Partie réseau
Module 3107

IUT Béziers, dépt. R&T © 2014
http://www.borelly.net/
Christophe@Borelly.net

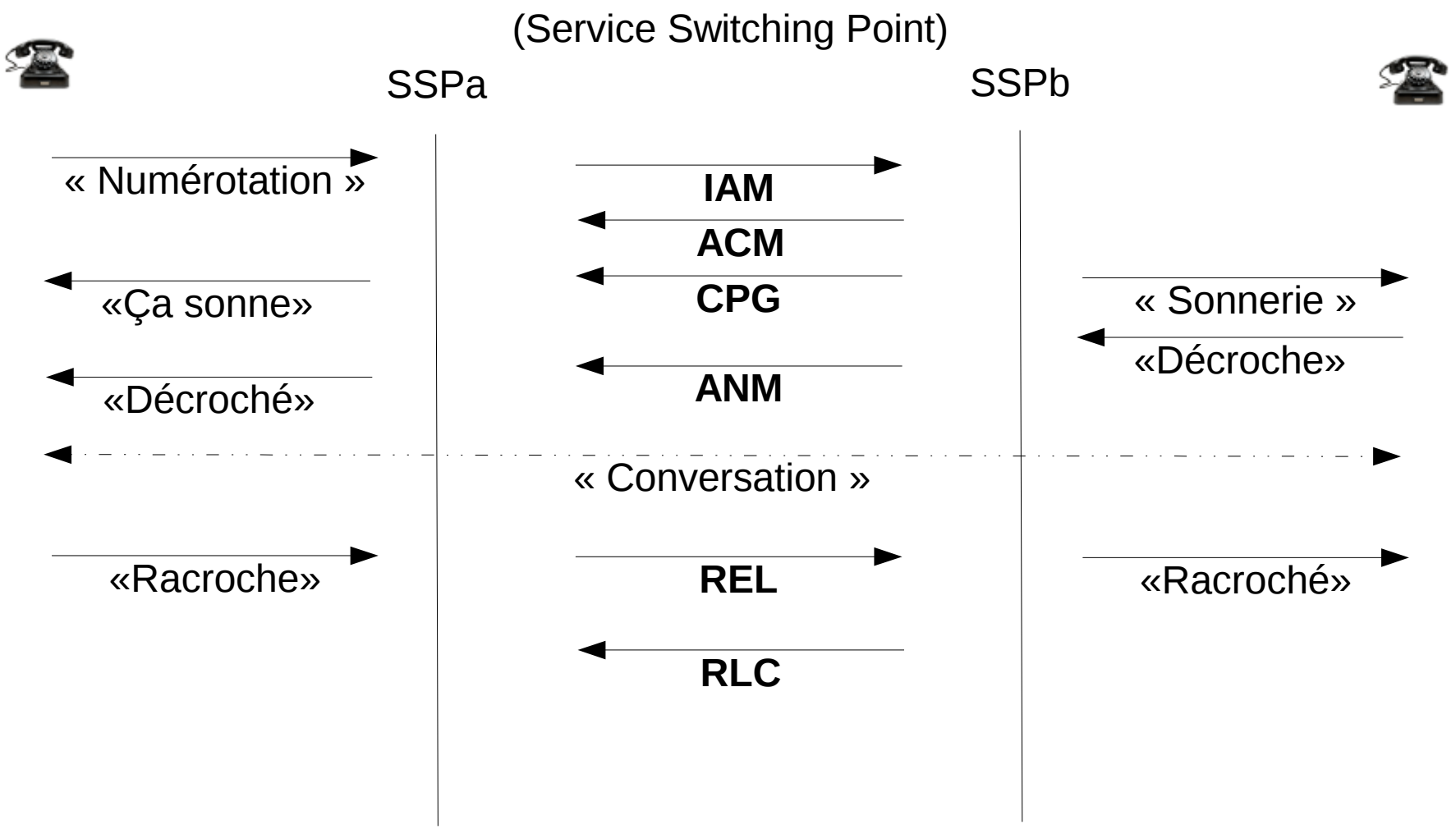
Signaling System n°7

- ITU-T en 1980 (Normes Q.7xx)
  - **ISUP** (Couches 5-7) : ISDN User Part
    - Q.761, Q.762, Q.763, Q.764 et Q.766
  - **SCCP** (Couche 4) : Signalling Connection Control Part
    - Q.711, Q.712, Q.713, Q.714, Q.715 et Q.716
  - **MTP** (Couches 1-3) : Message Transfer Part
    - Q.701, Q.702, Q.703, Q.704, Q.706 et Q.707
- **SIGTRAN** : SIGnaling TRANsport (RFC 2719 en 1999)
  - SS7 sur IP
  - **SCTP** : Stream Control Transmission Protocol

Messages SS7

- **IAM** : Initial Address Message
- **ACM** : Address Complete Message
- **CPG** : Call Progress
- **ANM** : Answer message
- **CON** : Connect
- **REL** : Release
- **RLC** : Release complete

Exemple d'appel



Numérotation et identification

- Norme GSM 03.03 / 23.003
- Réseau : **MCC**, **MNC**
  - **MCC** (Mobile Country Code) : 3 digits
  - **MNC** (Mobile Network Code) : 2 digits
- Cellule : LAI, RAI, CGI, BSIC
- Mobile : IMSI, TMSI, MSISDN, MSRN

Bulletin d'exploitation de l'UIT

- **UIT** : Union internationale des télécommunications
  - Orange France 208 01
  - Orange France 208 02
  - MobiquiThings 208 03
  - Sisteer 208 04
  - Globalstar Europe 208 05
  - Globalstar Europe 208 06
  - Globalstar Europe 208 07
  - S.F.R. 208 09
  - S.F.R. 208 10
  - S.F.R. 208 11
  - S.F.R. 208 13
  - RFF 208 14
  - Free Mobile 208 15
  - Bouygues Telecom 208 20
  - Bouygues Telecom 208 21
  - ...

Identifiants

