

L'Association Française des Opérateurs Mobiles :

L'AFOM regroupe les opérateurs mobiles français : Bouygues Telecom, Debitel France, M6 (M6 Mobile), Omer Telecom (Breizh Mobile et Virgin Mobile), Orange France, SFR et Universal Music (Universal Mobile). Elle est née il y a quatre ans de la volonté des opérateurs de traiter en commun certains sujets d'intérêt général et non concurrentiels et d'accompagner les effets de leur activité dans l'économie et la société française. L'objectif est de favoriser un développement durable, harmonieux et responsable de la téléphonie mobile.

Les missions de l'AFOM :

- ↪ Elle traite des sujets de société relatifs à la téléphonie mobile, non concurrentiels, et appelant une réponse collective des trois opérateurs.
- ↪ Sur ces sujets, elle définit avec les opérateurs, des pratiques responsables communes et en informe le public.
- ↪ Elle est l'interface des institutions et présente les points de vue du secteur dans les domaines législatifs et réglementaires relatifs à la téléphonie mobile.

Depuis décembre 2004, l'AFOM accueille au sein de son Conseil d'Administration deux Personnalités Qualifiées : Jean-Hervé Lorenzi et François Ewald.

En juillet 2005, elle a modifié ses statuts pour pouvoir s'ouvrir aux MVNO qui le désirent.

Mentions légales :

Toutes les marques commerciales, marques de services et appellations commerciales figurant dans le présent document sont la propriété de leurs détenteurs respectifs. Toute utilisation non autorisée est strictement interdite.

Livre Blanc sur le Sans Contact Mobile

Vision des opérateurs mobiles français sur les éléments techniques nécessaires au déploiement du NFC sur les téléphones mobiles

▪ OBJECTIFS DU LIVRE BLANC

Dans le cadre de l'AFOM, un groupe de Travail est constitué depuis fin avril 2006 par les opérateurs mobiles pour proposer des dispositions techniques visant à favoriser un développement dès 2008 des services mobiles utilisant la technologie NFC.

Les opérateurs ont en effet constaté que des applications sans contact sont aujourd'hui déployées en proposant des cartes dédiées aux utilisateurs. Il existe une demande des utilisateurs, des fournisseurs de services et des industriels, pour le développement de solutions analogues s'appuyant sur le mobile. Cette demande est renforcée par les succès asiatiques, notamment celui de FeliCa Mobile lancé début 2004.

Du fait d'une réelle complexité du sujet, cette demande ne s'est pas encore traduite par un ensemble consensuel de spécifications. Cette complexité tient d'une part au grand nombre d'interdépendances et d'autre part, au fait qu'aucun des acteurs n'a eu un poids suffisant pour fédérer seul les initiatives permettant d'aboutir à un écosystème interopérable.

C'est pourquoi, afin de converger vers un système interopérable, les opérateurs ont souhaité travailler ensemble au sein de l'AFOM notamment sur les points suivants:

- Identification des éléments techniques devant faire l'objet d'une standardisation pour développer le marché
- Elaboration de propositions de solutions techniques
- Communication vers les fournisseurs de services et industriels de la compréhension des opérateurs quant aux besoins et solutions techniques
- Clarification des évolutions qui paraissent requises de l'environnement pour tirer le meilleur parti du mobile dans les services sans contact.

Le groupe de travail a auditionné les industriels cités en annexe 2 afin d'alimenter sa réflexion et d'évaluer la maturité des solutions proposées.

▪ EXECUTIVE SUMMARY

Les éléments nécessaires à la technologie sans contact (NFC) sont en cours de standardisation (ETSI). Dans ce contexte, et notamment pour accélérer ces procédures de standardisation, les opérateurs mobiles membres de l'AFOM ont souhaité travailler ensemble afin de définir une vision commune des bases techniques nécessaires au bon développement de cette nouvelle technologie et à la satisfaction du client final.

