Sécurité d'un réseau mobile et responsabilité d'un opérateur

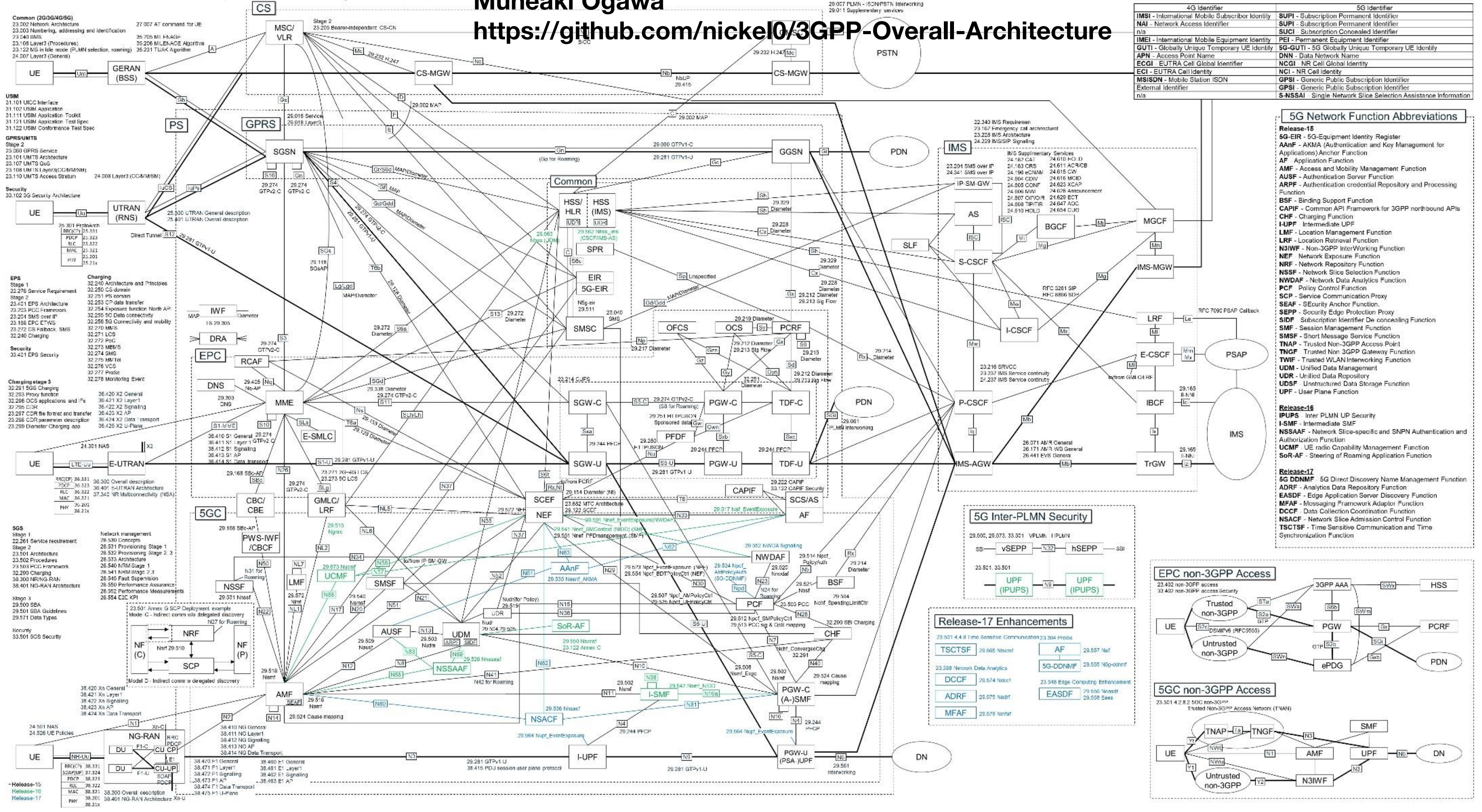
Pascal Nourry, Orange France

orange™

Orange Expert
Security

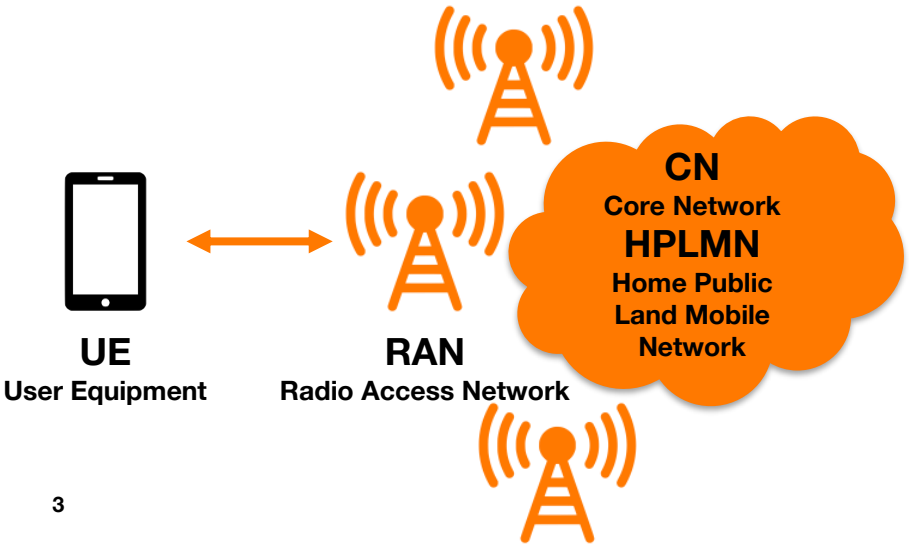
3GPP Overall Architecture and Specifications

