



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



1

Institut Mines-Télécom

A. Pelov, Procédures de sécurité



Introduction

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

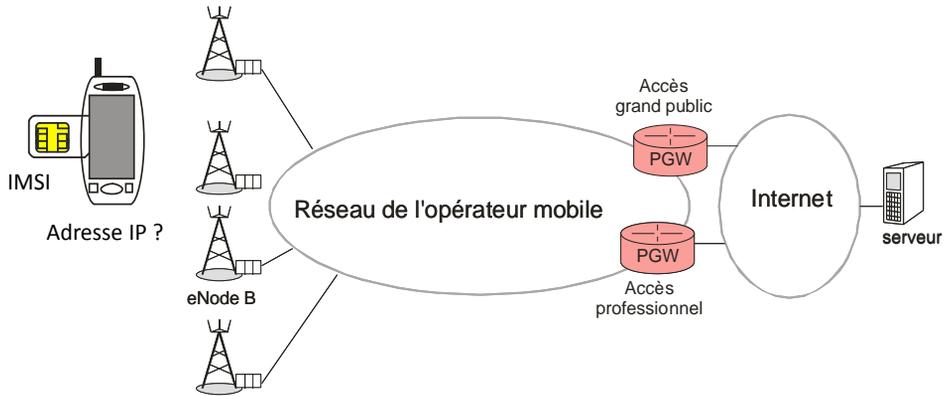
Comment sont organisés les mécanismes de sécurité ?



Institut Mines-Télécom

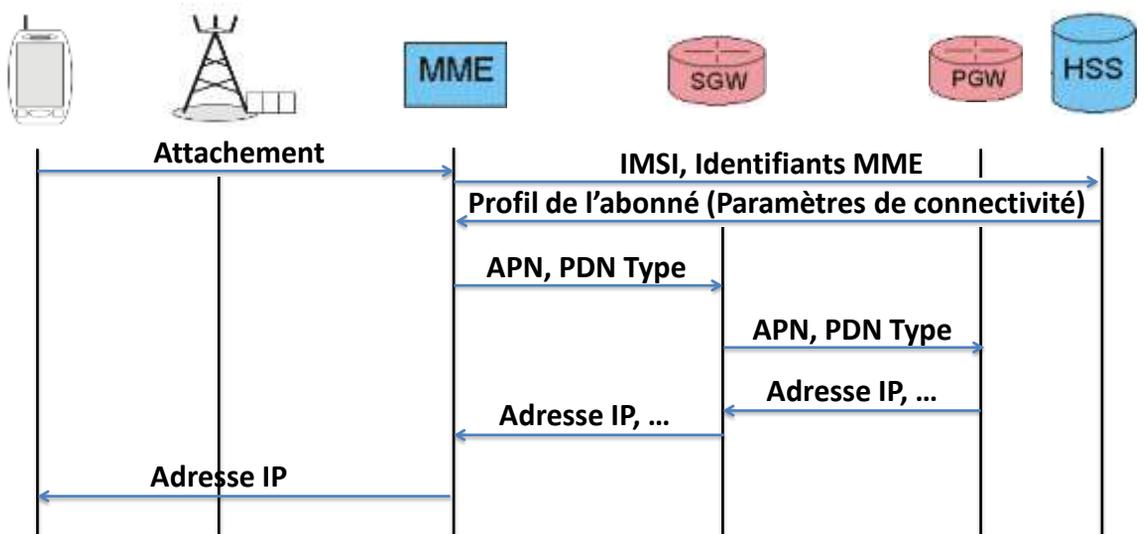
A. Pelov, Sécurité des réseaux 4G





APN = Access Point Name

Exemple : www.operateur.fr ou pro.operateur.fr



APN = Access Point Name
quel PGW utiliser

PDN Type = Packet Data Network Type
quel type d'IP utiliser (IPv6, IPv4, les deux)



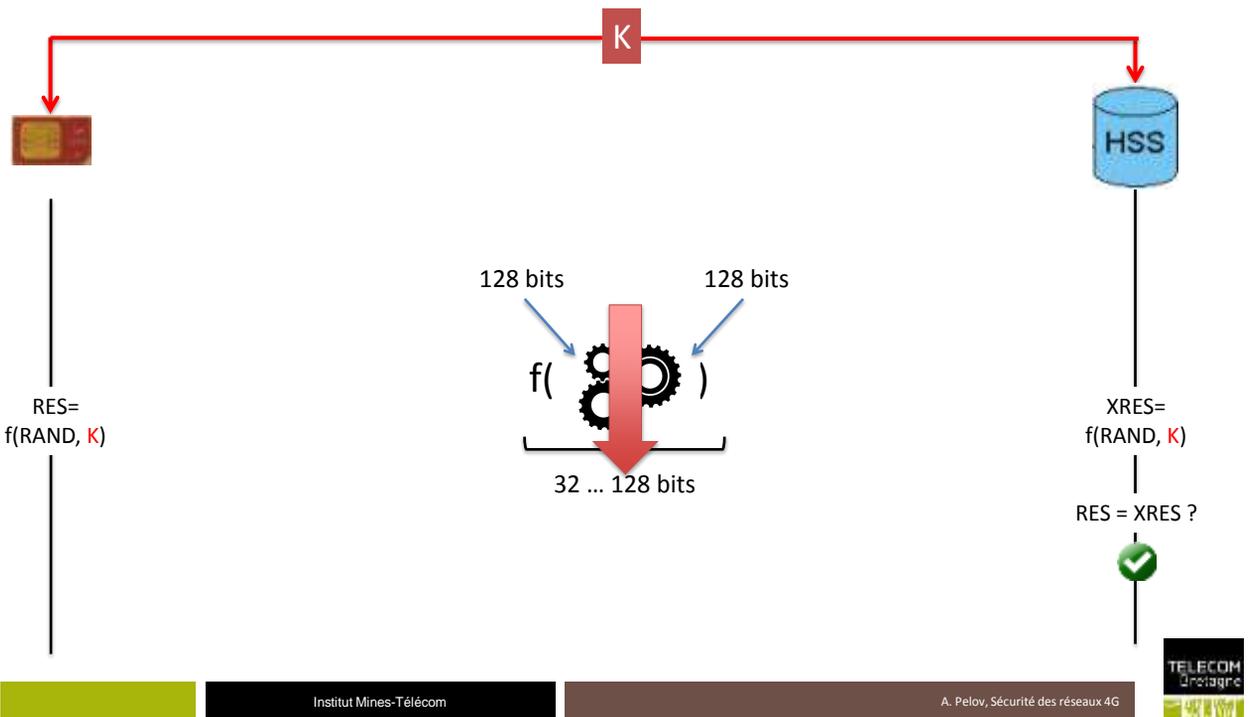
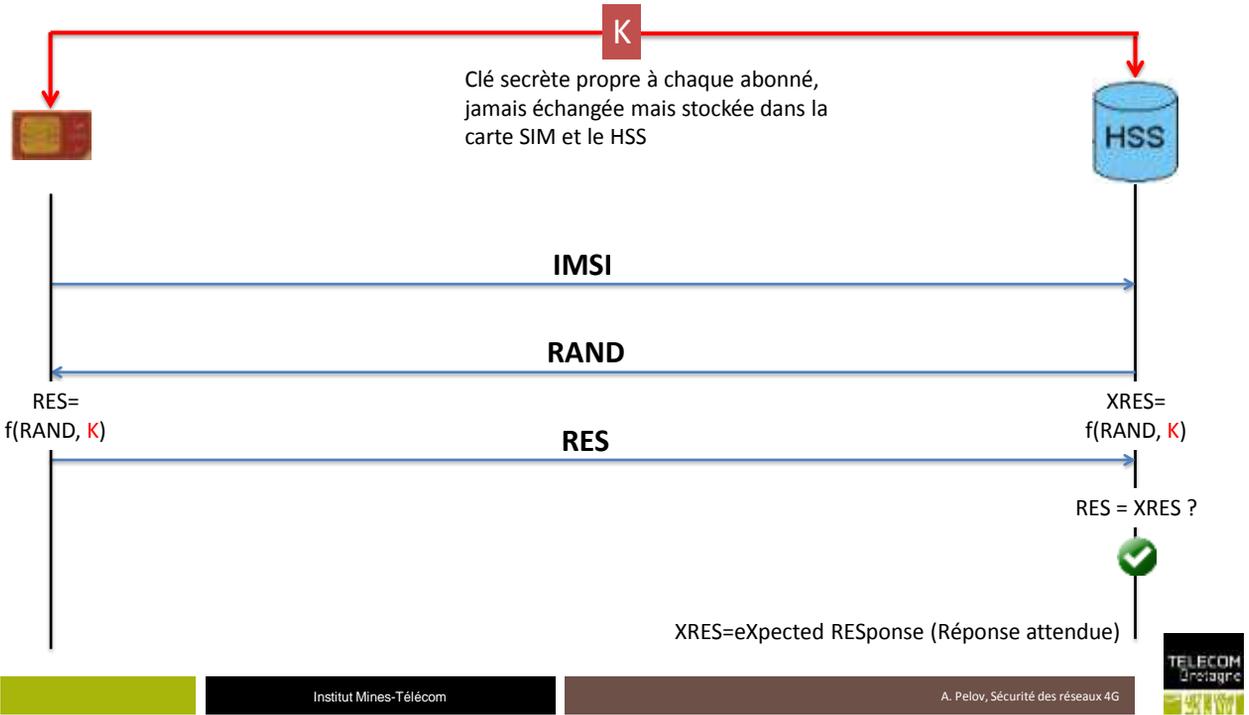
Les principaux mécanismes de sécurité

