Global Scientific JOURNALS

GSJ: Volume 10, Issue 11, November 2022, Online: ISSN 2320-9186

www.globalscientificjournal.com

Qu'est-ce qu'un SIM ou bien une Carte SIM ?

Jeannot FATAKI N. BAZONGA, PhD
Professeur

Jeannot FATAKI N. BAZONGA, PhD Professeur

RÉSUMÉ

La carte SIM ou carte à puces désigne les supports de sécurité contenant un circuit électronique intégré capable de mémoriser ou de traiter les informations. La carte à puces est à la base de la sécurité des systèmes informatiques. Elle a fait ses preuves dans de nombreux secteurs en tant que moyen de paiement, d'identification ou d'authentification. Aujourd'hui, à la vue des progrès des semi-conducteurs et de l'évolution des techniques de programmation, on prévoit des développements considérables de la carte à puces, qui constitue, pour beaucoup d'applications, une solution particulièrement bien adaptée aux enjeux socio-économiques de notre société.

ABSTRACT

The expression smart card refers to security supports containing an electronic circuit capable of memorizing or processing information. The smart card is at the basis of the safety of computer systems. It has proved its worth in many sectors as a means of payment, identification or authentication. At this time, taking into consideration the advances in semi-conductors and the evolution of the programing techniques, considerable developments are expected for the smart card which is an extremely well-adapted solution for the socio-economic challenges of our society.

Mots-clés

1. ***Puce*** : Le **circuit intégré** (**CI**), aussi appelé **puce électronique**, est un composant électronique reproduisant une, ou plusieurs, fonction(s) électronique(s) plus ou moins complexe(s), intégrant souvent plusieurs types de composants électroniques de base dans un volume réduit (sur une petite plaque), rendant le circuit facile à mettre en œuvre. Il existe une très grande variété de ces composants divisés en deux grandes catégories : analogique et numérique.
2. ***Microcontrôleur*** : (en notation abrégée **µc**, ou **uc** ou encore **MCU** en anglais) est un circuit intégré qui rassemble les éléments essentiels d'un ordinateur : processeur, mémoires (mémoire morte et mémoire vive), unités périphériques et interfaces d'entrées-sorties. Les microcontrôleurs se caractérisent par un plus haut degré d'intégration, une plus faible consommation électrique, une vitesse de fonctionnement plus faible (de quelques mégahertz jusqu'à plus d'un gigahertz) et un coût réduit par rapport aux microprocesseurs polyvalents utilisés dans les ordinateurs personnels. Par rapport à des systèmes électroniques à base de microprocesseurs et autres composants séparés, les microcontrôleurs permettent de diminuer la taille, la consommation électrique et le coût des produits. Ils ont ainsi permis de démocratiser l'utilisation de l'informatique dans un grand nombre de produits et de procédés. Les microcontrôleurs sont fréquemment utilisés dans les systèmes embarqués, comme les contrôleurs des moteurs automobiles, les télécommandes, les appareils de bureau, l'électroménager, les jouets, la téléphonie mobile, etc.
3. ***Téléphonie mobile*** : ou **téléphonie cellulaire** est un moyen de télécommunications, plus précisément de radiocommunication, par téléphone mobile. Ce moyen de communication s'est largement répandu à la fin des années 1990. La technologie associée bénéficie des améliorations des composants électroniques, notamment leur miniaturisation, ce qui permet aux téléphones d'acquérir des fonctions jusqu'alors réservées aux ordinateurs. L'appareil téléphonique en lui-même peut être nommé « mobile », « téléphone portable », « portable », « téléphone cellulaire » (en Amérique du Nord), « cell » (au Québec dans le langage familier), « natel » (en Suisse), « GSM » (en Belgique et au Luxembourg), « vini » (en Polynésie française). Quand il est doté de fonctions évoluées, c'est un smartphone, ordiphone ou téléphone intelligent.
4. ***Réseau mobile*** : Un **réseau de téléphonie mobile** est un réseau téléphonique qui permet l'utilisation simultanée de millions de téléphones sans fil, immobiles ou en mouvement, y compris lors de déplacements à grande vitesse et sur une grande distance. Pour atteindre cet objectif, toutes les technologies d'accès radio doivent résoudre un même problème : répartir aussi efficacement que possible, un spectre hertzien unique entre de très nombreux utilisateurs. Pour cela, diverses techniques de multiplexage sont utilisées pour la cohabitation et la séparation des utilisateurs et des cellules radio : le multiplexage temporel, le multiplexage en fréquence et le multiplexage par codes, ou le plus souvent une combinaison de ces techniques. Un réseau de téléphonie mobile a une structure « cellulaire » qui permet de réutiliser de nombreuses fois les mêmes fréquences ; il permet aussi à ses utilisateurs en mouvement de changer de cellule (handover) sans coupure des communications en cours. Dans un même pays, aux heures d'affluence, plusieurs centaines de milliers, voire plusieurs millions d'appareils sont en service avec (dans le cas du GSM) seulement 500 canaux disponibles.

5. ***GSM*** : ***Global System for Mobile Communications*** (historiquement « Groupe spécial mobile ») est une norme numérique de seconde génération pour la téléphonie mobile. Le groupe de travail chargé de la définir a été établi en 1982 par la Conférence européenne des administrations des postes et télécommunications (CEPT). Elle a été spécifiée et mise au point par l'ETSI (European Telecommunications Standard Institut) pour la gamme de fréquences des 900 MHz. Une variante appelée ***Digital Communication System*** (DCS) utilise la gamme des 1 800 MHz. Cette norme est particulièrement utilisée en Europe, en Afrique, au Moyen-Orient et en Asie. Deux autres variantes, en 850 MHz et en 1 900 MHz PCS (personal communications services), sont également utilisées. La protection des données est assurée par les algorithmes de chiffrement A5/1 et A5/2. Tel qu'il a été conçu, le réseau GSM est idéal pour les communications de type « voix » (téléphonie). Le réseau étant commuté, les ressources ne sont allouées que pour la durée de la conversation, comme lors de l'utilisation de lignes téléphoniques fixes. Les clients peuvent soit acheter une carte prépayée, soit souscrire un abonnement. Sous l'égide de l'organisation 3GPP la norme GSM a ensuite été étendue pour prendre en charge de plus hauts débits et le transport de données en mode « paquet » par les extensions GPRS (General Packet Radio Services) puis EDGE (Enhanced Data rates for GSM Evolution). Ces deux modes peuvent cohabiter avec le mode « voix commutée » du GSM et utilisent les mêmes antennes et les mêmes bandes de fréquence.