- Zone de localisation
  - **LAI** = MCC + MNC + LAC (2 octets)
- Zone de routage
  - **RAI** = LAI + RAC (1 octet)
- Numéro de cellule
  - **CGI** = LAI + CI (2 octets)
- Numéro de station de base
  - **BSIC** = NCC + BCC
    - Network Color Code : 3 bits
    - Base station Color Code : 3 bits

Identification du mobile

- **IMSI** (International Mobile Subscriber Identity)
  - MCC (Mobile Country Code) : 3 digits
  - MNC (Mobile Network Code) : 2 digits
  - MSIN (Mobile Subscriber Identification Number) max. 10 digits
- **MSISDN** (Mobile Station International ISDN Number) : Numéro de l'abonné
- **MSRN** (Mobile Station Roaming Number) : Numéro utilisé lors d'un routage inter-opérateurs

TMSI

- L'IMSI est connu uniquement à l'intérieur du réseau mobile, cette identité doit rester secrète autant que possible (recours au TMSI)
- Le **TMSI** (Temporary Subscriber Identification Number) est alloué temporairement par un VLR lors de la mise à jour de localisation ou lors de l'inscription du mobile sur le réseau
- Il est codé sur 4 octets

Recherche d'un mobile

- Lorsqu'un appel entrant se produit, le réseau va rechercher le mobile dans la dernière zone de localisation connue (plusieurs cellules)
- Messages de paging (couche 3) contenant en général le TMSI du mobile (PAGING REQUEST/RESPONSE)

La couche 3 (MS-BTS)

- Interface **Um** (GSM 04.08)
- 3 sous couches
  - **RR** : Radio Ressource
  - **MM** : Mobility Management
  - **CM** : Connection Management

TI/SI 4 bits	Protocol Discriminator 4 bits
Message Type 8 bits	
...	