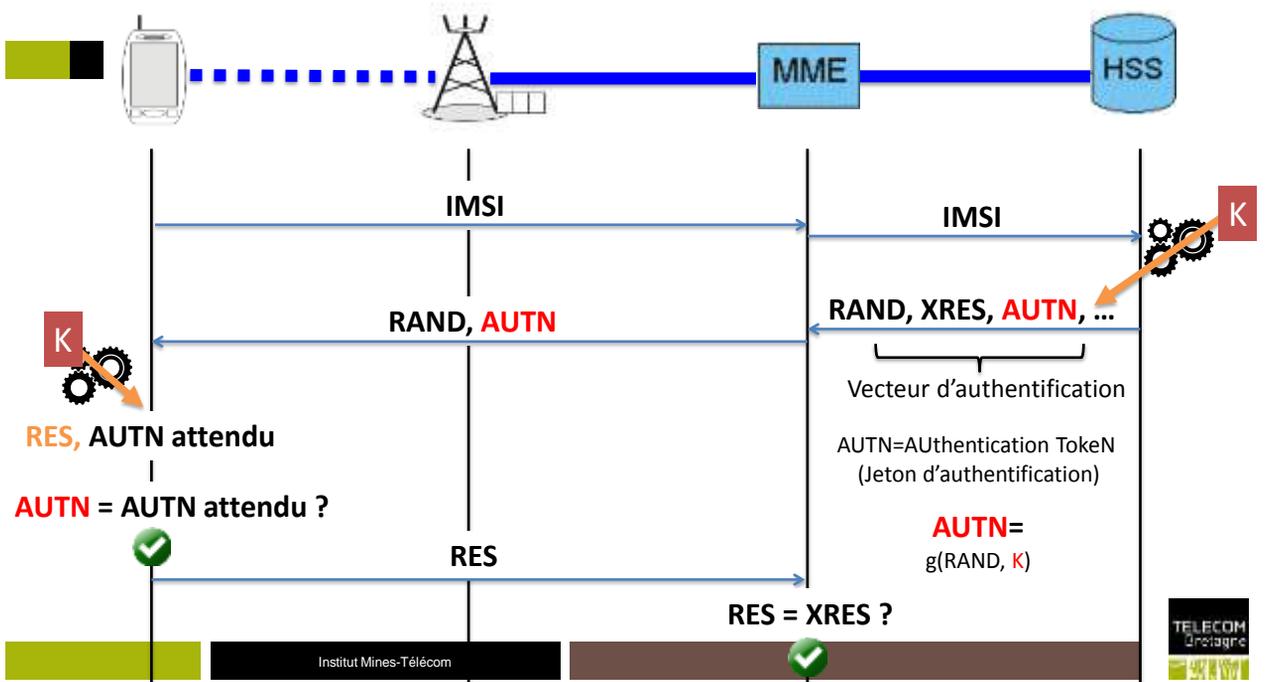
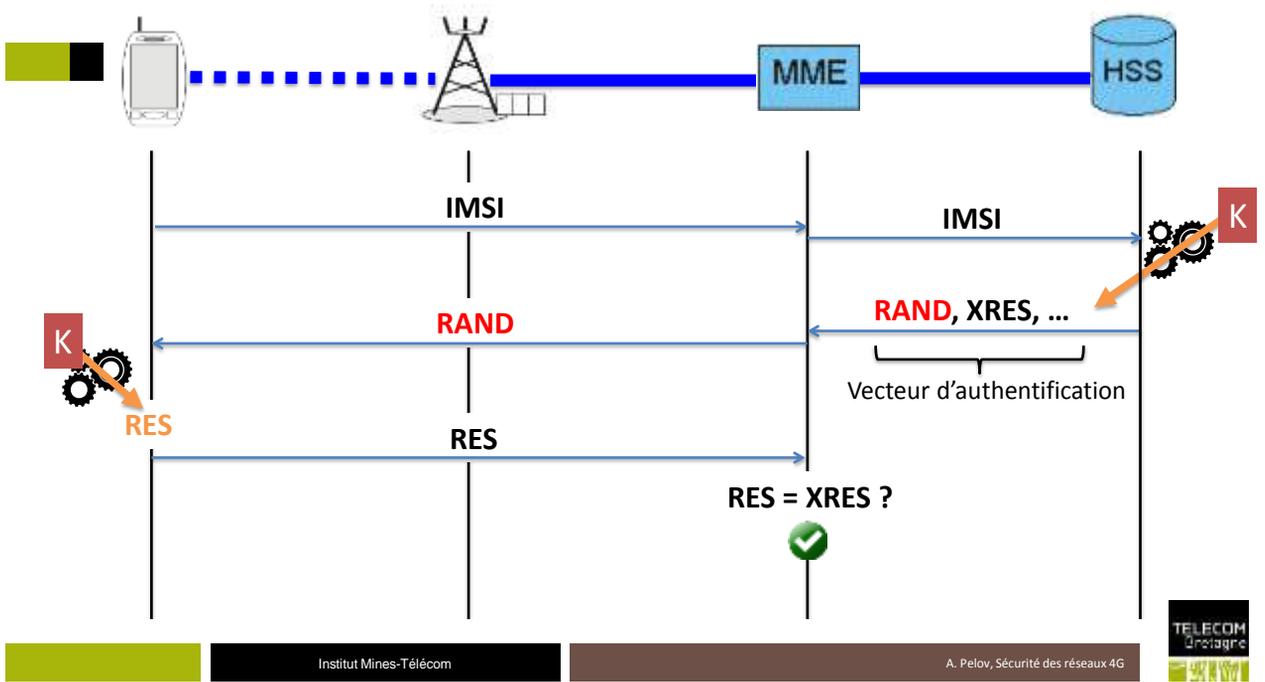
- Utilisation frauduleuse du réseau → Authentification
- Ecoute des échanges → Chiffrement
- Modification des messages → Intégrité
- Suivi/localisation d'un terminal → Identité temporaire