6. ***UMTS*** : L'**Universal Mobile Telecommunications System** est l'une des technologies de téléphonie mobile de troisième génération (3G). Elle est basée sur la technologie W-CDMA, standardisée par le 3GPP et constitue l'implémentation dominante, d'origine européenne, des spécifications IMT-2000 de l'UIT pour les systèmes radio cellulaires 3G. L'UMTS est parfois appelé 3GSM, soulignant la filiation qui a été assurée entre l'UMTS et le standard GSM auquel il succède. Elle est également appelée 3G, pour troisième génération.
7. ***LTE*** : (***Long Term Evolution***) est une évolution des normes de téléphonie mobile GSM/EDGE, CDMA2000, TD-SCDMA et UMTS. La norme LTE, définie par le consortium 3GPP, a d'abord été considérée comme une norme de troisième génération « 3.9G » (car proche de la 4G), spécifiée dans le cadre des technologies IMT-2000, car dans les « versions 8 et 9 » de la norme, elle ne satisfaisait pas toutes les spécifications techniques imposées pour les normes 4G par l'Union internationale des télécommunications (UIT). La norme LTE n'est pas figée, le consortium 3GPP la fait évoluer en permanence (en général, une nouvelle version tous les 12 à 18 mois). En octobre 2010, l'UIT a reconnu la technologie LTE-Advanced (évolution de LTE définie par le 3GPP à partir de sa release 10) comme une technologie 4G à part entière ; puis, il a accordé en décembre 2010, aux normes LTE et WiMAX définies avant les spécifications « IMT-Advanced » et qui ne satisfaisaient pas complètement à ses prérequis, la possibilité commerciale d'être considérées comme des technologies « 4G », du fait d'une amélioration sensible des performances comparées à celles des premiers systèmes « 3G » : UMTS et CDMA2000. Les réseaux mobiles LTE sont commercialisés sous l'appellation « 4G » par les opérateurs de nombreux pays, par exemple : Proximus, Base, VOO Mobile et Orange en Belgique, Swisscom et Sunrise en Suisse, Verizon et AT&T aux États-Unis, Vidéotron, Rogers et Fido Solutions au Canada, Orange, Bouygues Telecom, SFR et Free mobile en France, Algérie Télécom en Algérie, Maroc Telecom, Orange et Inwi au Maroc... Le LTE utilise des bandes de fréquences hertziennes d'une largeur pouvant varier de 1,4 MHz à 20 MHz dans une plage de

fréquences allant de 450 MHz à 3,8 GHz selon les pays. Il permet d'atteindre (pour une largeur de bande de 20 MHz) un débit binaire théorique de 300 Mbit/s en « liaison descendante » (*downlink*, vers le mobile). La « vraie 4G », appelée *LTE Advanced*[1] offre un débit descendant atteignant ou dépassant 1 Gbit/s ; ce débit nécessite l'utilisation de bandes de fréquences agrégées de 2×100 MHz de largeur qui sont définies dans les versions 10 à 15 (3GPP releases 10, 11, 12, 13, 14 et 15) des normes *LTE Advanced*.

8. ***Opérateur*** : Un **opérateur de réseau mobile** est une compagnie de télécommunication qui propose des services de téléphonie mobile ou d'accès mobile à Internet. L'opérateur fournit une carte SIM au client qui l'insère dans son téléphone mobile ou sa tablette tactile pour avoir accès au réseau cellulaire de l'opérateur (normes: GSM, CDMA, UMTS, WiMAX ou LTE). L'opérateur de réseau mobile est également chargé, du marketing, de la commercialisation, de la facturation et de l'assistance à sa clientèle ; toutefois, un opérateur peut externaliser n'importe laquelle de ces fonctions et être encore considéré comme un opérateur de réseau mobile. La téléphonie mobile est structurée autour de deux types d'opérateurs de réseau mobile : les opérateurs classiques (aussi appelés MNO) possédant leur propre réseau mobile, et les opérateurs virtuels (aussi appelés MVNO) qui utilisent le réseau des opérateurs classiques. Par exemple en France, on compte :

- quatre opérateurs classiques : Orange, SFR, Bouygues Telecom, et Free Mobile ;
- une quarantaine d'opérateurs de réseau mobile virtuels ;

Les opérateurs virtuels utilisent « en itinérance » le réseau d'un des opérateurs qui disposent d'un réseau physique et de fréquences hertziennes attribuées par l'autorité du pays (en France par l'ARCEP, voir par exemple « UMTS, fréquences FDD » pour les fréquences attribuées en France pour les réseaux UMTS). Le choix de l'opérateur de rattachement des MVNO peut changer en fonction des accords commerciaux entre les sociétés concernées. Chaque opérateur, classique ou virtuel peut commercialiser des offres sous une ou plusieurs marques.

9. ***CDMAOne*** : **Interim Standard 95**, souvent abrégé en **IS-95**, et souvent appelé **CDMAOne**, est une norme définissant la communication radioélectrique entre un terminal mobile et une station de base dans un réseau de téléphonie mobile utilisant la technique de multiplexage CDMA (Code Division Multiple Access). La norme IS-95 a été définie par Qualcomm. La norme concurrente GSM utilise deux autres techniques de multiplexage, TDMA (Time division multiple access) et FDMA (Frequency Division Multiple Access).
10. ***PDC*** : Le **Personal Digital Cellular**, plus communément appelé **PDC** est une norme de téléphonie mobile de seconde génération qui était utilisée au Japon jusqu'en 2012. Il s'agit d'une technique basée sur le *TDMA* (Time Division Multiple Access) à l'instar du GSM et qui a été lancée par NTT DoCoMo en 1991 pour remplacer le système 1G précédent.
11. ***CDMA2000*** : est une technologie de téléphonie mobile reconnue, dans sa variante 1x EV-DO, comme de troisième génération (3G) par l'Union internationale des télécommunications (UIT), tout comme l'UMTS et qui prolonge la technologie américaine de seconde génération (2G), le CdmaOne. D'autres technologies 2G ont choisi d'évoluer vers la technologie UMTS pour la 3G (exemple : le TDMA en Amérique, le PHS au Japon). CDMA2000 marque une évolution de la technologie de seconde génération IS-95, très minoritaire dans le monde mais présente sur des marchés clés : majoritaire aux États-Unis, minoritaire au Japon, 100 % du marché de la 2G en Corée du Sud… Son déploiement a commencé au début des années 2000 en Corée du Sud avec la technologie CDMA2000 1x EV-DO (pour « 1X Evolution - Data Optimized »), en attendant l'EV-DV (1X Evolution - Data and Voice). Le passage de la 2G à la 3G est plus facile dans la famille CDMA/CDMA2000 que dans la famille

