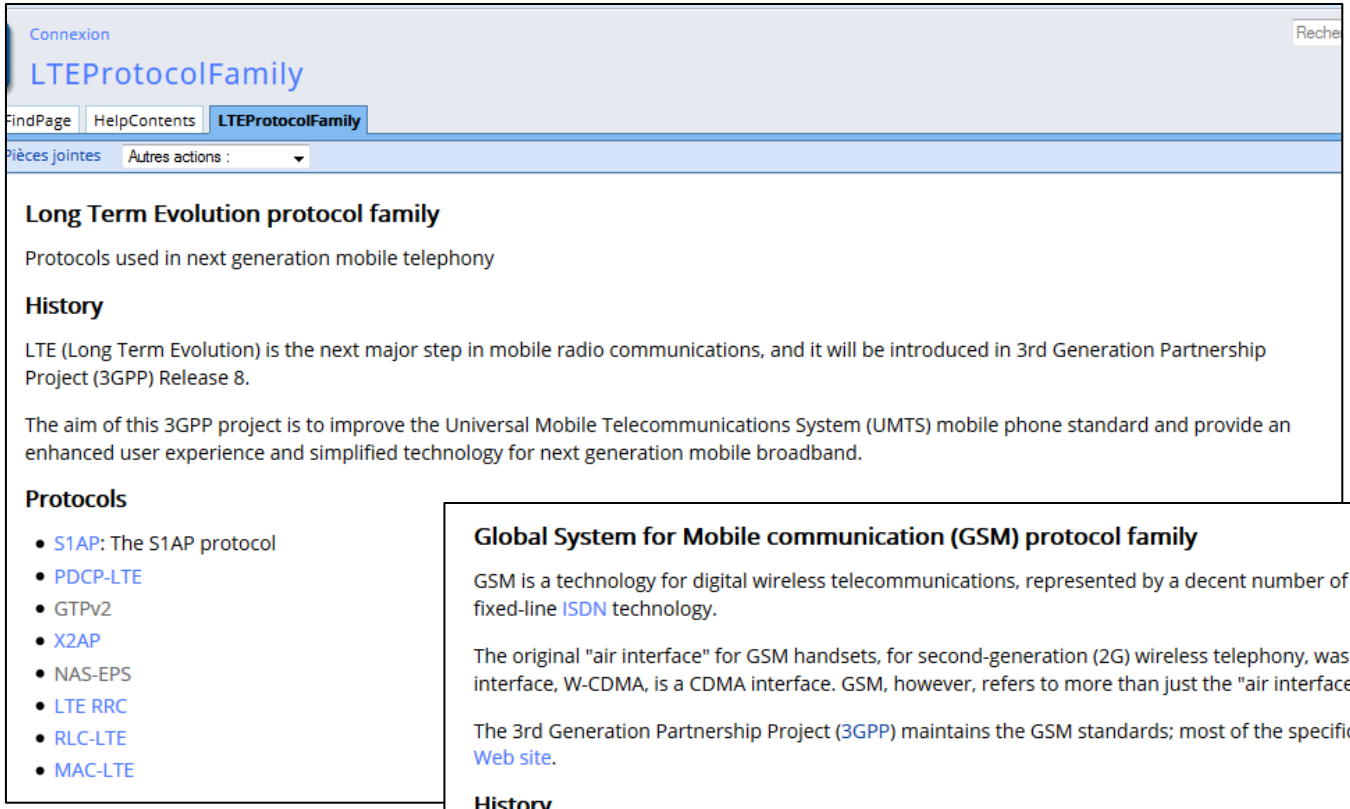
Des outils : manipulation des couches protocolaires hautes

