# La signalisation chez les opérateurs mobiles

2022 - SSTIC - Benoit Michau, Marin Moulinier
P1 Security

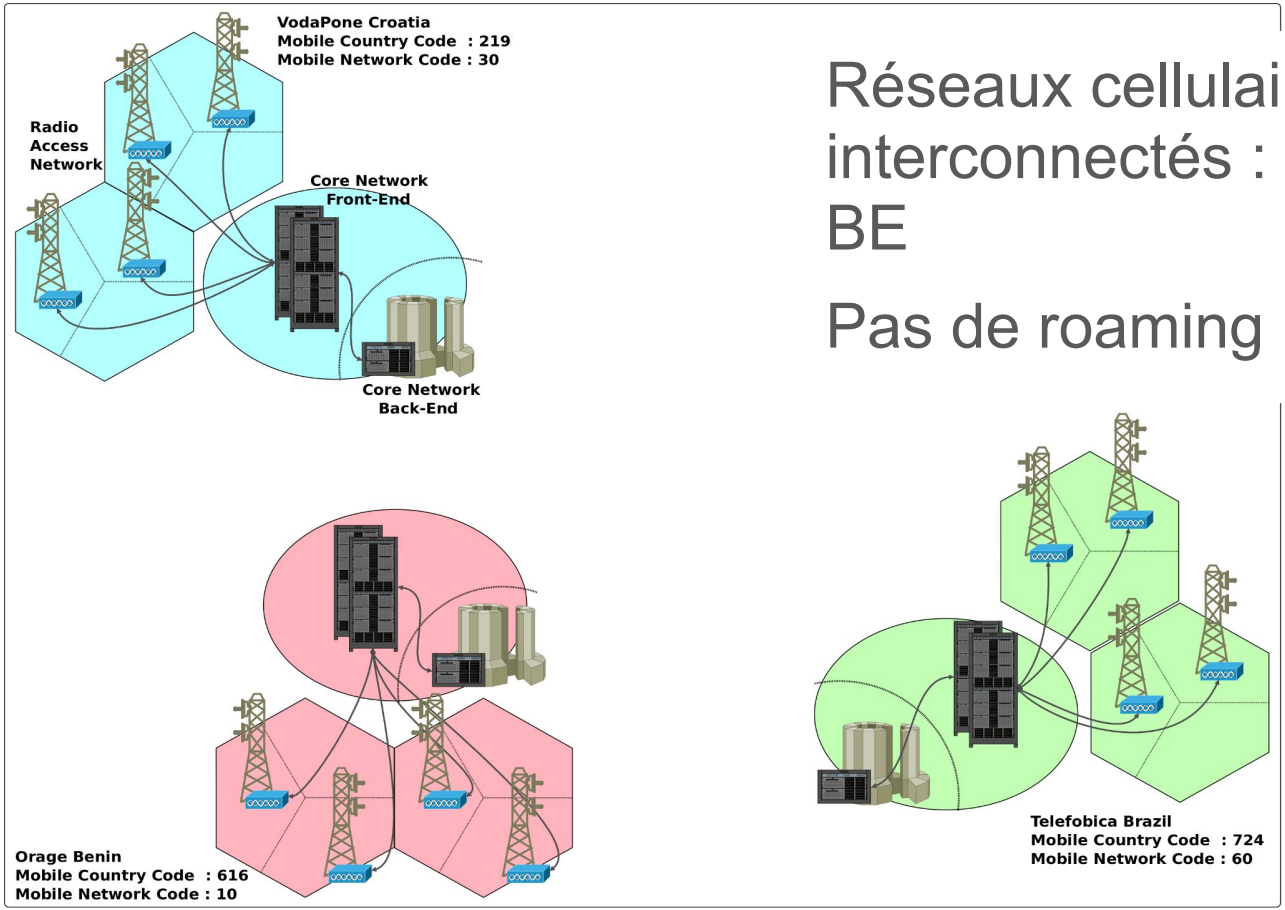
# La signalisation, qu'est-ce que c'est ?

- Étymologiquement, le fait de transmettre l'information sous forme de **signaux** (de **codes**)
  - Exemples de signalisation :
    - La signalisation au sens biologique :
      - Signalisation cellulaire/intracellulaire
      - Signalisation chimique : endocrine…
    - La signalisation sur les réseaux terrestres :
      - Signalisation ferroviaire
      - Signalisation aérienne/maritime
      - Signalisation routière

# La signalisation des réseaux mobiles, qu'est-ce que c'est ?

- En télécommunications, le trafic de **signalisation**, qui s'oppose au trafic de **données**, concerne :
  - L'attachement d'un abonné à un réseau
    - Identification, authentification, localisation de l'abonné (IMSI)
    - Identification du terminal (IMEI)
  - L'initiation et le routage des appels, des SMS, des connexions de données
  - La gestion de la mobilité d'un abonné : rester connecté et joignable
    - Au sein d'un réseau
    - Entre réseaux opérateurs : **roaming** (itinérance)
- Signalisation mobile : données à caractère **personnel**