Muneaki Ogawa
https://github.com/nickel0/3GPP-Overall-Architecture

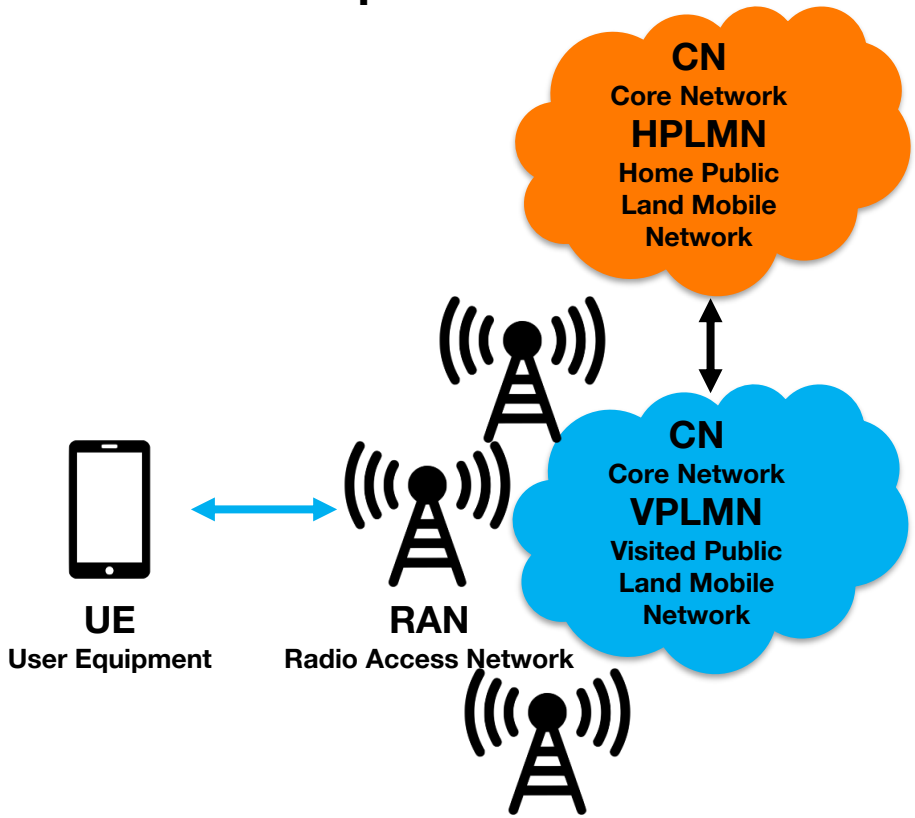


Quelques définitions (1/2)

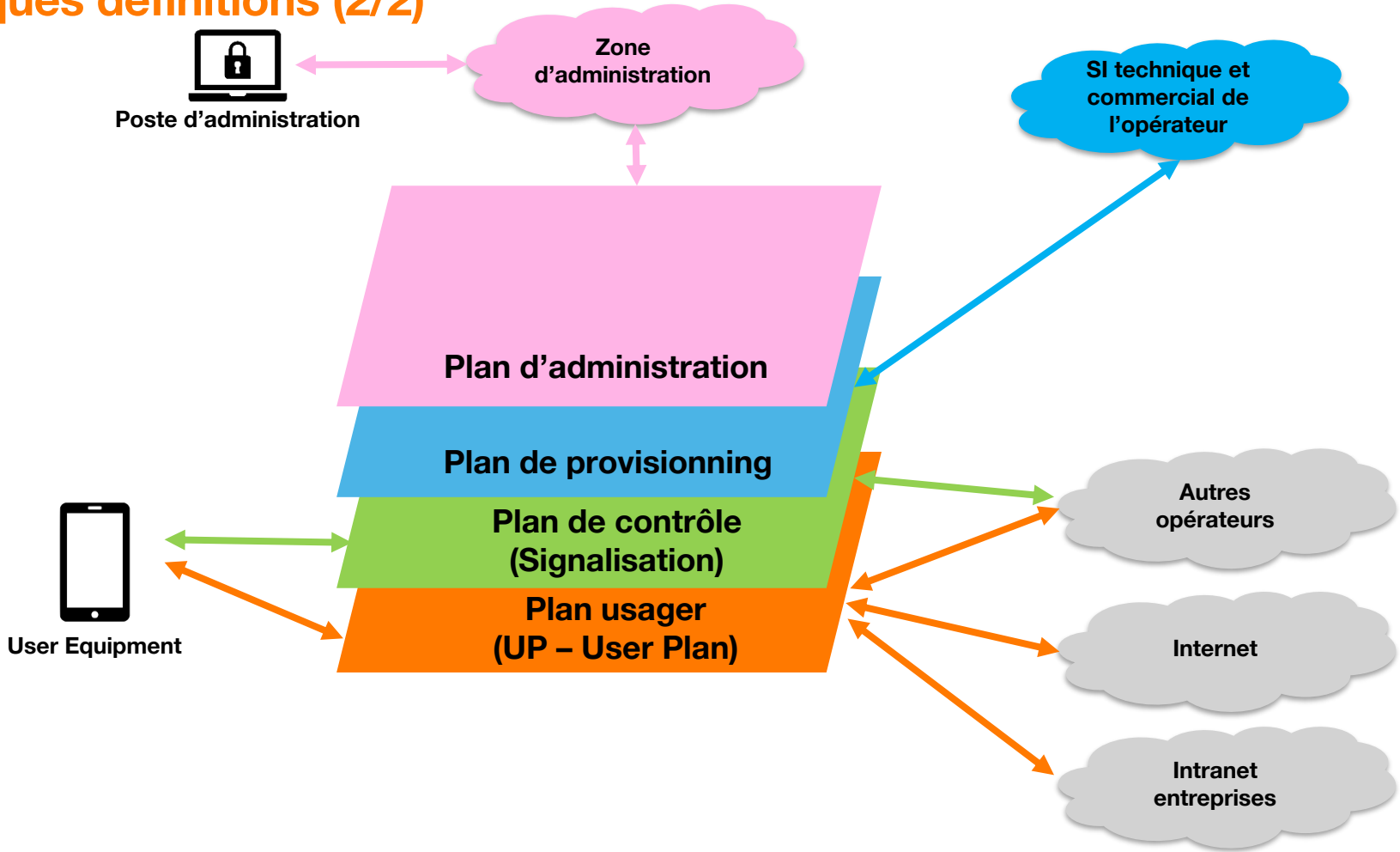
Attachement sur le réseau de son opérateur mobile



