Procédures de sécurité, Semaine 2

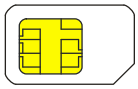
Vidéo 1 : Mise sous tension du terminal, fonctions de sécurité
Vidéo 2 : Authentification et autorisation
Vidéo 3 : Chiffrement
Vidéo 4 : Intégrité
Vidéo 5 : Hiérarchie des clés
Vidéo 6 : Identité temporaire
Vidéo 7 : Allocation de l'adresse IP par défaut

Introduction

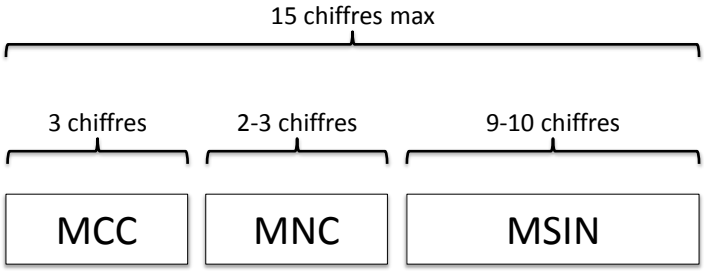
Que se passe-t-il quand j'allume mon terminal ?

Comment sont organisés les mécanismes de sécurité ?

IMSI (International Mobile Subscriber Identity)



Carte USIM

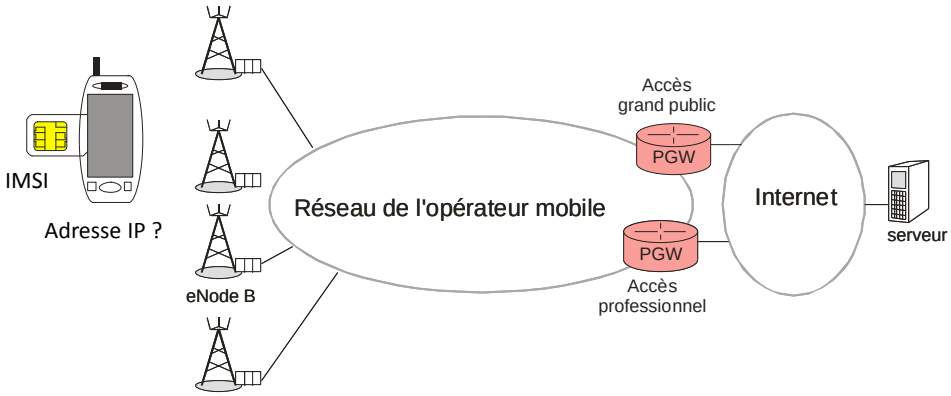


208 = FRANCE

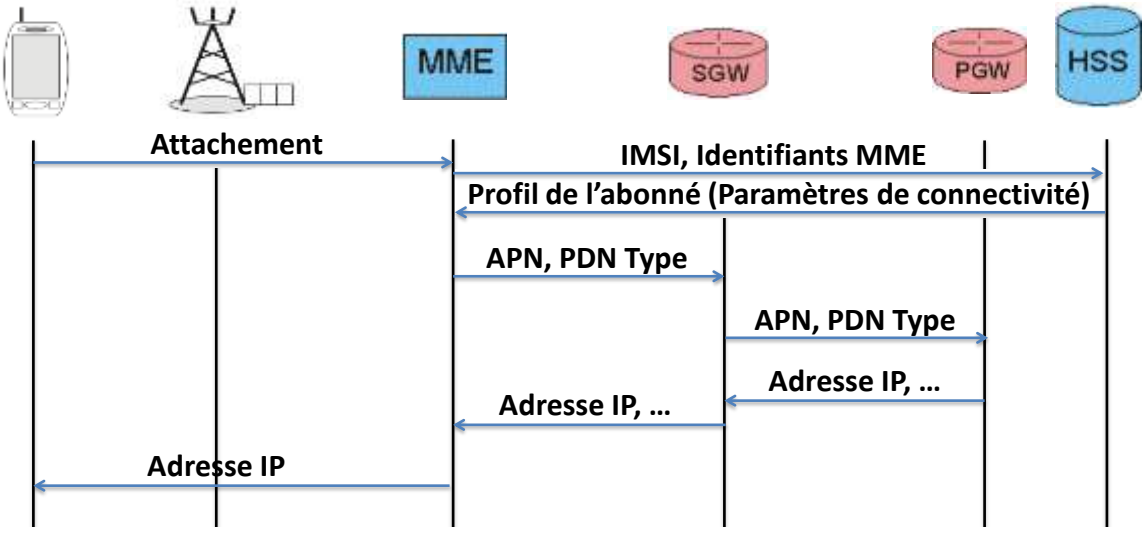
01 = ORANGE
10 = SFR
15 = FREE
20 = BOUYGUES TELECOM
…

208 10 1234567890

208 15 5123462346



APN = Access Point Name
Exemple : internet ou prooperator.mnc10.mcc208.gprs ou weboperator.fr



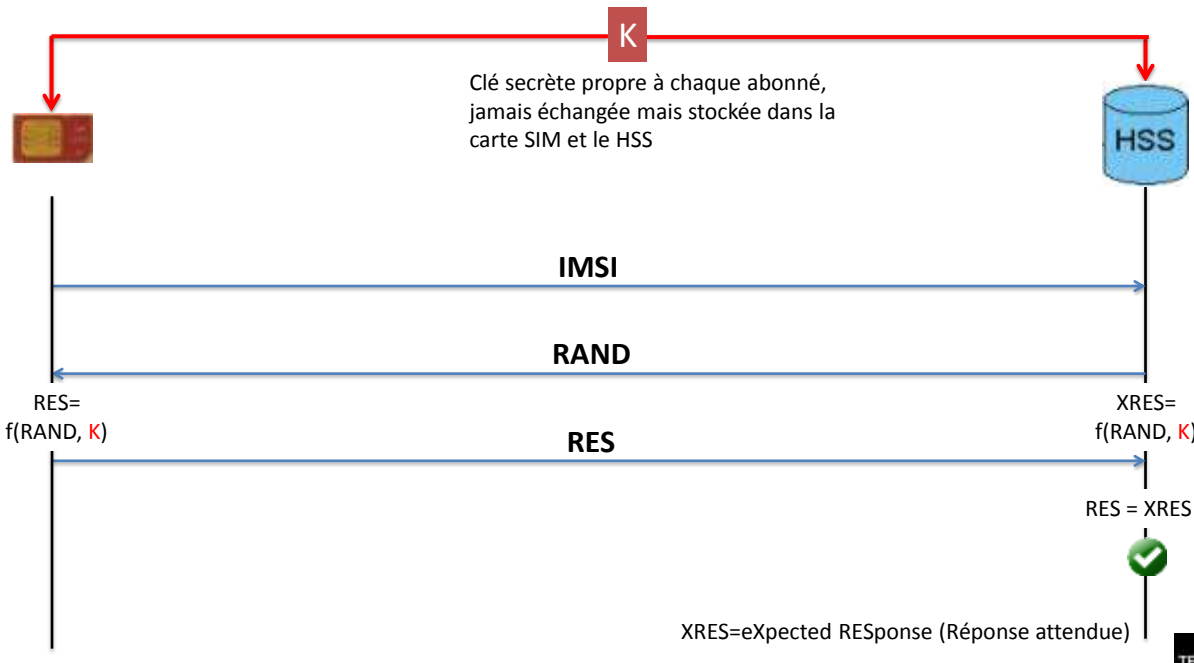
APN = Access Point Name
quel PGW utiliser
PDN Type = Packet Data Network Type
quel type d'IP utiliser (IPv6, IPv4, les deux)