Les points essentiels qui ressortent de ces travaux sont les suivants :

- L'intérêt commun des consommateurs, des opérateurs et des industriels est d'éviter la fragmentation qu'amènerait l'absence d'interopérabilité entre les systèmes déployés. La solution recherchée vise une interopérabilité entre l'équipement de téléphonie mobile sans contact et l'ensemble des technologies majoritairement déployées en Europe. C'est pourquoi les spécifications retenues par les opérateurs mobiles doivent **supporter les standards** du marché européen : protocoles de transport de données retenus par le NFC forum, en particulier de type **ISO 14443 type A et B, et les applications Mifare et Calypso**. En attendant que les infrastructures déployées convergent vers la norme ISO 14443, les solutions devront également **supporter le protocole B'** (protocole Innovatron), largement déployé.
- Afin d'assurer la sécurité des transactions (crédit/débit d'un titre de transport, ordre de paiement...) effectuées par les applications NFC, il est nécessaire que ces transactions s'exécutent au sein d'un environnement sécurisé (sécurité logique et physique). Le rôle d'un élément de sécurité est d'assurer l'intégrité des transactions électroniques effectuées par les applications hébergées. **La carte SIM, présente dans tous les téléphones mobiles, est l'élément de sécurité privilégié.**
- Concernant l'interface physique entre la carte SIM et le composant sans contact, et **pour un lancement à l'horizon 2008 en France, les opérateurs constatent que la technologie SWP est la plus mature**, car les roadmaps présentées à l'AFOM par les différents fournisseurs de composants NFC et les fournisseurs de cartes SIM sont compatibles avec l'industrialisation de cette solution dans les délais souhaités.
- Les mécanismes de gestion des applications et des **domaines de sécurité** sur la carte SIM sont basés sur le **standard Global Platform**, la référence en matière de gestion sécurisée d'application sur une carte à puce.
- Une **gestion homogène des applications** sans contact dans un téléphone mobile est **nécessaire** afin de garantir aux émetteurs d'applications que leur service sera correctement déployé sur l'ensemble des terminaux adressables, aux opérateurs mobiles la bonne coexistence des différents services sans contact dans les terminaux, aux utilisateurs une bonne compréhension et un bon fonctionnement de l'ensemble des services installés.

SOMMAIRE

- **OBJECTIFS DU LIVRE BLANC**

- **EXECUTIVE SUMMARY**

- **A/ CONTEXTE**
 - **A_1 Contexte international**
 - **A_2 Besoins exprimés par les tiers envers les opérateurs**
 - **A_3 Besoins des opérateurs mobiles**

- **B/ SOLUTION TECHNIQUE**
 - **B_1 La carte SIM comme élément de sécurité privilégié**
 - **B_2 Les solutions (SIM + composant sans contact) proposées par les industriels**
 - **B_3 Les applications**
 - **B_3_1 Les IHM des services évolués**
 - **B_3_2 La gestion des applications**
 - **B_3_3 Gestion du cycle de vie des applications**

- **Annexe 1 : Glossaire**

- **Annexe 2 : industriels auditionnés**

- **Annexe 3 : les contributeurs**

▪ **A/ CONTEXTE**

○ **A_1 Contexte international**

▪ **Typologie des usages du NFC**

Le NFC est une technologie de communication RFID fonctionnant dans la bande de fréquence 13,56 Mhz. Le NFC s'appuie notamment sur la norme ISO 14443 qui régit les systèmes dits de proximité pouvant porter jusque 10cm.

Trois modes sont à distinguer pour le NFC :

- le mode lecture qui permet au mobile d'interagir avec des étiquettes (en anglais : « tags ») communicantes pour recevoir de l'information ou accéder à du contenu,
- le mode émulation de carte : le mobile est un objet communicant et sécurisé susceptible de remplacer les traditionnelles cartes plastiques et apporter de nouveaux services grâce à son clavier et son écran (consultation) mais aussi à sa capacité de communication (rechargement, paiement...).
- Le mode P2P: permet l'échange local de données entre deux mobiles

Le livre blanc se limite au mode Emulation de carte sans contact dans le mobile.

