UNION DES TRANSPORTS PUBLICS ET FERROVIAIRES

Spécifications techniques et de sécurité de la billettique sur mobile NFC

Version 1.2

Juillet 2011

• UTP • AGIR • KEOLIS • RATP • SNCF • TRANSDEV • VEOLIA TRANSPORT

5-7 rue d'Aumale - 75009 Paris
Tél. : +33 (0)1 48 74 63 51
Fax : +33 (0)1 40 16 11 72

www.utp.fr

SPECIFICATIONS TECHNIQUES ET DE SECURITE DE LA BILLETTIQUE SUR MOBILE NFC

VERSION 1.2

DATE : 15/07/2011

- **UTP**
- **AGIR**
- **Keolis**
- **RATP**
- **SNCF**
- **Transdev**
- **Veolia Transport**

Spécifications techniques et de sécurité de la billettique sur mobile NFC

LISTE DE DIFFUSION

Société	*Nom*	*Email, Fax ou Adresse*
AGIR	Laurent BOUDOT	laurent.boudot @agir-transport.org
Keolis	Christophe BADESCO	cbadesco @keolis.com
RATP	Gilles GRIVEAUX	gilles.griveaux @ratp.fr
RATP	Marc BENSIMON	marc.bensimon @ratp.fr
RATP	Philippe GRASSER	philippe.grasser @ratp.fr
RATP	Pierre TERREE	pierre.terree @ratp.fr
SNCF	Joël EPPE	joel.eppe @sncf.fr
SNCF	Arnaud GESNOT	ext.arnaud.gesnot @sncf.fr
Spirtech	Emmanuel LEBEUL	emmanuel.lebeul @spirtech.com
Spirtech	Frédéric LEVY	frederic.levy @spirtech.com
Spirtech	Stéphane DIDIER	stephane.didier @spirtech.com
Transdev	Frédéric LINOSSIER	frederic.linossier @transdev.eu
Transdev	Romuald BODOY	romuald.bodoy @transdev.eu
Transdev	Hervé DE LA MORSANGLIERE	herve.delamorsangliere @transdev.eu
UTP	Anne MEYER	ameyer @utp.fr
Veolia Transport	Dominique DESCOLAS	dominique.descolas @veolia-transport.fr
Veolia Transport	Florent CETIER	florent.cetier @veolia-transport.fr

RÉDACTEUR

SPIRTECH
1 rue Danton - 75006 Paris - France
Fax : +33- 1 40 46 36 29

Suivi des évolutions du document

Version	Description	Date
1.2	Ajout en début de document d'une mention légale. Précisions concernant la technologie MIFARE Classic et remplacement de « protocole A' » par « protocole MIFARE Classic » Modifications rédactionnelles mineures et repagination.	15/07/2011
1.1	Ajout en introduction d'un chapitre sur les évolutions du document. Mise en cohérence des références aux protocoles B' et A'. Modifications rédactionnelles mineures.	13/01/2011
1.0	Première version.	17/09/2010

SOMMAIRE

1 INTRODUCTION

1.1 PERIMETRE D'APPLICATION DE CE DOCUMENT

Les Autorités Organisatrices de Transport, sous l'égide du GART, ont décidé, en juin 2008, la rédaction du référentiel national des services transport sur mobile NFC : le Document Fonctionnel Commun de la Billettique sur Mobile NFC, appelé *DoFoCo Mobile NFC* [1].

Ce référentiel s'appuie sur le document « Approche institutionnelle de la billettique multimodale » (aussi appelé DoFoCo+ - 2001) rédigé par le GART et sur le « Document fonctionnel sur la billettique avec cartes et son interopérabilité » (aussi appelé DoFoCo - 2000) rédigé par l'UTP. Ces deux documents ont servi de socle au déploiement de la télébillettique en France dans un cadre d'interopérabilité. Le DoFoCo Mobile NFC vient donc en complément.

Le DoFoCo Mobile NFC, de portée nationale, prépare l'arrivée des téléphones mobiles sans contact, afin d'anticiper et de définir au mieux la prise en compte de ces nouveaux supports et canaux de distribution, en l'intégrant dans un document fédérateur. Les opérateurs de transport public ont été associés aux travaux fonctionnels.