GSM/UMTS : sur le plan technique, il s'agit d'une simple évolution et non d'une révolution, et la technologie se révèle plus fruste et intégrée. Par exemple : il n'existe pas d'équivalent de la carte SIM ou USIM, un terminal ne peut donc être utilisé que chez l'opérateur qui fournit le terminal au départ. La famille des technologies CDMA, normalisée par l'organisme 3GPP2 a été développée de bout en bout par la société américaine Qualcomm. En tant que propriétaire des droits, Qualcomm réalisait une grande part de son chiffre d'affaires avec ses licences CDMA tout en investissant en parallèle sur les normes concurrentes telle le LTE), quitte à en ralentir la finalisation en multipliant les développements. Le CDMA2000 a tiré profit d'une fenêtre de tir avant le lancement de la 3G W-CDMA / UMTS : à fin 2004, grâce à 107 opérateurs dans 53 pays, il la dominait largement pour ce qui est du nombre de clients (145 millions contre 16). Mais si le W-CDMA ne pesait que 10 % du parc 3G mondial, sa part dans les royalties de Qualcomm a bondi en 2004 de 12 à 32 % en un an. La famille GSM / UMTS a remonté ensuite progressivement jusqu'à une part du marché 3G plus conforme à sa domination sur la 2G. En revanche, le 3GPP à l'origine des normes UMTS a retenu la leçon et a cherché à ne pas se faire prendre de vitesse pour les évolutions 3G-4G, alors que la pression montait depuis les technologies mobiles concurrentes (Wi-Fi, WiMAX, WiBro, UWB…). C'est pourquoi les investissements ont repris fortement à la fin des années 2000 sur les technologies 3G issues de l'UMTS comme la HSDPA et le HSPA+, puis sur le LTE (4G).

12. ***3GPP2*** : L'association **3GPP2** (de l'anglais « ***3rd Generation Partnership Project 2*** ») est issue d'un accord de collaboration établi en décembre 1998, entre ARIB (la société japonaise radio-industrielle et des entreprises), CCSA **(en)** (Chine), TIA **(en)** (l'association industrielle des télécommunications - Amérique du Nord) et TTA **(ko)** (Corée du Sud). L'objectif du 3GPP2 était de définir et de maintenir une des familles de spécifications pour les systèmes globaux de téléphonie mobile de troisième génération (3G) compatibles avec le projet IMT-2000 de l'UIT. Dans la pratique, 3GPP2 est le groupe de standardisation pour les normes CDMA 2000 et CDMA EVDO : l'ensemble des normes 3G basées sur la technologie issue du standard 2G américain CDMA. À noter que le 3GPP2 est différent et concurrent du 3GPP, lequel spécifie les standards pour d'autres technologies de téléphonie mobile connues sous les noms de W-CDMA (UMTS) et LTE.
13. ***IMSI*** : L'***International Mobile Subscriber Identity*** est un numéro unique, qui permet à un réseau de téléphonie mobile de type GSM, UMTS ou LTE d'identifier un usager. Ce numéro est stocké dans la carte SIM (ou USIM en UMTS et LTE) et n'est pas connu de l'utilisateur. Pour atteindre l'utilisateur, l'opérateur lui attribue un numéro MSISDN qui est la version avec préfixe international de ce qu'on appelle communément un « numéro de téléphone ».
14. ***MCC*** : Le **mobile country code** est un code pays sur trois chiffres, standardisé par l'Union internationale des télécommunications (UIT) dans sa recommandation E.212, pour les réseaux de téléphonie mobile, plus particulièrement dans les technologies GSM et UMTS. Le MCC constitue notamment les trois premiers chiffres de l'International Mobile Subscriber Identity (IMSI), qui identifie les abonnés et est enregistré sur les cartes SIM.
15. ***MNC*** : Un **Mobile Network Code** est utilisé en combinaison avec le Mobile country code (MCC) pour l'identification univoque du réseau d'un opérateur de réseau mobile utilisant les normes GSM, CDMA, TETRA, UMTS, LTE et certains réseaux satellite mobile. Cet identifiant (MCC+MNC) est diffusé par les antennes-relais du réseau mobile. En 3G (UMTS) et 4G (LTE), plusieurs codes MNC peuvent être diffusés par une même antenne pour permettre la mutualisation du réseau radio. La recommandation E.212 de l'ITU-T définit le format et les principes des *Mobile Country Code* et des *Mobile Network Codes*. Le « Mobile Network Code » (MCC+MNC) est aussi présent dans les cartes SIM (premiers

chiffres du n° IMSI) de tous les abonnés mobiles ; il permet aux BTS ou Node B des opérateurs dont les cellules radio sont « visitées » d'identifier et d'authentifier les téléphones mobiles présents dans leurs cellules radio et, en interrogeant le HLR et l'AuC de l'opérateur identifié grâce aux codes « MCC+MNC » du mobile, de déterminer si ce téléphone mobile est autorisé (ou pas) à accéder au réseau et avec quels droits ; en pratique, cela permet aussi de savoir si un accord d'itinérance a été conclu entre l'opérateur d'origine de l'abonné mobile et l'opérateur de la cellule où se trouve le mobile.