▪ **Les usages dans le monde : transport, paiement, autres**

Plusieurs usages sont répertoriés dans le monde et notamment en Asie (Japon, Corée) où l'on retrouve principalement des applications de billettique dans le secteur transport urbain ou de paiement de proximité de type porte monnaie électronique ou crédit.

La dématérialisation des supports physiques traditionnels tels que les cartes plastiques et les titres papiers favorise aussi l'émergence d'applications dans le domaine de la billettique événementielle, du contrôle d'accès ou encore de la fidélisation.

▪ **Compatibilité entre les pays**

Aujourd'hui, les solutions « sans contact » sont déjà largement déployées dans le monde. On estime à plus de 100 millions le nombre de porteurs de cartes sans contact pour des usages grand public dans le monde.

Les cartes sans contact déployées dans le monde dans le secteur du transport urbain s'appuient massivement sur la technologie Mifare développée par Philips (ex : Oyster en Angleterre), tandis qu'au Japon la technologie FeliCa développée par Sony est largement répandue. En Europe la spécification Calypso a été adoptée par de nombreux transporteurs.

Les consommateurs, les opérateurs mobiles et les industriels ont intérêt à ce qu'une même solution technique fonctionne dans le plus grand nombre de pays possible, au minimum sur l'ensemble du continent européen.

○ **A_2 Besoins exprimés par les tiers envers les opérateurs**

▪ **Par les consommateurs**

Les consommateurs attendent des opérateurs mobiles qu'ils leur fournissent une solution NFC prête à l'emploi, qui inclut un terminal mobile, sa carte SIM ainsi que la mise à disposition d'un grand nombre de services. De plus, les services attendus devront être interopérables.

▪ **Par les industriels SIM et terminaux**

Les roadmaps ne sont pas encore figées du côté des fabricants de cartes et de terminaux. De façon générale, ces industriels disent être convaincus que le marché serait plus important en cas de décision des opérateurs mobiles de déployer des solutions NFC. Mais ils estiment que les opérateurs mobiles n'ont jusqu'à ce jour pas donné de signal clair en ce sens.

▪ **Par les fournisseurs de services : transport, paiement, fidélité, autres**

Concernant les équipements de téléphonie mobile : de nombreux fournisseurs de service souhaitent avoir la possibilité de permettre à leurs clients ou usagers d'utiliser leur téléphone mobile comme support d'une carte sans-contact dématérialisée. Ils souhaitent ainsi :

- que cette possibilité de dématérialisation soit répandue dans un maximum de téléphones mobiles,
- pouvoir héberger leurs applications dans des espaces sécurisés dans l'équipement de téléphonie mobile, et disposer de solutions pour gérer le cycle de vie de ces applications,
- pouvoir effectuer des vérifications sur l'utilisateur avant tout téléchargement ou activation de service,
- permettre à leurs applications de dialoguer à distance avec des serveurs applicatifs permettant la mise à jour sécurisée de données applicatives dans le téléphone mobile (ex : mise à jour de droits pour une application de billetterie, crédit d'un porte monnaie...) et,
- pouvoir interagir avec leurs clients via l'interface locale ou distante du téléphone mobile.

Concernant les plateformes serveur : des outils d'administration sont requis pour que les fournisseurs de services. Ils souhaitent en effet :

- assurer un suivi des applications déployées sur les mobiles des opérateurs,
- suivre l'historique et les versions des applications,
- accéder aux données relatives au statut de l'application et,
- disposer d'un accès exclusif aux données de l'application sans-contact.

Afin de minimiser les efforts d'intégration, les interfaces avec les plateformes serveurs des opérateurs mobiles devront être homogénéisées.

Concernant les lecteurs : les fournisseurs de services souhaitent que l'ensemble des téléphones NFC mis sur le marché par les opérateurs mobiles soit compatible avec les infrastructures déployées (ex : lecteurs en place dans les transports urbains), et permette d'offrir des services et des performances au minimum équivalents aux cartes sans contact.