Afin de finaliser ce référentiel, le GART a mandaté, fin 2009, l'UTP pour la rédaction des présentes spécifications techniques et de sécurité de la billettique sur mobile NFC. Pour ce faire, l'UTP a constitué un groupe de travail composé de représentants des différentes composantes de l'UTP, sous l'égide de la Commission « Techniques, Énergies et Développement Durable ». Après appel à consultation, Spirtech a été retenu pour rédiger ce document.

1.2 OBJET DU DOCUMENT

Le présent document est la spécification technique et de sécurité de la billettique sur mobile NFC, et comprend notamment :

- au travers de parcours client identifiés dans le DoFoCo Mobile NFC, la description technique de la mise en œuvre de la billettique sur mobile (émission de l'application, distribution, validation, contrôle, SAV, etc.) ;
- les contraintes liées aux équipements actuels concernant l'interface avec les terminaux sans contact des transporteurs et les contraintes liées à l'interopérabilité billettique ;
- la description des interfaces techniques entre les éléments du système : mobile, équipements billettiques, réseau GSM, etc. ;
- l'instruction des deux solutions techniques définies par le GART (SIM centrique et Mobile centrique).

1.3 CERTIFICATION ET INTEROPERABILITE TECHNIQUE

L'utilisation d'objets portables « extérieurs » à un réseau de transport sur les équipements du réseau peut révéler des problèmes d'interopérabilité technique.

Cela peut déjà être le cas par exemple au sein d'une région, pour des cartes régionales émises par un des transporteurs, et qui doivent être acceptées par tous les équipements de la région.

Afin de garantir le bon fonctionnement des objets portables sur les différents équipements régionaux, il est indispensable de définir des critères de test et une plateforme permettant de valider les produits sur les différents équipements.

C'est encore plus vrai lorsqu'il s'agit de mobiles NFC, car ils ne sont généralement pas émis par le monde du transport et ont vocation à être utilisés dans différentes régions.

La description détaillée de ces procédures de certification et de ces tests d'interopérabilité sort du périmètre du présent document.

1.4 PERENNITE DES INVESTISSEMENTS

Les évolutions des technologies peuvent remettre en cause la pérennité des investissements dans les équipements billettiques.

Ceci explique l'importance d'utiliser des technologies normalisées et des produits multi-sources.

L'objectif de la technologie Calypso, largement utilisée en France, est le même : assurer une base technique stable et durable garantissant autant que possible les investissements des systèmes mis en place.

Toutefois, l'ajout de nouveaux besoins non prévisibles initialement (traitement de mobiles NFC Java Card par exemple) peut exiger une mise à jour des systèmes.

Parallèlement, les améliorations de l'électronique font diminuer le niveau de sécurité des anciens composants. Des cartes et des modules de sécurité produits il y a dix ans ont ainsi un niveau de résistance aux attaques physiques relativement faible aujourd'hui.

Si le maintien d'un très haut niveau de sécurité est nécessaire, cela exige donc le remplacement des cartes et des SAM après 5 à 10 ans d'utilisation.

1.5 ÉVOLUTIONS DU DOCUMENT

Offre technique

Ce document reflète l'état de l'offre technique en 2010, mais ne constitue pas une recommandation pour l'une ou l'autre des solutions envisagées.

En particulier :

- Les mécanismes sont mieux définis dans le cas de l'utilisation de la SIM GSM que dans les autres cas, car l'offre de produits et de services est plus aboutie et mieux standardisée.
- Les mécanismes décrits pour l'application transport sont principalement ceux du standard Calypso, car il est apparu comme le mieux adapté, le plus largement utilisé dans les systèmes billettiques français, et est le seul actuellement utilisé dans le standard Intercode.

Évolutions du document

L'offre technique étant appelée à évoluer rapidement, ce document sera mis à jour au fur et à mesure de la disponibilité de nouveaux standards et de produits les mettant en œuvre.

1.6 NIVEAUX DE RECOMMANDATION

Les choix technologiques et les recommandations associées sont décrits au chapitre 3.