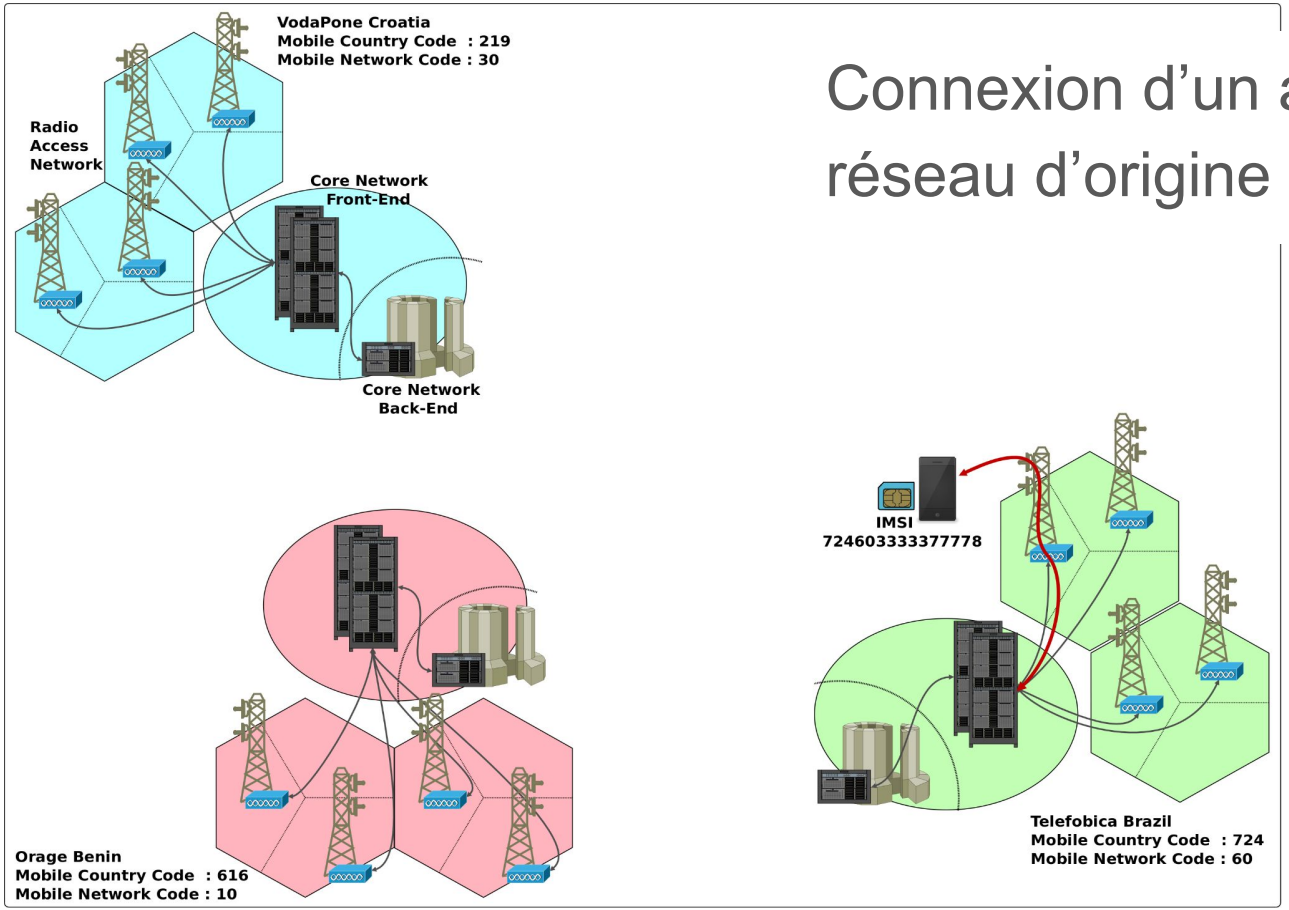
# Connexion d’un abonné mobile (1/3)