Concernant les services : les fournisseurs de services souhaitent pouvoir intégrer les applications NFC dans le mobile à l'ensemble des services d'information et de vente à distance qu'ils proposent via le canal du téléphone mobile.

Les fournisseurs de services souhaitent que les opérateurs proposent une assistance pour accompagner le changement de téléphone mobile et d'opérateur par un de leurs clients.

o **A_3 besoins des opérateurs mobiles**

▪ **Vis à vis des clients finaux**

Dans la relation de confiance tissée avec le client, l'opérateur mobile est le premier garant de l'efficacité du fonctionnement du service. Ainsi, son service client et/ou support technique intervient :

- en cas de perte ou de changement de téléphone ou de changement d'opérateur et,
- lorsque le client rencontre un problème dans l'utilisation des services (il met en place des procédures pour identifier la nature du problème et l'orienter si nécessaire vers le fournisseur de service en question).

En cas de renouvellement de mobile, le client souhaite aussi récupérer ses applications, l'interface utilisateur et ses données (sous condition et selon les règles du service).

L'opérateur mobile facilite l'accès aux applications pour le client et assure leur cohabitation. Il communique sur les services NFC, éduque sa base de client et offre des outils de découverte.

L'opérateur mobile est ultimement l'acteur de confiance du client pour un fonctionnement simple et sûr de l'ensemble des fonctionnalités de son mobile.

▪ **Vis à vis des fournisseurs de services**

Les opérateurs mobiles souhaitent rendre possible la gestion et la personnalisation des applications, notamment à distance.

L'opérateur mobile doit disposer des informations nécessaires à la facturation de ses services.

L'opérateur mobile souhaite que les applications proposées par les fournisseurs de services répondent à des normes de qualité, de sécurité, de respect du client voire de contenus conformes à des chartes contractuelles.

- **Vis-à-vis des organismes de standardisation**

Les opérateurs mobiles ont la volonté qu'une standardisation rapide aboutisse sur les éléments techniques indispensables à l'interopérabilité.

- **Cohérence avec les services existants et le High Speed Protocol**

L'architecture retenue pour le sans contact devra être compatible avec

- les services mobiles existants
- les services en cours de standardisation, et notamment le High Speed Protocol.

- **Sécurité**

De manière à garantir à son client le bon fonctionnement du téléphone mobile, l'opérateur mobile souhaite pouvoir agréer les applications avant toute installation.

L'opérateur mobile doit pouvoir désactiver l'accès à un service suivant ses propres règles de gestion.

L'accès aux applications embarquées dans le téléphone du client doit pouvoir être contrôlé pour éviter toute tentative de lecture ou de transaction malicieuse.

Le client détenteur d'un mobile NFC pourra disposer de fonctions de verrouillage et de désactivation d'une ou plusieurs applications. Un code PIN ou un acte de confirmation peut être requis pour effectuer des transactions sensibles, ces cas impliquant que le mobile soit allumé.

- **Couverture ISO 14443**

Les fournisseurs de services du domaine du transport ou du paiement ont équipé ou vont équiper des utilisateurs de cartes avec puce sans contact et déployé des matériels (i.e. lecteurs ou « readers ») capables de mener des transactions avec ces cartes : valideurs dans le transport, terminaux de paiement dans les magasins, etc.

Chacun des acteurs amenés à prendre cette décision a opté pour un ensemble cohérent de lecteurs & cartes, le plus souvent sans se préoccuper des choix réalisés par les autres, d'où une hétérogénéité des infrastructures installées. Dans une même ville, le club de football a pu proposer une carte sans contact à ses abonnés, l'opérateur de transport une autre carte sans contact à ses usagers, et les restaurants peuvent accepter une carte de paiement sans contact.

Les cartes existantes sont pour l'essentiel émises par un acteur vers ses clients ou usagers, et porteuses d'un seul usage (ex : accès ou paiement).

