Sécurité Mobile 2G, 3G et 4G:
Concepts, Principes et Architectures

EFORT
http://www.efort.com

Ce tutoriel présente la sécurité dans les réseaux mobiles 2G (sécurité dans les domaines circuit et paquet), 3G (sécurité dans les domaines circuit et paquet) et 4G (Sécurité uniquement dans le domaine paquet). Trois aspects de la sécurité sont traités : l'authentification, la confidentialité et la protection de l'intégrité de la signalisation.
L'authentification consiste à vérifier l'identité d'un usager. La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction, en la chiffrant. Protéger l'intégrité des données de signalisation consiste à déterminer si les données de signalisation échangées n'ont pas été altérées (de manière fortuite ou intentionnelle).
Le premier chapitre traite de la sécurité 2G. Le deuxième chapitre présente la sécurité 3G. Le troisième chapitre introduit la sécurité dans le futur réseau mobile appelé EPS (Evolved Packet System) ou 4G.

1 Sécurité 2G

1.1 Clés et algorithmes pour la sécurité 2G

Lorsqu 'un abonné souscrit à un abonnement mobile auprès d 'un opérateur, il reçoit un identifiant unique appelé IMSI (International Mobile Subscriber Identity). Ce numéro d 'IMSI est stocké sur la carte SIM. Un téléphone mobile ne peut être utilisé que si une carte SIM valide a été insérée dans l 'équipement mobile.

Une clé Ki est attribuée à l'usager, lors de l'abonnement, avec l'IMSI. (Figure 1) Elle est stockée dans la carte SIM de l'abonné et dans l'AUC (Authentication Center qui fait généralement partie du HLR) au niveau du réseau. Afin d'éviter toute possibilité de lecture de la clé Ki, celle-ci n'est jamais transmise, ni sur l'interface radio, ni sur le réseau.

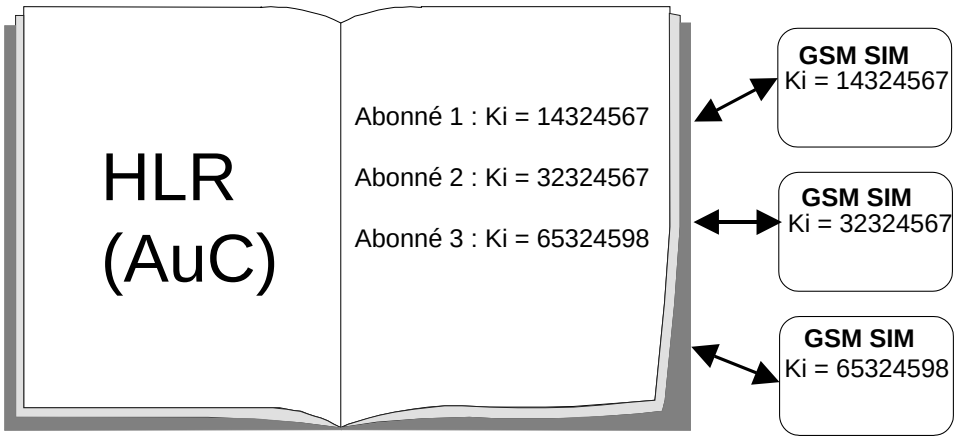


Figure 1 : Clé d'authentification Ki

Le centre d'authentification AuC dispose de l'algorithme d'authentification A3, de l'algorithme de génération de la clé de chiffrement A8 et des clés Ki des clients du réseau GSM.
Le BTS dispose de l'algorithme de chiffrement A5 pour le chiffrement des données usager et des données de signalisation.
La carte SIM du mobile dispose de l'algorithme d'authentification A3, de l'algorithme de génération des clés de chiffrements A8, de la clé d'authentification individuelle de l'utilisateur Ki.
L 'algorithme de chiffrement A5 est contenu dans l 'équipement mobile.
Les algorithmes A3 et A8 sont quant à eux les mêmes pour tous les clients d'un même réseau GSM.