Réseaux cellulaires non interconnectés : RAN, CN FE, CN BE

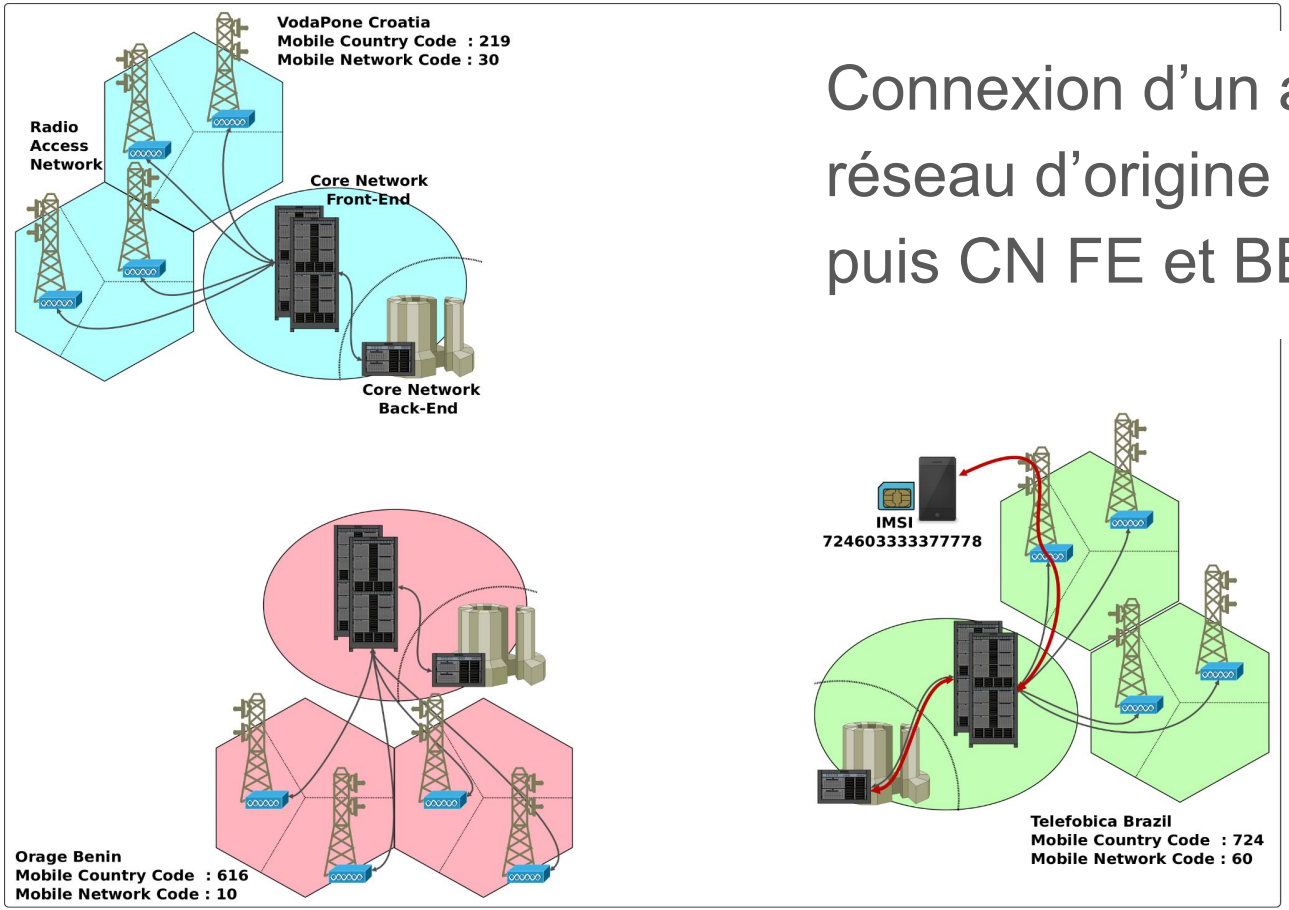
Pas de roaming possible

# Connexion d’un abonné mobile (2/3)



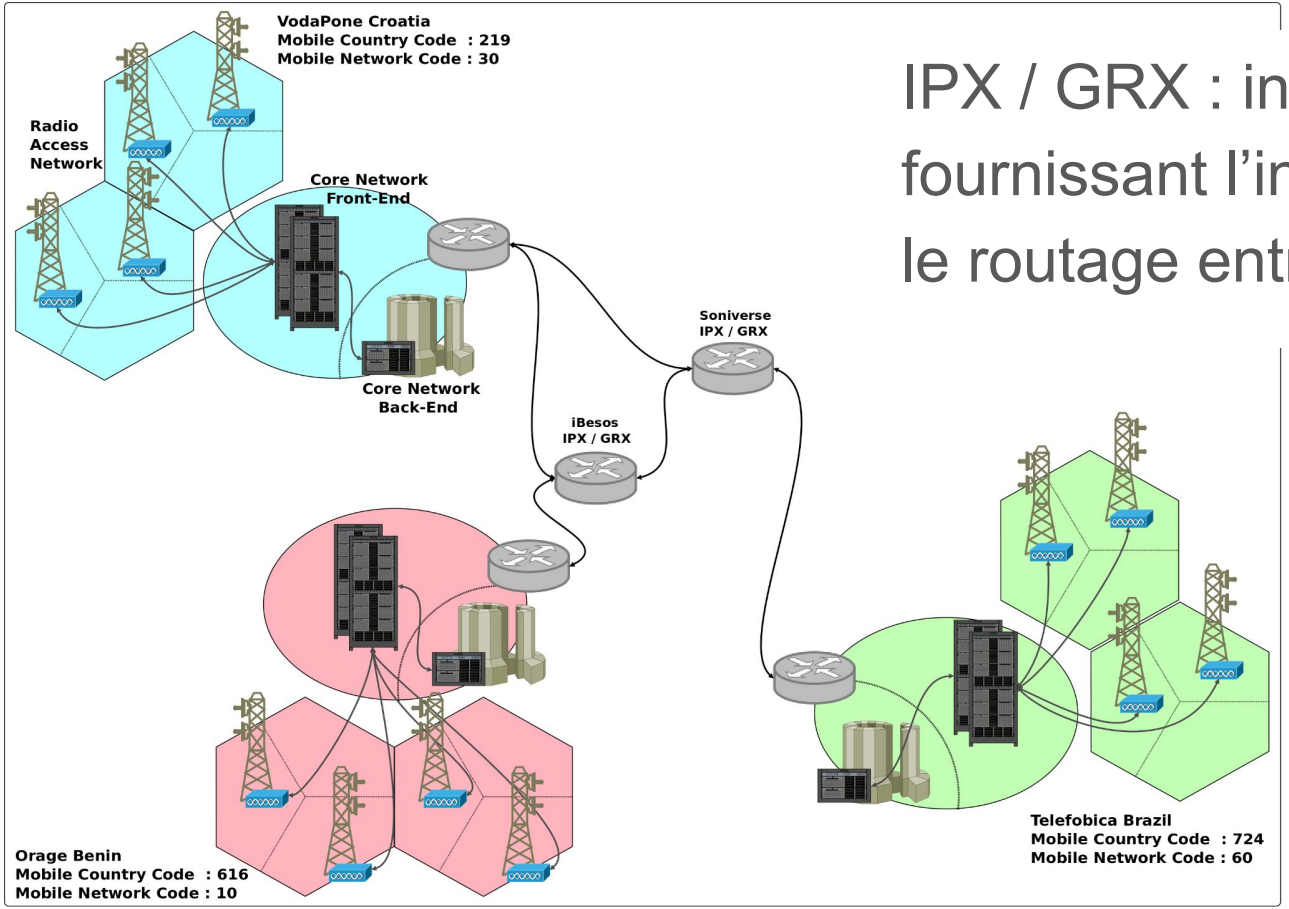

Connexion d’un abonné sur son réseau d’origine : RAN et CN FE