0011 Call Control messages
0101 Mobility Management messages
0110 Radio Resource management messages

Exemple Paging

- 06 21 00 05 f4 a5 02 21 49
- 06 27 01 03 23 58 01 05 f4 a5 02 21 49
- Couche RR (06)

```
0 0 1 0 0 - - -  Paging messages:
          0 0 1  - PAGING REQUEST TYPE 1
          0 1 0  - PAGING REQUEST TYPE 2
          1 0 0  - PAGING REQUEST TYPE 3
          1 1 1  - PAGING RESPONSE
```

Table 10.1/GSM 04.08 (page 1 of 2)
Message types for Radio Resource management

Contenu du message

- 06 21 00 05 f4 a5 02 21 49

IEI	Information element	Type / Reference	Presence	Format	length
	L2 Pseudo Length	L2 Pseudo Length 10.5.2.19	M	V	1
	RR management Protocol Discriminator	Protocol Discriminator 10.2	M	V	½
	Skip Indicator	Skip Indicator 10.3.1	M	V	½
	Paging Request Type 1 Message Type	Message Type 10.4	M	V	1
	Page Mode	Page Mode 10.5.2.26	M	V	½
	Channels Needed for Mobiles 1 and 2	Channel Needed 10.5.2.8	M	V	½
→	Mobile Identity 1	Mobile Identity 10.5.1.4	M	LV	2-9
17	Mobile Identity 2	Mobile Identity 10.5.1.4	O	TLV	3-10
	P1 Rest Octets	P1 Rest Octets 10.5.2.23	M	V	0-17

Table 9.22/GSM 04.08
PAGING REQUEST TYPE 1 message content

Codage de l'identité du mobile

- 10.5.1.4 Mobile identity
  - 05 f4 a5 02 21 49

Longueur 8 bits		
Digit 1 4 bits	Ind. 1 bit	Type 3 bits
Digit p+1 4 bits	Digit p 4 bits	
...		

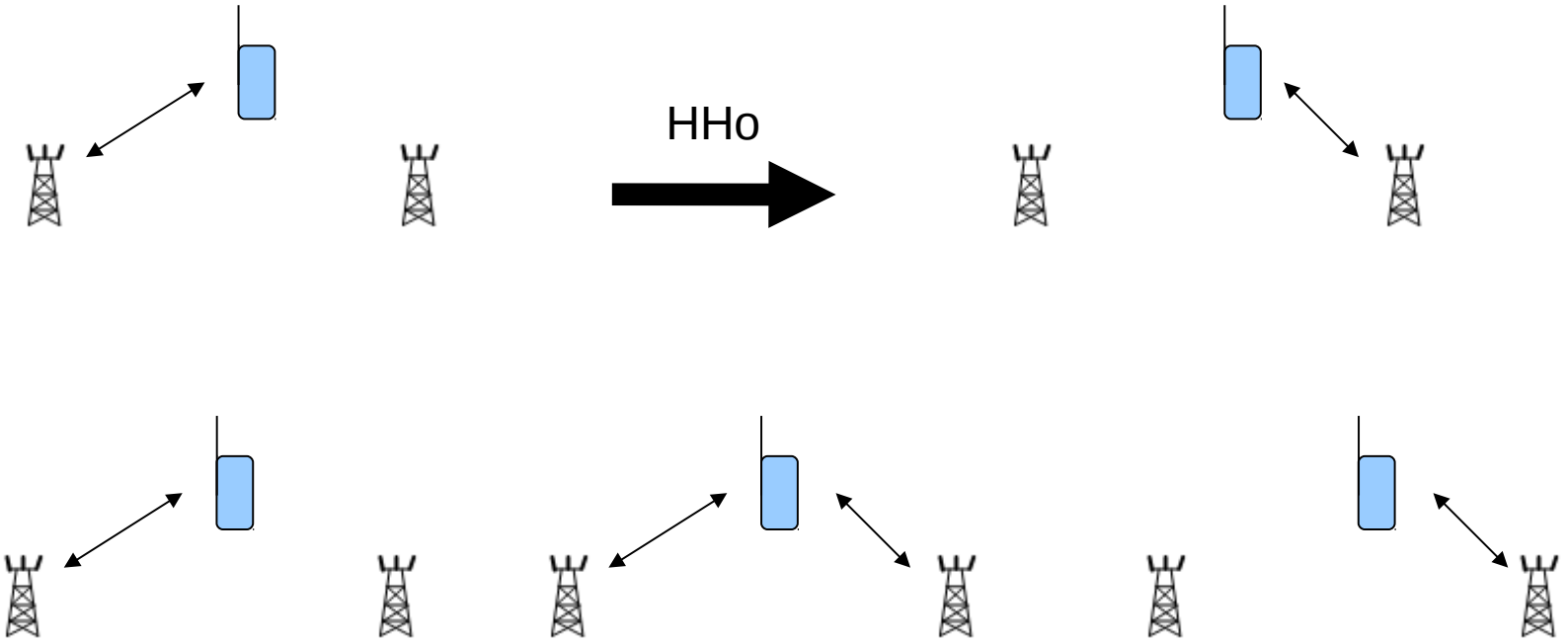
001 IMSI
010 IMEI
011 IMEISV
100 TMSI
000 No identity