Roaming sur le réseau d'un opérateur tiers



Quelques définitions (2/2)



Quelques éléments de contexte (1/3)

Besoins croissants en disponibilité des clients des réseaux mobiles

- **Appels vers les numéros d'urgence (112, 15, 17, 18, etc.)**
- **Réseau privé pour le Ministère de l'Intérieur**
  - RRF (Réseau Radio du Futur) pour les forces de l'ordre, les pompiers, le SAMU, etc.
- **Utilisation des réseaux par les OIV (Opérateurs d'Importance Vitale), y compris dans le contexte de leurs SIIV (Systèmes d'Information d'Importance Vitale)**
  - Industrie 4.0, couverture de sites macro, etc.

Contexte géopolitique

- **Opérations de renseignement**
  - Vodafone Greece, Belgacom
- **Tensions entre les pays de l'OTAN d'un côté, la Chine et la Russie de l'autre**
  - Question de souveraineté (ex : interdiction des équipements réseaux Huawei/ZTE aux US)
- **Nouveau théâtre d'opération militaire**
  - Compromission de KA-SAT concomitant à l'invasion de l'Ukraine par la Russie

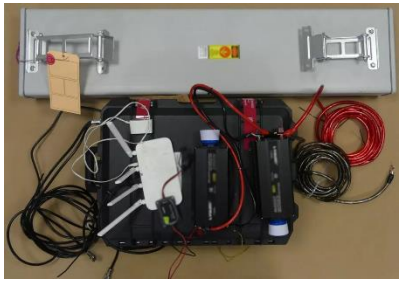
Quelques éléments de contexte (2/3)

Contexte réglementaire

- **Sécurité des réseaux**
  - CPCE- Code des Postes et des Communications Electroniques
  - Code de la Défense (SAIV – Secteur d'Activité d'Importante Vitale - Communications Electroniques)
- **Protection des données personnelles**
  - Facture détaillée des appels, données de connexion, géolocalisation, etc.
- **Secret des correspondances (autorisations R.226-3/-7 code pénal)**
- **Techniques de renseignement (code de sécurité intérieur, CPCE)**
- **LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles**
  - Autorisations « 5G » préalable à l'exploitation de fonctions 5G par les OIV
- **A venir**
  - Projet de Loi de Programmation Militaire 2024-2030
  - Directives européennes NIS2 (Network and Information Security) et CER (Critical Entities Resilience) qui doivent être transposées en droit français avant octobre 2024
  - Projet de directive européenne CRA (Cyber Resilience Act)

Quelques éléments de contexte (3/3)

