



Université Mohammed V – Agdal

Faculté des sciences – Rabat

Laboratoire Mathématiques, Informatique et Applications

Fonctionnement et sécurité de la carte USIM

**Saïd EL HAJJI
Ghizlane ORHANOU**



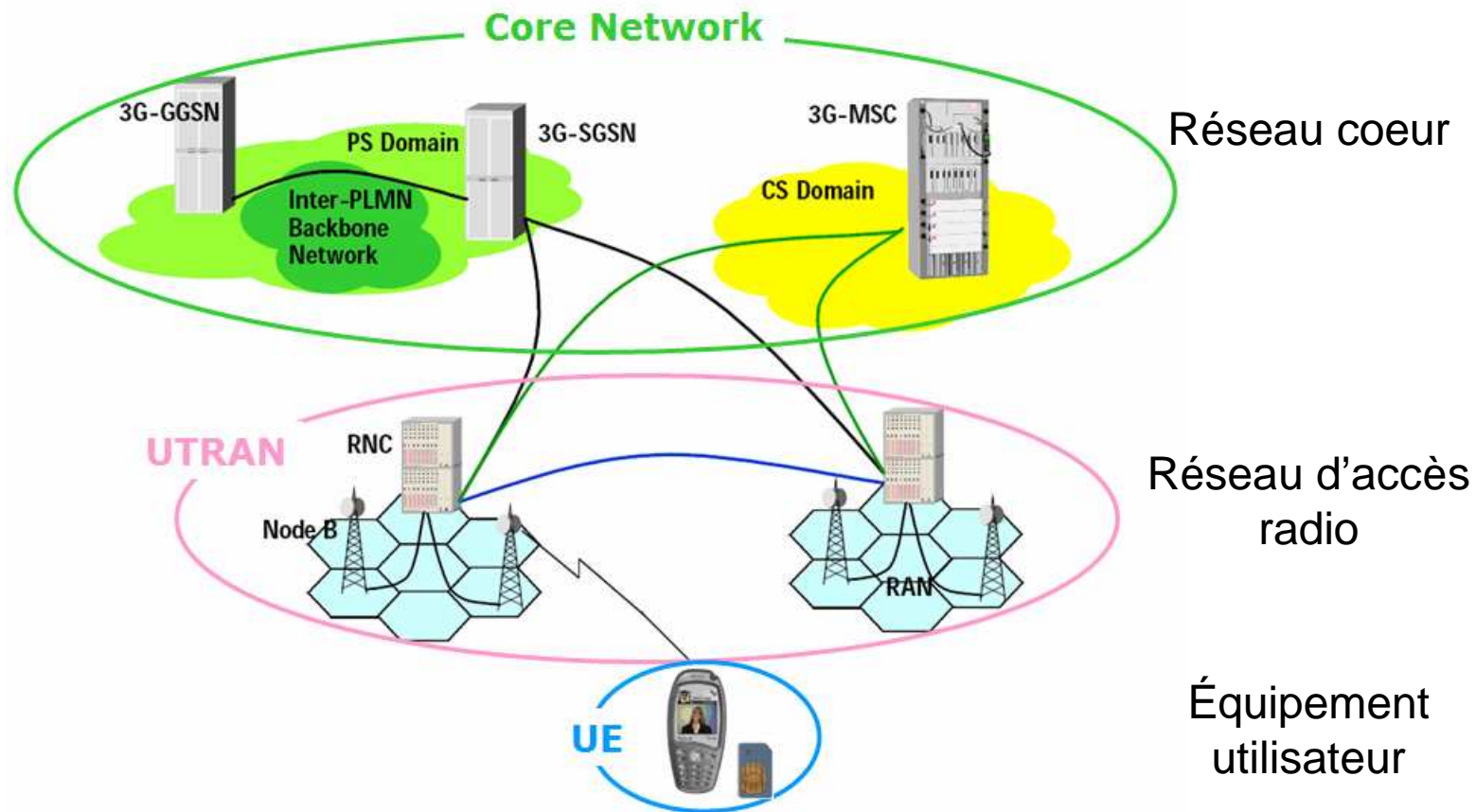
PLAN

- Introduction
- USIM dans le réseau UMTS
- USIM et sécurité du réseau UMTS
- Structure d'une carte UICC/USIM
- Communication avec UICC/USIM
- Conclusion