1.2 Authentification et Chiffrement 2G

La sécurité GSM est adressée sur deux plans (Figure 2) : authentification et chiffrement.
L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.
Après que l'usager se soit identifié au réseau à l'aide de son IMSI ou de son TMSI (Temporary IMSI), il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification A3 sont utilisés. L'AuC (fonction du HLR physique) et la carte SIM contiennent la même clé Ki et l 'algorithme A3. Pour initier le processus d'authentification, l'AuC génère un nombre aléatoire, RAND, d'une longueur de 128 bits. Ce nombre RAND ainsi que la clé Ki de l'usager mobile servent de paramètres d'entrée à l'algorithme d'authentification A3. Le résultat est appelé SRES. Il s'agit du résultat d'authentification attendu. Les même paramètres RAND et Ki sont passés en paramètres de l'algorithme A8 qui produit un résultat Kc. Cette clé Kc sert de clé de chiffrement pour le trafic de l'usager et le trafic de signalisation entre le mobile et le BTS.
Le HLR retourne au MSC/VLR plusieurs triplets (RAND, SRES, Kc).
Le MSC/VLR utilise le premier triplet et demande au mobile de s'authentifier à partir de la valeur RAND.
Le mobile réalise la même procédure que l'AuC et produit un résultat d'authentification RES et une clé de chiffrement Kc à partir de la valeur RAND reçue du réseau, de la clé Ki présente sur la SIM et des algorithmes A3 et A8 aussi présents sur la SIM.
Le mobile soumet le résultat RES au réseau (i.e., MSC/VLR) qui le compare au SRES soumis pas le HLR. S'ils sont égaux, l'authentification du mobile a réussi.

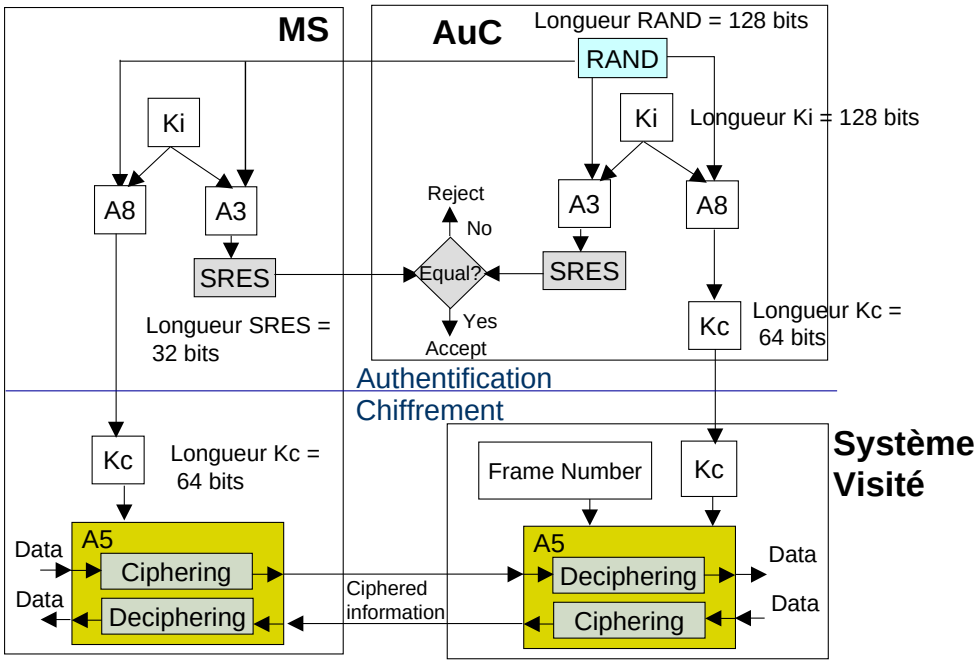


Figure 2 : Sécurité 2G

Un algorithme de chiffrement A5 présent sur la station mobile et la BTS est alors utilisé pour chiffrer / déchiffrer les données de signalisation et de trafic en utilisant Kc. Cet algorithme A5 est normalisé et est le même pour tous les opérateurs mobiles.
La carte SIM contient les informations Ki, A3, A8. L'AuC/HLR contient les informations A3, A8, IMSI/Ki. La station mobile et la BTS contiennent l'algorithme A5.

C'est COMP128-2, l'algorithme de base utilisé par les opérateurs GSM pour la procédure d'authentification et d'échange de clés (Figure 3).
COMP-128 génère le SRES en utilisant l'algorithme A3 et Kc en utilisant l'algorithme A8 en une seule étape. Il prend en entrée les paramètres Ki et RAND et produit un résultat sur 128 bits. Les 32 premiers bits de ce résultat forment le SRES et les 54 derniers bits de ce résultat de ce résultat forment la clé secrète Kc. Les derniers 10 bits du Kc sont positionnés à 0 pour bourrage.