L'offre des opérateurs mobiles est de proposer à leurs clients de dématérialiser leurs cartes plastiques pour les stocker dans leur téléphone mobile. Ce téléphone mobile devra donc être capable d'interagir avec les lecteurs déployés dans les pays.

Afin de bénéficier au plus vite d'économies d'échelle permettant de proposer le service NFC aux meilleures conditions à leurs clients, l'intérêt commun des opérateurs et des industriels est d'éviter la fragmentation qu'amènerait l'absence d'interopérabilité entre les systèmes déployés. Les clients finaux devraient choisir entre un téléphone mobile capable de stocker une carte de paiement sans contact, ou un téléphone mobile capable de stocker une carte de transport sans contact, etc. La valeur d'usage en serait réduite, les séries industrielles aussi, les coûts unitaires plus élevés...

La solution à rechercher consiste donc à viser une interopérabilité entre l'équipement de téléphonie mobile NFC et l'ensemble des technologies majoritairement déployées en Europe.

C'est pourquoi les spécifications retenues par les opérateurs mobiles doivent supporter les standards du marché européen : protocoles de transport de données de type ISO 14443 type A et B et les applications Mifare et Calypso.

En attendant que les infrastructures déployées convergent vers la norme ISO 14443, les solutions devront également supporter le protocole B' (protocole Innovatron).

- **Mode sans batterie**

Un certain nombre de cas d'usage nécessitent que l'utilisateur puisse utiliser ses services mobiles sans contact alors que son téléphone est éteint, ou que la batterie est déchargée.

A cette fin, les mobiles doivent offrir un mode sans batterie qui permet d'assurer uniquement le service sans contact de base, c'est-à-dire identique à celui d'une carte plastique. Ce mode fonctionne selon une double modalité, en mode « alimenté par le champ » et/ou en mode « batterie faible (mobile éteint) ».

- **Traitement des données liées à l'usage**

Les opérateurs mobiles traiteront les éléments d'informations liées à l'usage conformément aux réglementations nationales en vigueur.

B/ SOLUTION TECHNIQUE

- **B_1 la carte SIM comme élément de sécurité privilégié**

Afin d'assurer la sécurité des transactions (crédit/débit d'un titre de transport, ordre de paiement...) effectuées par les applications NFC, il est nécessaire que ces transactions s'exécutent au sein d'un environnement sécurisé (sécurité logique et physique). Le rôle d'un élément de sécurité est d'assurer l'intégrité des transactions électroniques effectuées par les applications hébergées.

- **La SIM au cœur de la solution**

Le support du mode émulation de cartes dans les terminaux mobile doit viser au minimum une équivalence fonctionnelle des cartes sans contact. Le mode émulation cartes devrait donc avoir un support ayant une durée de vie équivalente aux cartes sans contact du marché.

Sur le marché Français, la durée de vie moyenne d'un téléphone mobile est de 20 mois (source AFOM Observatoire 23 décembre 2005). Dès lors l'élément de sécurité doit être :

- **amovible** : pour que le client puisse porter ses droits d'un terminal à l'autre (exigence client)

- **répandu** : pour atteindre un parc maximum (exigence des fournisseurs de services)

La carte SIM est le seul élément sécurisé, portable, standardisé, universel et répandu dans absolument tous les téléphones mobiles 2G/3G en Europe.

Au-delà de cette exigence fonctionnelle, l'usage de la carte SIM comme élément de sécurité offre de multiples bénéfices par rapport à des solutions alternatives telle qu'une carte mémoire sécurisée additionnelle ou un élément de sécurité dédié intégré dans le terminal :