USIM dans le réseau UMTS

Architecture du réseau UMTS





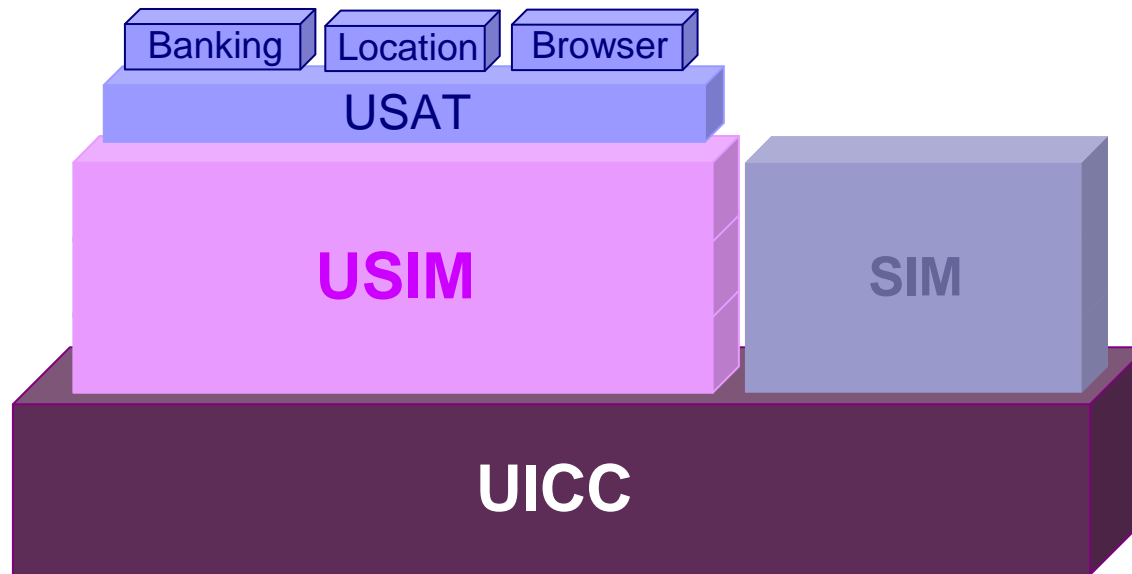
SIM, USIM et UICC

- SIM (Subscriber Identity Module):
 - Carte à puce 2G;
 - Entité physique et logique (aucune distinction entre la plateforme et l'application);
 - En 3G, SIM peut être une application au niveau de la carte à puce 3G;

- USIM (Universal Subscriber Identity Module);
 - Purement une application logique;
 - Compatible avec la famille de standards ISO/IEC 7816;
 - Réside au niveau de la carte à puce UICC;

- UICC (Universal Integrated Circuit Card)
 - Carte à puce 3G;
 - Une plateforme logique et physique pour l'USIM;
 - Abrite une ou plusieurs applications USIM, une application SIM et autres applications (ex. commerce mobile).

SIM, USIM et UICC



USAT: USIM Application Toolkit

USIM: Universal Subscriber Identity Module

UICC: Universal Integrated Circuit Card



Rôles de la carte UICC/USIM

Les principaux rôles de l'application USIM (*Universal Subscriber Identity Module*) :

- contient une identité qui doit identifier sans aucune ambiguïté l'abonné;
 - IMSI (*International Mobile Subscriber Identity*);
- contient les détails de l'abonnement :
 - Services, langage de préférence, carnet d'adresses, etc.
- contient les secrets permettant d'authentifier l'utilisateur et de s'authentifier vis-à-vis du réseau et vice-versa :
 - Les codes secrets PIN (*Personal Identification Number*), PIN2, PUK (*Personal Unlocking Key*);
 - La clé secrète K;
 - Les clés de cryptage CK et d'intégrité IK.
 - Les algorithmes de cryptage UEA et d'intégrité UIA;
- permet le chargement de services sur la carte dans un environnement sécurisé permettant :
 - l'interaction avec le mobile, l'affichage d'information sur l'écran,
 - la saisie des données par l'utilisateur, composer des appels,
 - interagit avec le réseau, obtient des informations de localisation.