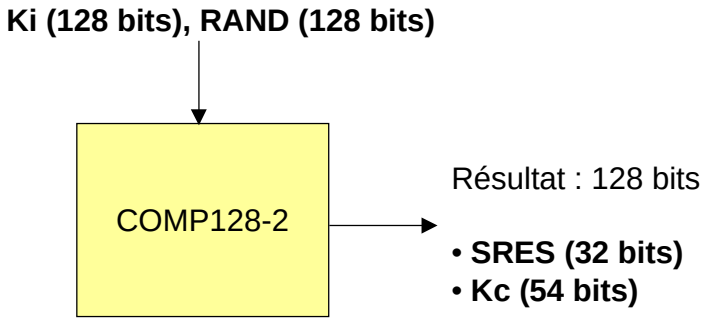


Figure 3 : Algorithmes A3/A8

L 'authentification 2G circuit est réalisée lorsque :
- Le mobile se rattache au réseau
- Le mobile établit un appel sortant
- Le mobile reçoit un appel entrant
- Le mobile envoie un SMS
- Le mobile reçoit un SMS
- Le mobile met à jour sa localisation (Location Area)

L 'authentification est réalisée entre le mobile et le VLR.
Le chiffrement a lieu entre le mobile et la BTS.

L'authentification 2G paquet est similaire à l'authentification 2G circuit. Elle induit des interactions entre le SGSN et le HLR.
Il existe des différences notables entre le chiffrement GSM et le chiffrement GPRS.
En GSM, le chiffrement est réalisé entre le mobile et la BTS et utilise trois version de l 'algorithmes A5 (A5-0, A5-1 ou A5-2), en fonction du niveau de chiffrement permis. En GPRS, le chiffrement a lieu entre le mobile et le SGSN et utilise une nouvelle version de l 'algorithme A5 conçue spécialement pour la transmission de paquets (A5-3).

L 'authentification 2G paquet est réalisée lorsque :
- Le mobile se rattache au réseau
- Le mobile établit un contexte PDP
- Le mobile envoie un SMS
- Le mobile reçoit un SMS

Le mobile met à jour sa localisation (Routing Area)
L 'authentification est réalisée entre le mobile et le SGSN.
Le chiffrement a lieu entre le mobile et le SGSN.

1.3 Limites de la sécurité 2G

- L'authentification 2G est basée sur un protocole de type challenge/response ainsi que sur des algorithmes de cryptographie à clé secrète. La 2G ne fournit pas d ’authentification mutuelle. Seule une authentification du client est réalisée. La carte SIM du mobile n’est pas en mesure de vérifier l’identité et la validité du réseau auquel le mobile est rattaché. Ceci laisse en théorie la porte ouverte à des attaques de l'homme du milieu. Cependant, de part le coût élevé des stations de base GSM (Base Transceiver Station, BTS) ou de solutions commerciales dédiées a l'interception, l'attaque n'est possible qu'avec des moyens financiers assez conséquents.
- GSM ne fournit pas de protection de la signalisation (mis à part le chiffrement GSM qui protège les données de l’usager ou la signalisation sur l’interface radio). Cela signifie que les messages de signalisation peuvent être altérés par les équipements radios. C’est ce que la protection de l’intégrité (integrity protection) cherche à prévenir.
- Le chiffrement (2G circuit) s ’arrête à la BTS, donc vulnérabilité de l ’interface BTS-BSC.

2 Sécurité 3G

Le protocole AKA (Authentication and Key Agreement) a été conçu afin de sécuriser l ’accès aux réseaux mobiles, plus précisément les réseaux UMTS/3G et LTE/EPS. Il est aussi utilisé pour l ’authentification du client IMS (cf tutoriel EFORT sur l’authentification IMS).
La partie « authentication » du protocole AKA permet de vérifier l ’identité de l ’usager alors que la partie Key Agreement permet de générer des clés qui sont ensuite utilisées pour le chiffrement du trafic de l ’usager dans le réseau d ’accès et aussi pour la protection de l ’intégrité des messages de signalisation.

L’AKA 3G se différencie de son homologue en 2G appelé A3 par deux points importants:

- AKA permet une authentification du réseau auprès du mobile grâce à un jeton d’authentification appelé AUTN soumis par le réseau à la carte USIM qui le valide.
- AKA permet la protection de l ’intégrité de la signalisation.