If the mobile identity is the TMSI then bits 5 to 8 of octet 2 are coded as '1111' and bit 8 of octet 3 is the most significant bit.

Handover

- Si au cours du déplacement d'un MS, le signal reçu de la cellule serveuse est plus faible que sur une cellule voisine, le réseau peut demander au mobile de changer de cellule serveuse.
- Cette opération porte le nom de Handover ou Handoff suivants les systèmes.
  - Hard Handover : commutation directe
  - Soft Handover : commutation avec 2 liaisons simultanées

Hard et Soft Handover

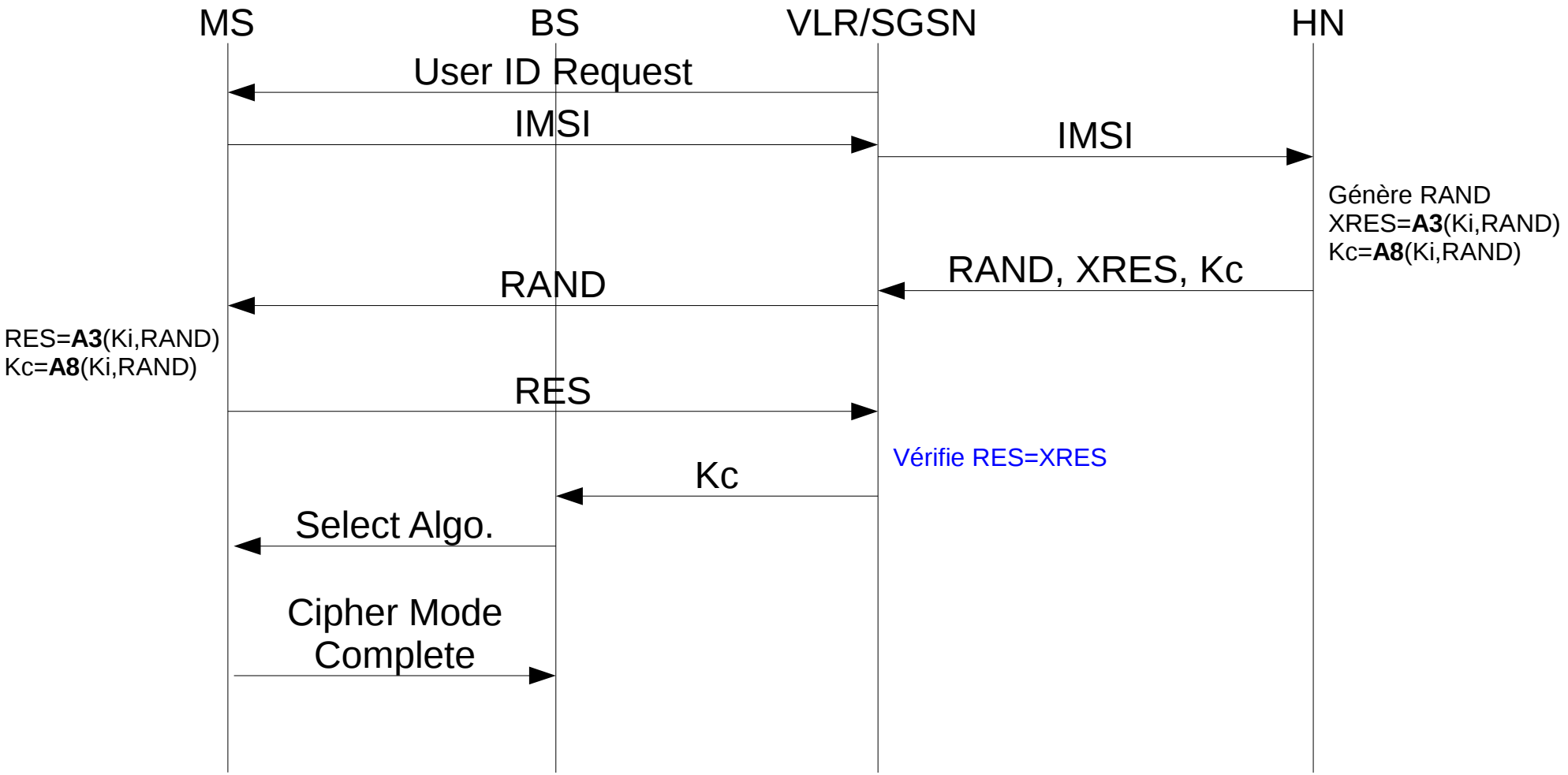


SHo : 2 Liaisons simultanées

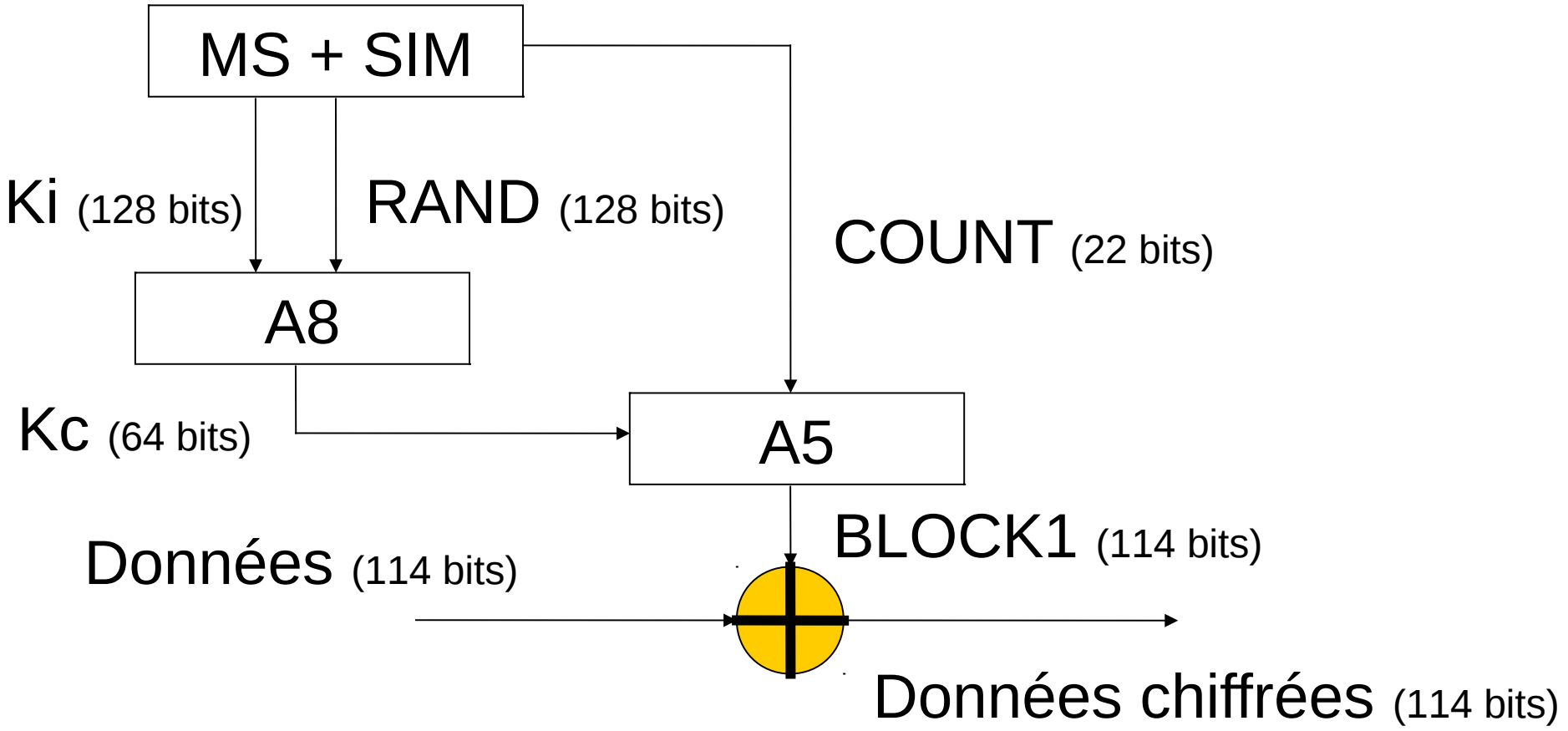
Sécurité 2G

- Utilisation de 3 algorithmes (A3, A5 et A8)
- Authentification du MS uniquement
  - Vérification de **Ki** (Clé utilisateur – 128 bits)
- Chiffrement par XOR des données
  - **Kc** (Clé de chiffrement - 64 bits)