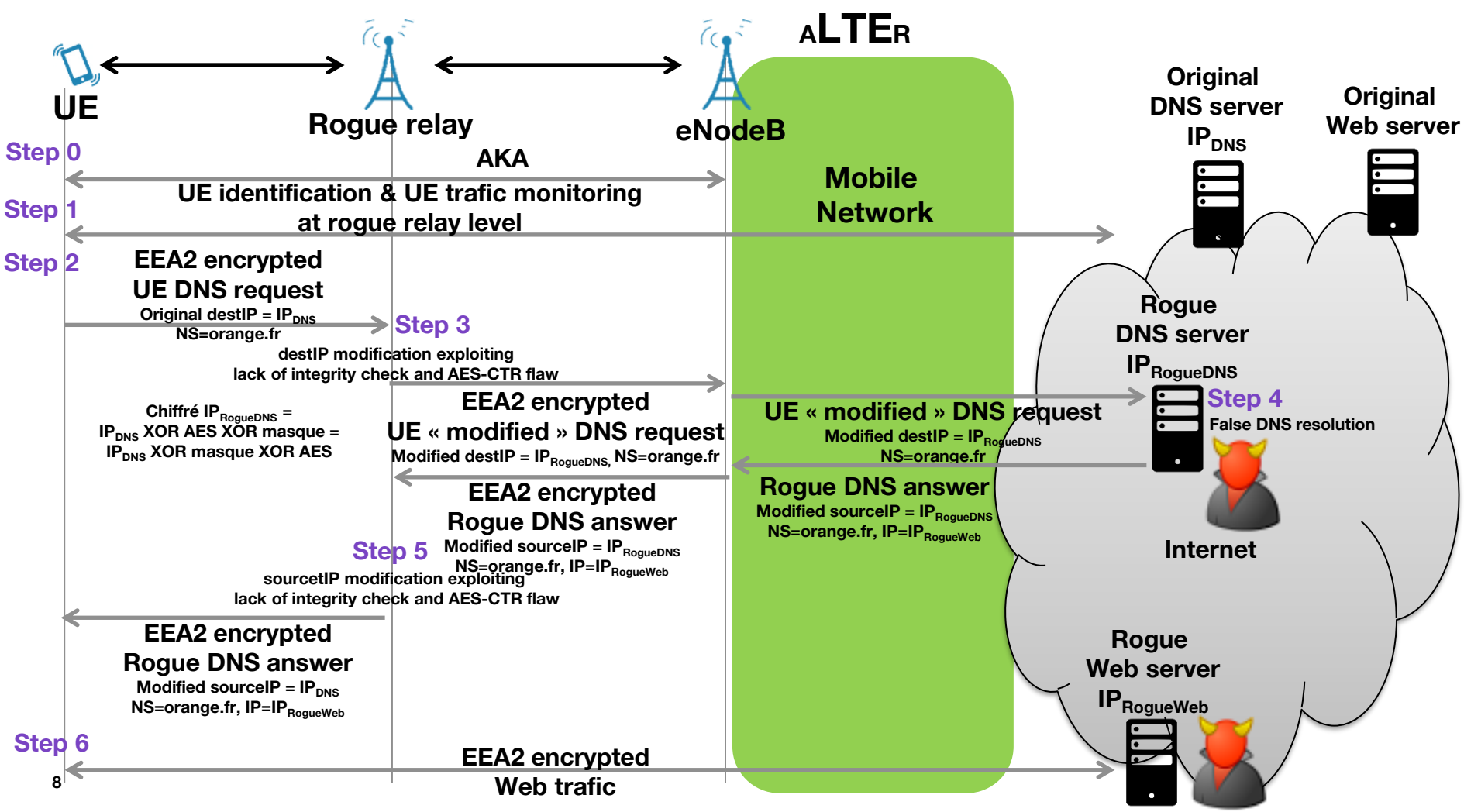
30/12/2022, Paris



18/02/2023, Paris
(source = SIRPA Gendarmerie)

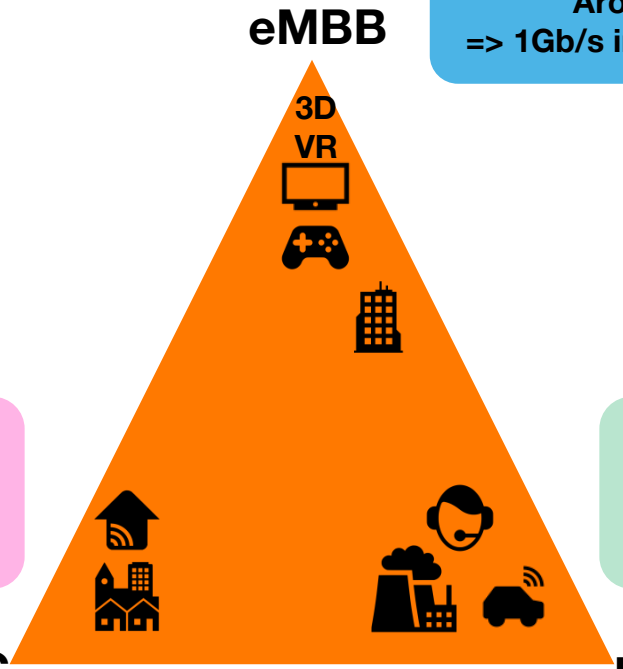
Vulnérabilités des réseaux mobiles 2G/3G/4G

- **Identité des UE passe en clair sur la voix radio**
  - IMSI Catcher
  - SMSBlaster utilisé pour l'envoie de SMS malveillants
- **Absence d'authentification de l'UE au niveau du HPLMN en cas de roaming**
  - Utilisation malveillante des interco entre opérateurs pour certains scénarios de détournement de trafic, notamment SMS
- **Absence de protection de la signalisation sur le cœur de réseau**
  - Risque d'écoute ou d'altération
- **Absence de contrôle d'intégrité sur la voix radio/data**
  - Attaque ALTER (https://alter-attack.net/)


ALTER
UE
Rogue relay
eNodeB
Mobile Network
Original DNS server IPDNS
Original Web server
Step 0
AKA
Step 1
UE identification & UE trafic monitoring at rogue relay level
Step 2
EEA2 encrypted UE DNS request
Original destIP = IPDNS
NS=orange.fr
Step 3
destIP modification exploiting lack of integrity check and AES-CTR flaw
Chiffré IPRogueDNS = IPDNS XOR AES XOR masque = IPDNS XOR masque XOR AES
EEA2 encrypted UE « modified » DNS request
Modified destIP = IPRogueDNS, NS=orange.fr
UE « modified » DNS request
Modified destIP = IPRogueDNS
NS=orange.fr
Rogue DNS server IPRogueDNS
Step 4
False DNS resolution
Rogue DNS answer
Modified sourceIP = IPRogueDNS
NS=orange.fr, IP=IPRogueWeb
EEA2 encrypted Rogue DNS answer
Modified sourceIP = IPRogueDNS
NS=orange.fr, IP=IPRogueWeb
Step 5
sourcetIP modification exploiting lack of integrity check and AES-CTR flaw
Internet
EEA2 encrypted Rogue DNS answer
Modified sourceIP = IPDNS
NS=orange.fr, IP=IPRogueWeb
Rogue Web server IPRogueWeb
Step 6
EEA2 encrypted Web trafic