Les principaux mécanismes de sécurité

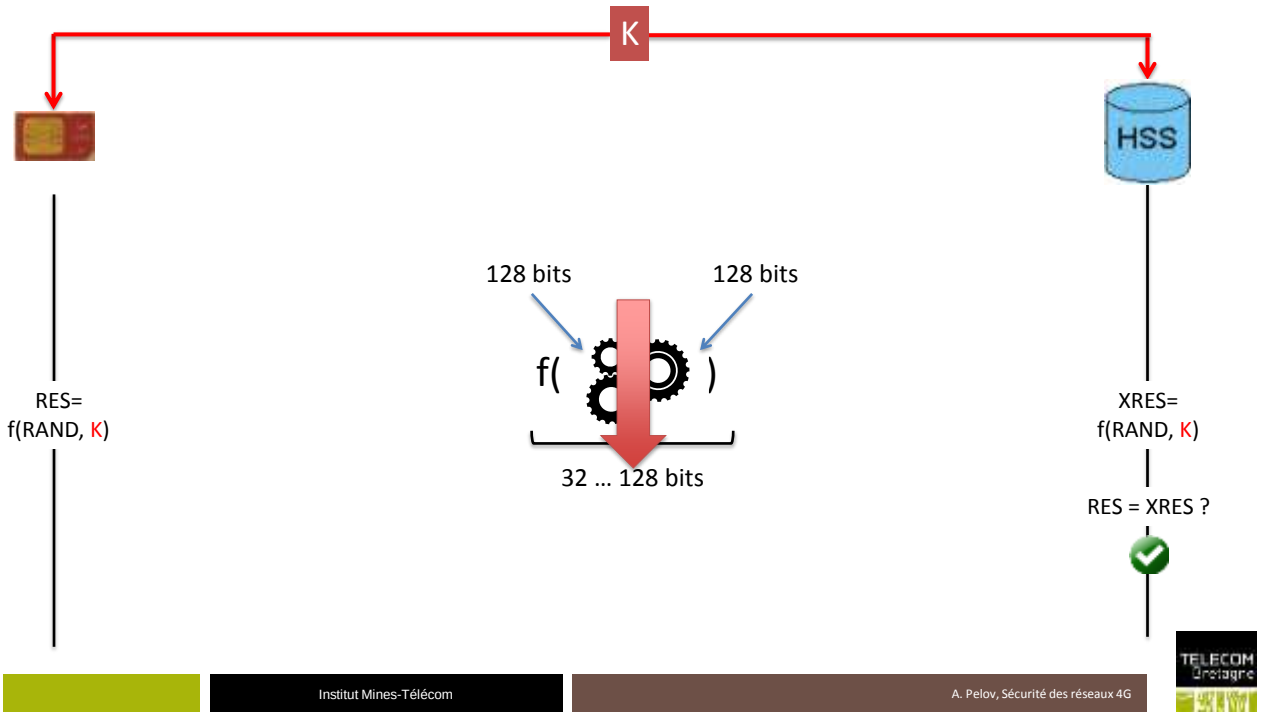
- Utilisation frauduleuse du réseau ➔ Authentification
- Ecoute des échanges ➔ Chiffrement
- Modification des messages ➔ Intégrité
- Suivi/localisation d'un terminal ➔ Identité temporaire

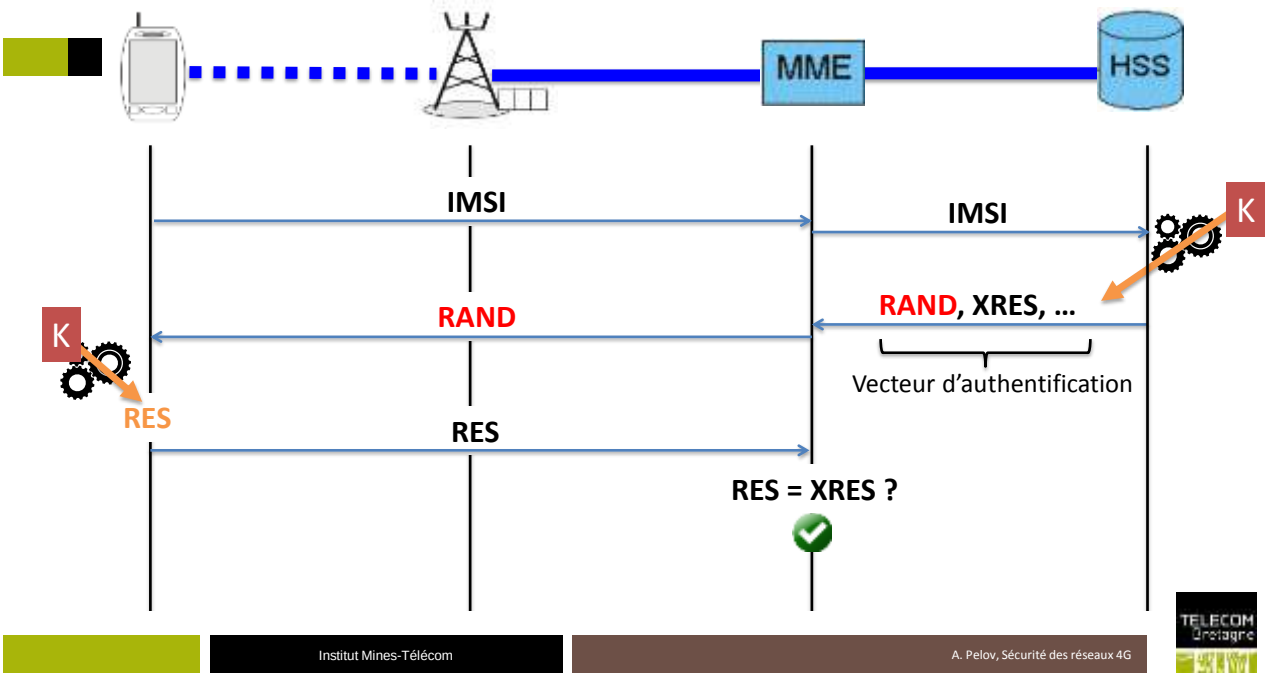
Authentification et autorisation

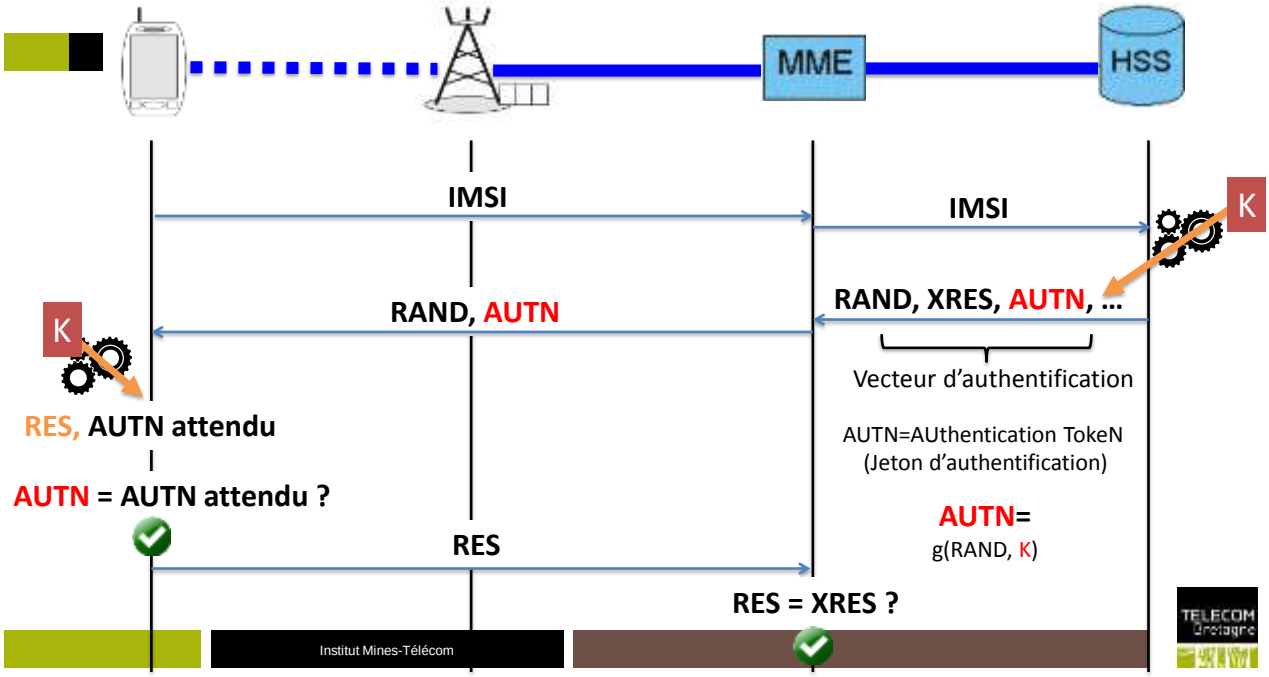
Comment un utilisateur est identifié par le réseau?