1. Le marché des services embarqués sur des cartes sans contact est fragmenté, il nécessitera vraisemblablement de couvrir des personnalisations usines qui pourront notamment être propres à chaque région. A ce jour les fournisseurs de téléphones mobiles ne permettent pas ce niveau de flexibilité. A l'inverse, la carte SIM permet une personnalisation fine et ciblée,
2. La carte SIM est systématiquement présente dans un mobile en état de fonctionnement. Dès lors, son utilisation en tant qu'élément de sécurité permet d'affranchir le client de toute manipulation,
3. Des outils, des processus et des organisations permettant la personnalisation sécurisée de la carte SIM en usine ou à distance (OTA) sont déjà en places et opérationnels chez les opérateurs mobiles, L'utilisation de la carte SIM comme élément de sécurité permet donc de minimiser le surcoût d'un système NFC en les réutilisant.
4. La carte SIM et le réseau mobile ont la possibilité d'interagir. Dès lors, les services embarqués sur la carte SIM pourront être bloqués, activés ou suspendus à distance.
5. Les fournisseurs de cartes SIM (encarteurs) fournissent la plupart des opérateurs de services faisant usages de cartes sans contacts ; dès lors l'industrie peut bénéficier de la relation de confiance ainsi que de la connaissance métiers des encarteurs avec ces fournisseurs de services.
6. La carte SIM est un élément présent dans tous les terminaux. Son usage en tant qu'élément de sécurité limitera le surcoût de la fonction NFC dans les terminaux ainsi que les impacts sur le facteur de forme du terminal mobile.

▪ **Le rôle de la carte SIM**

La carte SIM accueillera donc les secrets de différents opérateurs de services ainsi que les applications usuellement embarquées dans les cartes sans contacts en fournissant un environnement de stockage et d'exécution sécurisé.

La carte SIM devra permettre une gestion de multiples requêtes simultanées à travers différentes interfaces physiques. Par exemple, l'utilisateur passe son mobile sur une borne au moment où ce dernier reçoit un appel.

Dans le cas du mode sans batterie l'environnement applicatif sur la carte SIM devra se lancer et répondre dans un temps compatible avec les infrastructures sans contact.

○ **B_2 les solutions (SIM + composant sans contact) proposées par les industriels**

Il convient de distinguer l'interface logicielle de l'interface physique.

- L'interface logicielle et protocolaire doit permettre de distinguer les responsabilités et rôles du composant sans contact et de la carte SIM notamment en ce qui concerne l'implémentation des différentes couches de l'ISO 14443. Les opérateurs mobiles souhaitent une normalisation rapide de cette interface.
- L'interface physique qui va permettre d'assurer la liaison entre le composant sans contact et la carte SIM. Les principales contraintes fonctionnelles de cette interface sont le support du mode sans batterie ainsi que le débit de ce lien.

Concernant l'interface physique, deux interfaces ont été présentées au groupe de travail: l'interface S2C et l'interface SWP.

Le support de l'interface SWP est annoncé de manière industrielle dès le début 2007 et ne nécessite d'utiliser qu'un unique contact sur la carte SIM (contact C6). Les composants sans contact la supportant n'impactent donc pas l'une des technologies High Speed Protocol en lice dans des organismes de standardisation: l'USB. De plus, les implémentations permettent de supporter le cas où la batterie du terminal est déchargée. En revanche, cette interface n'est pas compatible avec une des principales implémentations High Speed Protocol: le MMC. Par ailleurs, bien que certains fournisseurs annoncent le support de MiFare pour 2007, la compatibilité de l'interface SWP avec certains systèmes MiFare reste à démontrer.

L'interface S2C est quant à elle compatible avec les infrastructures MiFare. Le groupe de travail n'a pas été informé de la disponibilité de couples [composants sans contact - cartes SIM] dans des délais similaires aux composants supportant le SWP¹. De plus, aucune information concernant la disponibilité de composants supportant le mode batterie déchargée n'est disponible à date. Enfin, sa compatibilité avec le High Speed Protocol reste à démontrer.

Pour une solution cible, les opérateurs mobiles souhaitent une standardisation par l'ETSI dans les délais les plus courts de l'interface physique SIM – composant sans contact, avec une coexistence avec la ou les solutions HSP.

D'ici là et pour un lancement à l'horizon 2008 en France, les opérateurs constatent que la technologie SWP est la plus mature, car les roadmaps présentées à l'AFOM par les différents fournisseurs de composants NFC et les fournisseurs de cartes SIM sont compatibles avec l'industrialisation de cette solution dans les délais souhaités.