Les niveaux de recommandation suivants sont possibles :

- **Incontournable :** la mise en œuvre de la fonctionnalité est incontournable pour le bon fonctionnement de la billettique transport sur mobile NFC.
- **Fortement recommandé :** la mise en œuvre de la fonctionnalité, sans être nécessaire, apporte une réelle valeur ajoutée justifiant ce nouveau média**.**
- **Optionnel :** la mise en œuvre de la fonctionnalité apporte un plus au service, sans être indispensable.
- **Déconseillé** : la mise en œuvre de la fonctionnalité peut nuire au développement du service ou être associée à un coût non maitrisé.

1.7 CONVENTIONS

Les documents techniques de référence sont énumérés et numérotés au chapitre 6.3. La première citation d'un de ces documents est suivie de son numéro placé entre crochets, par exemple « [1] » pour le DoFoCo Mobile NFC.

1.8 GLOSSAIRE

Note : Les termes et expressions en *italiques* dans le tableau ci-dessous sont également définis dans le DoFoCo Mobile NFC (dans le glossaire ou dans le corps du document).

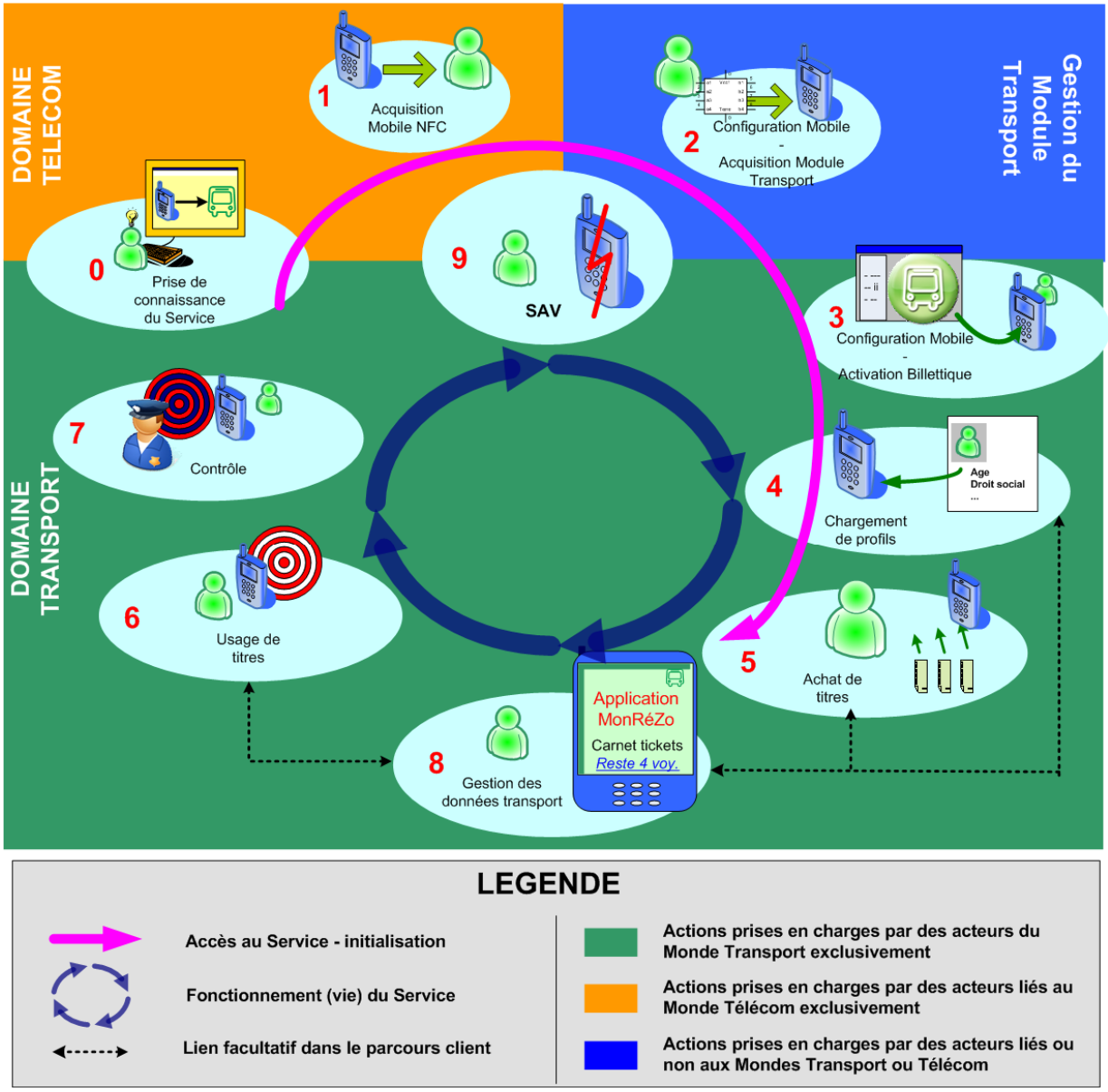
Glossaire	
Applet	Terme générique qualifiant un logiciel en langage Java.
Application billettique	Logiciel du module transport qui héberge le programme et les données relatives à la billettique sur mobile NFC. Il utilise et protège les ressources cryptographiques qui sécurisent les transactions. Lorsque le module transport est une Java Card, l'application billettique est un cardlet.
Application transport	Ensemble des ressources logicielles du mobile NFC spécifiques à la billettique : l'application billettique et l'application d'interface voyageur.
Application d'interface voyageur	Logiciel du mobile en charge des traitements spécifiques à la billettique du mobile NFC, en particulier des interactions avec le voyageur. Dans un environnement Java ME, c'est un midlet.
Cardlet	Applet spécifique à l'environnement Java Card. Dans le contexte de ce document, qualifie le logiciel du module transport lorsqu'il s'agit d'une Java Card.