16. ***MSIN*** : Un ***Mobile identification number*** (**MIN**) aussi appelé **MSIN** (*Mobile Subscriber Identification Number*) dans les normes 3GPP, est un identifiant unique à 10 chiffres décimaux qu'un opérateur de réseau mobile utilise pour identifier un téléphone mobile dans son réseau. Le MIN/MSIN constitue les 10 chiffres de poids faible du n° IMSI qui permet d'identifier un abonné GSM ou UMTS et est inscrit dans sa carte SIM (associé au codes MCC + MNC qui identifient l'opérateur mobile). Certains numéros réservés permettent aussi d'identifier les équipements du cœur de réseau d'un opérateur donné (via leur APN). Un MIN sert également d'identifiant unique pour un téléphone mobile qui respecte les standards américains TIA/3GPP2 qui s'appliquent aux appareils de technologie cellulaire ou PCS (par exemple, EIA/TIA–553 analog (AMPS), IS–136 TDMA, IS–95 ou IS-2000 CDMA).

INTRODUCTION

La carte **SIM** (de l'anglais *Subscriber Identity Module*) est une puce contenant un microcontrôleur et de la mémoire. Elle est utilisée en téléphonie mobile pour stocker les informations spécifiques à l'abonné d'un réseau mobile, en particulier pour les réseaux GSM, UMTS et LTE.

Elle permet également de stocker des données et des applications de l'utilisateur, de son opérateur ou dans certains cas de tierces parties. D'autres systèmes de téléphonie mobile comme le CDMAOne, le PDC japonais ou le CDMA2000 défini par le 3GPP2 prennent en charge optionnellement une telle carte.

La carte SIM contient un numéro IMSI, constitué du code pays (MCC), de l'identifiant de l'opérateur (MNC), et de l'identifiant de l'abonné (MSIN).

Le nom de **carte à puces** est couramment utilisé pour désigner des supports de sécurité qui ont les mêmes dimensions qu'une carte de crédit en matière plastique et qui contiennent un circuit électronique intégré capable de mémoriser ou de traiter les informations. L'AFNOR (Association Française de Normalisation) a retenu le terme de **cartes à microcircuits à contacts**, car l'interface électrique de ces cartes est assurée par des liaisons galvaniques. De nouvelles cartes à interface sans contact, basée sur liaison radiofréquence sont cependant de plus en plus répandues.

La carte à puces, dont la gestation a pu sembler très longue, est à la base de la sécurité des systèmes informatiques. Elle a désormais fait ses preuves dans de nombreux secteurs de l'activité humaine en tant que moyen de paiement, d'identification sur les réseaux fixes (de

type Internet), mobiles (GSM ou UMTS) ou multimédia (télévision à péage), d'authentification pour les services gouvernementaux (cartes d'identité, passeports électroniques). Aujourd'hui, la **carte SIM**, **ou USIM**, clé d'accès aux réseaux de téléphonie mobile, constitue probablement le composant électronique intelligent le plus utilisé dans le monde (plus d'un milliard d'unités vendues en 2005 !). De même, la **carte bancaire** à microcalculateur, dont l'utilisation s'est généralisée en France depuis 1992, a connu une croissance quasi exponentielle avec une généralisation de son utilisation en Europe et des perspectives de déploiement très fortes au Japon, en Chine ainsi qu'aux États-Unis en version « sans contact ».

À la vue des progrès continuels des semi-conducteurs et de l'évolution des techniques de programmation utilisables, on avait prévu à moyen et long terme des développements considérables de la carte à puces, qui constitue, pour beaucoup d'applications, une solution particulièrement bien adaptée aux enjeux socio-économiques de notre société.

Notez bien :

En électronique et en informatique, il existe un grand nombre de termes ou d'abréviations anglais non traduisibles. Ces termes sont donc repris en tant que tels dans cet article.

Cartes SIM.

1. Généralités

Carte SIM avec le logo de l'opérateur, E-Plus (en).

Tiroir carte SIM et son extracteur en métal, sur un iPhone 3G.

Le choix de l'intégration d'une carte à puce dans les systèmes de téléphonie mobile est basé sur la nécessité de disposer des éléments suivants :

- Un élément **sécurisé** contenant l'identifiant et les données de connexion d'un utilisateur donné ;

- Un élément **amovible** permettant de personnaliser un nouveau téléphone avec les données de connexion ; l'intérêt est de séparer le choix d'un terminal de la notion d'abonnement ;
- Un espace de **stockage d'information** pour les données personnelles de l'abonné (son annuaire), mais également des paramètres de personnalisation de son terminal (paramètres de messagerie, etc.) ;
- Un espace pour les applications de l'opérateur de téléphonie.

Il convient de signaler que le terme « carte SIM » est un abus de langage (un raccourci en fait), SIM désignant en fait l'application GSM, définie dans la spécification ETSI/3GPP TS 51.011[1], qui réside sur une carte, nommée, en anglais, UICC (pour « *Universal Integrated Circuit Card* »).

Les cartes SIM ont progressivement été remplacées par des cartes USIM (l'équivalent de l'application SIM pour l'UMTS), définies dans les spécifications 3GPP TS 31.102 (application USIM) et TS 21.111[2] et qui sont compatibles avec les réseaux GSM, EDGE, UMTS et LTE.

L'UICC et l'application SIM gèrent l'authentification de l'abonné dans le réseau GSM (l'USIM pour le réseau UMTS) et génèrent des clés qui permettent le chiffrement du flux de données, ceci étant réalisé au sein du terminal mobile.

L'UICC peut également contenir et exécuter des applications sur la base du SIM Application Toolkit (USIM Application Toolkit dans le cas de l'UMTS) et d'un environnement applicatif Java Card. Ces applications sont généralement la propriété de l'opérateur qui peut les télécharger sur la carte.

Une carte SIM donnée est issue d'un seul opérateur ou d'un seul MVNO et permet son identification univoque (grâce au numéro IMSI, constitué des codes MCC + MNC + MSIN, intégré dans la carte).