# Connexion d’un abonné mobile (3/3)



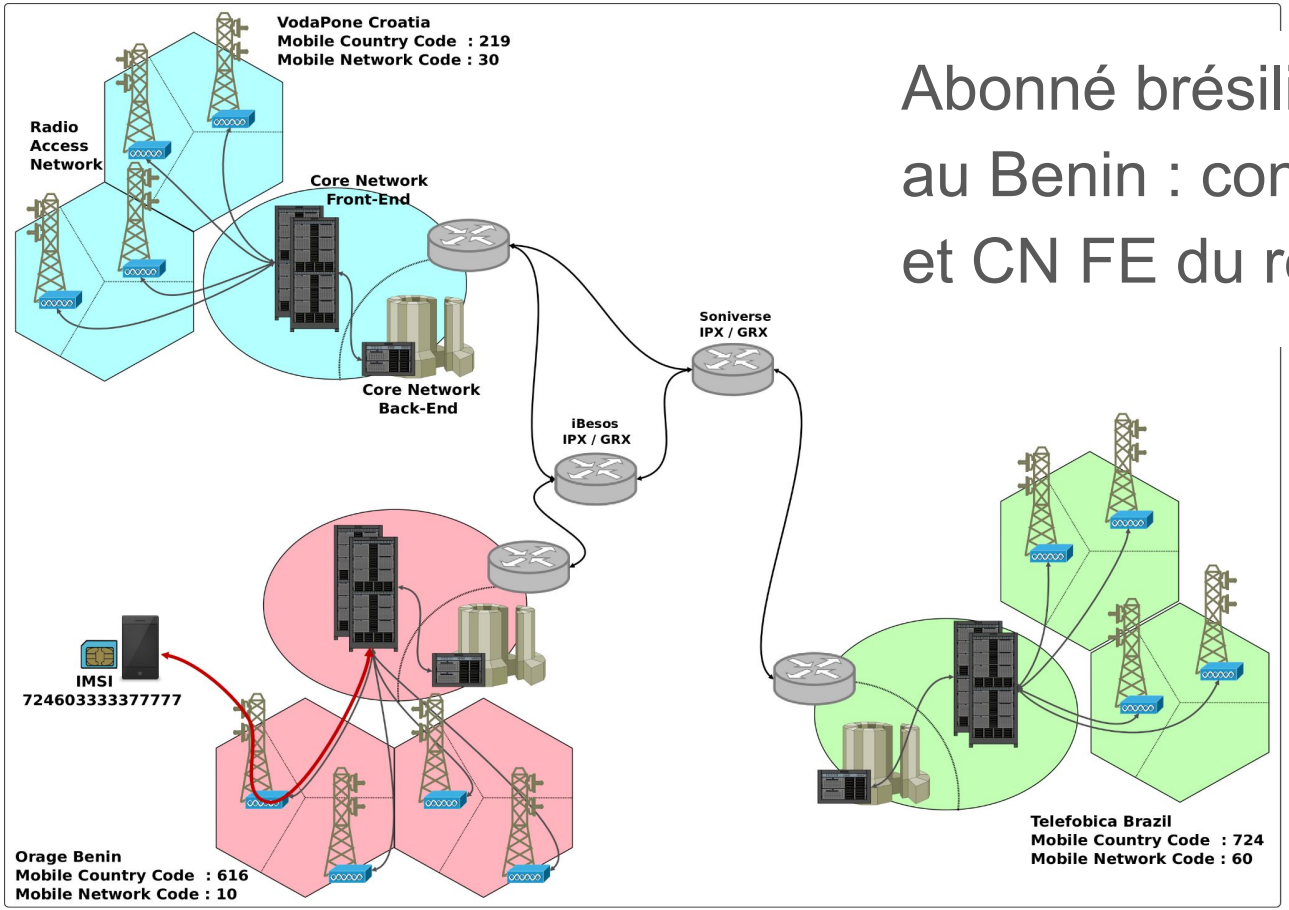

Connexion d’un abonné sur son réseau d’origine : RAN et CN FE, puis CN FE et BE

# Interconnexions entre opérateurs mobiles (1/3)



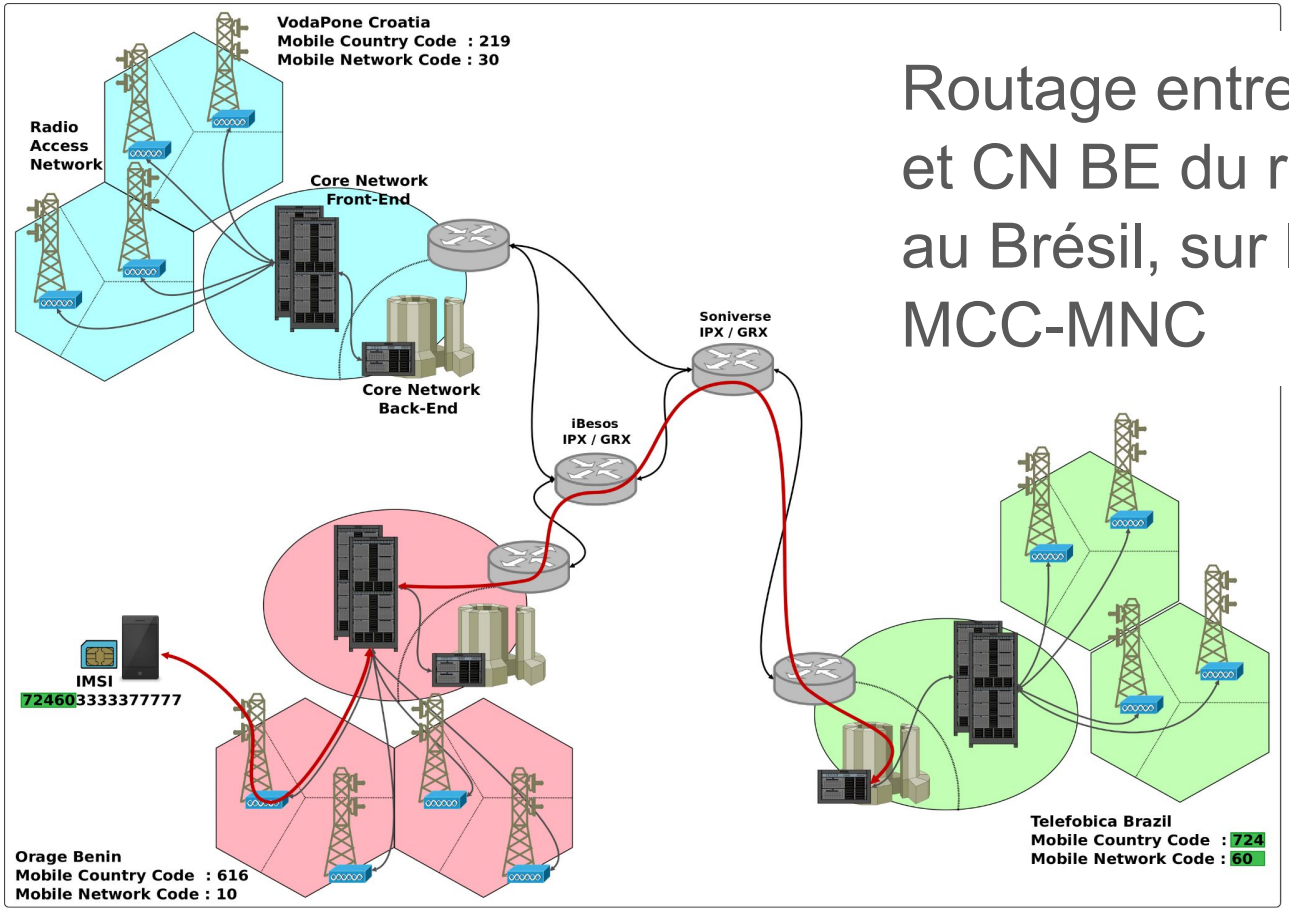