Promesses de la 5G

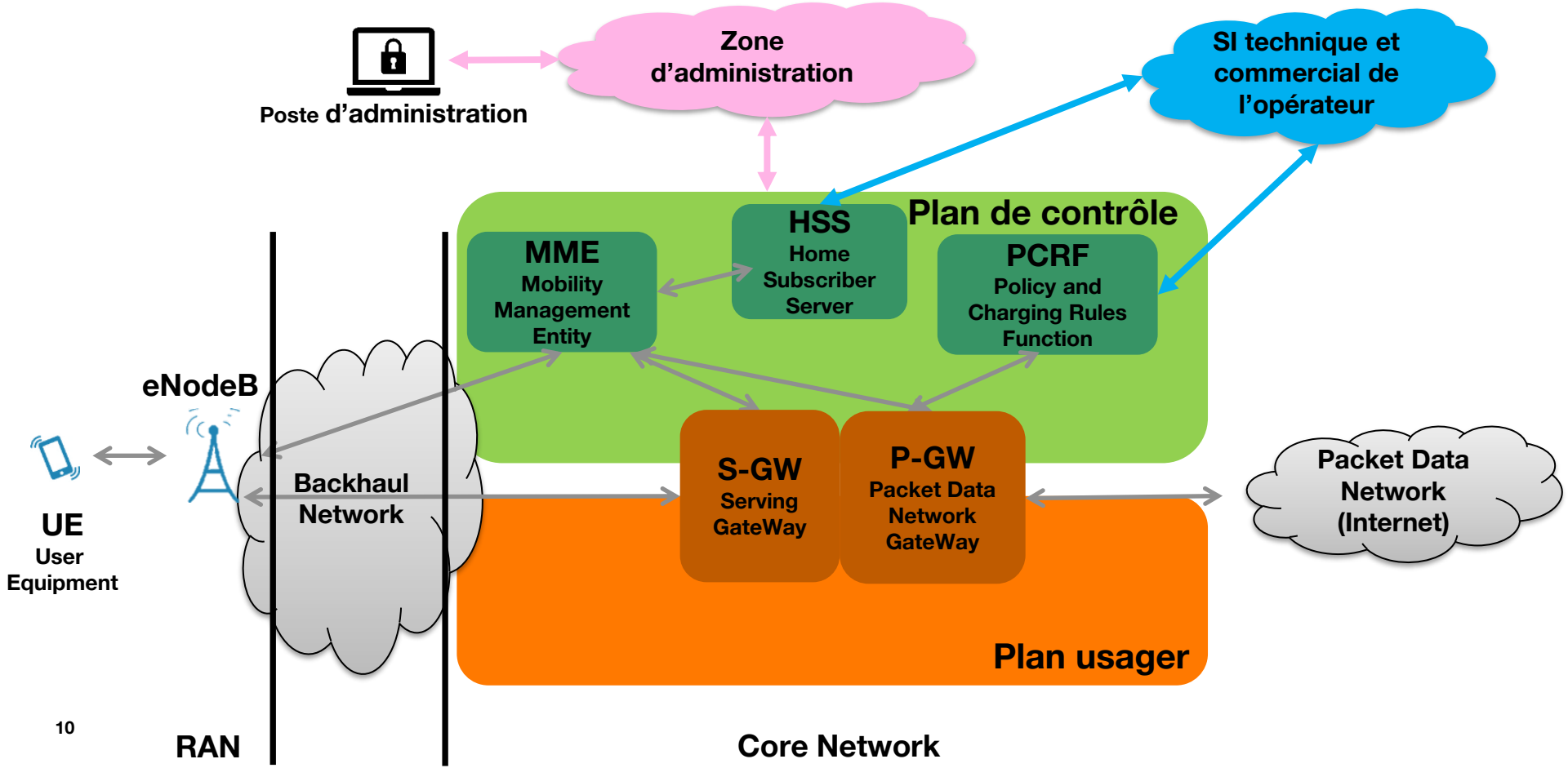
enhanced Mobile BroadBand
Around 100 Mb/s in 4G
=> 1Gb/s in 5G (10 Gb/s in long term)



massive Machine Type Communications
Low power consumption (10 years) and x100 more devices

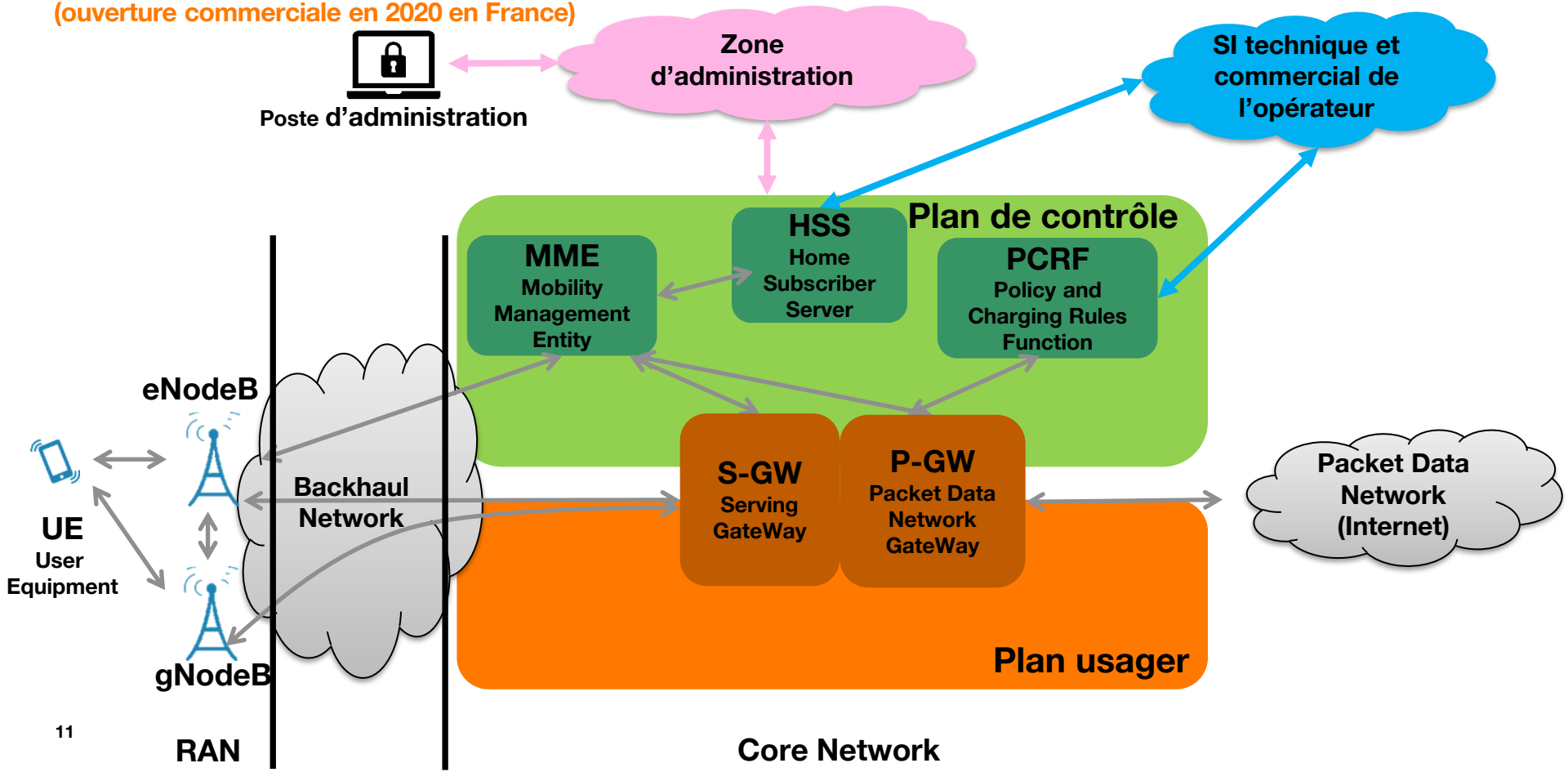
ultra Reliable & Low Latency Communications
40ms (4G) => 1ms (5G)