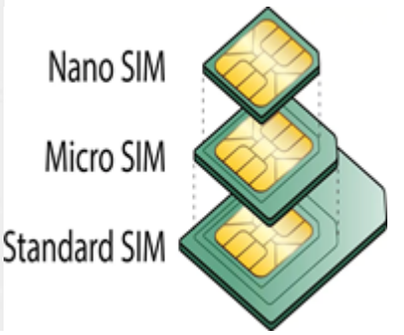
2. Caractéristiques physiques

2.1. Formats

Pour utiliser son smartphone, il faut utiliser une carte SIM. Il en existe différents formats :

- La **carte SIM** : 86 x 54 x 0,76 mm.
- La mini **SIM** : 25 x 15 x 0,76 mm.
- La micro **SIM** : 15 x 12 x 0,76 mm.
- La nano **Sim** : 12,3 x 8,8 x 0,67 mm.
- L'e-**SIM** : directement intégrée au smartphone (6 x 5 x moins de 1 mm).

1 (en) ETSI TS 51.011, rel.4 - Specification of the Subscriber Identity Module, ETSI/3GPP standard, mars 2001.
[2] (en) 3GPP TS 21.111, rev.8 - USIM card requirements, 3GPP standard, janvier 2010.



Les 4 formats de carte SIM (de gauche à droite :
1) Full size SIM
2) Standard / Mini SIM (2FF)
3) Micro SIM (3FF)
4) Nano SIM (4FF)

Carte SIM livrée au format carte de crédit par l'opérateur T-Mobile. La partie centrale se détache pour pouvoir être insérée dans le téléphone.

L'UICC (carte SIM) a été définie avec plusieurs formats[3] :

- format ID-1 (ISO/CEI 7810), le format des cartes de crédit, rapidement écarté car trop contraignant pour la conception des téléphones mobiles (85,6 mm de long, 54,0 mm de large et 0,76 mm d'épaisseur[4]).
- format ID-000 (ISO/CEI 7810) ou Plug-in UICC ou 2FF, aussi appelée *Mini SIM* ou *Standard SIM*, le plus répandu des formats dans les téléphones mobiles GSM ou UMTS (25 mm de long, 15 mm de large et 0,76 mm d'épaisseur[4]).
- format Mini-UICC ou 3FF, commercialement nommé *Micro SIM* par les opérateurs, spécifié en 2000 par l'ETSI à l'initiative de l'opérateur mobile japonais NTT DoCoMo. Ce format (rétrocompatible avec un adaptateur) a été imaginé pour permettre la miniaturisation extrême de terminaux. Ce format a été utilisé la première fois par LG Electronics pour l'opérateur « 3 » en Italie[5, 6] en guise de SIMLock

[3] Voir ETSI TS 102 221, sur le site de l'ETSI
[4 a et b] SIM Card Dimensions, Dimensions guide.com, consulté en mai 2012.
[5] GSM Arena, LG U900 caractéristiques techniques
[6] (en) LG U900 Press Release

physique, puis en volume par Apple (2010) pour l'iPad[7]. Le format est maintenant largement répandu (15 mm de long, 12 mm de large et 0,76 mm d'épaisseur[8]).

- format 4FF, commercialement nommé *Nano SIM* a été proposé par Apple avec le support de la plupart des opérateurs mobiles. Comme pour le 3FF, il s'agit de réduire la taille de la carte (approximativement 30 %) sans changer l'emplacement des contacts[9]. Apple est en septembre 2012 le premier fabricant à avoir adopté ce nouveau format, avec l'iPhone 5[10], suivi de Nokia qui l'utilisera pour le Lumia 1520.

Tailles des cartes SIM				
Carte SIM	**Norme de référence**	**Longueur (mm)**	**Largeur (mm)**	**Épaisseur (mm)**
Full size / 1FF / ID-1 UICC	ISO/CEI 7810:2003, ID-1	85,60	53,98	0,76
Standard SIM / 2FF / Plug-in UICC	ISO/CEI 7810:2003, ID-000	25,00	15,00	0,76
Micro SIM / 3FF / Mini-UICC	ETSI TS 102 221	15,00	12,00	0,76
Nano SIM / 4FF	ETSI TS 102 221	12,30	8,80	0,67
Embedded SIM	JEDEC Design Guide 4.8, SON-8	6,00	5,00	<1,0

2.2. Composants

L'UICC utilise un microprocesseur et de la mémoire.

Les capacités mémoire typiques en 2006 sont de 32 ou 64 ko. Dans le cas de cartes « haut de gamme » pour des fonctionnalités comme un annuaire utilisateur important ou le support d'applications, les grands opérateurs européens achetaient alors des cartes d'une capacité de 128 ou 256 ko. La carte pouvait alors héberger des fichiers, des paramètres d'applications et de services du mobile, et même des applications exécutables dans la carte elle-même, par exemple, en Java Card.

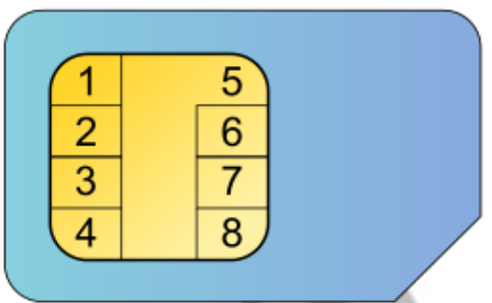
Une tendance s'était dessinée dès 2006 à l'extension de la capacité mémoire vers des mégaoctets ou des giga-octets. L'UICC pouvait alors reprendre en son sein les fonctions habituellement associées aux MMC ou SD Cards : stockage agrandi, mais également sécurisation de contenu et d'applications. Toutefois, devant le coût de ces solutions, un

[7] iPad : mais qu'est-ce qu'une carte microSIM ? - Maxime Johnson, 2 février 2010.
[8] Apple a annoncé que le nouvel iPad contient une « micro-SIM ». Qu'est-ce qu'une micro-SIM ? Just ask gemalto.com, consulté en mai 2012.
[9] Les industriels des télécoms se déchirent sur le futur de la carte SIM - Maxime Amiot et Solveig Godeluck, *Les Échos*, 29 mars 2012.
[10] PCINpact - Quid de la disponibilité de la nano SIM chez les opérateurs.

modèle d'affaire inexistant et certaines difficultés d'implémentation, les solutions techniques n'avaient vu le jour que sous la forme de prototypes.