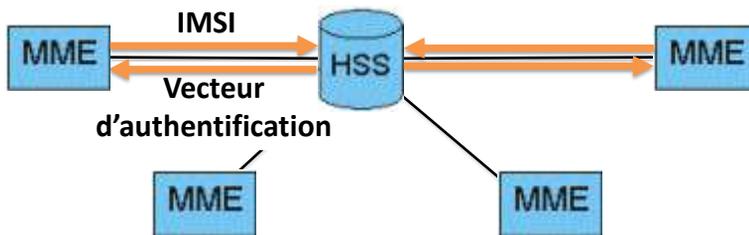
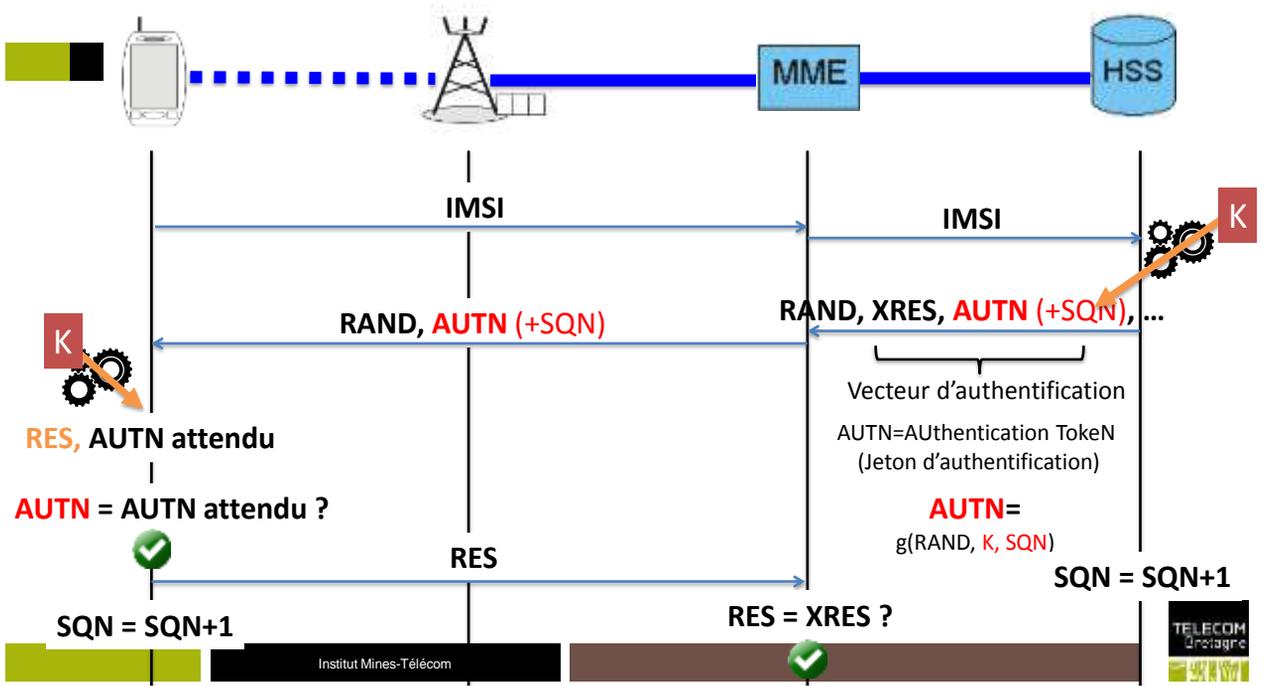


Authentification et autorisation

Comment un utilisateur est identifié par le réseau?



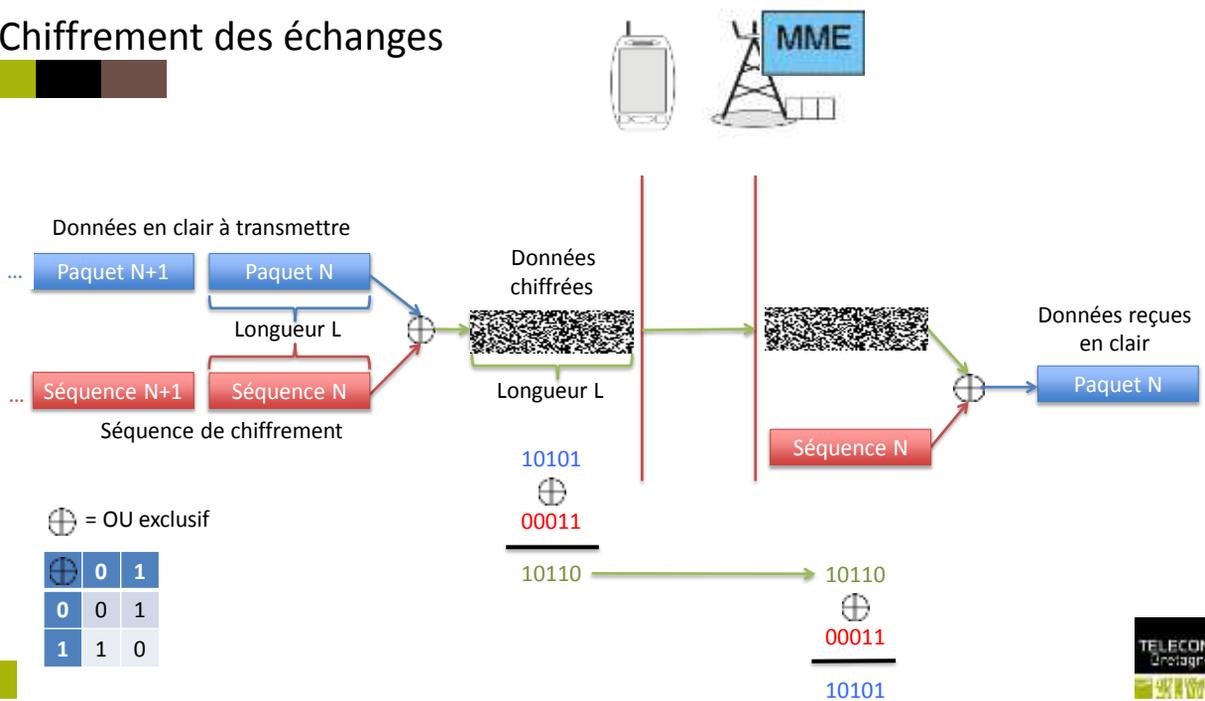


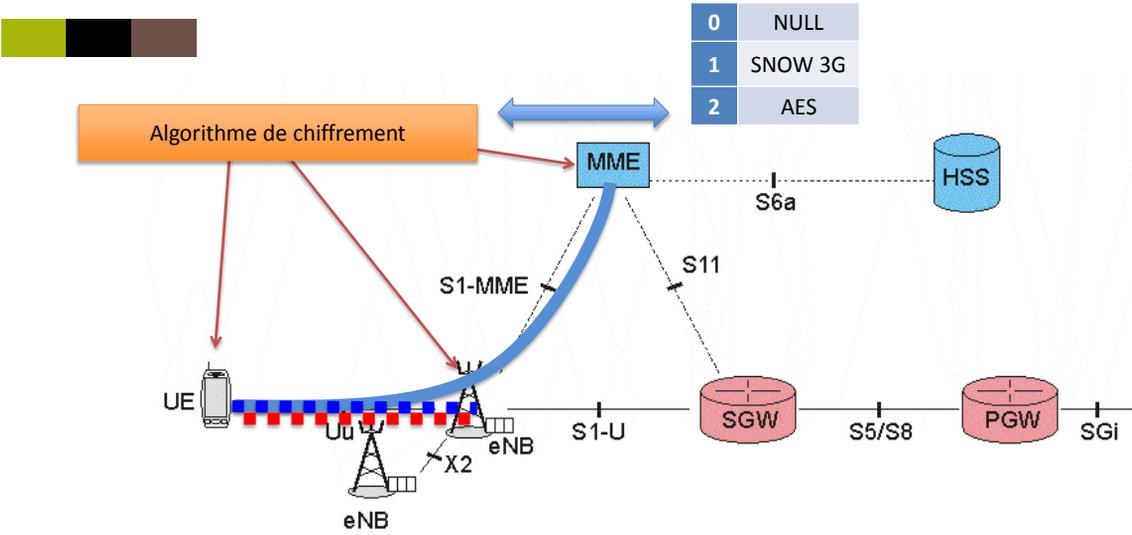
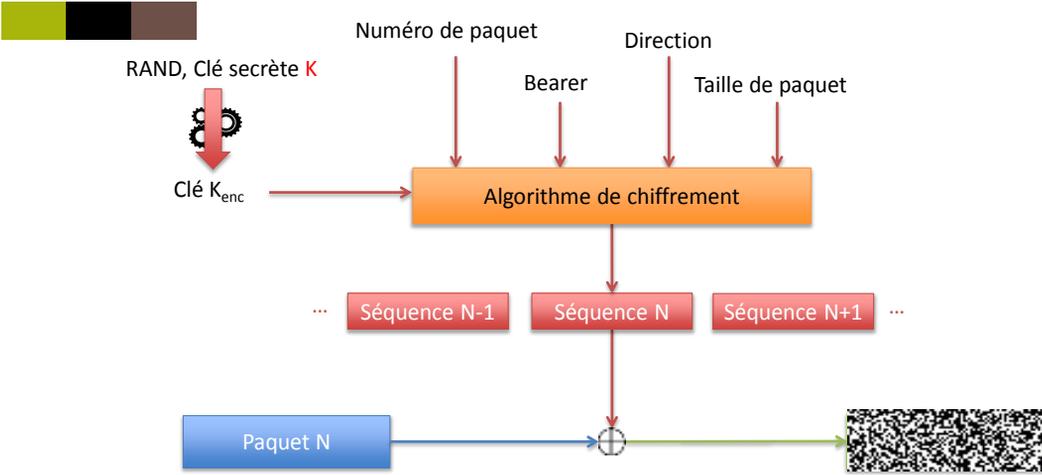