2.1 Authentification 3G

L’authentification 3G (AKA, Authentication and Key Agreement) est basée sur une clé partagée qui est uniquement présente dans le HLR et la carte USIM de l ’UE. Comme le HLR ne communique jamais directement avec l ’UE, le MSC Server réalise la procédure d ’authentification.
1 à 5 vecteurs d ’authentification (AV, Authentication Vector) sont téléchargés par le MSC Server à partir du HLR à travers l ’interface D lorsque le MSC Server reçoit de l ’UE le message Attach Request (Figure 4).
Les paramètres présents dans l ’AV sont :

- RAND – le challenge qui sert en tant qu’un des paramètres d’entrée pour générer les 4 autres paramètres de l ’AV (128 bits)
- XRES – Le résultat attendu, utilisé par le réseau pour l ’authentification de l ’USIM de l ’UE (32-128 bits)
- AUTN – Le jeton d ’authentification utilisé par l ’USIM pour l ’authentification réseau (128 bits)
- CK – La clé de chiffrement (128 bits). Cette clé permet le chiffrement du trafic de l’usager et du trafic de signalisation entre l’UE et le RNC.
- IK – La clé d ’intégrité (128 bits). Cette clé permet la protection de l’intégrité de la signalisation entre l’UE et le RNC.

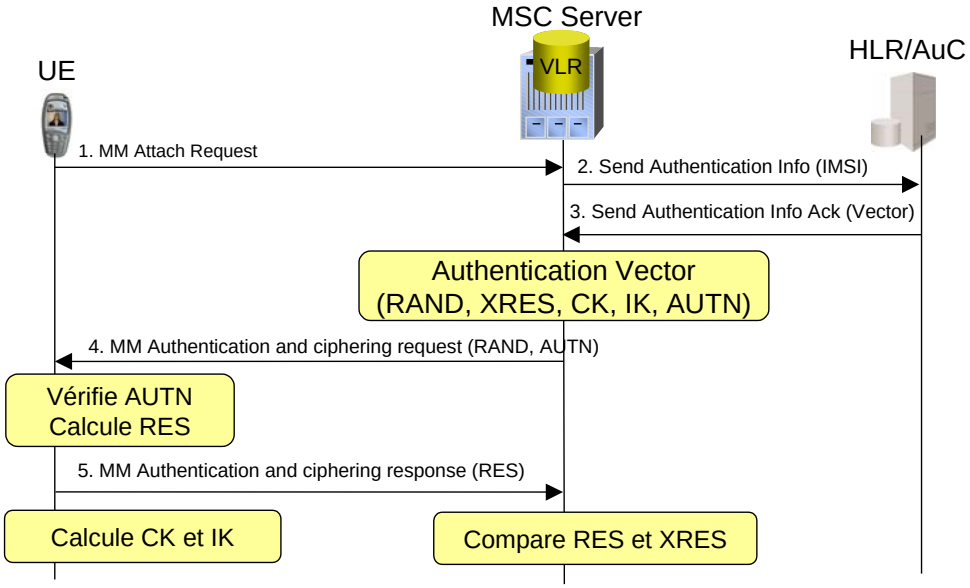


Figure 4 : Sécurité 3G

Le centre d'authentification génère un vecteur d 'authentification à partir de la clé Ki qu'il partage avec la carte USIM du terminal ainsi que deux autres paramètres qui sont : un numéro de séquence et un nombre pseudo aléatoire.
Le vecteur d'authentification généré comporte cinq parties : un résultat qui sera demandé dans la procédure challenge/response avec le terminal (XRES), un nombre (AUTN) qui permet l 'authentification du réseau auprès de l 'UE, une clé de session (CK) qui servira pour le chiffrement et une clé de contrôle d'intégrité qui servira à la protection de l'intégrité des messages de signalisation.
Le VLR/SGSN à la réception du quintuplé (RAND, AUTN, XRES, CK, IK), transmet le challenge RAND et le nombre AUTN qu'il a reçu du HLR à l'UE et attend une réponse RES ce dernier. La procédure challenge/response peut être représentée comme suit :
Le mobile est authentifié si le résultat RES transmis est identique à XRES reçu du centre d'authentification. Le nombre AUTN permet au module USIM de vérifier si le centre d'authentification est authentique et qu'il ne s'agit pas d'une attaque de type man in the middle par le réseau d 'accès.