La technologie mémoire utilisée dans la carte a d'abord été de l'EEPROM, mais s'est rapidement tourné vers la Flash (en NAND plus qu'en NOR), bien plus flexible dans l'utilisation et maîtrisée pour les grandes capacités. Cependant, de plus en plus et à cause de l'intégration du multimédia, on sépara la mémoire et la carte SIM en s'orientant vers l'utilisation d'une carte Flash additionnelle permettant ainsi une plus grande flexibilité d'usage des données, sauf pour ce qui concerne le carnet d'adresse qui reste souvent encore traditionnellement sur la carte afin de faciliter le changement de GSM même si certains veulent encore croire au modèle intégré en insérant une micro Flash au sein même de la puce[11].

2.3. Interface physique



Les contacts d'une carte SIM.
1 : VCC (alimentation)
2 : RST (remise à zéro)
3 : CLK (horloge)
4 : D+ (USB Inter-chip)
5 : GND (masse)
6 : SWP
7 : I/O (entrée/sortie)
8 : D- (USB Inter-chip)

L'interface physique de la carte a huit contacts.

Pendant longtemps, seuls cinq contacts ont été utilisés pour l'implémentation de l'interface dite ISO[12]. L'implémentation de nouvelles fonctions implique l'utilisation des contacts supplémentaires définis mais reste optionnelle.

L'USB (choisi comme interface rapide) utilise les contacts C4 et C8 ; cette interface est définie dans le standard ETSI TS 102.600. Le contact C6 est utilisé pour une interface vers un module *contactless* qui permet l'accès à des services de type NFC quel que soit le mode (émulation de carte, lecteur et peer to peer) afin d'adresser des applications de transport (de type Navigo), de paiement, de lecture de tags RFID et d'échange de données (P2P).

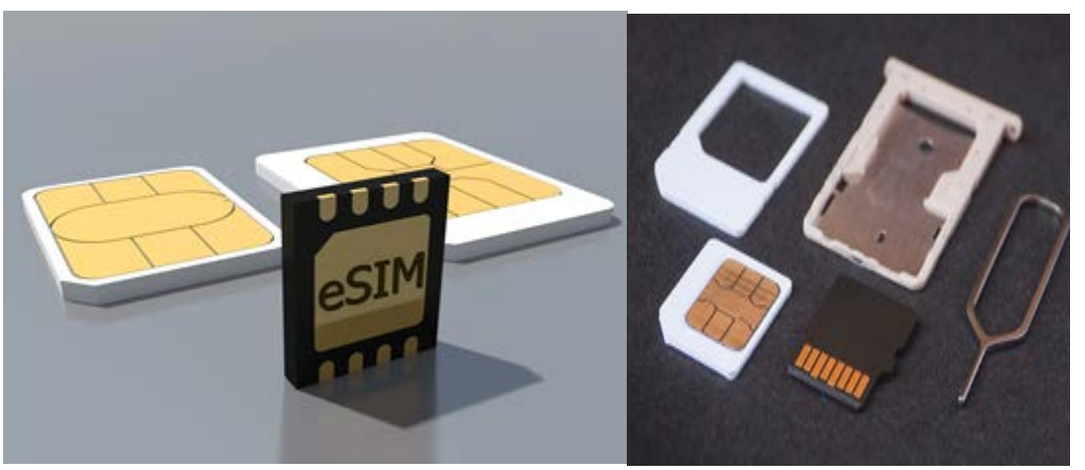
[11] Oberthur une solution à forte capacité mémoire en partenariat avec Spansion.
[12] Voir les spécifications ISO 7816.

L'interface vers le module sans contact est définie dans les standards TS 102.613 (SWP) et TS 102.622 (HCI).

Il existe également des cartes SIM ne disposant que de six contacts, sur lesquelles les contacts C4 et C8 sont absents. Cela est d'office le cas pour les cartes compatibles avec le format Nano SIM (4FF).

Suivant les générations de puces, la tension peut varier de 5 V (voire 5,5 V) pour les modèles les plus gourmands (tous les modèles antérieurs à 1998 ainsi que certains modèles plus récents) à 1,8 V pour les plus économes, en passant par la valeur intermédiaire, la plus fréquente, de 3 ou 3,3 V[13,14]. Certains appareils récents ne supportent plus les cartes SIM exigeant une tension de 5 V (par exemple l'Alcatel 1010[15]) sorti en 2015.

Une nouvelle spécification de la carte SIM, la eSIM, a été définie, pour virtualiser totalement la carte SIM, et ainsi intégrer ses fonctions dans une puce soudée à la carte mère, voire directement au sein des processeurs des téléphones mobiles[16, 17].



Le logo de la carte SIM virtuelle eSIM

3. Caractéristiques logicielles

3.1. Numéro de série de carte externe

En France, le numéro de série de carte externe ou NSCE est une séquence correspondant à une suite de quatorze chiffres inscrite sur la carte SIM permettant d'identifier l'opérateur ayant mis en service la carte.

3.2. Protocoles

[13] La carte SIM nouvelle génération de Free Mobile poserait des problèmes de compatibilité, Univers Freebox, publié le 12 février 2012 par Olivier Viaggi. Consulté le 15 février 2015.

[14] Free Mobile et les cartes SIM : pas de NFC ou de 5,5 V… , Tom's Hardware, publié le 13 février 2012 par Pierre Dandumont. Consulté le 15 février 2015.

[15] Manuel d'utilisation des Alcatel OneTouch 1010D et 1010X [PDF] (cf. note de bas de page en p. 13), alcatelonetouch.com. Consulté le 15 février 2015

[16] (en-GB) « Highlights of Mobile World Congress 2017 Seminar: eSIM – a New SIM for a New Generation of Connected Consumer Devices - eSIM », *eSIM*, 31 sram2017.

[17] www.gsma.com/esim/wp-content/uploads/2017/03/4.Qualcomm_iUICCDemo-for- MWC_Final_Feb02_2017.pdf

Le protocole utilisé à l'origine sur la carte SIM est le protocole de base de la carte à puce, le protocole T=0. Les caractéristiques principales de ce protocole sont les suivantes :

- asynchrone ;
- en mode caractère ;
- en semi-duplex.