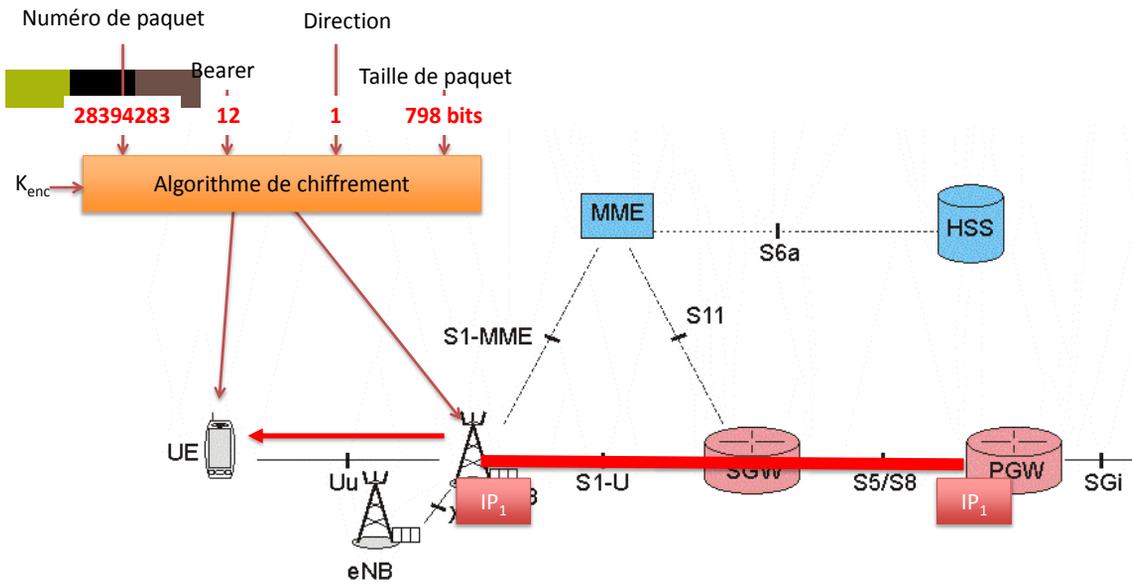
Chiffrement de données

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

Chiffrement des échanges



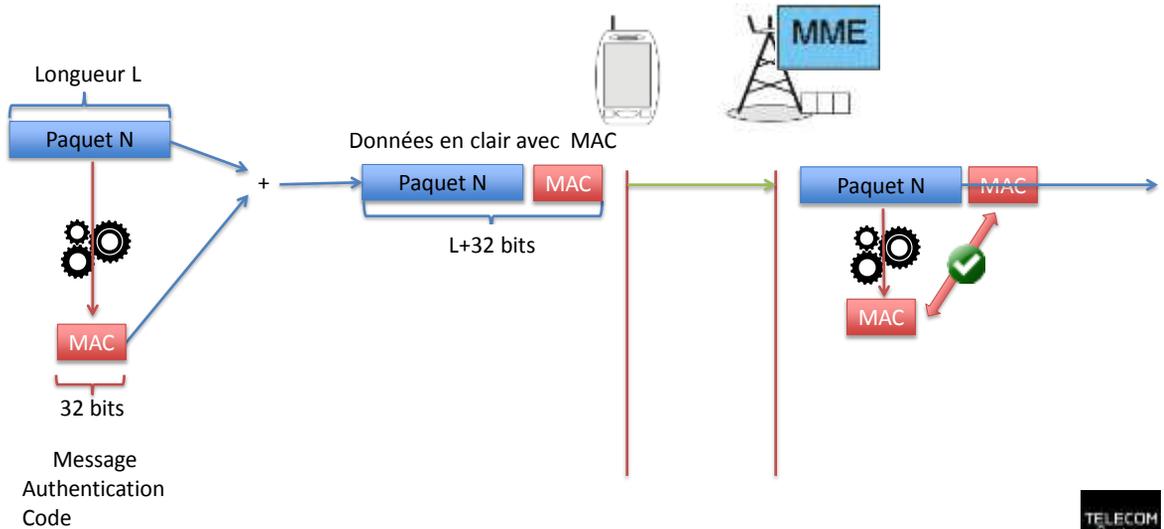




Intégrité

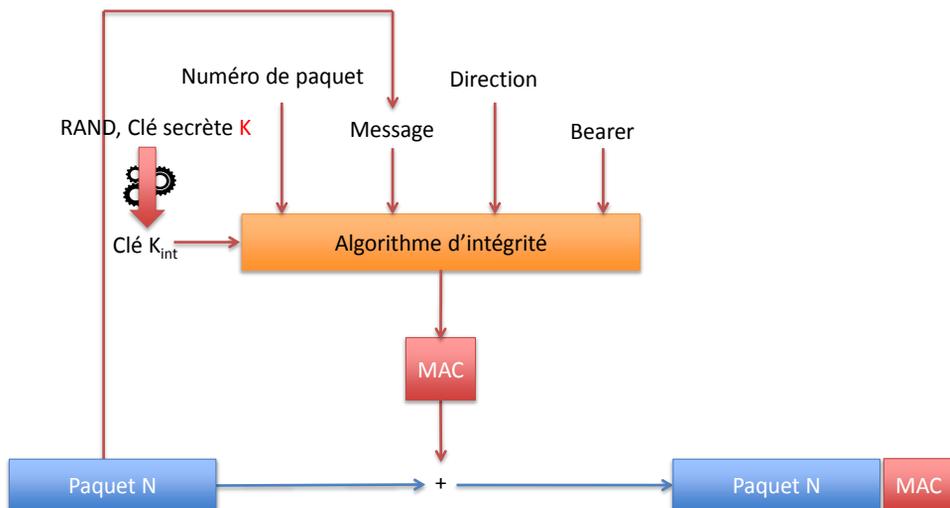
Est-ce que je peux être sûr que le message que je viens de recevoir n'a pas été modifié par un équipement intermédiaire ?