USIM

et sécurité du réseau UMTS



Rôles de l'USIM dans la sécurité du réseau UMTS

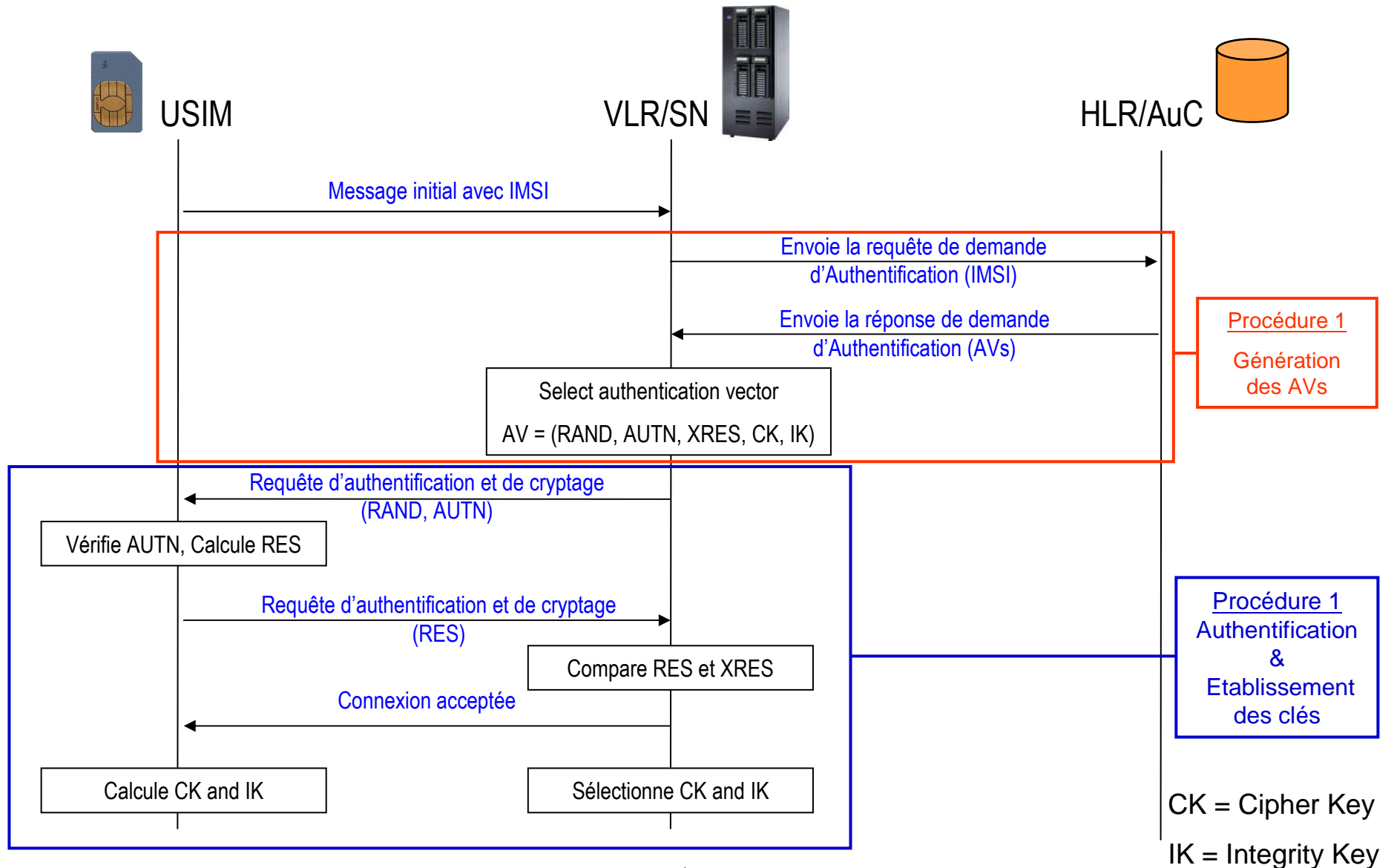
- Confidentialité de l'identité de l'utilisateur:
 - Utilisation d'une identification temporaire (TMSI/P-TMSI)
 - Utilisation de LAI et RAI

- Authentification mutuelle des entités:
 - Authentification de l'USIM par le réseau
 - Authentification du réseau par l'USIM

- Confidentialité des données:
 - Calcul de la clé CK
 - Négociation de l'algorithme UEA

- Intégrité des données:
 - Calcul de la clé IK
 - Négociation de l'algorithme UIA

Protocole AKA (Authentication & Key Agreement Protocol)





Structure d'une carte UICC/USIM



Normalisation

■ USIM

- Gestion des Fichiers et Authentification :
3GPP TS 31.102
- USIM Toolkit Applet Management : 3 GPP TS
31.111
- USIM API for Java Card : 3 GPP TS 31.130