Deux nouveaux protocoles ont été ajoutés en 2006 et 2007 à savoir :

- l'USB IC (Inter-Chip) qui présente les caractéristiques de performance de l'USB full speed (12 Mbit/s half duplex) et est défini dans le standard ETSI TS 102.600. Cependant, l'interface électrique a été adaptée pour une communication à courte distance au sein d'un équipement afin de réduire l'énergie nécessaire à l'interface physique. Trois classes sont disponibles sur cette interface USB :
  - ICCD (Integrated Circuit Card Devices) permet d'émuler l'interface historique et le transport d'informations suivant le standard ISO/IEC 7816-4,
  - Mass storage permet d'émuler un disque ou une clé de stockage mémoire,
  - EEM (Ethernet Emulation Mode) permet de transporter des paquets IP et donc de supporter des protocoles comme TCP/IP ou UDP/IP ;

- le SWP (Single Wire Protocol) est définie dans les standards ETSI TS 102.613 et ETSI TS 102.622 et fonctionne suivant les caractéristiques suivantes :
  - full duplex,
  - jusqu'à 1,6 Mbit/s,
  - transmission de paquets (bit oriented).

3.3. Système d'exploitation

Le système d'exploitation des cartes SIM est le plus souvent propriétaire, codé par les encarteurs et généralement inscrit sur les composants par les fondeurs. Microsoft a tenté au début des années 2000 de proposer un système Windows Mobile for Smart Card, sans succès. L'initiative a été abandonnée, les opérateurs préférant l'expertise propriétaire de leurs fournisseurs.

La mémoire est organisée en répertoires et fichiers (identifiant de l'opérateur, données liées au réseau, numéros d'appels d'urgence, entrées du répertoire, etc.). Le microcontrôleur assure l'accès à ces données (droits), les fonctions de cryptographie (par exemple liées au code PIN) et l'exécution des applications de l'opérateur.

3.4. Boîtes à outil SIM

Les cartes SIM contiennent de plus des boîtes à outil permettant de contrôler l'ensemble des fonctions du téléphone (micro, caméra, appel, SMS).

- En 2G, SIM Application Toolkit (en) (STK) est utilisé
- En 3G, USIM Application Toolkit (en) (USAT) est utilisé
- La norme 4G utilisée est le LTE (Long Term Evolution) et elle utilise les bandes de fréquences des 2 600 MHz et des 800 MHz.

- Il existe depuis une version plus générique appelée Card Application Toolkit[18].

Des agences de renseignements comme la NSA, ont dans leur catalogue (NSA ANT catalog (en)) des outils permettant de modifier ce firmware et de prendre le contrôle de toutes ces opérations[19].

3.5. Machines virtuelles

Les cartes SIM de générations plus récentes sont capables d'héberger des applications destinées à l'abonné, par exemple l'information à la demande (météo, horoscope). Ces applications sont le plus souvent décrites dans un sous-ensemble du langage Java : le Java Card, spécifié dans le cadre du Java Card Forum.

3.6. Téléchargement

La carte dispose de la possibilité de modifier et mettre à jour à distance le contenu de certains fichiers de la carte par téléchargement *over the air* (OTA).

Le canal SMS peut être utilisé pour cela depuis longtemps de manière transparente au travers du terminal mobile. Un autre système, nommé *Bearer Independent Protocol* (BIP) permet de réaliser un téléchargement à partir d'autres médias proposés par le terminal (par exemple GPRS). Cela a ouvert des horizons d'applications comme la sauvegarde du répertoire de la SIM sur un serveur.

Plus récemment, la standardisation de l'interface USB_IC (Interchip USB) a ouvert la possibilité de transfert rapide et important de données entre une carte et un terminal.

3.7. Verrouillage

Le verrouillage SIM (ou SIM lock) permet aux opérateurs de téléphonie mobile de restreindre l'utilisation de leur terminal mobile (téléphone) à une carte SIM ou un groupe de cartes SIM. De ce point de vue, le SIM lock n'est pas une fonctionnalité de la carte SIM, mais du téléphone qui identifie une carte pour fonctionner normalement. Cette fonctionnalité est demandée par les opérateurs ou fournisseurs de service qui subventionnent l'achat de terminaux et qui ne souhaitent pas en retour que ces terminaux soient utilisés chez leurs concurrents.

À ce jour, ce type de verrouillage d'un téléphone peut limiter l'utilisation d'un terminal grâce à l'exploitation d'informations sur la carte SIM au niveau :

- d'un opérateur ;
- d'un groupe d'utilisateurs (une flotte, une offre particulière d'un opérateur, etc.) ;
- d'une unique carte SIM.

Le verrouillage le plus utilisé est celui forçant un opérateur donné (*service provider lock* ou SP-lock). Les téléphones proposés à la vente par les opérateurs de téléphonie mobile sont

[18] (en) « ETSI TS 102 223 V9.1.0 » , etsi.org (consulté le 5 octobre 2017).
[19] (en) « A Peek Inside The NSA's Spy Gear Catalogue », Gizmodo Australie, 1er janvier 2014 (consulté le 5 octobre 2018).

souvent verrouillés et moins onéreux que les mêmes modèles sans verrou, du fait des revenus supplémentaires attendus de la part de l'abonné sous contrat.

Le verrouillage le plus restrictif est celui forçant l'utilisation d'une carte SIM unique donnée.

Un téléphone peut être déverrouillé (désimlocké[20]) en entrant un code spécifique (le code NCK) au clavier. Dans certains cas, l'opérateur peut procéder à l'opération à distance. Le déverrouillage nécessite la connaissance du numéro IMEI d'identifiant du téléphone, obtenu en tapant *#06# au clavier. Il existe des cadres légaux. En Europe par exemple, mais également à des niveaux nationaux qui imposent aux opérateurs utilisant cette fonctionnalité de donner à l'utilisateur qui le demande la faculté de déverrouiller leur téléphone à l'issue d'une période donnée (maximum six mois selon la Commission européenne et l'ARCEP[21]).