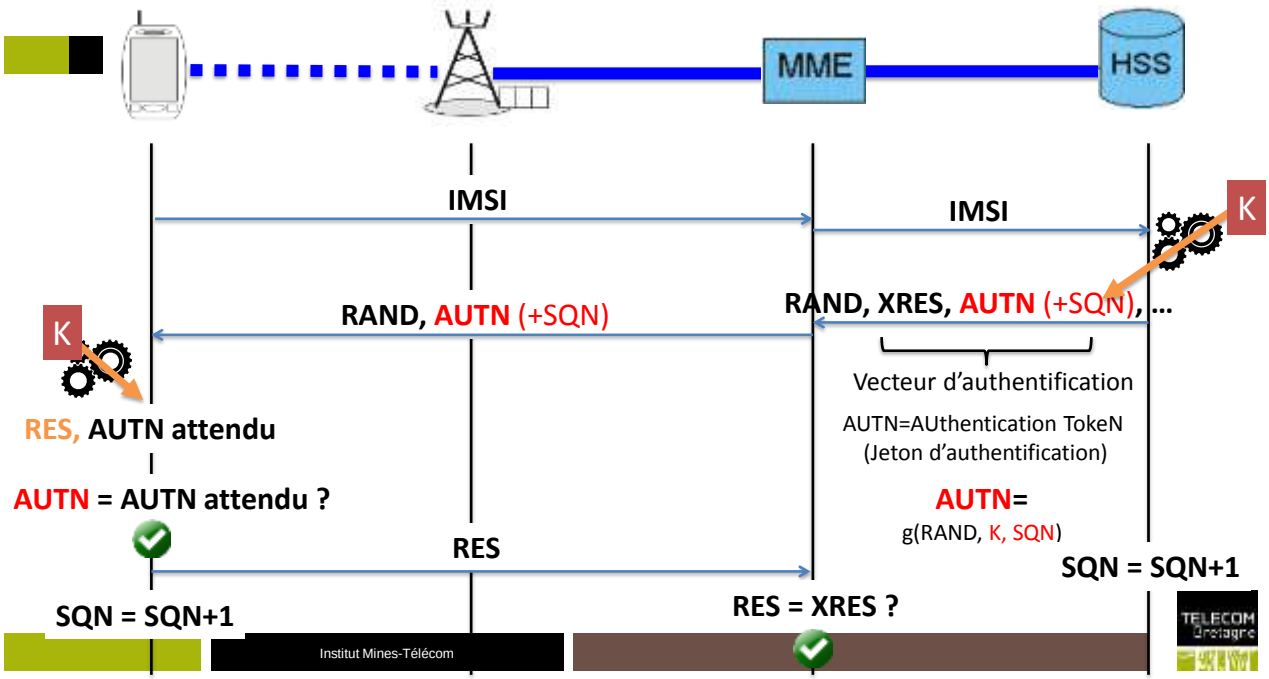


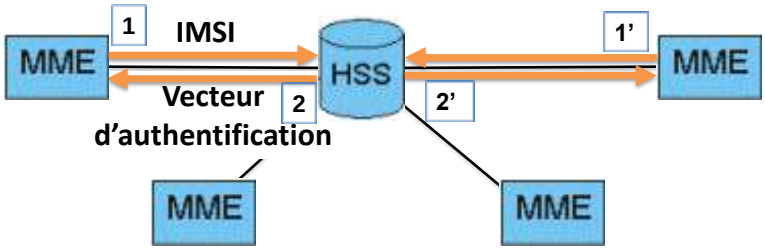
Institut Mines-Télécom A. Pelov, Sécurité des réseaux 4G


K
HSS
128 bits
128 bits
f(
)
32 … 128 bits
RES=
f(RAND, K)
XRES=
f(RAND, K)
RES = XRES ?


MME
HSS
IMSI
IMSI
K
RAND
RAND, XRES, …
K
Vecteur d'authentification
RES
RES
RES = XRES ?


MME
HSS
IMSI
IMSI
K
RAND, AUTN
RAND, XRES, AUTN, …
K
Vecteur d'authentification
RES, AUTN attendu
AUTN=AUthentication TokeN
(Jeton d'authentification)
AUTN = AUTN attendu ?
AUTN=
g(RAND, K)
RES
RES = XRES ?
Institut Mines-Télécom
TELECOM Bretagne


MME
HSS
IMSI
IMSI
K
RAND, AUTN (+SQN)
RAND, XRES, AUTN (+SQN), …
K
Vecteur d'authentification
RES, AUTN attendu
AUTN=AUthentication TokeN
(Jeton d'authentification)
AUTN = AUTN attendu ?
AUTN=
g(RAND, K, SQN)
RES
SQN = SQN+1
SQN = SQN+1
RES = XRES ?
Institut Mines-Télécom
TELECOM Bretagne

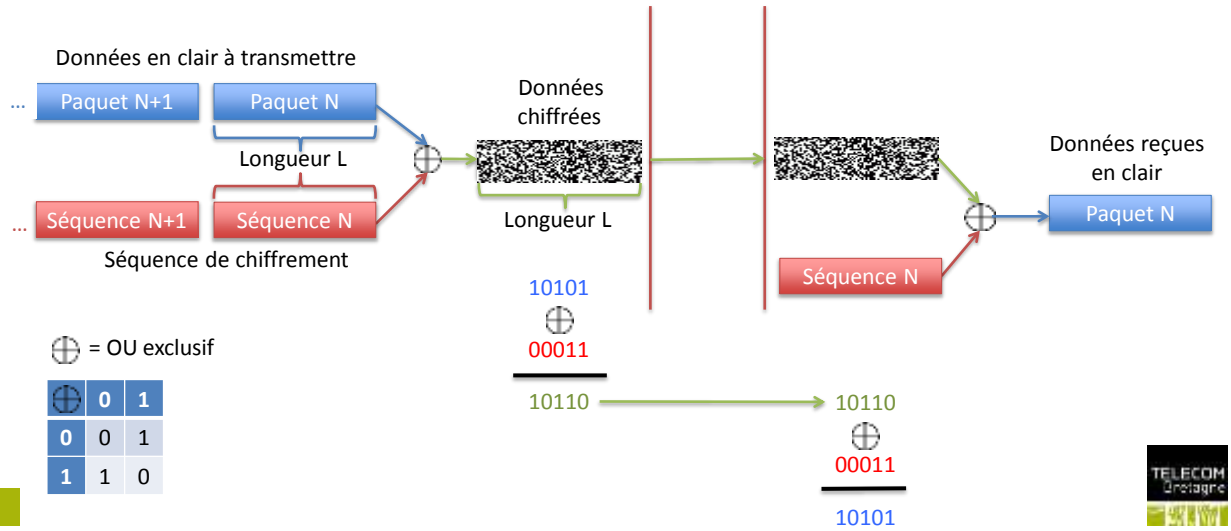


Chiffrement de données

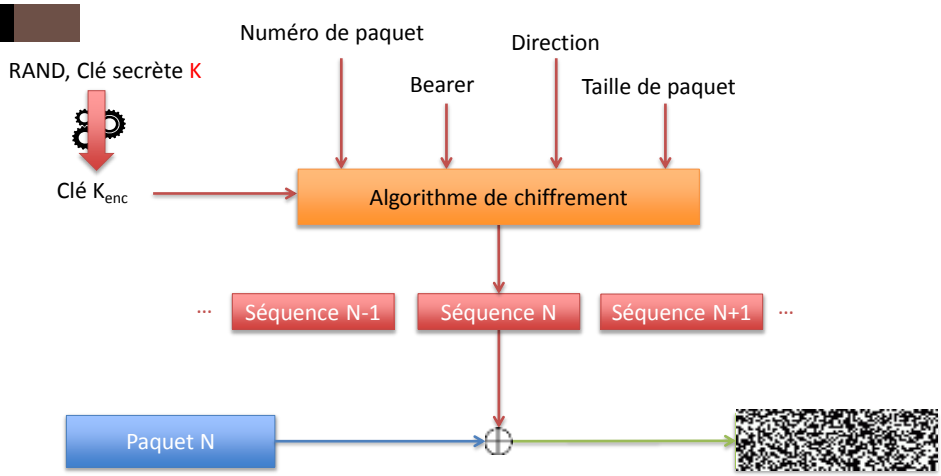
Est-ce que quelqu'un peut écouter mes communications ?

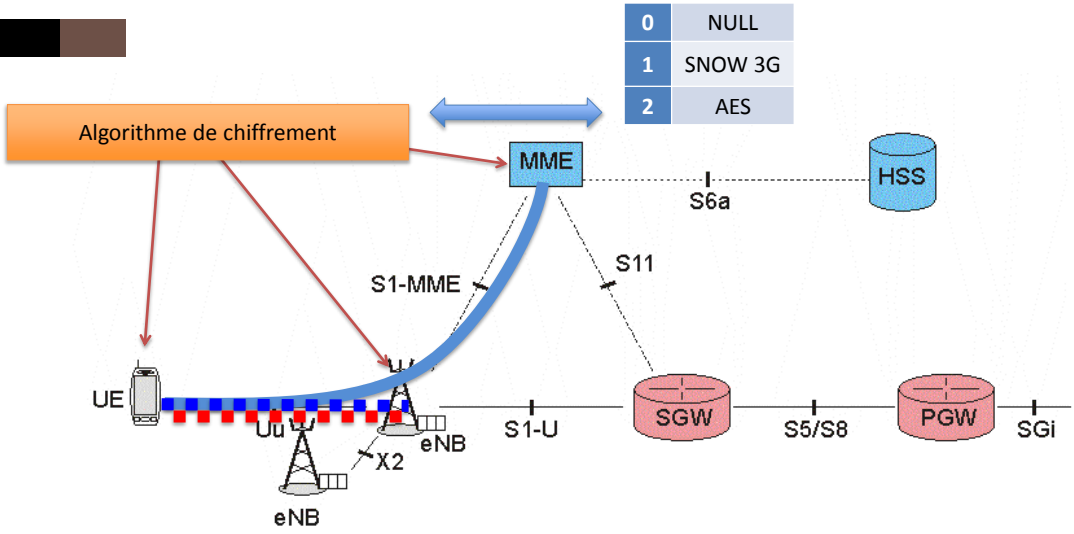
Institut Mines-Télécom
A. Pelov, Sécurité des réseaux 4G