IPX / GRX : intermédiaires fournissant l'interconnexion et le routage entre MNOs

# Interconnexions entre opérateurs mobiles (2/3)



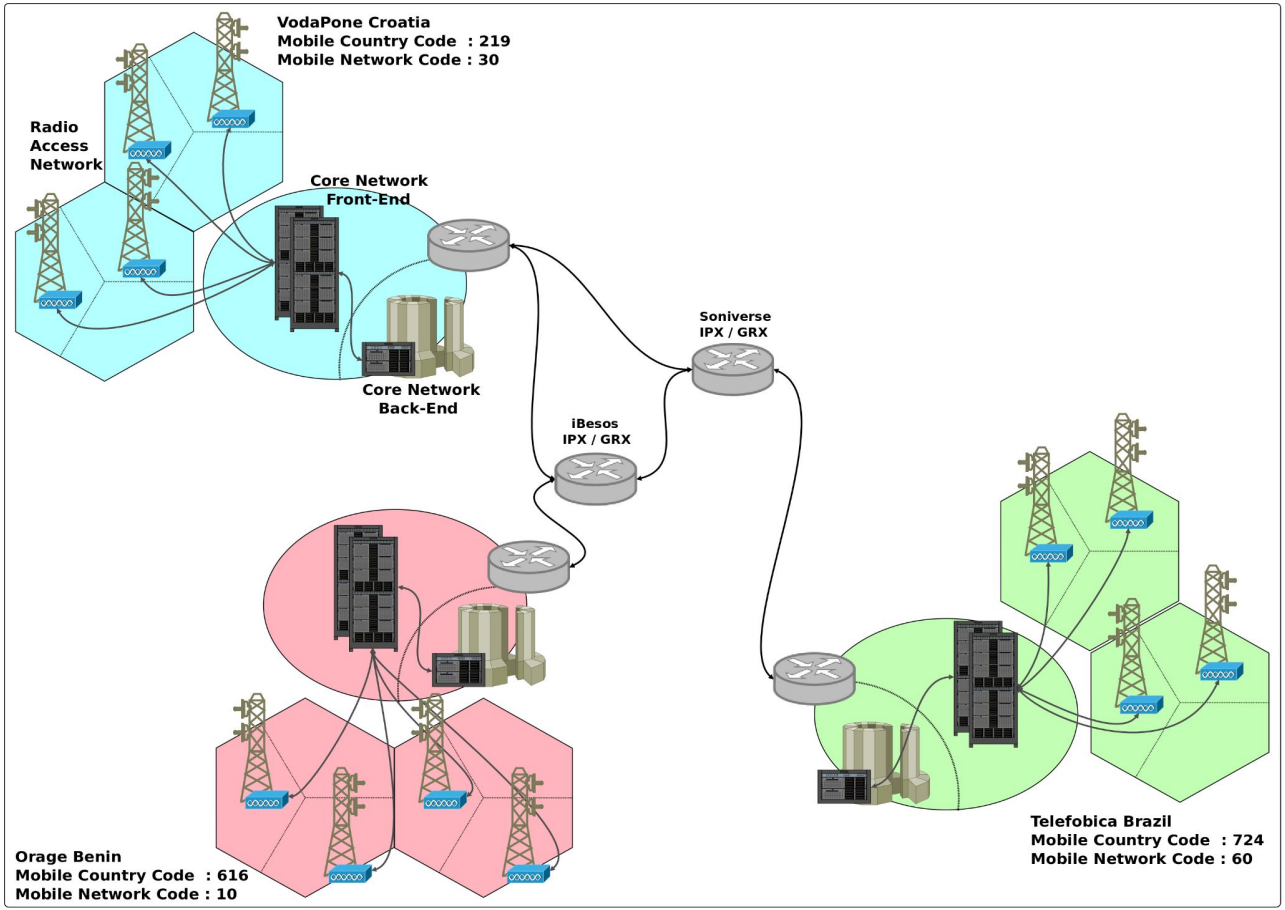

Abonné brésilien en roaming au Benin : connexion au RAN et CN FE du réseau visité