En France, en 2015, la période donnée par les opérateurs Bouygues Telecom, Orange et SFR était de trois mois à l'initiative de la Fédération française des télécoms. Free mobile ne verrouillait pas ses terminaux, la plus grande partie n'ayant pas été subventionnée mais potentiellement vendue à crédit. La formule fut reprise par B &You, l'intérêt étant d'appuyer le principe du « sans engagement » en n’empêchant pas l'abonné de changer d'opérateur en réutilisant son terminal. En contrepartie, les téléphones furent moins ou pas subventionnés chez ces opérateurs.

4. Acteurs du domaine

Les principaux acteurs du domaine sont les fournisseurs de composants (dits fondeurs) et les fabricants de carte (dits encarteurs).

4.1. Fondeurs

Les fabricants de composants (fondeurs de silicium) pour carte à puce fournissent le composant vierge ou « masqué » dans le cas de composants disposant de mémoire ROM.

Les plus connus sont :

- Infineon Technologies ;
- Samsung Electronics ;
- ST Microelectronics ;
- Inside Secure ;
- EM Microelectronic-Marin (en) ;
- Renesas Technology ;
- StarChip.

4.2. Encarteurs

Les encarteurs conçoivent toute la partie logicielle (OS et applications), l'insertion du composant dans le plastique (encartage), la personnalisation graphique du support de carte,

[20 a et b] Les obligations de désimlockage des téléphones mobiles brizawen.com, consulté le 15 février 2015

[21] Arcep - Décision n° 2005-1083, voir article 5.

la personnalisation des fichiers, la distribution aux opérateurs ou aux fournisseurs de service de manière plus générale.

Les plus connus sont :

- Gemalto (fusion de Gemplus et de Axalto) ;
- Oberthur Technologies ;
- Giesecke & Devrient ;
- Morpho e-Documents (anciennement Sagem Orga) ;
- ST Incard ;
- Valid (anciennement Microelectrónica Española) ;
- CardLogix ;
- Datang ;
- Watchdata.

5. Mesures anti-terrorisme

En Belgique, il n'est plus possible d'acheter une carte SIM prépayée de manière anonyme depuis fin 2016. Il faut maintenant être identifié par sa carte d'identité lors de l'achat. Les cartes existantes avant cette date et qui n'ont pas été identifié au 7 juin 2017 avaient été bloqué par les opérateurs de téléphonie mobile.

CONCLUSION

Nous venons de voir que la carte **SIM** (de l'anglais *Subscriber Identity Module*) est une puce contenant un microcontrôleur et de la mémoire. Elle est utilisée en téléphonie mobile pour stocker les informations spécifiques à l'abonné d'un réseau mobile, en particulier pour les réseaux GSM, UMTS et LTE.

Elle permet également de stocker des données et des applications de l'utilisateur, de son opérateur ou dans certains cas de tierces parties. D'autres systèmes de téléphonie mobile comme le CDMAOne, le PDC japonais ou le CDMA2000 défini par le 3GPP2 prennent en charge optionnellement une telle carte.

La carte SIM contient un numéro IMSI, constitué du code pays (MCC), de l'identifiant de l'opérateur (MNC), et de l'identifiant de l'abonné (MSIN).

Le nom de **carte à puces** est couramment utilisé pour désigner des supports de sécurité qui ont les mêmes dimensions qu'une carte de crédit en matière plastique et qui contiennent un circuit électronique intégré capable de mémoriser ou de traiter les informations. L'AFNOR (Association Française de Normalisation) a retenu le terme de **cartes à microcircuits à contacts**, car l'interface électrique de ces cartes est assurée par des liaisons galvaniques. De

nouvelles cartes à interface sans contact, basée sur liaison radiofréquence sont cependant de plus en plus répandues.

À la vue des progrès continuels des semi-conducteurs et de l'évolution des techniques de programmation utilisables, on avait prévu à moyen et long terme des développements considérables de la carte à puces, qui constitue, pour beaucoup d'applications, une solution particulièrement bien adaptée aux enjeux socio-économiques de notre société.

Nous osons croire que cette notion de carte SIM ne prêtera plus des confusions quant à son employabilité.

Bibliographie sommaire

1. (en) ETSI TS 51.011, rel.4 - Specification of the Subscriber Identity Module ETSI/3GPP standard, mars 2001.
2. (en) 3GPP TS 21.111, rev.8 - USIM card requirements [archive] 3GPP standard, janvier 2010.
3. [a et b] SIM Card Dimensions [archive], Dimensions guide.com, consulté en mai 2012.
4. GSM Arena, LG U900 caractéristiques techniques.
5. (en) LG U900 Press Release.
6. iPad : mais qu'est-ce qu'une carte microSIM ? - Maxime Johnson, 2 février 2010.
7. Apple a annoncé que le nouvel iPad contient une « micro-SIM ». Qu'est-ce qu'une micro-SIM ? [archive] Just ask gemalto.com, consulté en mai 2012.
8. Les industriels des télécoms se déchirent sur le futur de la carte SIM - Maxime Amiot et Solveig Godeluck, *Les Échos*, 29 mars 2012.
9. PCINpact - Quid de la disponibilité de la nano SIM chez les opérateurs.
10. Oberthur une solution à forte capacité mémoire en partenariat avec Spansion.
11. Voir les spécifications ISO 7816.
12. La carte SIM nouvelle génération de Free Mobile poserait des problèmes de compatibilité, Univers Freebox, publié le 12 février 2012 par Olivier Viaggi. Consulté le 15 février 2015.
13. Free Mobile et les cartes SIM : pas de NFC ou de 5,5 V… , Tom's Hardware, publié le 13 février 2012 par Pierre Dandumont. Consulté le 15 février 2015.
14. Manuel d'utilisation des Alcatel OneTouch 1010D et 1010X (cf. note de bas de page en p. 13), alcatelonetouch.com. Consulté le 15 février 2015.
15. (en) « ETSI TS 102 223 V9.1.0 » [archive], etsi.org (consulté le 5 octobre 2017).
16. (en) « A Peek Inside The NSA's Spy Gear Catalogue », Gizmodo Australie, 1er janvier 2014 (consulté le 5 octobre 2018).
17. [a et b] Les obligations de désimlockage des téléphones mobiles, brizawen.com, consulté le 15 février 2017.
18. Arcep - Décision n° 2005-1083, voir article 5.