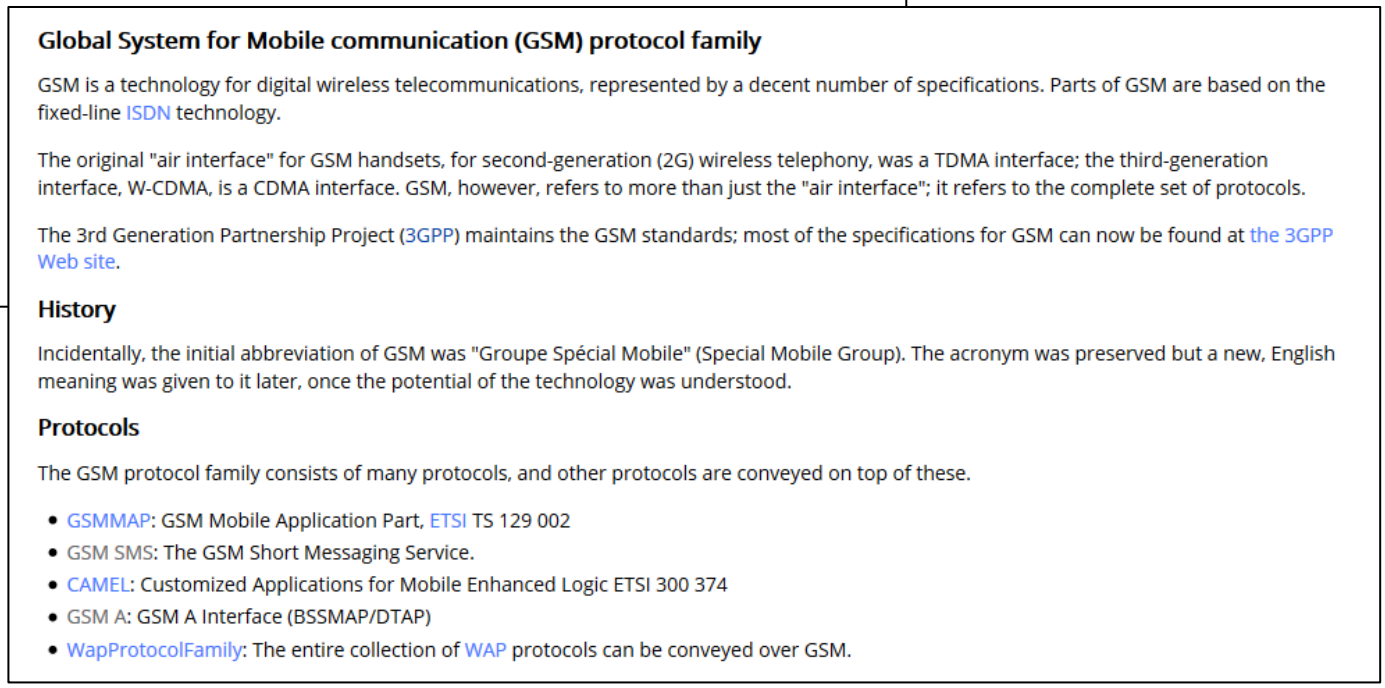
- Scapy
  - peu / pas de protocoles réseau mobile legacy
  - implémentation de nombreux protocoles du monde IP
  - possibilité de capturer / générer / modifier des paquets

- Libmich
  - https://github.com/mitshell/libmich
  - Implémentation de protocoles exotiques 3GPP
  - Approche similaire à Scapy, avec une syntaxe un peu différente

- Wireshark
  - Outil de visualisation

Des outils : visualisation des traces réseau





Des outils : émulations d'équipements réseau

- Des émulations d'équipements réseau

- SGSN : http://openbsc.osmocom.org/trac/wiki/osmo-sgsn
- GGSN : http://sourceforge.net/projects/ggsn/

Conclusion et perspectives

En bref

- La sécurité des réseaux mobiles s'améliore de génération en génération

- Mais :
  - De nombreuses interfaces
  - De nombreuses interconnexions
    - Réseaux legacy
    - Réseaux non 3GPP (Wi-Fi…)
  - Des protocoles nouveaux / complexes / peu testés