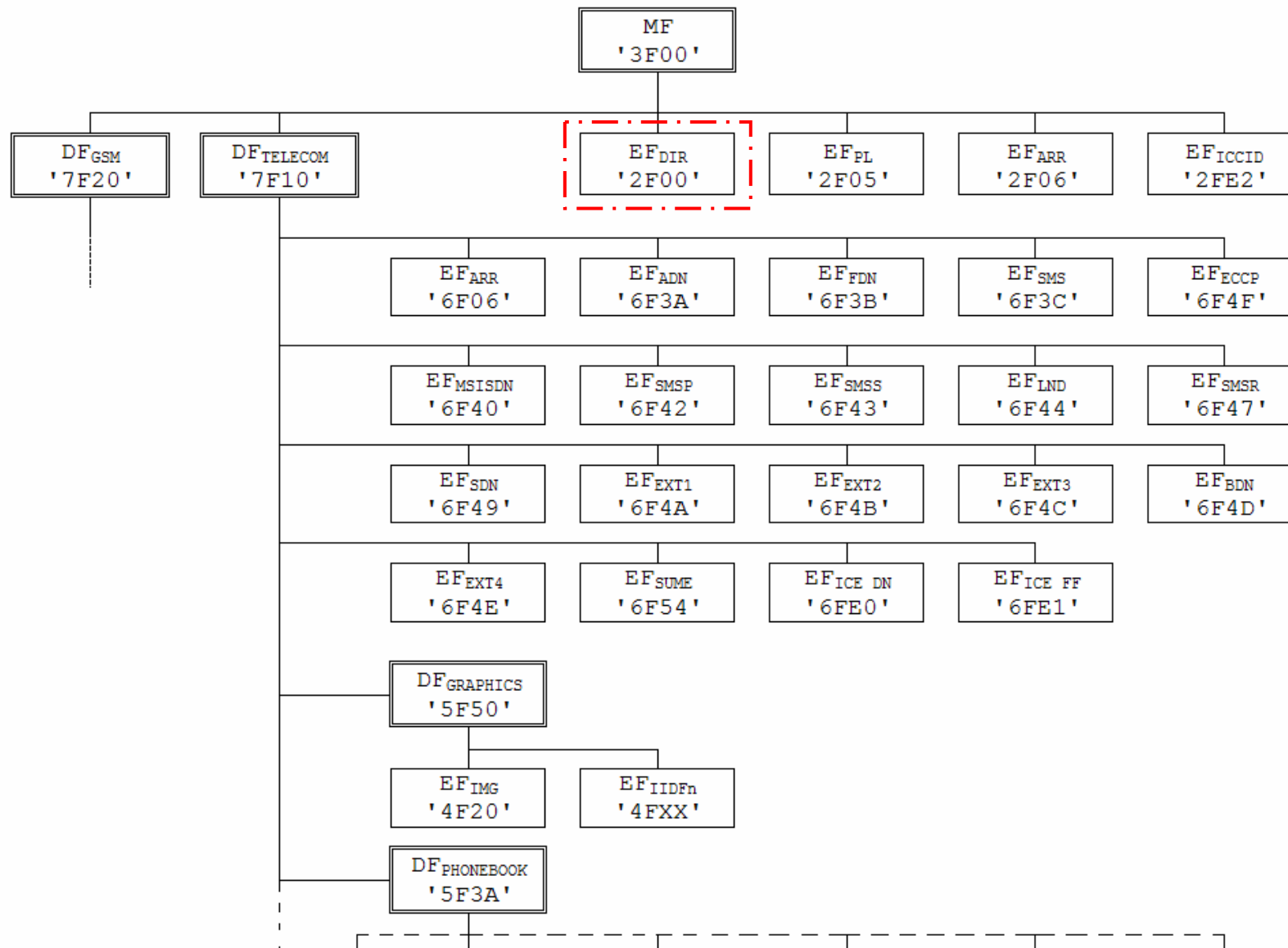
Le système de fichier de l'UICC

- MF: Master File;
- DF: Dedicated Files;
- EF: Elementary File;

- ADF: Application DF, contient les DF et EF d'une application donnée;

- Exemples:
 - - '3F': Master File;
 - - '7F': DF de 1er niveau;
 - - '5F': DF de 2ème niveau;
 - - '2F': EF sous la racine MF;
 - - '6F': EF sous DF de 1er niveau;
 - - '4F': EF sous DF de 2ème niveau;