¹ Certains téléphones actuellement disponibles utilisant le S2C comme liaison entre le composant sans contact et un élément de sécurité dédié (hors SIM) dans le téléphone mobile.

○ **B_3 Les applications**

Un service sans contact dans un téléphone mobile se décompose entre :

- un service de base, l'émulation de carte sans contact, qui reproduit le fonctionnement habituel d'une carte sans contact, et qui est exécuté dans la carte SIM ;
- un service évolué, reposant sur une interface utilisateur, qui permet à ce dernier d'intervenir dans le déroulement de la transaction sans contact (par ex. saisie d'un code PIN), de consulter les informations présentes dans la carte (par ex. solde d'un porte-monnaie), de mettre à jour ses droits (par ex. chargement d'un titre de transport, rechargement d'un porte-monnaie électronique, etc...) ; cette interface peut être exécutée dans la carte SIM

▪ **B_3_1 Les IHM des services évolués**

A ce jour 3 principales technologies sont disponibles pour l'implémentation des IHM des services sans contact dans les mobiles : la technologie SIM Toolkit, la technologie Java/MIDP, la technologie SmartCard Web Server (en cours de normalisation).

▪ **B_3_2 La gestion des applications**

Une gestion homogène des applications sans contact dans un téléphone mobile est nécessaire afin de garantir :

- aux émetteurs d'applications que leur service sera correctement déployé sur l'ensemble des terminaux adressables
- aux opérateurs mobiles la bonne coexistence des différents services sans contact dans les terminaux
- aux utilisateurs une bonne compréhension et un bon fonctionnement de l'ensemble des services installés

▪ **Stockage des applications dans un espace sécurisé**

Les cartes SIM sont maintenant des plateformes multi applicatives permettant le stockage et l'exécution d'applications sécurisées fournies par des tiers. Les applications sont associées à des domaines de sécurité qui représentent le fournisseur de service émetteur sur la carte. Un domaine de sécurité est une application de gestion de sécurité qui est régie par ses propres règles d'accès, de gestion, de personnalisation, et possède un jeu de clés dédié, ce qui permet une gestion cloisonnée des applications. Ce mécanisme assure une complète séparation des clés entre l'émetteur de la carte et les autres fournisseurs de services. De plus en paramétrant leurs privilèges et leurs conditions d'accès, les domaines de sécurité peuvent être adaptés aux contraintes de sécurité des différents fournisseurs de services.

▪ **Pré chargement & OTA**

Les applications peuvent être pré chargées en personnalisation, soit téléchargées "Over The Air" de manière sécurisée, ce dernier mode offrant aux fournisseurs de service toute la souplesse de la téléphonie mobile.

De même les domaines de sécurité peuvent être soit pré chargés lors de la personnalisation des cartes, soit téléchargés OTA en post personnalisation de manière sécurisée.

Les mécanismes de gestion des applications et des domaines de sécurité sont basés sur le standard Global Platform, la référence en matière de gestion sécurisée d'application sur une carte à puce. Les protocoles utilisés pour charger, installer les applications, mettre à jour des clés, et personnaliser les applications de façon sécurisée sont basés sur des standards de communication comme le standard 3GPP 23.048, qui est reconnu comme Secure Channel par Global Platform.

- **Lieu de stockage des applications**

La partie "émulation de cartes" des applications, ainsi que les domaines de sécurité sont stockés sous forme d'applets javacard dans la carte SIM; Ces applications sont chargées dans un environnement d'exécution qui offre des APIs indépendantes du matériel permettant la portabilité des applications.

- **Portabilité logicielle**

Afin d'être en mesure d'accueillir les applications et de maximaliser leurs portabilités d'une carte SIM à une autre, les cartes SIM devront fournir un environnement d'exécution javacard au moins version 2.2.1. Il est souhaitable que les applications ne fassent appel qu'à cet ensemble d'APIs. En effet, le recours par les services provider à d'autres APIs, notamment des APIs natives pour des raisons de performance, pose un problème majeur concernant la portabilité de ces applications.