  ⇒ Sujet complexe

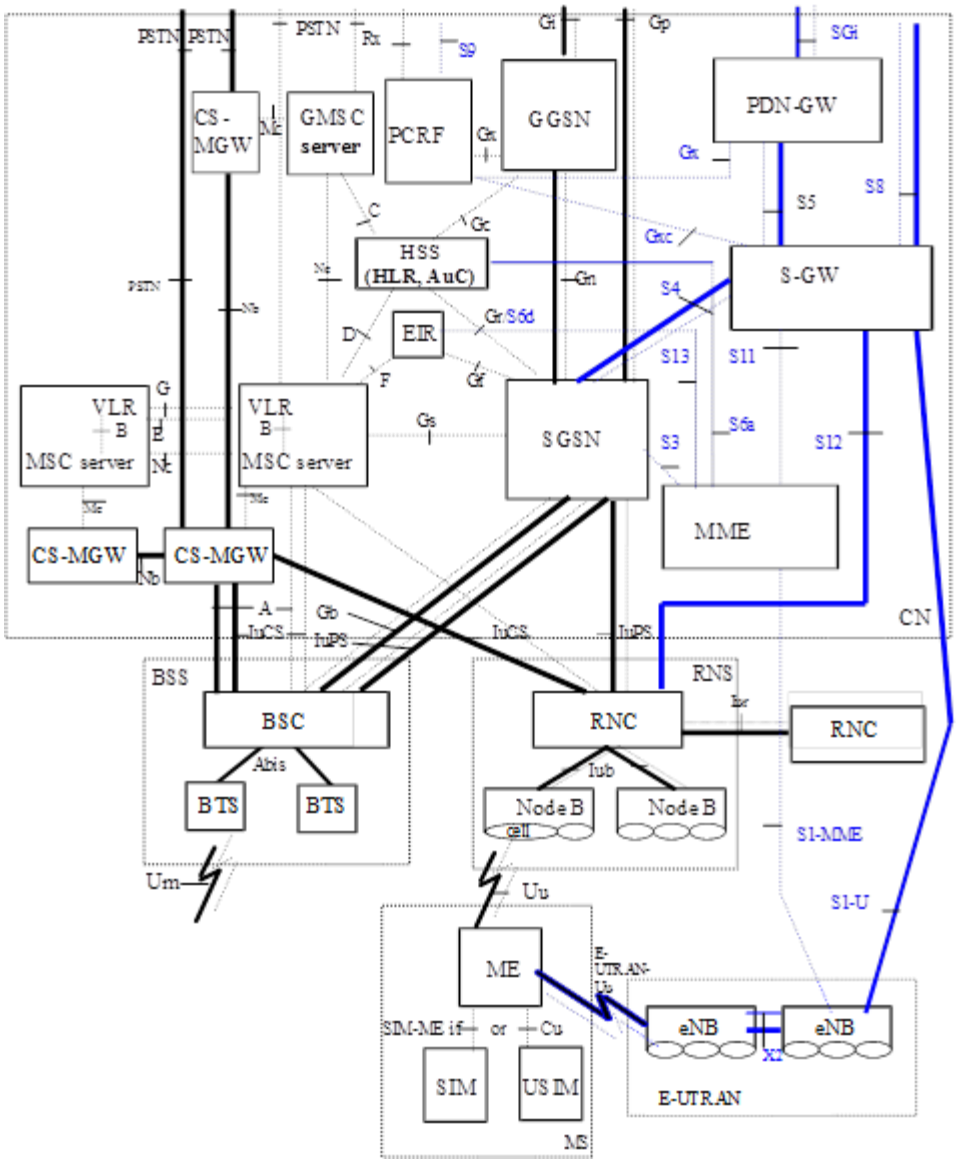


Figure extrtaite de 3GPP TS 23.002 (V11.2.0)