Protection contre les modifications



Institut Mines-Télécom

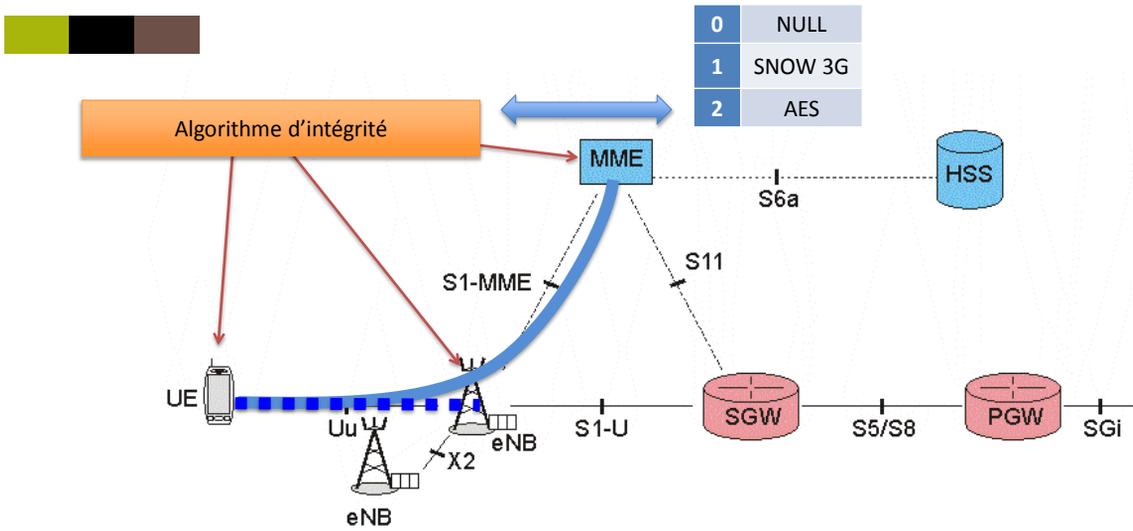
A. Pelov, Sécurité des réseaux 4G



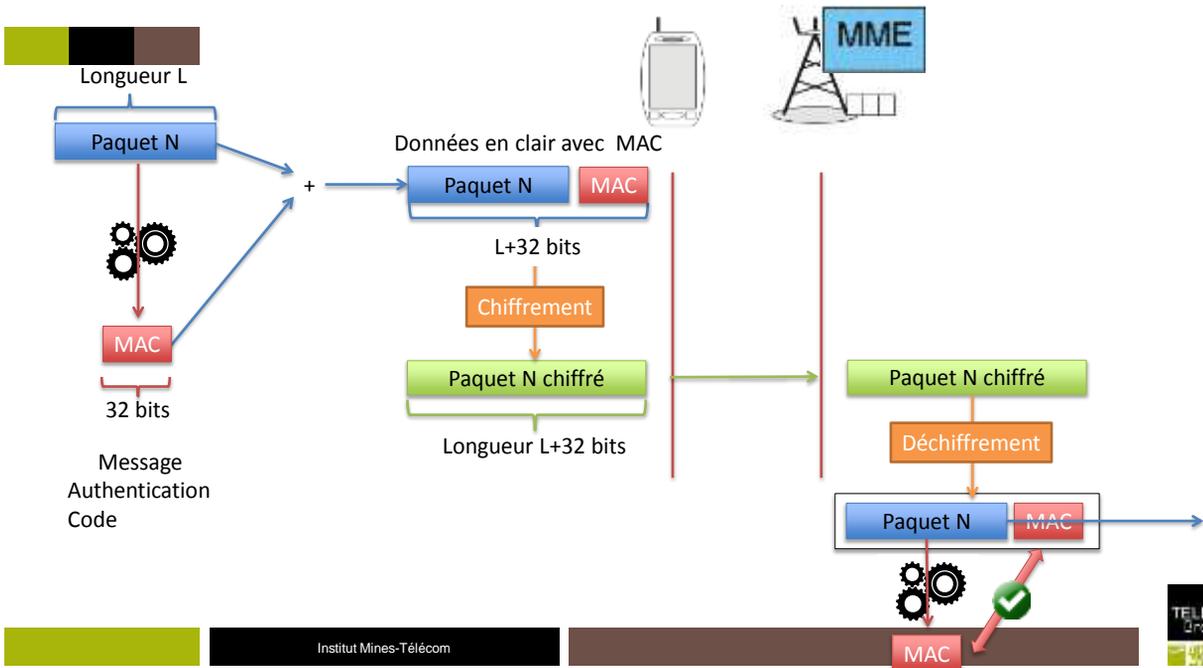
Institut Mines-Télécom

A. Pelov, Sécurité des réseaux 4G

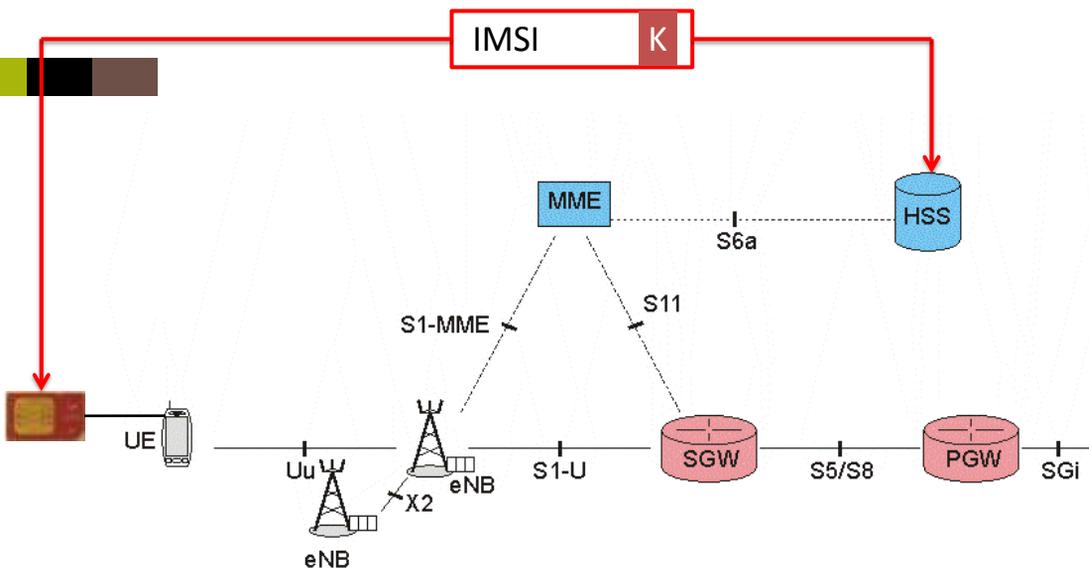


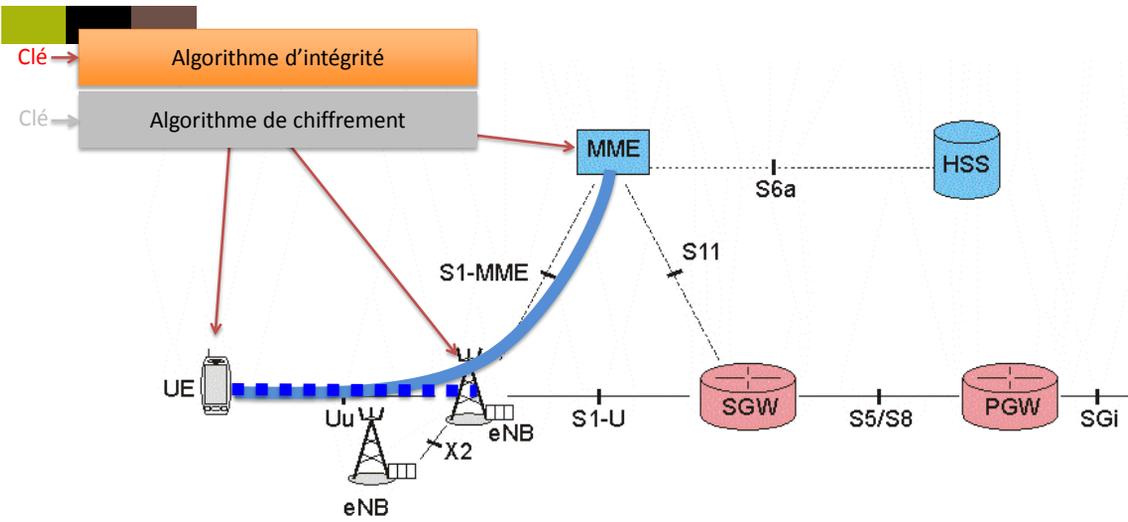
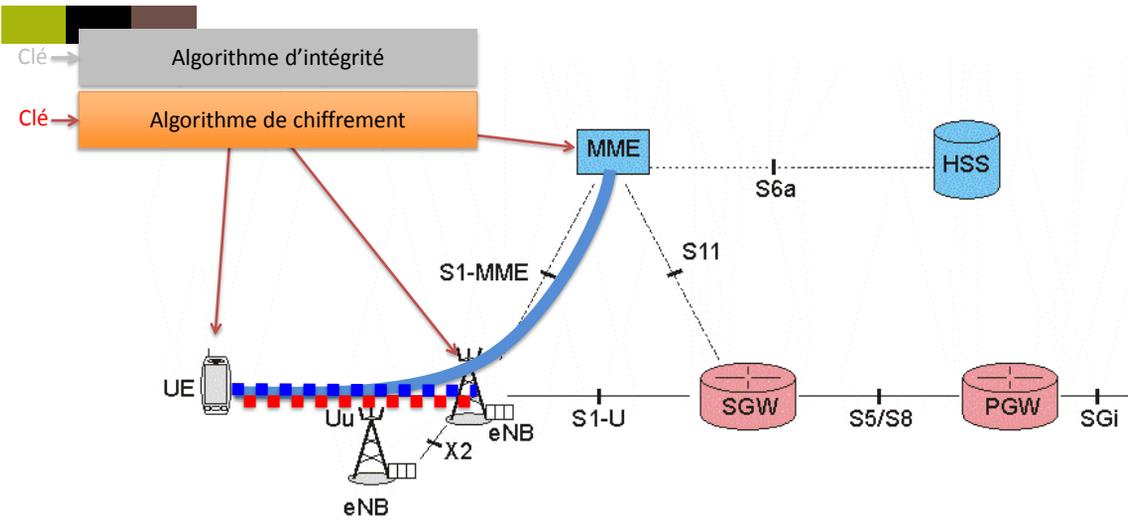