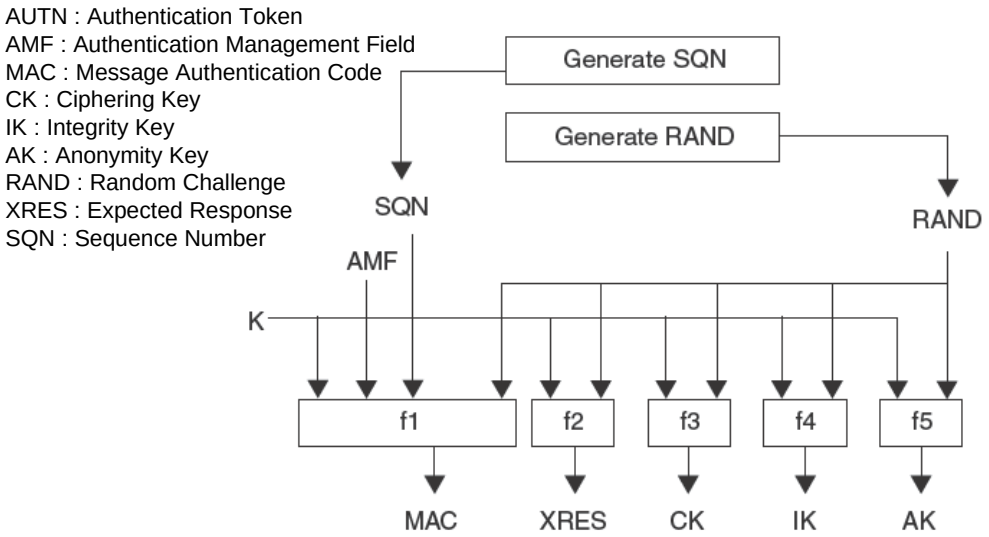


Figure 5 : Génération du vecteur d 'authentification du côté HLR

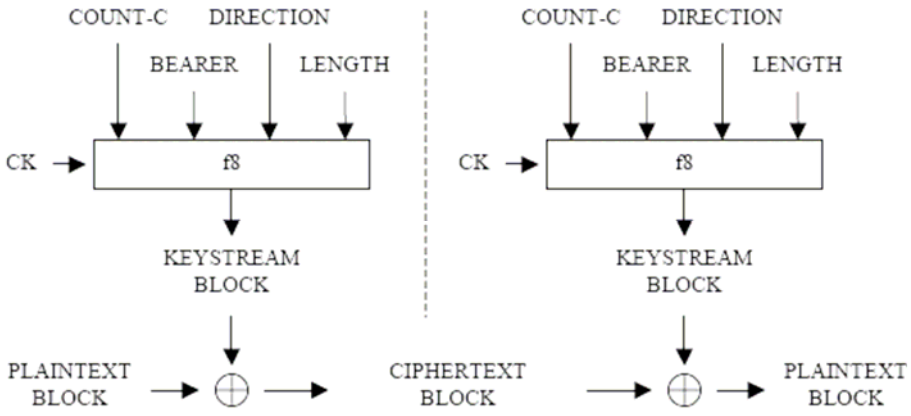
K : Clé d 'authentification, sur 128 bits
RAND: nombre aléatoire, sur 128 bits
XRES : Résultat d 'authentification attendu à partir du RAND, sur 32 bits (peut avoir une taille variable de 4 à 16 octets).
CK : Clé de chiffrement sur 128 bits
IK : Clé d 'intégrité sur 128 bits
AUTN : Jeton d 'authentification réseau sur 128 bits
AMF : Authentication Management Field sur 16 bits
SQN: Numéro de séquence sur 48 bits
AK : Anonymity Key sur 48 bits.

Lorsque le HLR reçoit du VLR ou du SGSN une demande de vecteurs d 'authentification, il commence par générer une valeur RAND et une valeur SQN.
Les valeurs RAND, SQN, Ki et AMF (Authentication Management Field) servent d 'entrées à 5 fonctions (f1 à f5) qui génèrent le quintuplé (Figure 5).
Le premier composant est le message authentication code (MAC). Il est obtenu par : MAC = f1(K, SQN, RAND, AMF); f1 est une fonction d 'authentification, et AMF fournit une nouvelle clé d 'authentification stockée dans l 'USIM.
Le second composant est le résultat attendu appelé Expected RESult XRES obtenu par : f2(K,RAND)); f2 est une fonction d 'authentification
Les trois composants suivants sont la cipher key (CK), l 'integrity key (IK), et l 'anonymity key (AK). Ils sont obtenus par : CK = f3(K, RAND), IK = f4(K, RAND), and AK = f5(K, RAND); f3, f4 et f5 sont des fonctions de génération de clés spécifiques.
Le dernier composant est l 'authentication token AUTN. Il est calculé en utilisant l 'expression: AUTN= <SQN⊕AK, AMF, MAC>
Le choix des algorithmes f1, f2, f3, f4 et f5 est spécifique à l 'opérateur. Cependant un choix d 'algorithme appelé MILENAGE a été proposé par 3GPP (TS 35.206).