# Interconnexions entre opérateurs mobiles (3/3)

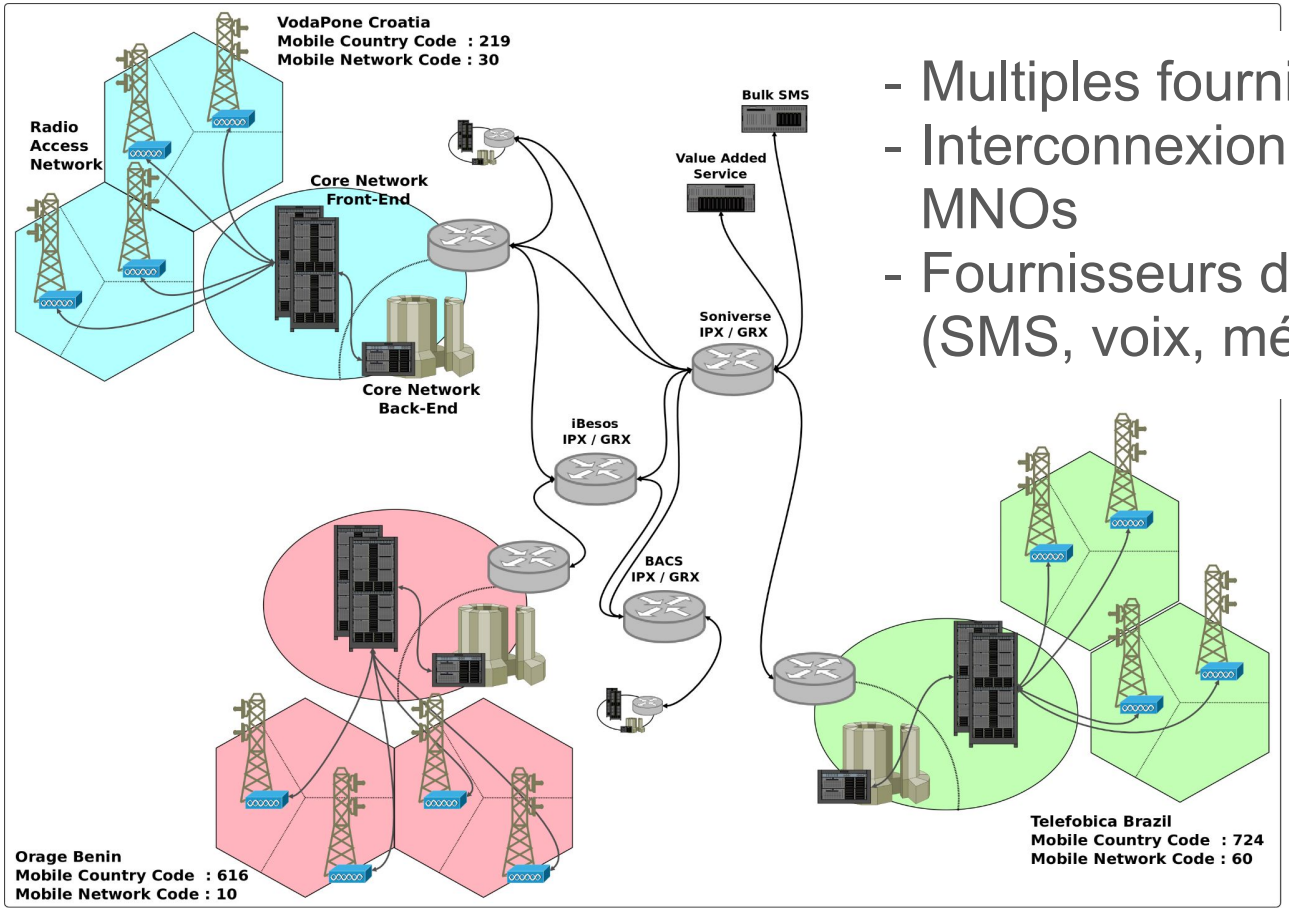



Routage entre CN FE au Benin et CN BE du réseau d'origine au Brésil, sur la base du MCC-MNC