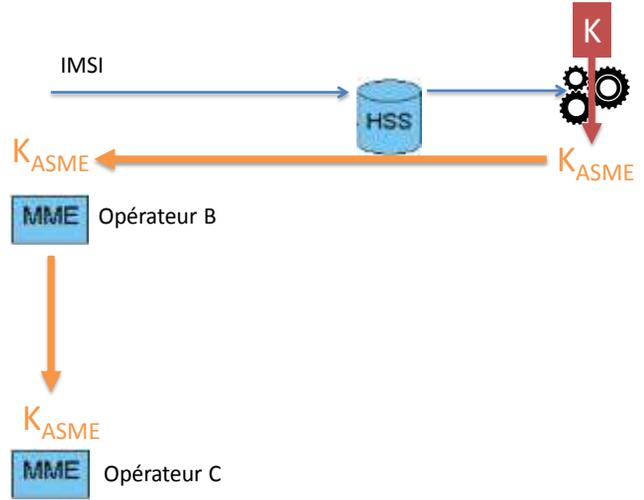
Intégrité et chiffrement



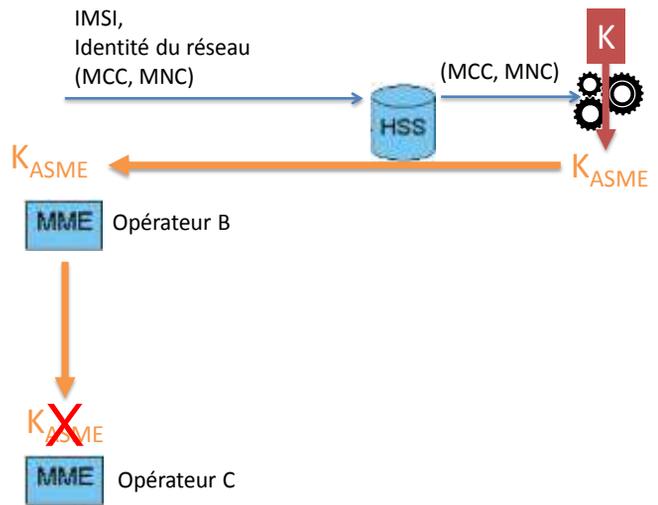
Hiérarchie de clés





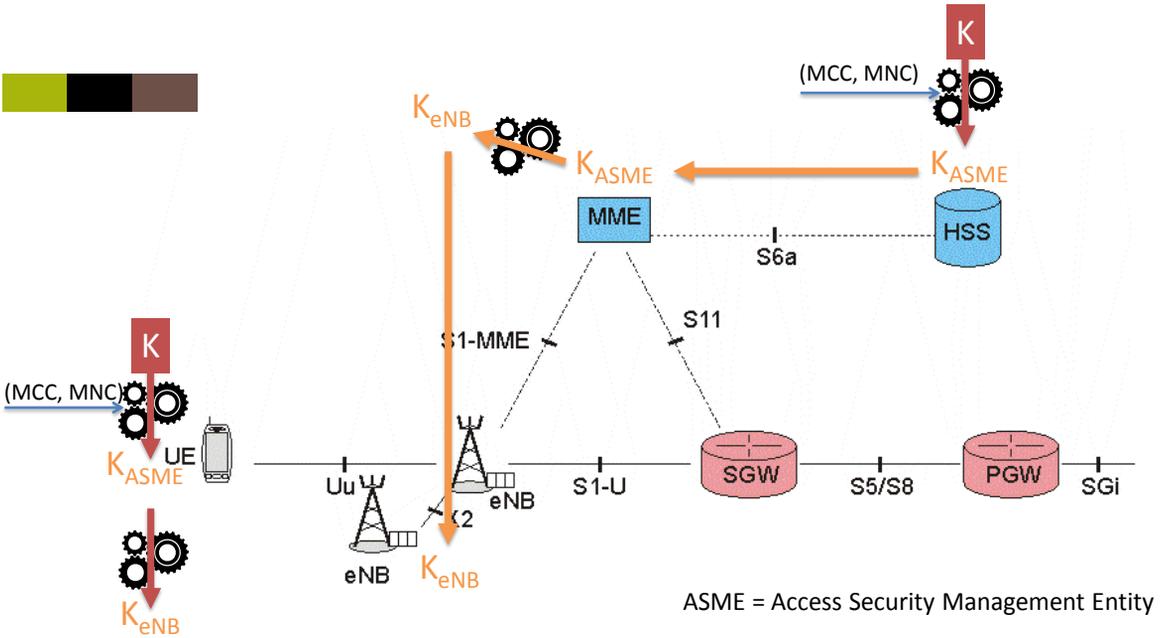


ASME = Access Security Management Entity

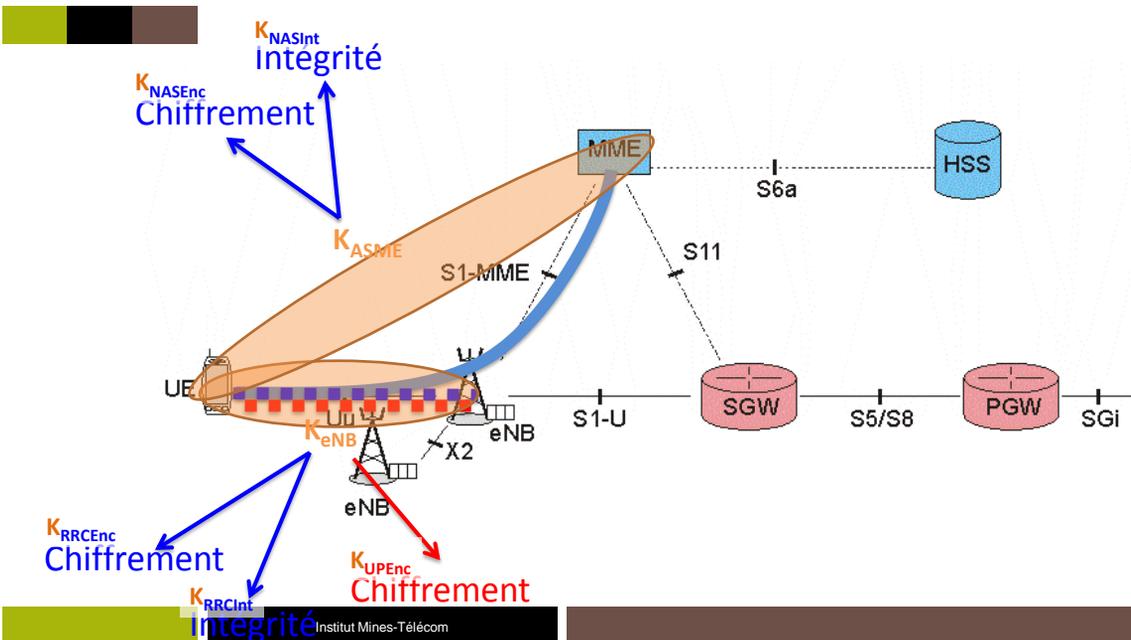


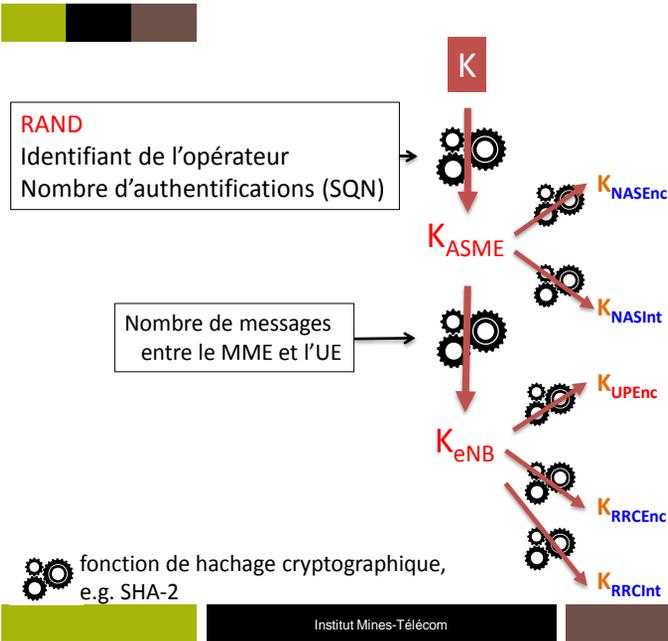
ASME = Access Security Management Entity