2.2 Confidentialité 3G

Une fois que l 'usager et le réseau se soient authentifiés mutuellement, il peuvent initier une communication sécurisée. Nous avons étudié que la clé CK était partagée entre l 'UE et le réseau après que l 'authentification ait réussi. Il s 'agit d 'une clé de longueur 128 bits.
Avant que le chiffrement ne commence les parties en communication doivent aussi négocier un algorithme de chiffrement. La 3G n 'a défini qu »un seul algorithme, appelé f8.

Le chiffrement et le déchiffrement prennent place dans le terminal et dans le RNC (Radio Network Controller) du réseau 3G, ce qui signifie que la clé CK doit être transférée du VLR au RNC. Ceci est réalisé par la commande du protocole RANAP (Radio Access Network Application Part) appelée « security mode command ». Après que le RNC ait obtenu le CK, il peut activer le chiffrement en émettant un message RRC (Radio Resource Control) à l 'UE appelé « security mode command ».
La figure 6 illustre l 'utilisation de l 'algorithme f8 afin de chiffrer le plaintext en appliquant un keystream en utilisant une opération XOR.
Les paramètres en entrée de f8 sont la clé de chiffrement (CK), l 'entrée dépendante du temps (COUNT-C) sur 32 bits, l 'identité du bearer radio (BEARER) sur 5 bits, la direction de la transmission (DIRECTION) et la longueur du bloc de données à chiffrer (LENGTH).
La direction a deux valeurs possibles. 0 = uplinks (UE → RNC) et 1= downlink (RNC → UE)
La clé CK est renouvelée à chaque processus d 'authentification. COUNT-C, BEARER et DIRECTION peuvent être considérés comme des paramètres d 'initialisation puisqu 'ils sont renouvelés pour chaque Keystream block.
La longueur des données de l 'usager (plaintext block) est comprise entre 1 et 20000 bits. LENGTH est donc un paramètre de longueur 16 bits afin d 'indiquer la longueur des données de l 'usager. Pour un bearer donné et une direction donnée, le plaintext block transmis dans une trame de la couche physique peut varier (couche RLC). Cette donnée est d 'ailleurs la partie donnée utile de la PDU RLC.
La longueur du keystream block est égale à la valeur du paramètre LENGTH.
Sur la base de ces paramètres, l 'algorithme f8 génère un résultat appelé keystream block (KEYSTREAM), qui est utilisé afin de chiffrer l 'entrée appelée plaintext block (PLAINTEXT) et ainsi produire le résultat ciphertext block (CIPHERTEXT).



Emetteur : UE ou RNC

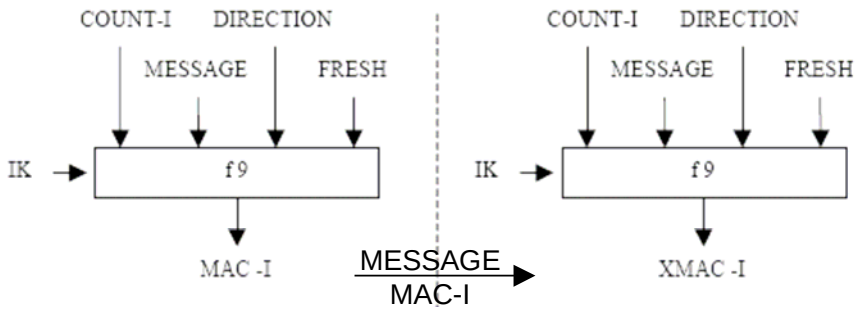
Récepteur : UE ou RNC

Figure 6 : Chiffrement 3G

2.3 Protection de l'Intégrité 3G

L 'algorithme f9 génère un code d 'authentification de message (MAC, Message Authentication Code) de longueur fixe à partir d 'un message de longueur variable sous le contrôle de la clé secrète IK et un ensemble de valeurs d 'initialisation. La clé IK a une longueur de 128 bits.
L 'émetteur et le récepteur génère le code MAC en utilisant la même fonction. L 'émetteur envoie son résultat MAC au récepteur, qui compare la valeur du code MAC reçu avec la valeur attendue qui est celle calculée par le récepteur.
Le récepteur accepte le code MAC si la valeur calculée et celle reçue sont égales.
La figure ci-dessus illustre comment f9 est utilisé pour dériver un MAC-I (MAC-Integrity of signaling data) sur un message de signalisation.