# Qui accède aux réseaux de signalisation (1/3)

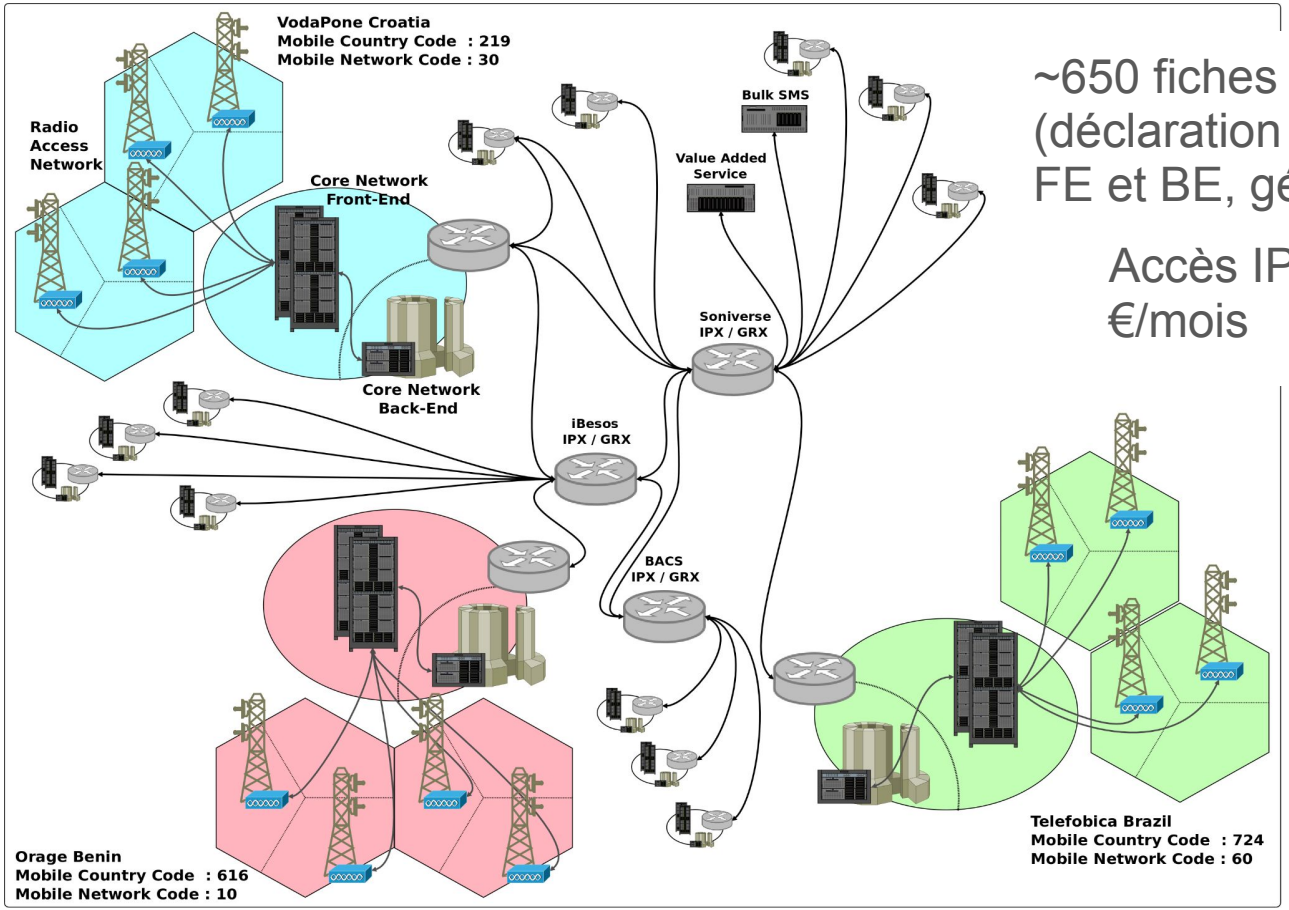


# Qui accède aux réseaux de signalisation (2/3)




- Multiples fournisseurs IPX / GRX
- Interconnexions directes entre MNOs
- Fournisseurs de services tiers (SMS, voix, médiation…)

# Qui accède aux réseaux de signalisation (3/3)




~650 fiches IR.21 dans RAEX (déclaration des infrastructures CN FE et BE, gérées via la GSMA)

Accès IPX / GRX à partir de 1k €/mois

# Facteurs de risque concernant l'échange de signalisation

- Tout IP
- Mécanismes d'adressage et de routage multiples
  - SS7 (2G/3G) : basé sur le GT, ou les SSN, ou le PC, ou l'IMSI de l'abonné ciblé (E.214)
  - Diameter (4G) : basé sur le *Realm*, ou le *Host*
- Protocoles et messages de signalisation en clair
- Pas de cryptographie entre les infrastructures

# Principaux types d’attaques

- Obtention de l’IMSI à partir du MSISDN
  - Précurseur à toutes les autres attaques
  - Traduction MSISDN / IMSI durable (plusieurs années)
- Localiser un abonné
  - Quel CN FE le prend en charge
    - précurseur aux attaques de détournements
  - Géolocalisation
- Détournement des SMS, appels ou connexions de données
- Séquencement :
  - Obtenir l’IMSI de l’abonné ciblé à partir de son MSISDN
  - Localiser le CN FE en charge de l’IMSI
  - Relocaliser l’abonné ciblé sur un CN FE de l’attaquant, auprès du CN BE de son réseau d’origine
    - L’attaquant va alors recevoir les communications destinées à l’abonné
  - Renvoyer ces communications vers le CN FE légitime

# Protections possibles

- Fournisseurs IPX / GRX
  - Anti-spoofing
  - Filtrage simple des messages de signalisation
- Opérateurs mobiles
  - *SMS-HomeRouter*
    - Eviter l'obtention de l'IMSI à partir du MSISDN
  - Pare-feu de signalisation
    - Filtrage simple, et à état, des messages de signalisation
- Pas de régulateur mondial : auto-régulation par le business :)

# Protections possibles : catégorisation des messages

- La GSMA fournit des guides techniques pour la sécurité du roaming
  - Bonnes pratiques générales
  - Catégorisation des messages de signalisation
    - Cat.1 : messages interdits pour le roaming
    - Cat.2 : messages autorisés pour les *roamers-in*
    - Cat.3 : messages autorisés pour les *roamers-out*

      Comment différencier une localisation légitime d'une illégitime ?

      Filtrage sur la base de la distance et durée…

# Etats de lieux de la sécurité des interconnexions

- Chaque jour, réception de 100x à 1000x messages de signalisation illégitimes
  - Scans de plage de MSISDN
  - Tentative de contournements des protections
    - Modifications sur les mécanismes d'identification et de routage, sur le format
    - Spoofing éventuel

# Conclusion

- Protection inégale des abonnés dans le monde
  - Certains MNOs n'ont aucune protection
- Nécessité d'investissement : $$$ (ou €€€) et en compétences
  - Les MNOs d'Europe sont plutôt bons
  - Les régulateurs peuvent « forcer » à des investissements
- En tant qu'abonné : utiliser Signal
  - Protéger sa géolocalisation : éteindre son portable, ou le laisser à la maison

# Pour aller plus loin

- Outils open-source : Osmocom (2G-3G), Open5GS (4G-5G), QCSuper, pycrate…
- Article MISC sur la 5G
  - En 5G, le réseau d'origine authentifie les abonnés, y compris en roaming
- CTF SS7 P1 Security : https://ctf.p1sec.fr/

(ne pas casser le serveur SVP)

- P1 Security recrute !