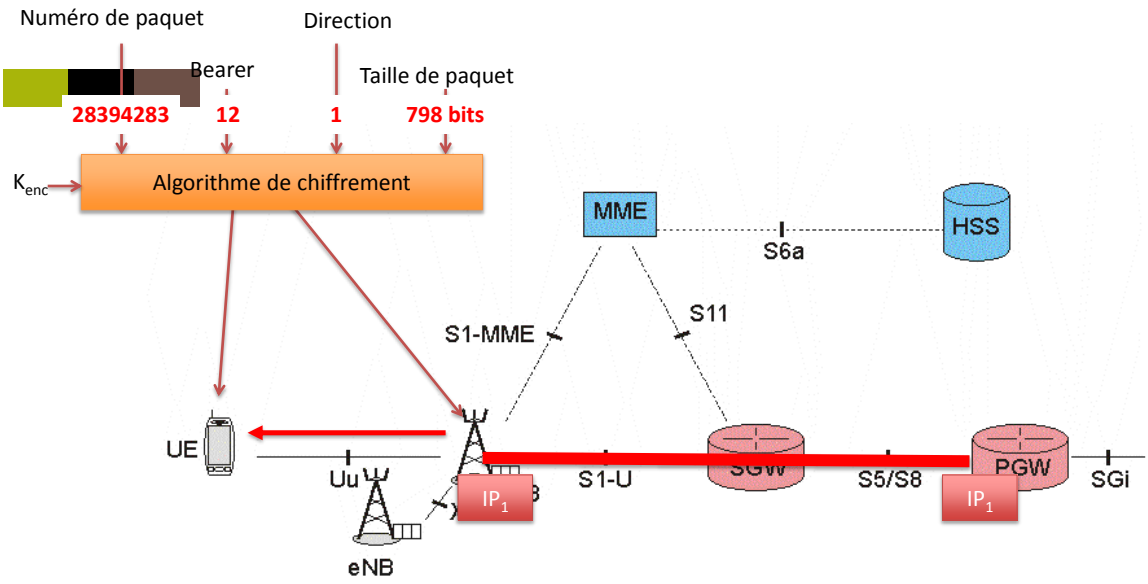
Chiffrement des échanges



⊕	0	1
0	0	1
1	1	0



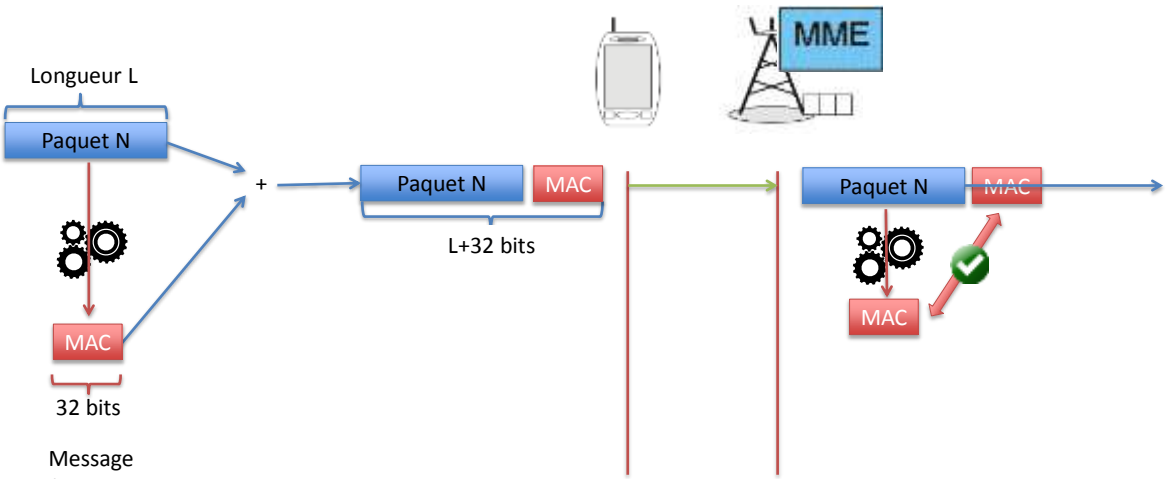

0 NULL
1 SNOW 3G
2 AES
Algorithme de chiffrement
MME
HSS
S6a
S11
S1-MME
UE
Uu
eNB
X2
S1-U
SGW
S5/S8
PGW
SGi
eNB


Numéro de paquet
Direction
Bearer
Taille de paquet
28394283
12
1
798 bits
K_{enc}
Algorithme de chiffrement
MME
HSS
S6a
S11
S1-MME
UE
Uu
eNB
IP1
S1-U
SGW
S5/S8
PGW
IP1
SGi

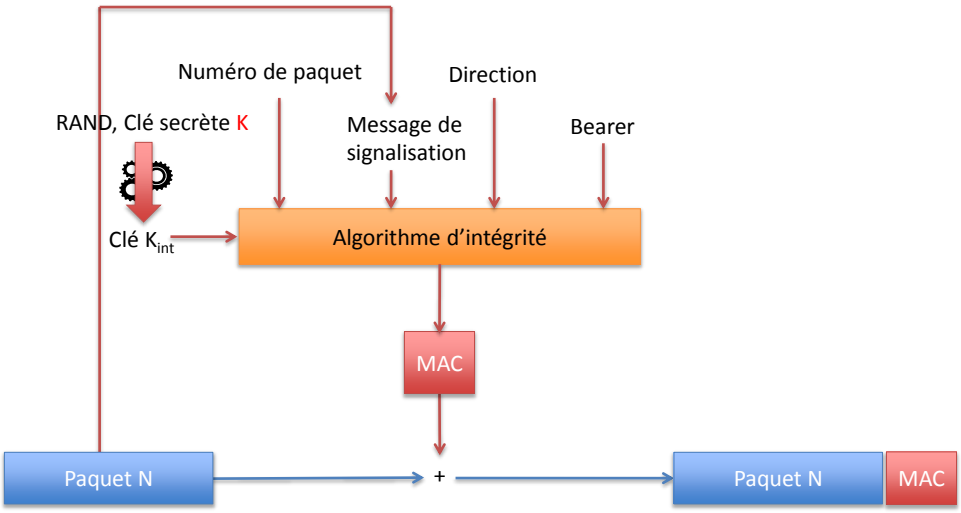
Intégrité

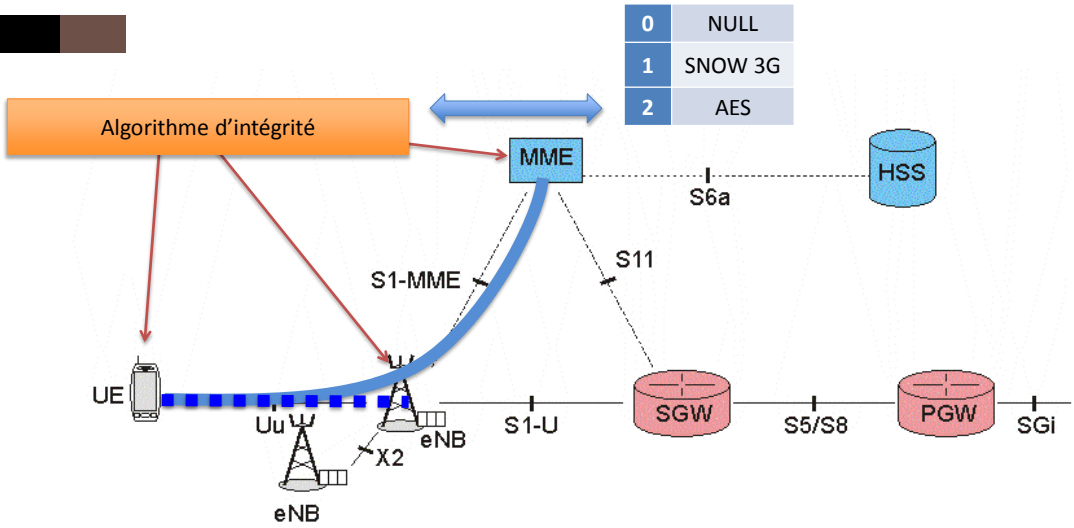
Est-ce que je peux être sûr que le message que je viens de recevoir n'a pas été modifié par un équipement intermédiaire ?