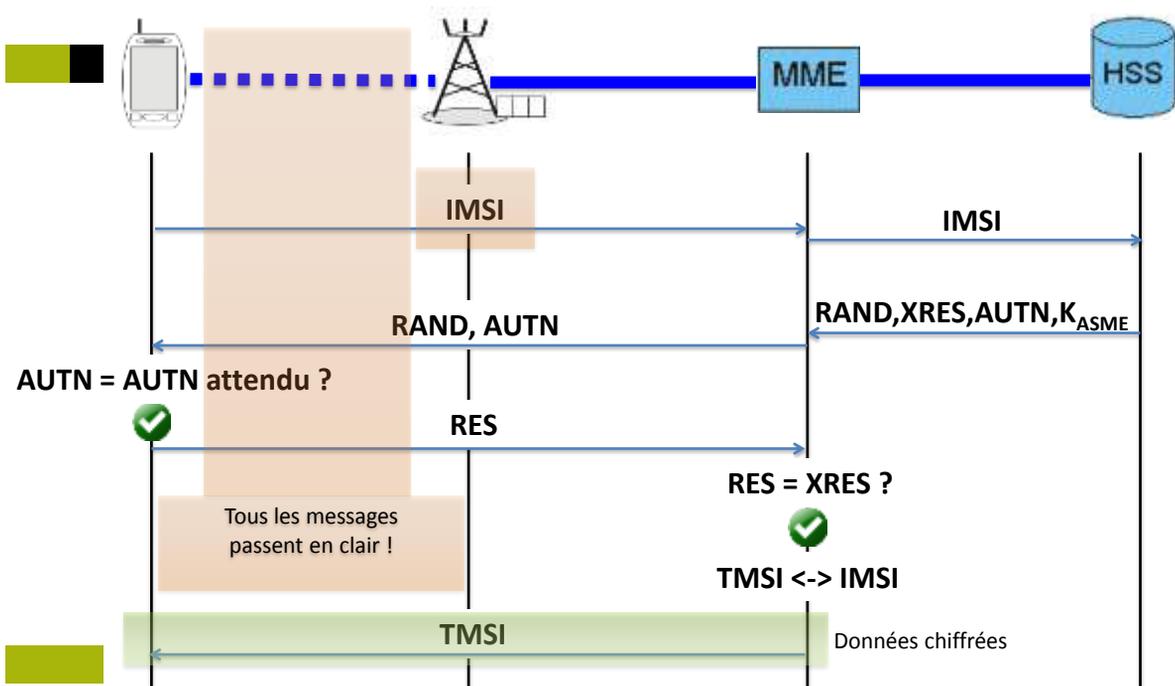
ASME = Access Security Management Entity



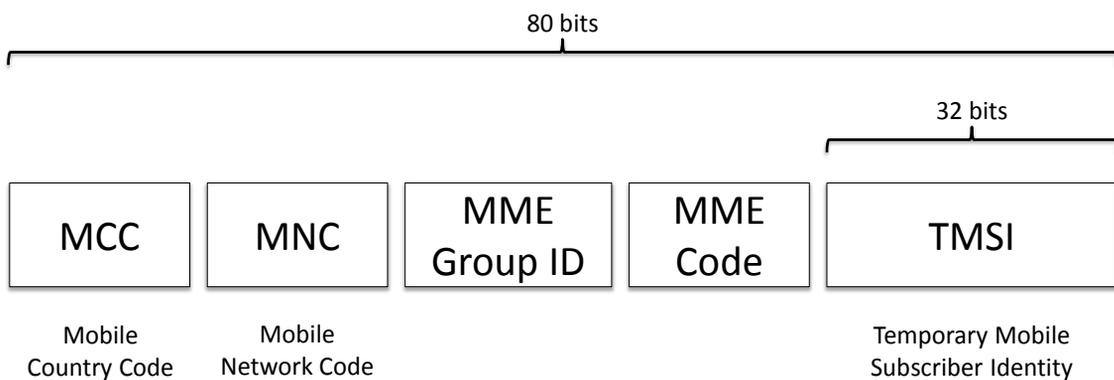


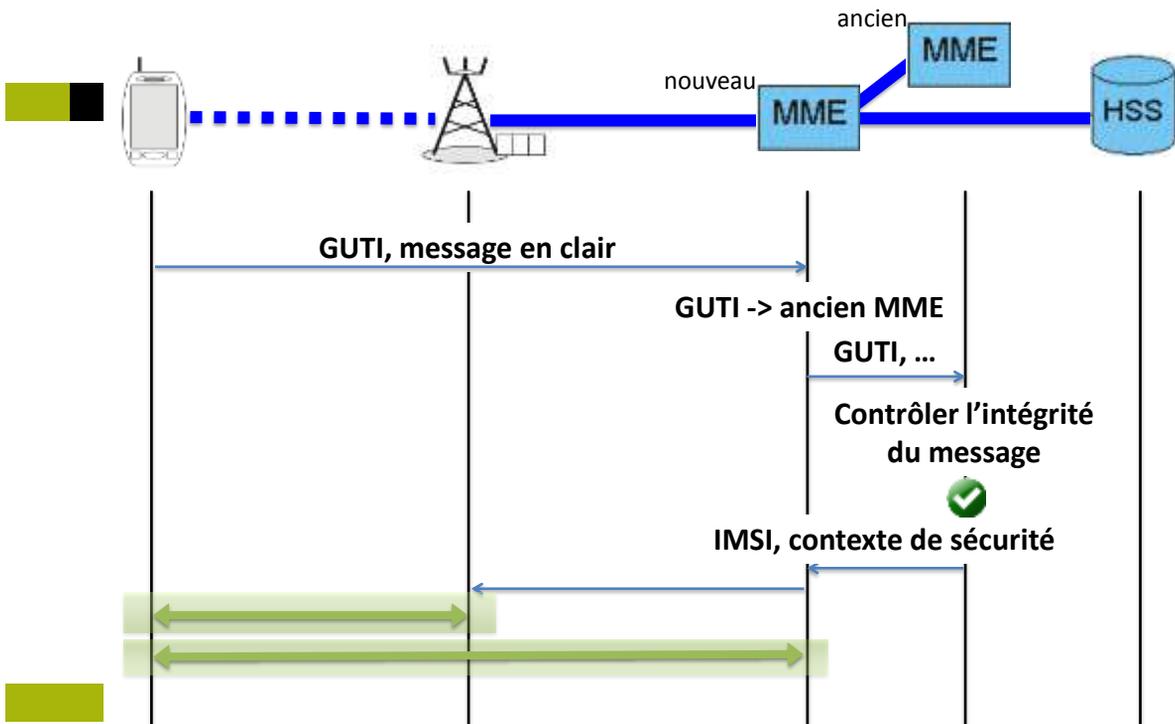
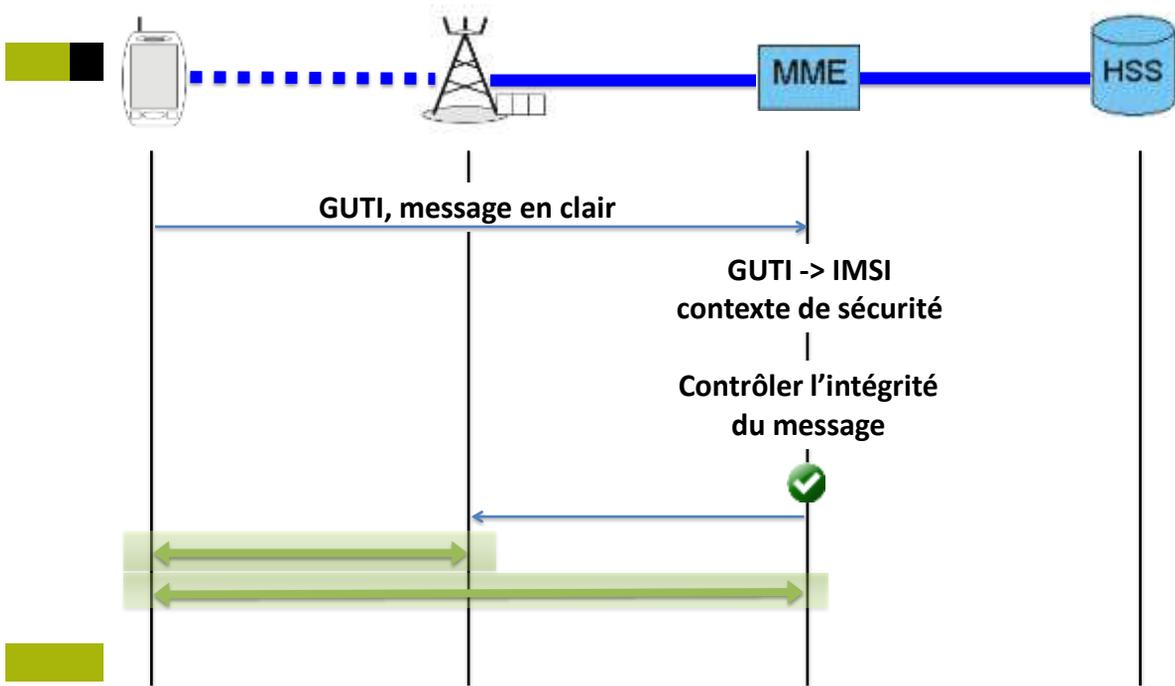
Identité temporaire