Principes 4G



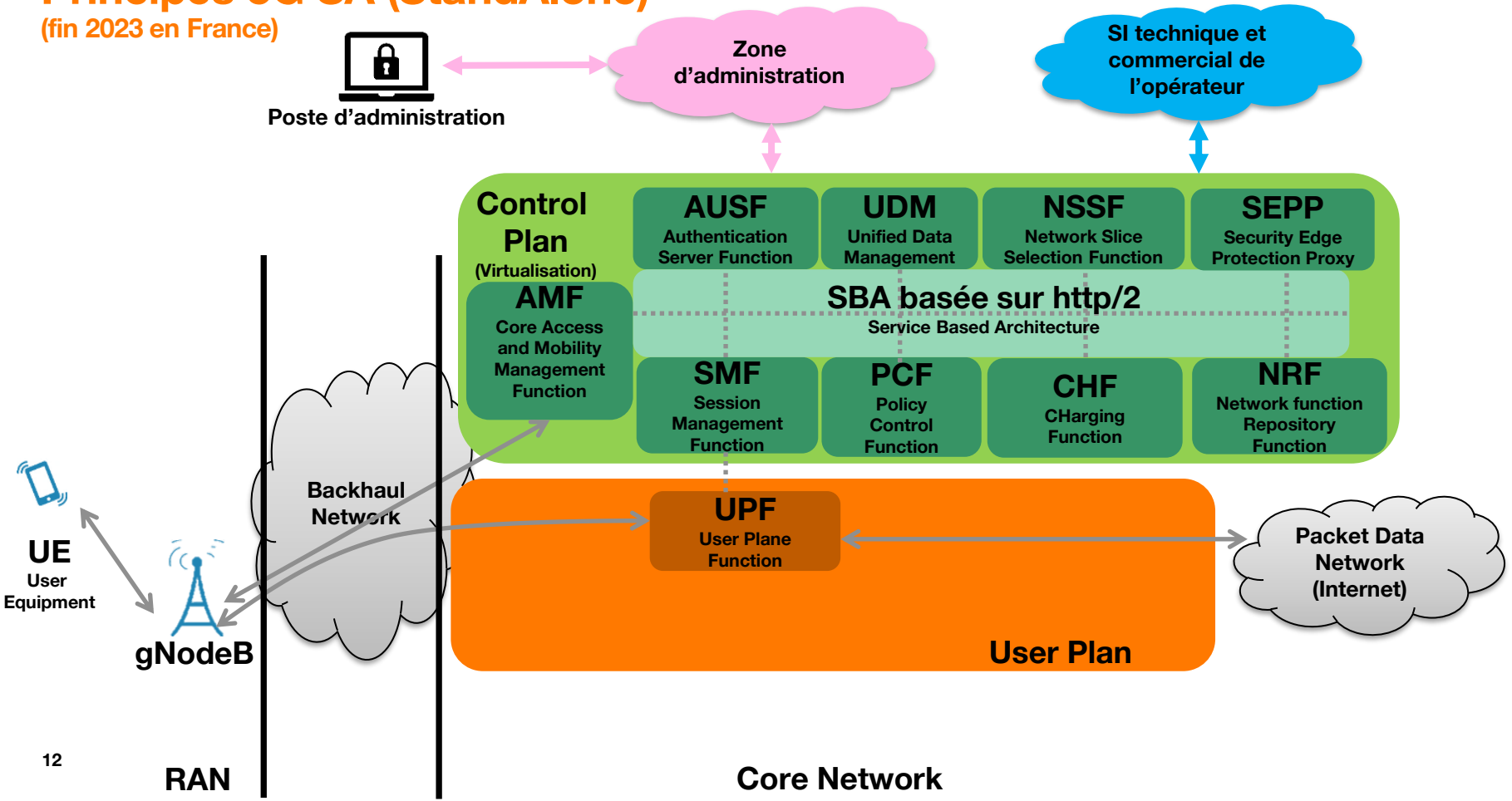
Principes 5G NSA (Non StandAlone) - option 3X

(ouverture commerciale en 2020 en France)