Les paramètres en entrée de l 'algorithme d 'intégrité sont la clé d 'intégrité (IK), une entrée dépendant du temps (COUNT-I), une valeur aléatoire générée par le réseau (FRESH), le bit de direction '(DIRECTION) et le message de signalisation (MESSAGE).
COUNT-I a une longueur de 32 bits ainsi que FRESH. DIRECTION a une longueur de 1 bit
La taille maximum d 'un message de signalisation n 'est pas spécifiée mais en théorie la limite est la même que celle des messages de donnée de l 'usager, à savoir 20000 bits.
Sur la base de ces paramètres d 'entrée, l 'usager utilise la fonction f9 pour calculer MAC-I pour l 'intégrité des données (Figure 7). MAC-I est ensuite ajouté au message lors de la transmission sur le canal radio. Le récepteur calcule la valeur de MAC attendue (XMAC-I) sur le message reçu de la même façon que l 'émetteur a calculé MAC-I sur le message envoyé.
MAC-I a une longueur de 32 bits.



Emetteur : UE ou RNC

Récepteur : UE ou RNC

MAC-I : Message Authentication Code Integrity
IK : Integrity Key

Figure 7 : Protection de l'intégrité 3G

L 'authentification 3G circuit est réalisée lorsque :

- Le mobile se rattache au réseau
- Le mobile met à jour sa localisation (Location Area)
- Le mobile établit un appel téléphonie ou visiophonie sortant
- Le mobile reçoit un appel téléphonie ou visiophonie entrant
- Le mobile envoie un SMS
- Le mobile reçoit un SMS

L 'authentification est réalisée entre le mobile et le VLR.
Le chiffrement a lieu entre le mobile et le RNC.
La protection de l 'intégrité de la signalisation a lieu entre le mobile et le RNC.

L 'authentification 3G paquet est réalisée lorsque :

- Le mobile se rattache au réseau
- Le mobile établit un contexte PDP
- Le mobile envoie un SMS
- Le mobile reçoit un SMS
- Le mobile met à jour sa localisation (Routing Area)

L 'authentification est réalisée entre le mobile et le SGSN.
Le chiffrement a lieu entre le mobile et le RNC.
La protection de l 'intégrité de la signalisation a lieu entre le mobile et le RNC.

3 Sécurité 4G

La LTE (Long Term Evolution of 3G) est un projet mené par l'organisme de standardisation 3GPP visant à rédiger les normes techniques de la future quatrième génération en téléphonie mobile. Elle permet le transfert de données à très haut débit. Tous les services incluant les services de téléphonie sont offert par un domaine paquet. Le domaine circuit est émulé par l'IMS. Pour les opérateurs, la LTE implique de modifier le coeur du réseau et les émetteurs radio. En terme de vocabulaire, le futur réseau mobile s'appelle EPS (Evolved Packet System). Il est constitué d'un nouveau réseau d'accès appelé LTE (Long Term Evolution) et d'un nouveau réseau coeur appelé ePC (Evolved Packet Core). Le mobile doit d'abord se rattacher et s'authentifier au réseau EPS avant de pouvoir transérer ou recevoir des paquets IP. L'élément qui permet l'authentification est appelé MME (Mobility Management Entity) (Cif tutoriel EFORT sur le thème LTE+SAE = EPS). Le HLR/AuC est caractérisé par un HSS dans l'architecture EPS.

Des vecteurs d 'authentification (AV, Authentication Vector) sont téléchargés par le MME à partir du HSS (Figure 8) à travers l 'interface S6 (basée sur DIAMETER) lorsque le MME reçoit de l 'UE les messages Attach Request ou Service Request.
Les paramètres présents dans le vecteur d'authentification (quadruplé) sont :

- RAND – le challenge (non aléatoire généré par le HSS) qui sert en tant qu'un des paramètres d'entrée pour générer les autres paramètres de l 'AV.
- XRES – Le résultat attendu, utilisé par le réseau pour l 'authentification de l 'USIM de l 'UE.
- AUTN – Le jeton d 'authentification utilisé par l 'USIM pour l 'authentification réseau.
- KASME – La clé permettant de dériver les clés de chiffrement et d 'intégrité.