Systeme de Fichiers de la carte UICC

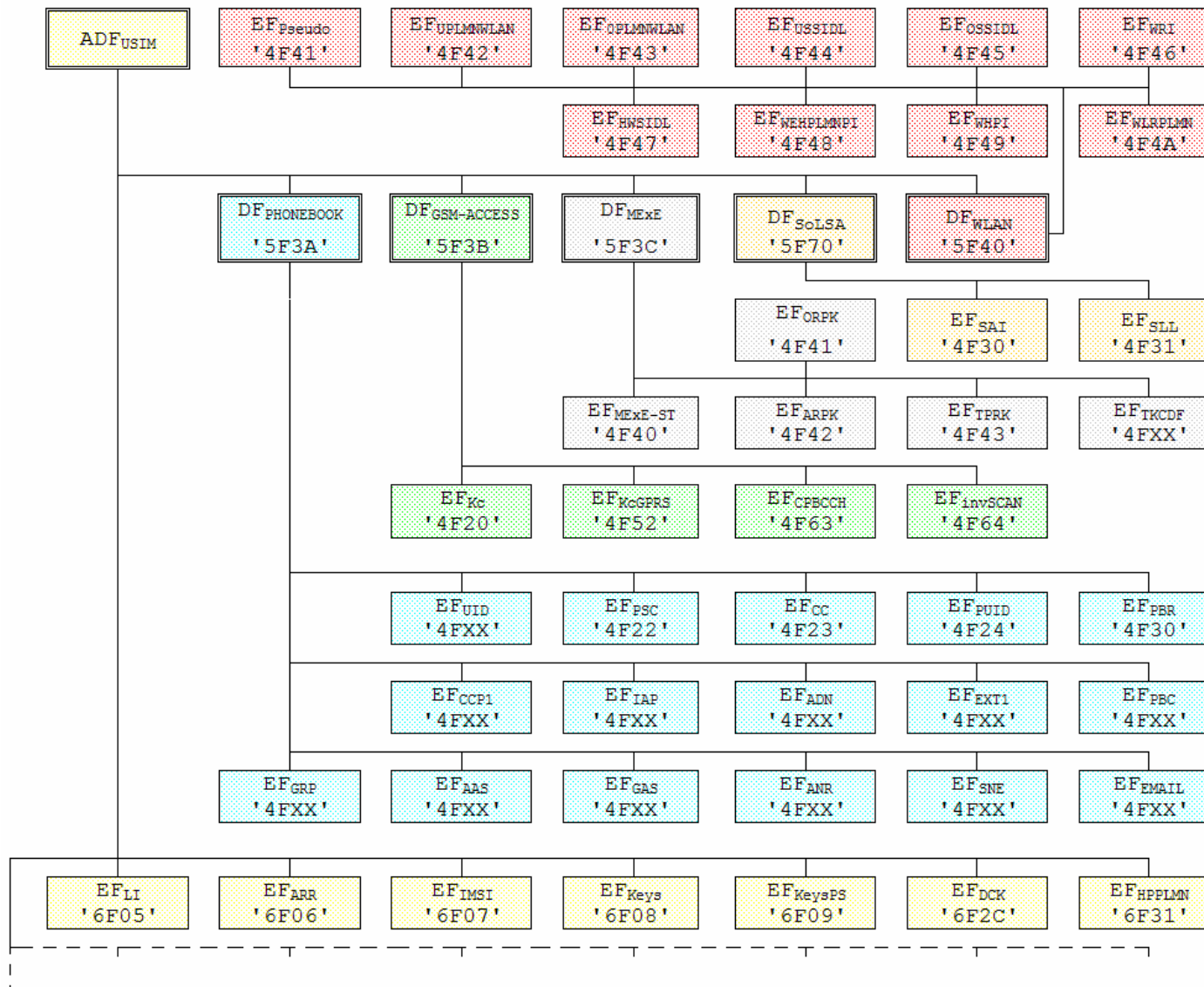




Sélection d'une application USIM

- Le fichier élémentaire EF_{DIR} contient les AIDs (*Application Identifier*) des applications USIM contenues au niveau de la carte UICC;
- Une application 3GPP peut être sélectionnée uniquement par le biais de son AID.