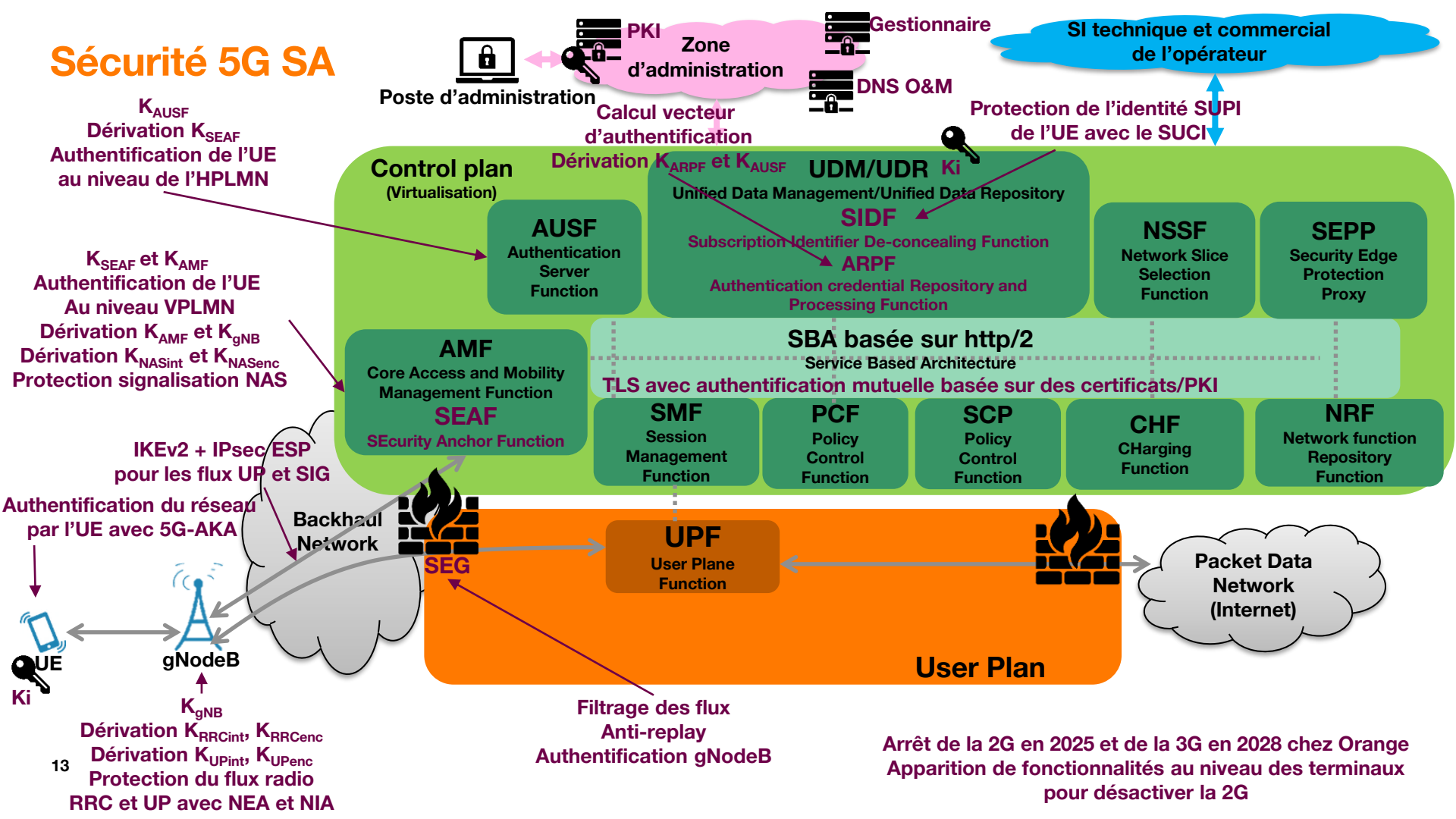


Principes 5G SA (StandAlone)

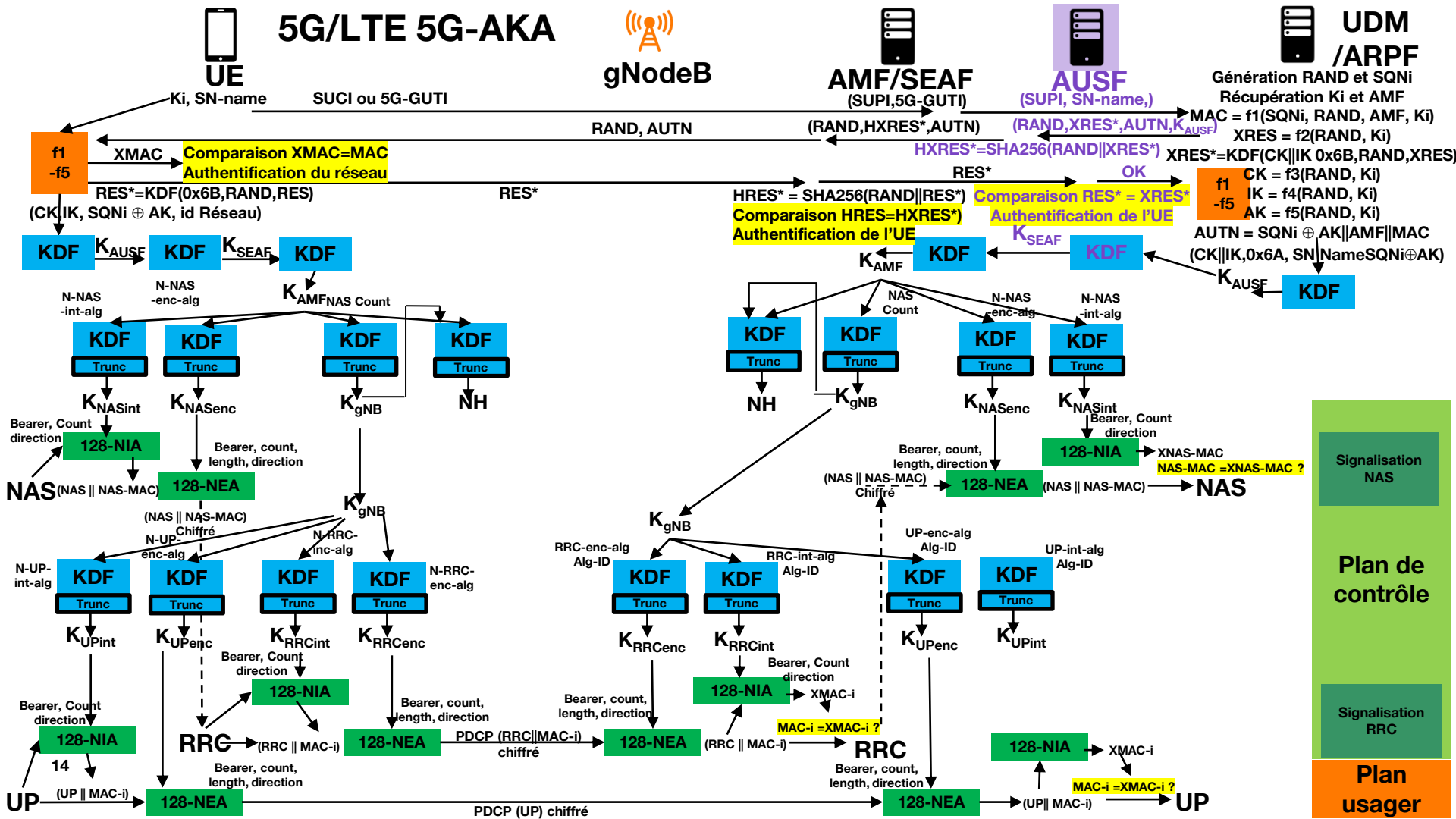
(fin 2023 en France)