Protection contre les modifications

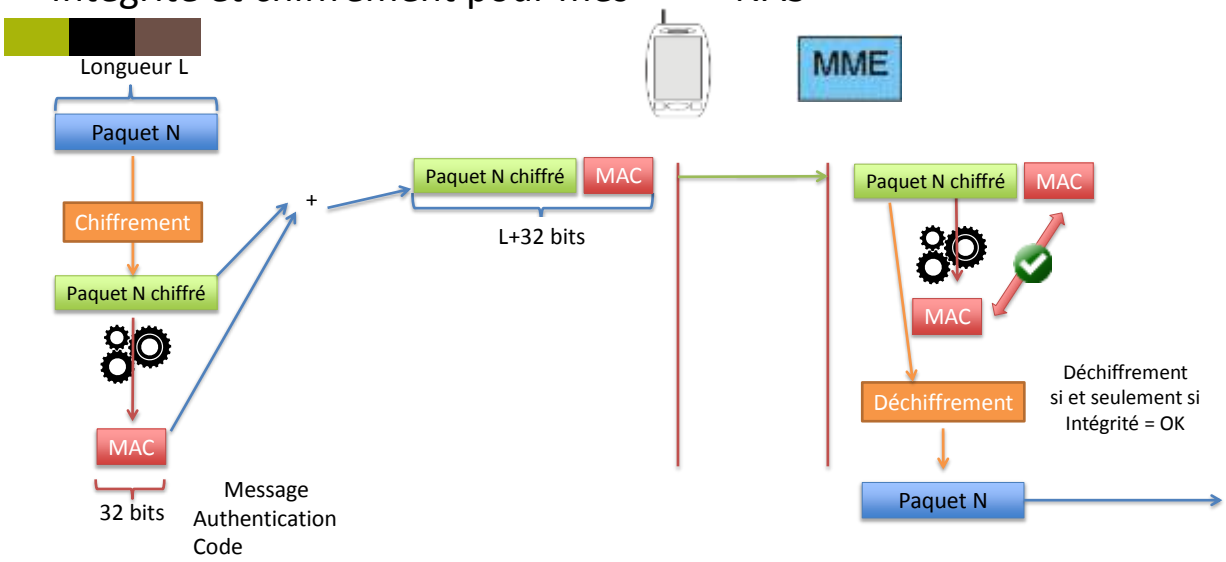


Seulement pour les messages de signalisation entre MME et UE

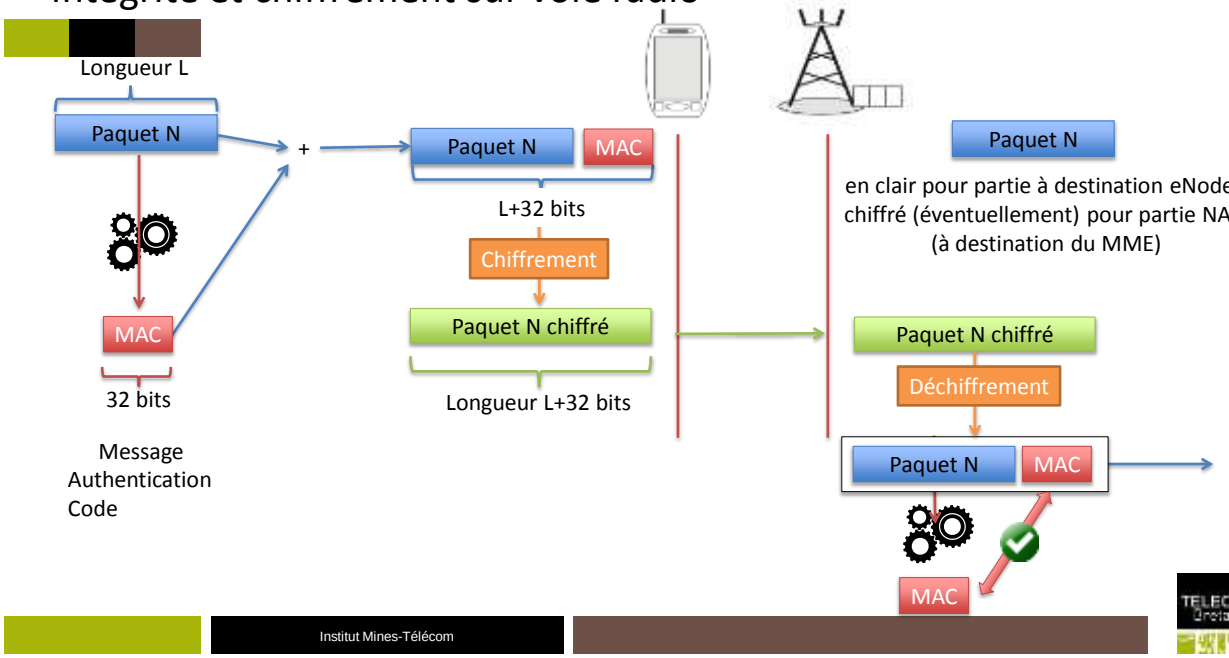

Numéro de paquet
Direction
RAND, Clé secrète K
Message de signalisation
Bearer
Clé K_{int}
Algorithme d'intégrité
MAC
Paquet N
+
Paquet N
MAC


0 NULL
1 SNOW 3G
2 AES
Algorithme d'intégrité
MME
HSS
S6a
S11
S1-MME
UE
Uu
eNB
X2
eNB
S1-U
SGW
S5/S8
PGW
SGi

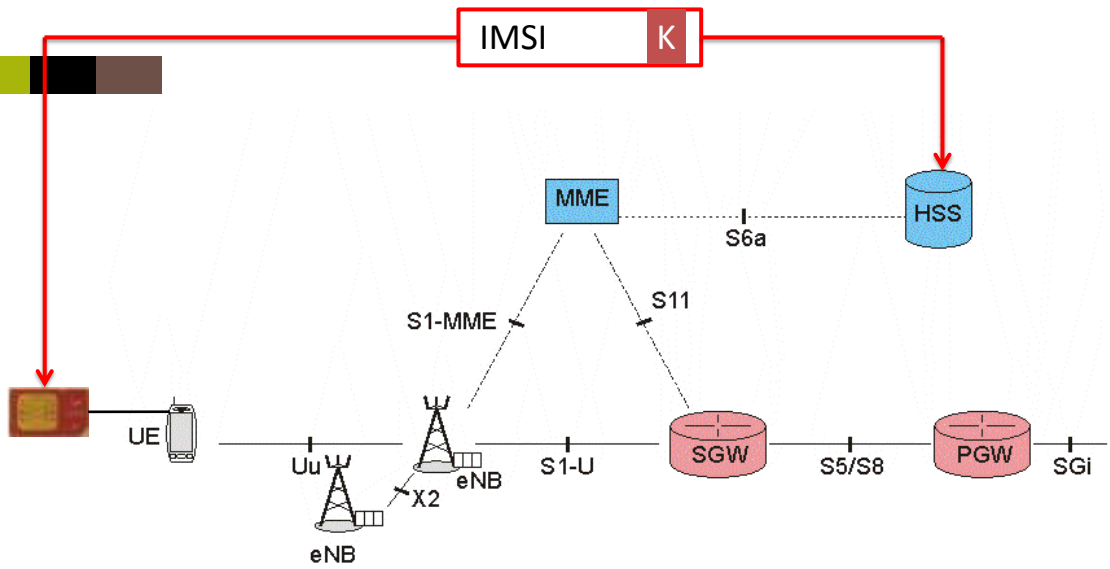
Intégrité et chiffrement pour messages NAS



