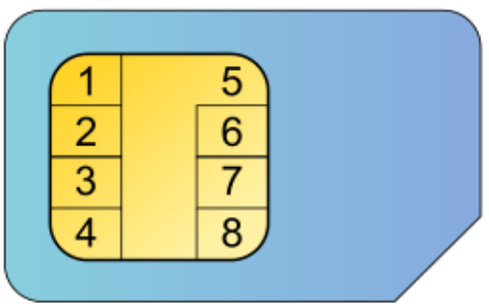
modèle d'affaire inexistant et certaines difficultés d'implémentation, les solutions techniques n'avaient vu le jour que sous la forme de prototypes.

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).

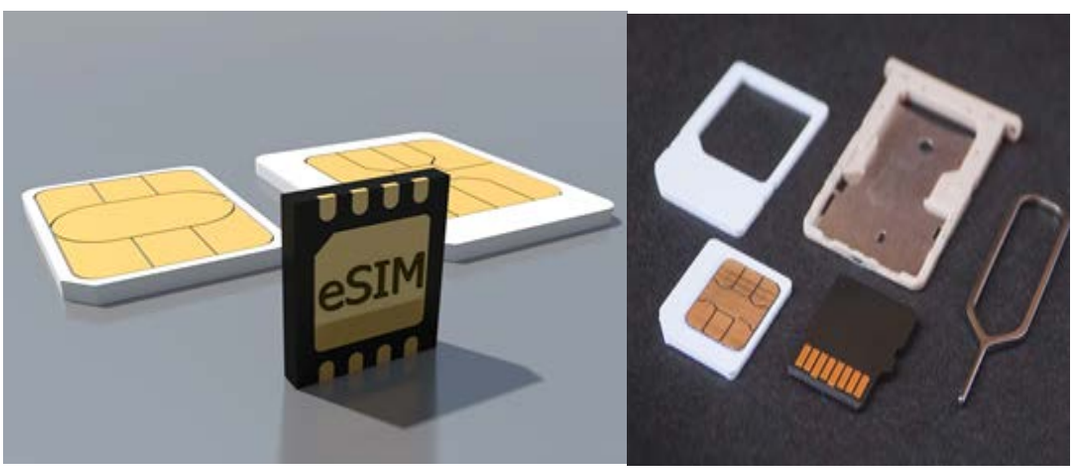
[11] Oberthur une solution à forte capacité mémoire en partenariat avec Spansion.
[12] Voir les spécifications ISO 7816.

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.