Sécurité 5G SA



Arrêt de la 2G en 2025 et de la 3G en 2028 chez Orange
Apparition de fonctionnalités au niveau des terminaux pour désactiver la 2G


5G/LTE 5G-AKA
UE
gNodeB
AMF/SEAF
AUSF
UDM /ARPF
Ki, SN-name
SUCI ou 5G-GUTI
(SUPI,5G-GUTI)
(SUPI, SN-name,)
Génération RAND et SQNi
Récupération Ki et AMF
RAND, AUTN
(RAND,HXRES*,AUTN)
(RAND,XRES*,AUTN,K_AUSF)
MAC = f1(SQNi, RAND, AMF, Ki)
XRES = f2(RAND, Ki)
HXRES*=SHA256(RAND||XRES*)
XRES*=KDF(CK||IK 0x6B,RAND,XRES)
f1 -f5
XMAC
Comparaison XMAC=MAC
Authentification du réseau
RES*
OK
CK = f3(RAND, Ki)
IK = f4(RAND, Ki)
AK = f5(RAND, Ki)
RES*=KDF(0x6B,RAND,RES)
RES*
HRES* = SHA256(RAND||RES*)
Comparaison HRES=HXRES*)
Authentification de l'UE
Comparaison RES* = XRES*
Authentification de l'UE
AUTN = SQNi ⊕ AK||AMF||MAC
(CK,IK, SQNi ⊕ AK, id Réseau)
(CK||IK,0x6A, SN_NameSQNi⊕AK)
KDF
K_AUSF
K_SEAF
K_AMF
NAS Count
N-NAS -int-alg
N-NAS -enc-alg
K_AMFNAS Count
Trunc
K_NASint
K_NASenc
K_gNB
NH
Bearer, Count direction
128-NIA
Bearer, count, length, direction
128-NEA
NAS
(NAS || NAS-MAC)
XNAS-MAC
NAS-MAC =XNAS-MAC ?
Chiffré
N-UP-enc-alg
N-RRC-inc-alg
N-UP-int-alg
N-RRC-enc-alg
K_UPint
K_UPenc
K_RRCint
K_RRCenc
RRC-enc-alg Alg-ID
RRC-int-alg Alg-ID
UP-enc-alg Alg-ID
UP-int-alg Alg-ID
XMAC-i
MAC-i =XMAC-i ?
RRC
(RRC || MAC-i)
PDCP (RRC||MAC-i) chiffré
14
UP
(UP || MAC-i)
PDCP (UP) chiffré
Signalisation NAS
Plan de contrôle
Signalisation RRC
Plan usager

Sécurité 5G SA

Côté opérateur

- **Prise en compte de la sécurité de bout en bout**
  - Politique de sécurité 5G dès 2020
    - Définit la cible à atteindre
  - Analyse de risque EBIOS-RM sur chacun des composants 5G

Sécurité 5G SA

Côté opérateur

- **Prise en compte de la sécurité de bout en bout**
  - Haute disponibilité locale + Redondance géographique multisites
  - Durcissement système, virtualisation et applicatif avec les fournisseurs
    - Utilisation de HSM (Hardware Secure Module)
    - Chiffrement systématique y compris pour les flux internes
  - Activation de toutes les options de sécurité activables 3GPP
    - Chiffrement du SBA avec déploiement de la PKI Orange
  - Focus particulier sur la chaîne d'administration
    - PC d'administration
    - Zone d'hébergement dédiée pour les outils d'administration
    - Bastion (flux web et flux en ligne de commande)
    - Stockage des secrets
    - VPNs dédiés à l'administration des différentes ressources 5G

Sécurité 5G SA

Côté opérateur

- **Prise en compte de la sécurité de bout en bout**
  - Audits techniques internes sur l'ensemble des composants 5G et de la chaine d'administration
  - Analyse des dossiers techniques de demande d'autorisation L34-11 par l'ANSSI
  - Audits par l'ANSSI du cœur 5G et de la chaine d'administration

Et après ?

Travaux préliminaire en cours pour définir l'après 5G

- **Plusieurs projets sont lancés au niveau européen**

Définition des objectifs pour la 6G à horizon 2025

- **Chantier spécifique sur la cryptographie post-quantique**
- **Probablement une stabilisation du nouveau cœur 5G avec des améliorations/optimisations**

Merci