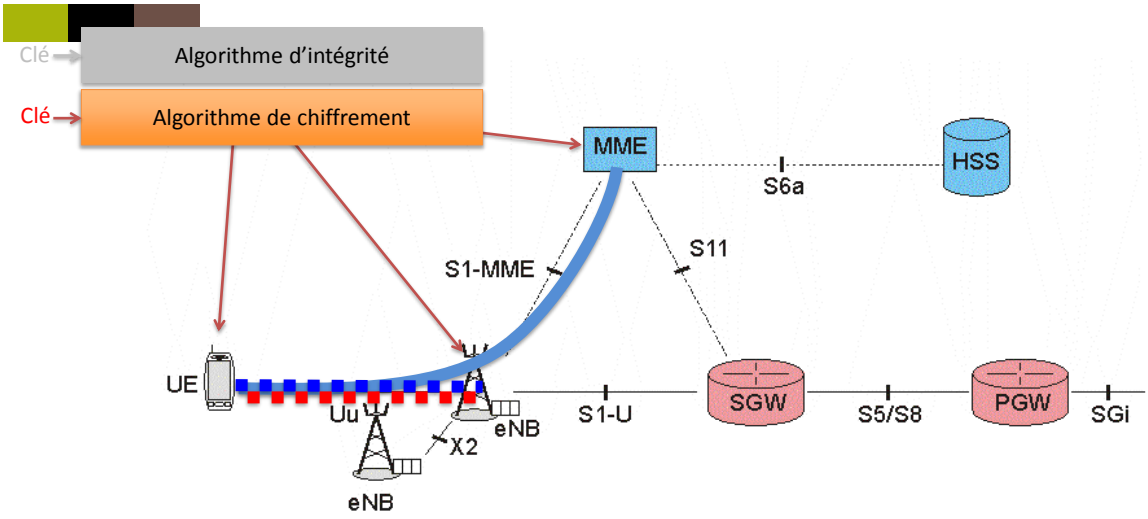
Intégrité et chiffrement sur voie radio

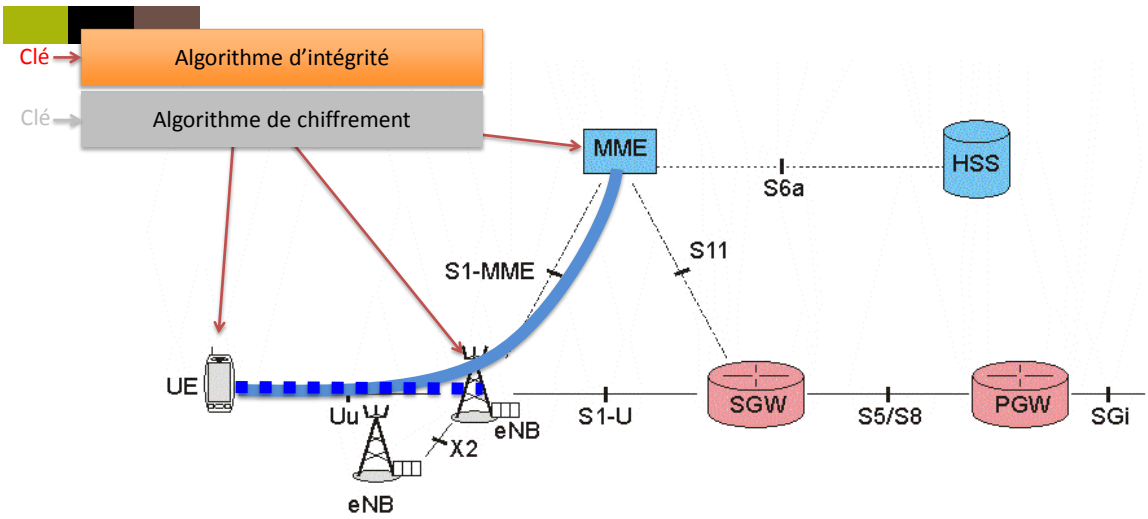


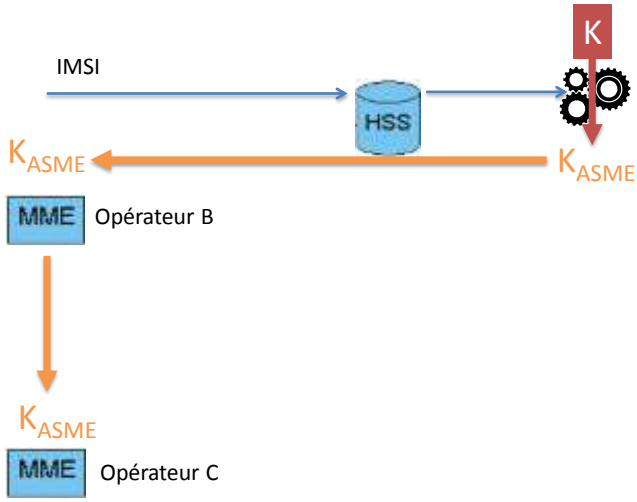
Hiérarchie de clés



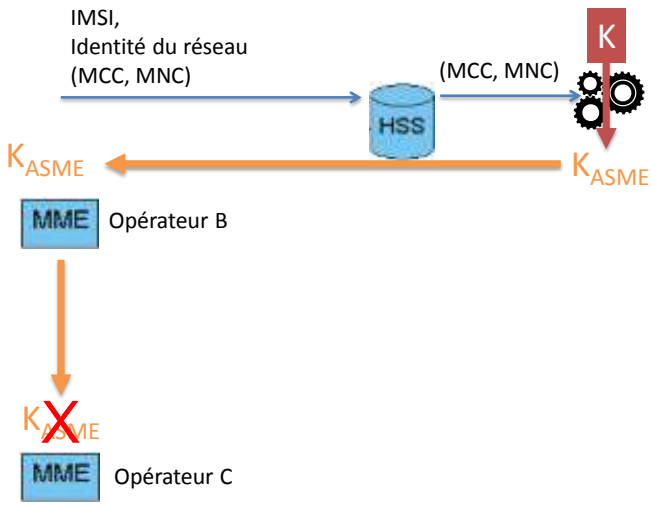
Institut Mines-Télécom A. Pelov, Sécurité des réseaux 4G


Clé
Algorithme d'intégrité
Clé
Algorithme de chiffrement
MME
HSS
S6a
S11
S1-MME
UE
Uu
eNB
X2
eNB
S1-U
SGW
S5/S8
PGW
SGi

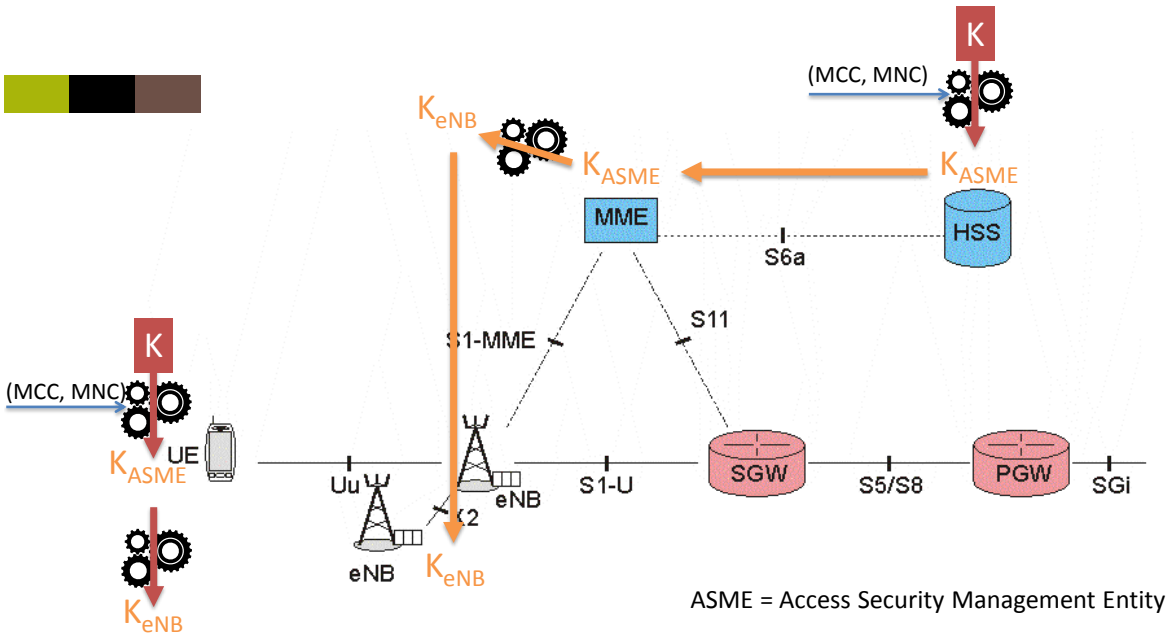

Clé
Algorithme d'intégrité
Clé
Algorithme de chiffrement
MME
HSS
S6a
S11
S1-MME
UE
Uu
eNB
X2
eNB
S1-U
SGW
S5/S8
PGW
SGi



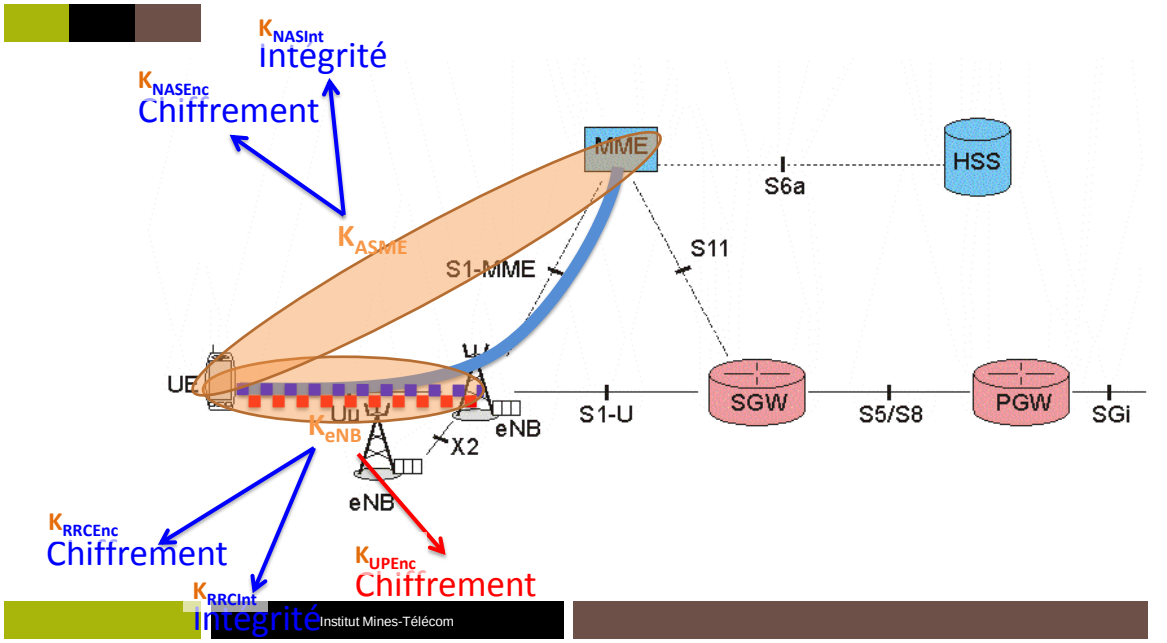
ASME = Access Security Management Entity