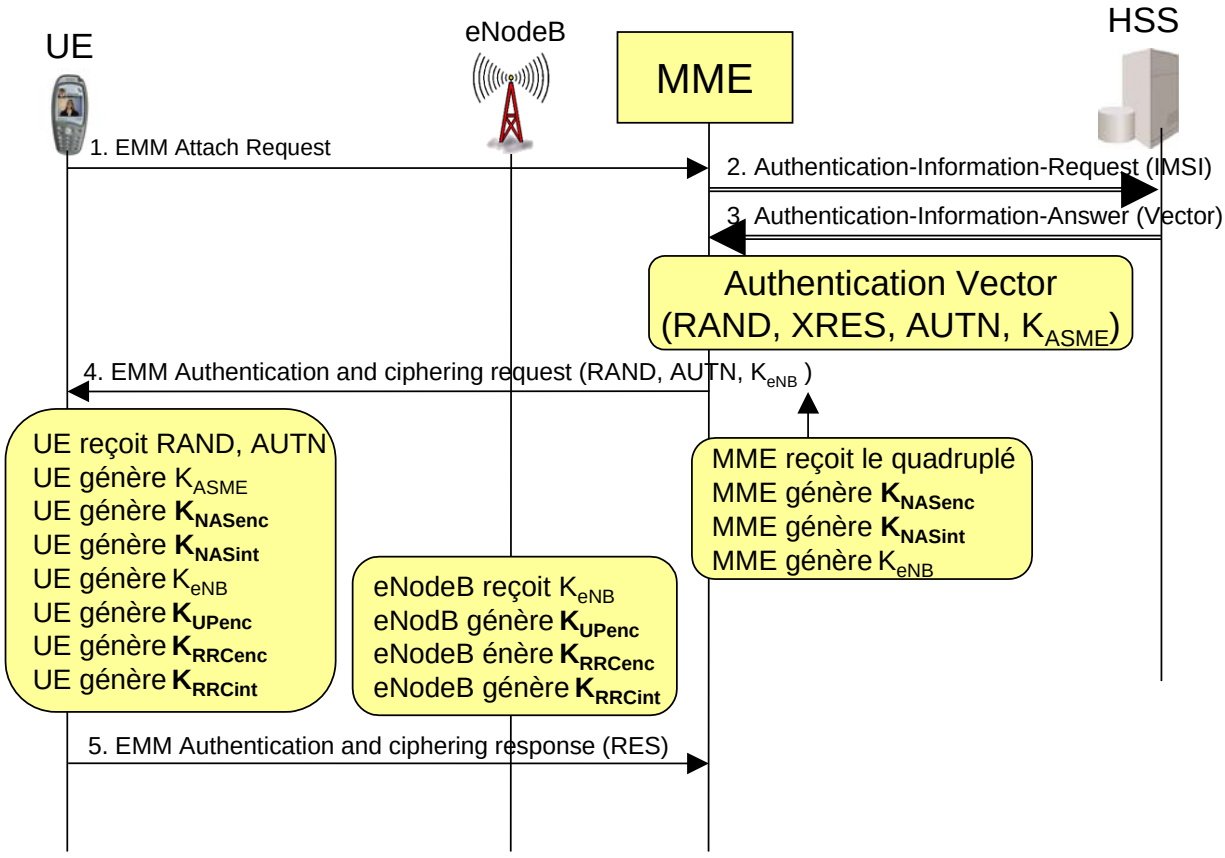


Figure 8 : Sécurité EPS

- KNASenc est calculé par le terminal et le MME à partir de KASME. Il est utilisé pour la protection du trafic NAS avec un algorithme de chiffrement particulier.
- KNASint est calculé par le terminal et le MME à partir de KASME. Il est utilisé pour la protection du trafic NAS avec un algorithme d 'intégrité particulier.
- KUPenc est calculé par le terminal et l 'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic usager avec un algorithme de chiffrement particulier.
- KRRCenc est calculé par le terminal et l 'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic de signalisation RRC avec un algorithme de chiffrement particulier.
- KRRCint est calculé par le terminal et l 'eNodeB à partir de KeNB. Il est utilisé pour la protection du trafic de signalisation RRC avec un algorithme d 'intégrité particulier.

L 'authentification EPS est réalisée lorsque :
- Le mobile se rattache au réseau
- Le mobile établit un default bearer
- Le mobile établit un dedicated bearer
- Le mobile met à jour sa localisation (Tracking Area)
- L 'authentification est réalisée entre le mobile et le MME.

Le chiffrement a lieu à deux niveaux :
- entre le mobile et l 'eNodeB (trafic usager et trafic de signalisation)
- entre le mobile et le MME (trafic de signalisation)

La protection de l 'intégrité de la signalisation a lieu :
- entre le mobile et l 'eNode B pour la signalisation RRC
- entre le mobile et le MME pour la signalisation NAS (Non-Access Stratum)

La formation « Sécurité Mobile pour les services Mobiles, Wireless et Internet » d'EFORT décrit les procédures d'authentification 2G, 3G et 4G ainsi que l'usage de ces techniques pour l'authentification de l'usager lors de son accès aux services IP depuis son mobile (e.g., UMA, WLAN, IMS, etc).