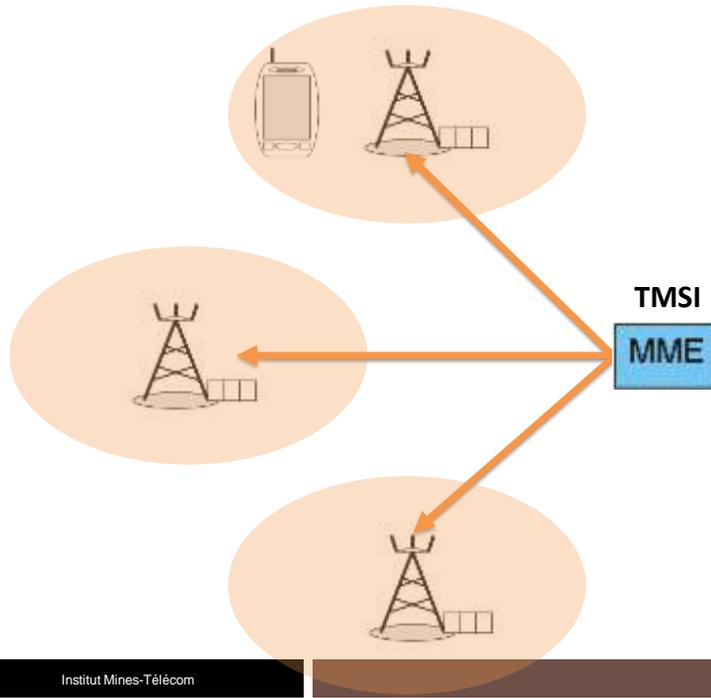
Et si quelqu'un pouvait suivre mes déplacements?
L'IMSI m'identifie d'une manière unique dans le
monde..



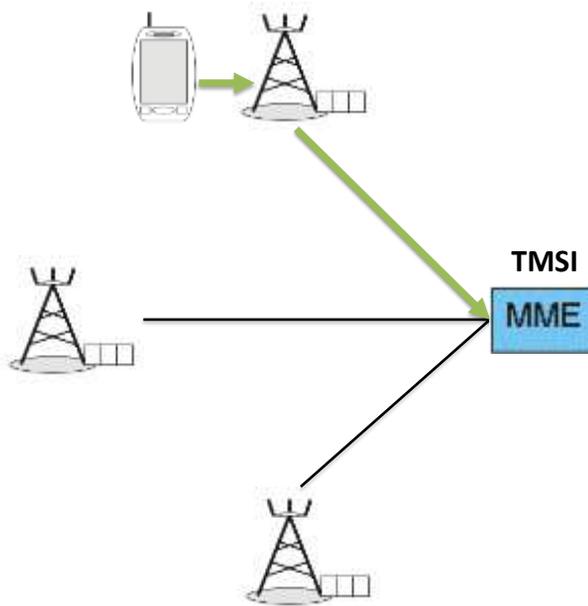
GUTI (Globally Unique Temporary UE Identity)







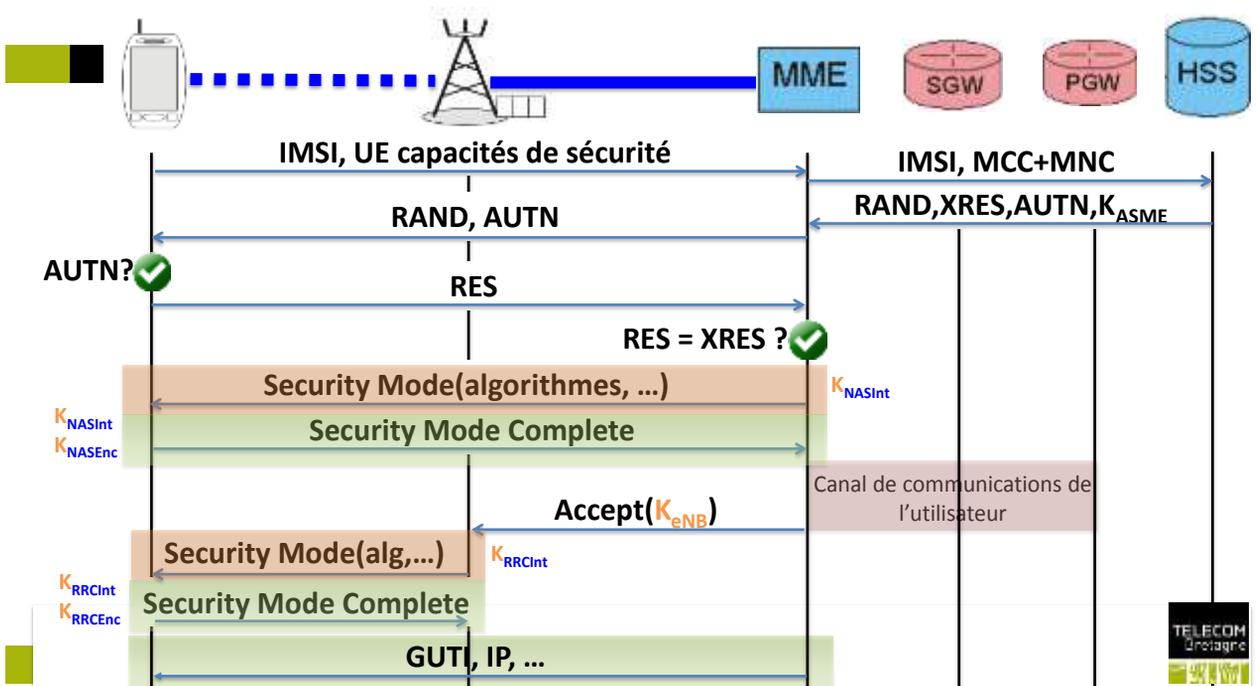
Institut Mines-Télécom

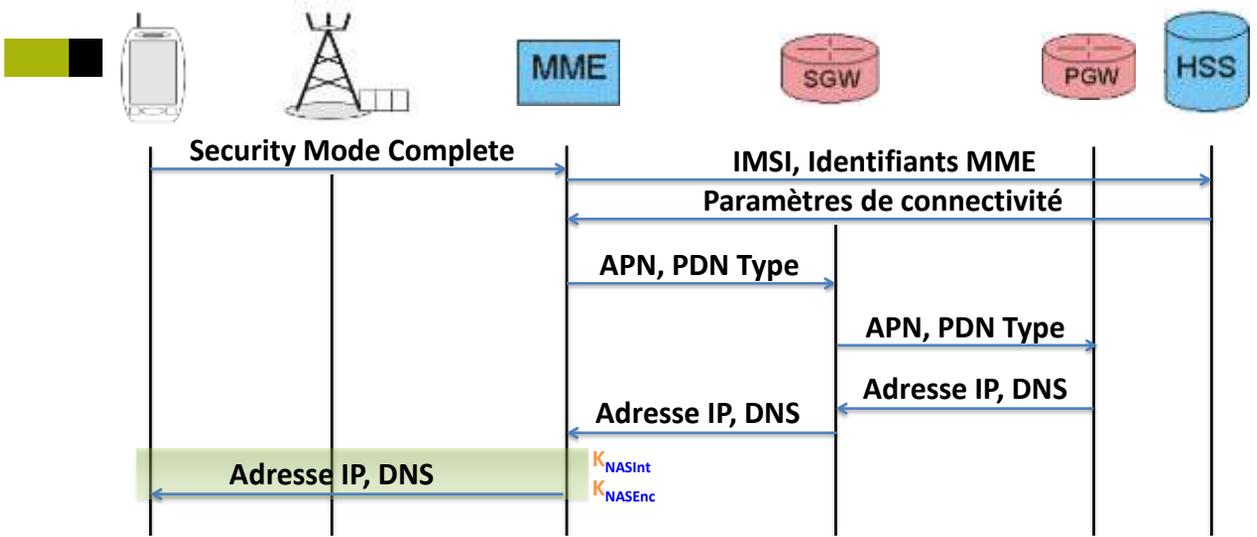


Institut Mines-Télécom



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)