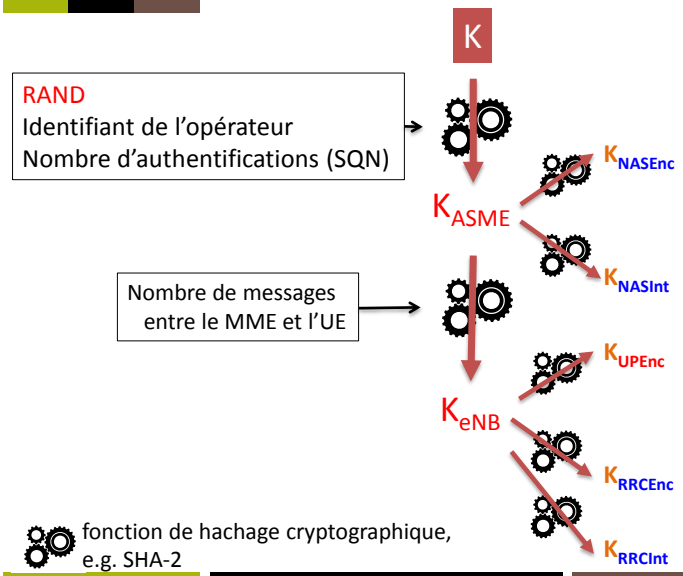


ASME = Access Security Management Entity



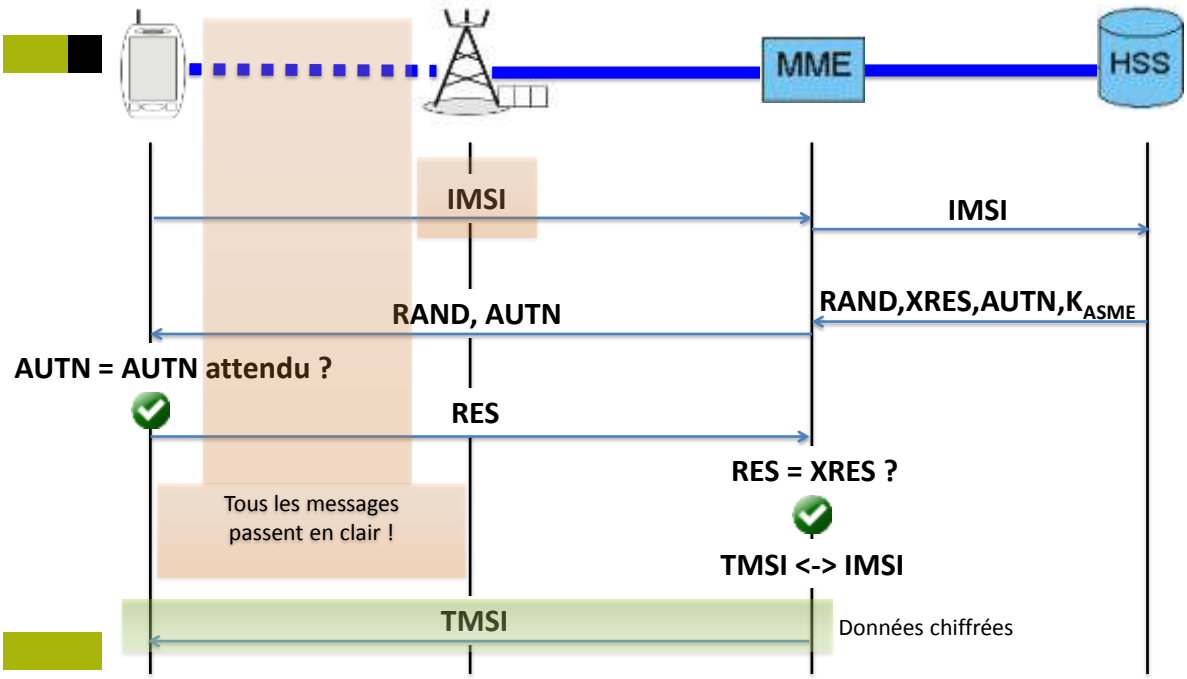
ASME = Access Security Management Entity



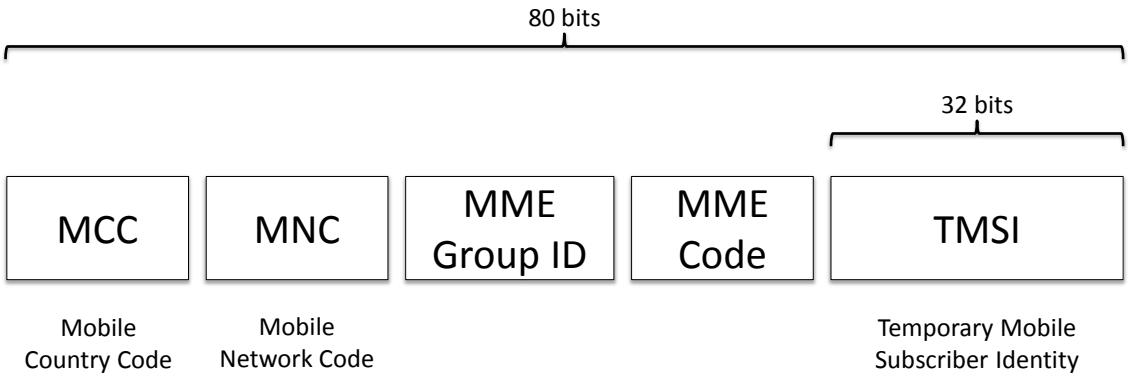


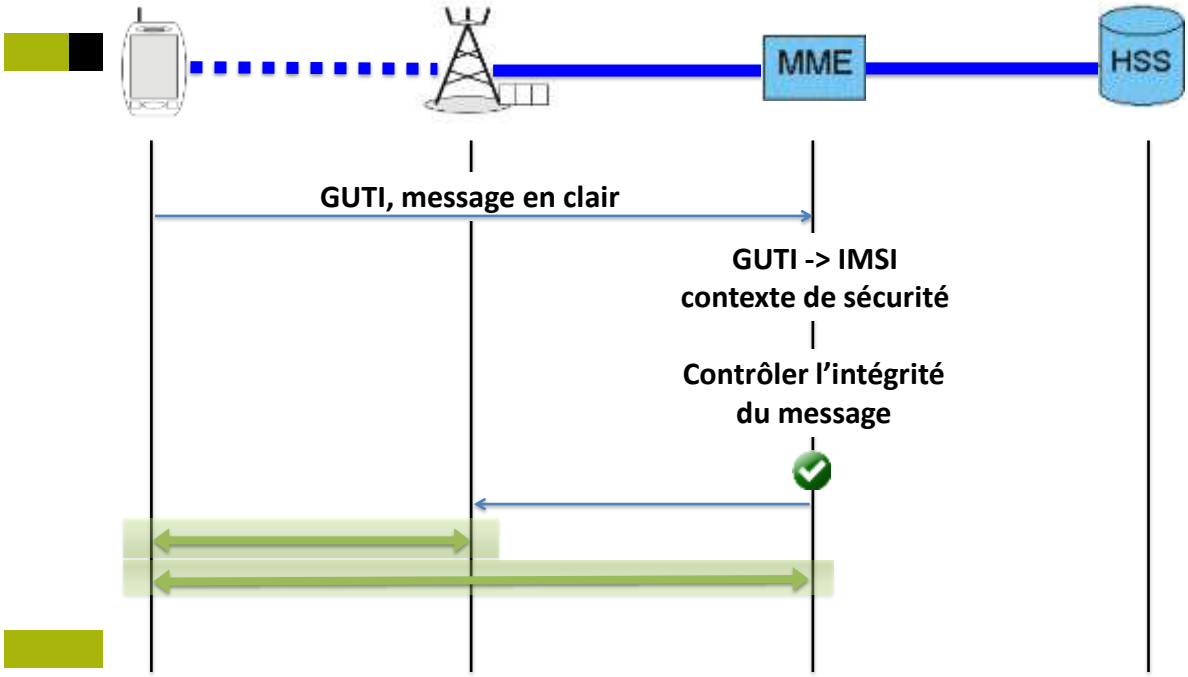
Identité temporaire

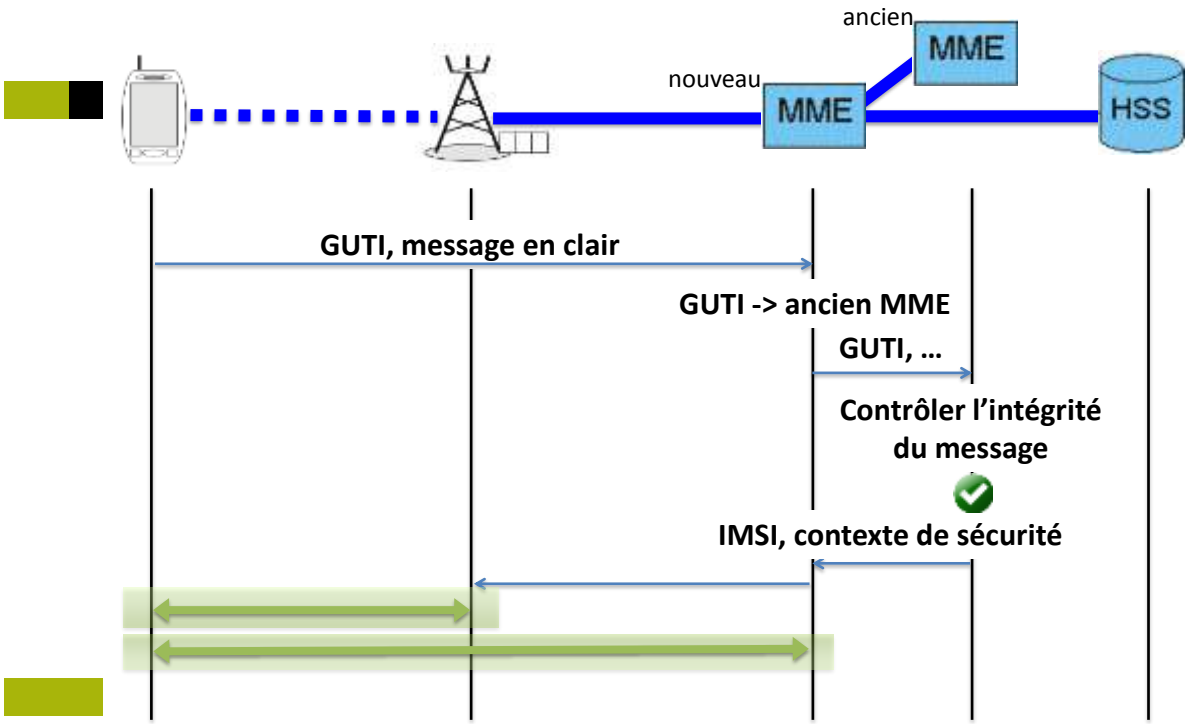
Et si quelqu'un pouvait suivre mes déplacements? L'IMSI m'identifie d'une manière unique dans le monde..