Authentification 2G



Le chiffrement 2G



Sécurité 3G/4G

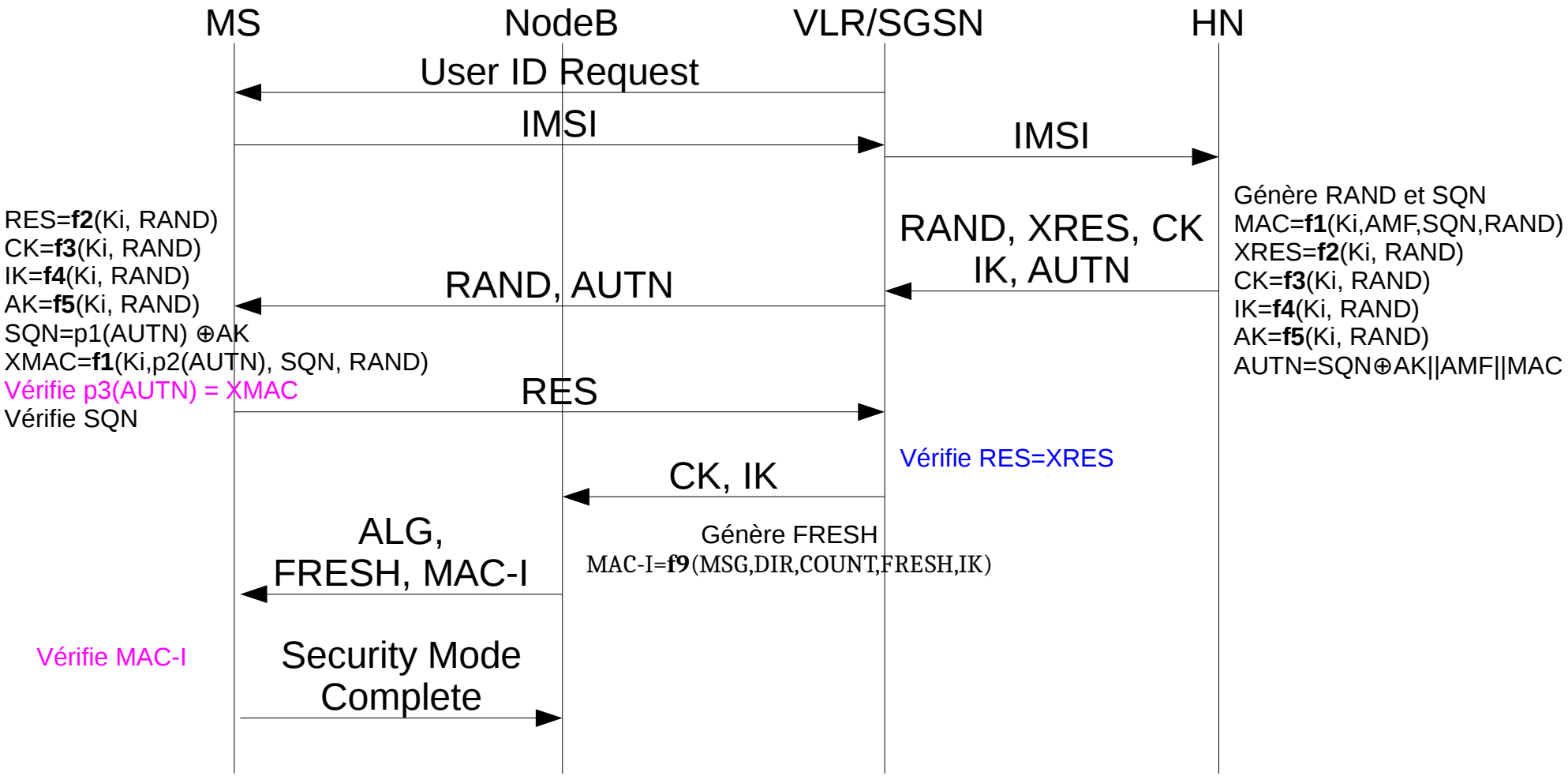
- Authentication and Key Agreement (AKA)
- Authentification mutuelle
- RFC 3310 / RFC 4187 (EAP-AKA)
- 3G : 10 algorithmes (de f0 à f9)
- 4G : **KDF** (Key Derivation Function)
- Chiffrement par XOR :
  - KeyStream=**f8**(CK,COUNT,BEARER,DIR,LEN)

Paramètres et sigles 3G

Parameter	Definition	Bit size
K	Pre-shared secret key	128
RAND	Random challenge	128
SQN	Sequence number	48
AK	Anonymity Key	48
AMF	Authentication Management Field	16
MAC	Message Authentication Code	64
CK	Cipher Key	128
IK	Integrity Key	128
RES	Response	32-128
X-RES	Expected Response	32-128
AUTN	Authentication Token	128 (16+64+48)
AUTS	Authentication re-Synchronisation Token	96-128
MAC-I	Message authentication code for data integrity	32

Page 33 de la référence [3]

Authentification 3G



Authentification 4G

- Protection différenciée pour les liens AS et NAS
  - **AS** : Access Stratum UE<=>eNB
  - **NAS** : Non Access Stratum UE<=>MME (Mobile Management Entity)
- Ajout de K_{ASME}=**KDF**(CK,IK,SNid,SQN⊕AK)
  - SN identifier (Serving Network)
- Ajout de K_{eNB}=**KDF**(K_{ASME})

Références

- [1] http://www.3gpp.org/
- [2] http://fr.wikipedia.org/
- [3] Thèse « UMTS Authentication and Key Agreement » de Jon Robert Dohmen et Lars Sømo Olaussen 2001