Systeme de Fichiers de l'application USIM





Communication avec UICC/USIM



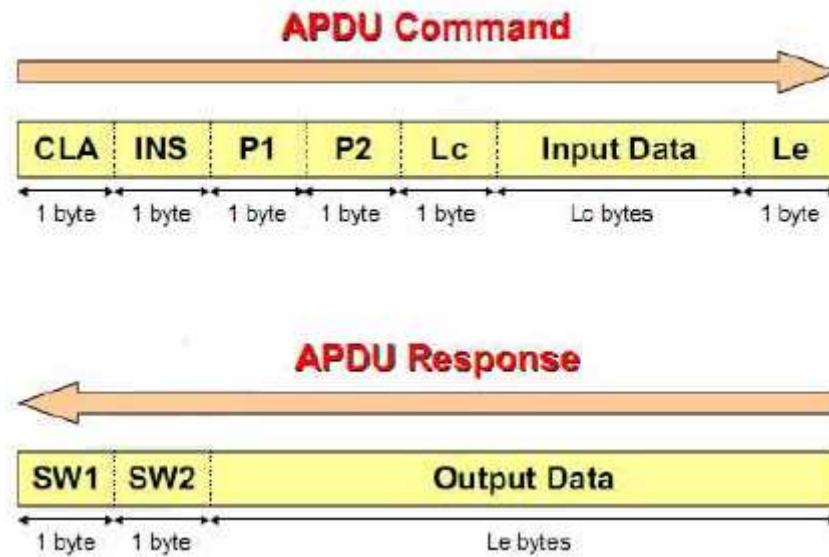
Les commandes APDU

- Les commandes APDU (Applications Protocol data Unit) sont utilisées pour tout échange de données entre le mobile ME et la carte à puce UICC/USIM;
- On distingue deux types d'APDUs:
 - C-APDU: Command APDUs, représentent les commandes vers la carte.
 - R-APDU: Response APDUs, représentent les réponses de la carte à ces commandes;

Format des commandes APDU



ME



USIM



Sélection d'un fichier

La commande **SELECT**:

- **00 A4 00 04 02 XX XX** (XX XX : FID du fichier/répertoire à sélectionner).

- Exemples :

SELECT MF : **00 A4 00 04 02 3F00**
SW1 SW2 = **61 2B**

SELECT EF_{DIR}: **00 A4 00 04 02 2F00**
SW1 SW2 = **61 28**



Lecture du fichier EF_{DIR}

La commande GET RESPONSE:

- **00 C0 00 00 28** (SW2 = **28**).

SW1 SW2 = 90 00

Output: 62 26 82 **05 42 21 00 26 02** 83 02 2F 00 A5 06 80 01 71 C0 01 00
8A 01 05 8B 03 2F 06 02 80 02 00 4C 81 02 00 5A 88 01 F0



Algorithme d'authentification

- **Sur la carte SIM:**
RUN-GSM-ALGORITHM
- **Sur la carte UICC/USIM:**
AUTHENTICATE



Conclusion

- Travail actuel:
 - Authentification
 - Confidentialité et Intégrité des données

- Perspective:
 - USIM Application Toolkit
 - JAVA Card & UICC/USIM



Références

- 3GPP TS 31.102: “*Characteristics of the Universal Subscriber Identity Module (USIM) application*”
- 3GPP TS 21.111: “*USIM and IC card requirements*”
- 3GPP TS 31.121: “*UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification*”

- ETSI TS 101 220: “*ETSI numbering system for telecommunication application providers*”
- ETSI TS 102 221: “*Smart Cards; UICC-Terminal interface; Physical and logical characteristics*”
- ETSI TS 102 226: “*Smart Cards; Remote APDU structure for UICC based applications*”

- Dr. Klaus Vedder - Chairman ETSI TC SCP. Présentation: “*The SIM Turns 20*”. 3rd ETSI Security WorkShop Sophia Antipolis, France, 14-15 January 2008

- Saïd El Hajji, Ghizlane Orhanou. Université Mohammed V-Faculté des sciences Rabat, Laboratoire Mathématique, Informatique et Applications. “*Cryptography in the UMTS Network Access Security*”, International Conference NGN'S09 - Morocco.



Slogan du groupe SMG9 (1998)

Billions of Calls
Millions of Subscribers
Thousands of Different Types of Telephones
Hundreds of Countries
Dozens of Manufacturers ...

... and only one Card
The SIM

Et sa version 3G UICC/USIM