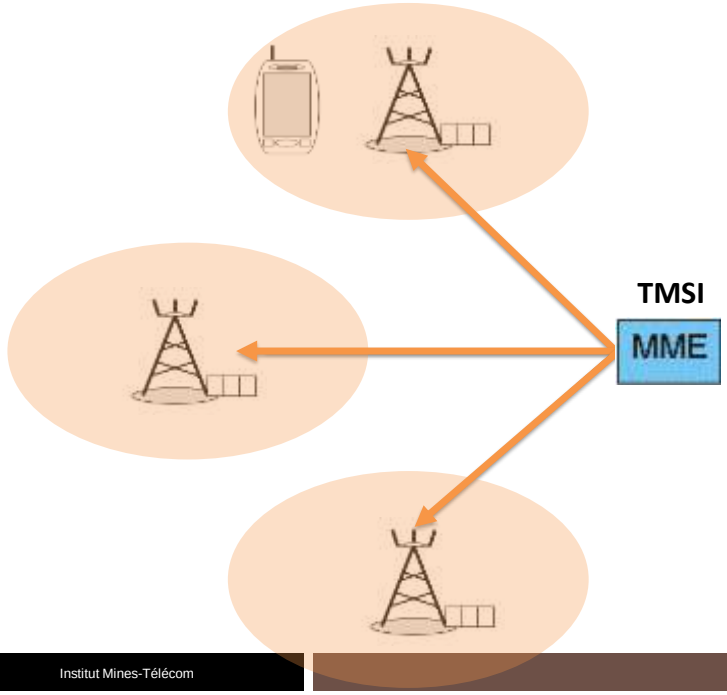


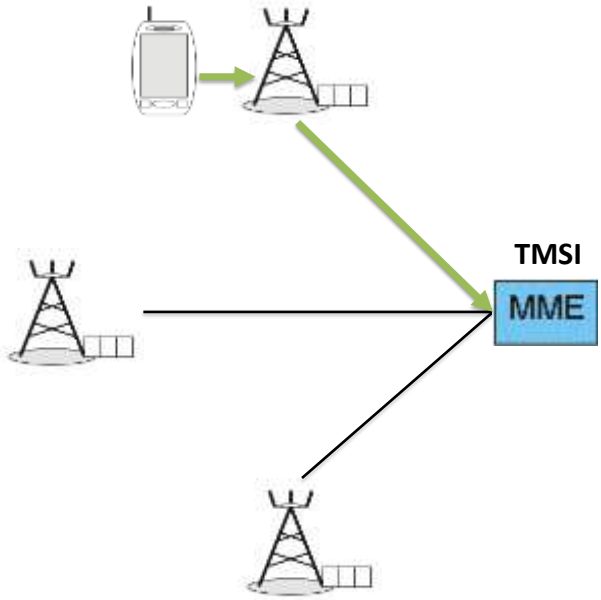
GUTI (Globally Unique Temporary UE Identity)



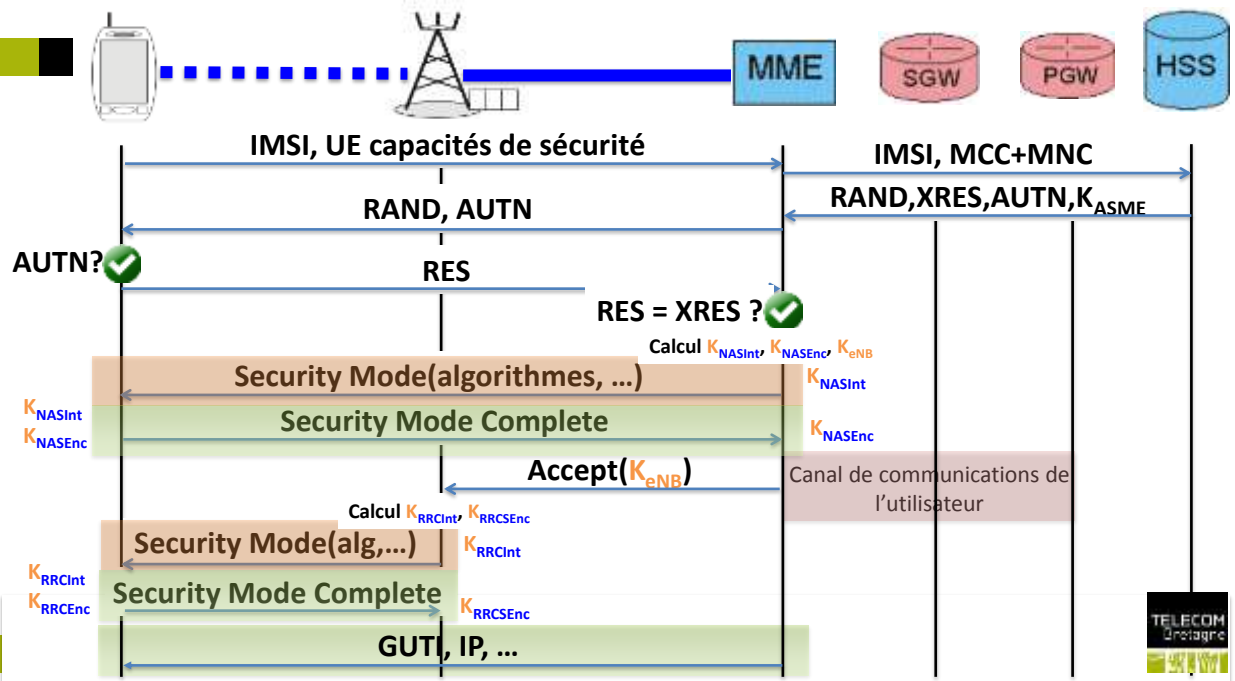

MME
HSS
GUTI, message en clair
GUTI -> IMSI
contexte de sécurité
Contrôler l'intégrité
du message

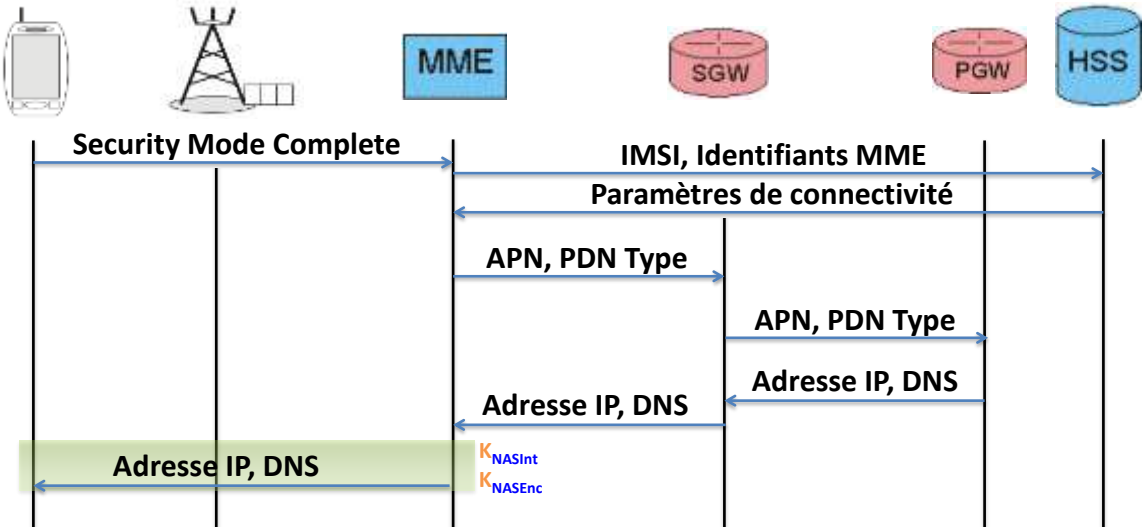

ancien
MME
nouveau
MME
HSS
GUTI, message en clair
GUTI -> ancien MME
GUTI, …
Contrôler l'intégrité
du message
IMSI, contexte de sécurité


TMSI
MME


TMSI
MME

Attribution de l'adresse IP par défaut





APN = Access Point Name
quel PGW utiliser
PDN Type = Packet Data Network Type
quel type d'IP utiliser (IPv6, IPv4, les deux)