# Merci

## Des questions ?

# Annexes

# Annexe 0 : autres types d'attaques sur la signalisation

- Obtention de vecteurs d'authentification auprès du CN BE de l'abonné ciblé
  - Message dit "Cat.3"
  - Interception des communications 2G/3G/4G avec un *IMSI-catcher*
- Compromission d'infrastructure d'opérateurs ou de fournisseurs d'interconnexions
  - Accès à toute la signalisation des abonnés pris en charge
  - Le Graal : accès à toutes les clés d'authentification des abonnés d'un opérateur, stockées dans le CN BE

# Annexe 1 : équipements correspondants aux FE et BE

| | **2G/3G CS** | **2G/3G PS** | **4G** |
|---|---|---|---|
| **Front-End** | MSC / VLR (*Mobile Switching Center, Visitor Location Register*)<br>GMSC (*Gateway MSC*) | SGSN (*Serving GPRS Support Node*)<br>GGSN (*Gateway GPRS Support Node*) | MME (*Mobility Management Entity*)<br>S-GW (*Serving-Gateway*)<br>P-GW (*Packet Data Network-Gateway*) |
| **Back-End** | HLR (*Home Location Register*)<br>SMS-Center | HLR (*Home Location Register*) | HSS (*Home Subscriber Server*) |

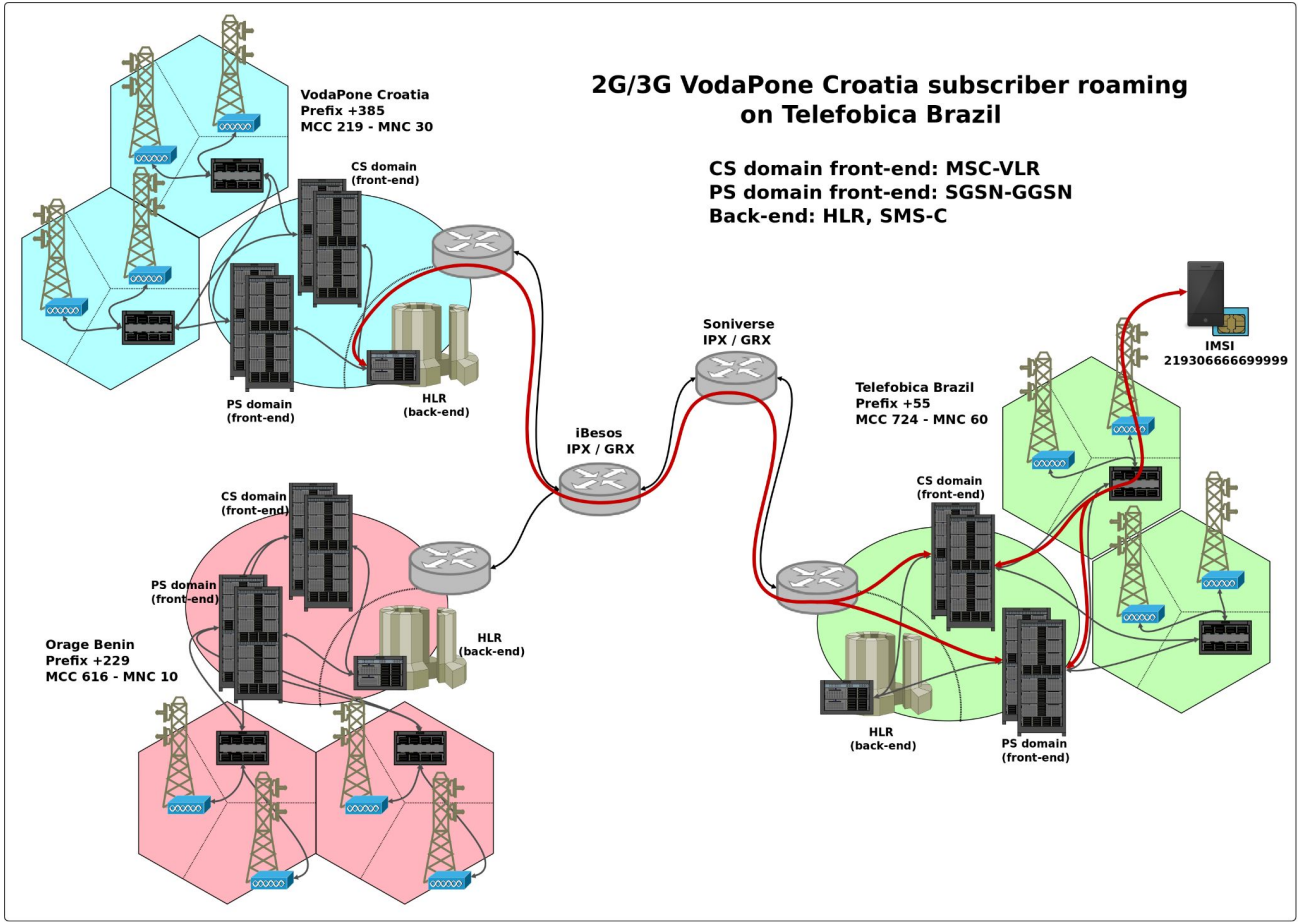
# Annexe 1bis : équipements correspondants aux FE et BE, avec home-routing

| | **2G/3G CS** | **2G/3G PS** | **4G** |
|---|---|---|---|
| **Front-End** | MSC / VLR (*Mobile Switching Center, Visitor Location Register*)<br>GMSC (*Gateway MSC*) | SGSN (*Serving GPRS Support Node*) | MME (*Mobility Management Entity*)<br>S-GW (*Serving-Gateway*) |
| **Back-End** | HLR (*Home Location Register*)<br>SMS-Center | HLR (*Home Location Register*)<br>GGSN (*Gateway GPRS Support Node*) | HSS (*Home Subscriber Server*)<br>P-GW (*Packet Data Network-Gateway*) |

# Annexe 2 : pcap de signalisation Diameter en roaming

- Correspondant au slide 9
- pcap de signalisation Diameter

# Annexe 3 : pcap de signalisation SS7 en roaming




[pcap](#) de signalisation SS7