- **Certification / homologation / validation des applications à charger**

Les fournisseurs de services auront à certifier leurs applications auprès des organismes compétents avant de les charger sur la carte SIM, en adaptant les processus de certification actuels à l'environnement multiapplicatif de la carte et en tenant compte d'une gestion de risque permise par le téléphone mobile.

L'opérateur mobile pourra exiger que les applications soient homologuées et validées avant d'être chargées sur la carte, de façon à respecter des règles de sécurité, de cohabitation, d'éthique, d'interaction avec l'utilisateur, d'utilisation d'APIs fournies par l'environnement d'exécution de la carte SIM.

- **B_3_3 Gestion du cycle de vie des applications**

- **Activation, suspension, résiliation**

L'opérateur mobile permettra d'activer, suspendre, désactiver OTA les applications des fournisseurs de services stockées sur la carte SIM par une commande standard de type 23.048. L'initiative de cette commande dépendra de la relation entre l'opérateur mobile et le fournisseur de service.

- **Mise à jour des applications**

La mise à jour d'applications pourra être effectuée par les fournisseurs de services via une plateforme AMS (Application Management System) et CMS (Card Management System); Les applications pourront être signées par le fournisseur de service et une vérification de cette signature sera ainsi effectuée par le domaine de sécurité de l'émetteur de la carte ou par le domaine de sécurité associé à l'application, selon les privilèges de ce domaine de sécurité.

Pour permettre à un fournisseur de service d'adresser facilement les parcs des différents opérateurs, il serait souhaitable que les liens entre AMS et CMS soient uniformisés.

- **Multi instanciation d'application**

Certaines applications pourront être instanciées plusieurs fois avec des données et clés appartenant à des fournisseurs de services différents; de cette façon, cela permettra d'utiliser une application unique sur des réseaux d'acceptation différents.

- **Gestion de la mémoire**

L'opérateur mobile gèrera l'espace mémoire utilisé par les applications de façon à ce qu'elles ne perturbent pas le fonctionnement général de la carte et des autres applications. L'opérateur doit connaître à distance la place mémoire restante sur la carte pour autoriser le chargement des applications dans de bonnes conditions.

Annexe 1 : Glossaire

Abréviation	Signification
NFC	Near Field Communication
RFID	Radio Frequency IDentification
ISO	International Organization for Standardization
SIM	Subscriber Identity Module
HSP	High Speed Protocol
OTA	Over The Air
API	Application Programming Interface
SWP	Single Wire Protocol
S2C	SigIn SigOut Connection
USB	Universal Serial Bus
MMC	MultiMedia Card
ETSI	European Telecommunications Standards Institute
PIN	Personal Identification Number
IHM	Interface Homme Machine
STK	SIM ToolKit
MIDP	Mobile Information Device Profile
SCWS	Smart Card Web Server
HW	HardWare
BIP	Bearer Independent Protocol
APDU	Application Protocol Data Unit
CMS	Card Management System
AMS	Application Management System

Annexe 2 : industriels auditionnés

Calypso Networks Association	le 4 octobre
Gemalto	le 27 juin
G&D	le 4 juillet
Inside Contactless Technologies	le 6 juin
OCS	le 20 juin
Philips	le 23 mai
SAGEM-ORGA	le 18 juillet

Annexe 3 : les contributeurs

L'AFOM a convié l'ensemble des opérateurs membres à participer aux travaux du groupe de travail.

Les membres du groupe de travail sont :

AFOM

- Frédéric Geraud de Lescazes

Bouygues Télécom

- Mathias Fraisse
- Bruno Prexl

Orange-Groupe France Telecom

- Vincent Barnaud
- Jean-Christophe Bernard
- David Picquenot
- Yves Thorigné

SFR

- Michael Bensimon
- Olivier Deuffic
- Jérôme Devisme
- Mireille Poggi