Carte tierce	Module transport lorsqu'il n'est pas la carte SIM de l'opérateur télécom. Elle peut être une Java Card ou non, solidaire du mobile ou non, et peut ou non disposer de sa propre interface NFC.
CSM	*Calypso Secure Module* : SAM (Secure Application Module) ou HSM (Hardware Security Module) Calypso.
ISD	*Issuer Security Domain* : environnement de sécurité principal d'une carte GlobalPlatform.
Logiciel du mobile	Tout logiciel exécuté par le mobile NFC lui-même (système d'exploitation, application d'interface voyageur, etc.) et non par un périphérique (même intégré, comme le composant « baseband », la SIM GSM, le module d'interface NFC, etc.).
Midlet	Applet spécifique à l'environnement Java ME (un midlet est un logiciel du mobile).
Mode Carte	Mode de la norme NFC où le mobile se comporte comme une carte au sens de la norme ISO 14443. Le mobile est passif, et son interlocuteur est actif (il est en Mode Lecteur). Dans le DoFoCo Mobile NFC, ce mode est appelé « émulation de carte ». C'est le mode utilisé par le mobile pour dialoguer avec les terminaux billettiques, qui généralement ne fonctionnent qu'en Mode Lecteur.
Mode Égal à Égal	Mode de fonctionnement de la norme NFC (« peer to peer ») où les deux interlocuteurs sont actifs. Dans le DoFoCo Mobile NFC, ce mode est appelé « peer to peer ». C'est le mode utilisé pour le dialogue entre deux mobiles [1].

[1] Lorsque le Mode Égal à Égal n'est pas disponible, les échanges de mobile à mobile pourraient être réalisés avec l'un en Mode Carte et l'autre en Mode Terminal.

Mode Lecteur	Mode de la norme NFC où le mobile se comporte comme un terminal au sens de la norme ISO 14443. Le mobile est actif, et son interlocuteur est passif (il est en Mode Carte). Dans le DoFoCo Mobile NFC, ce mode est appelé « lecture / écriture ». C'est le mode utilisé par le mobile pour dialoguer avec une carte à puce sans contact ou un tag NFC (toujours alimentés par le terminal).
Mode pull	Mode de transfert de données OTA où le mobile initie les échanges.
Mode push	Mode de transfert de données OTA où un SI initie les échanges.
Module transport	Environnement sûr dans lequel est stockée et fonctionne une application billettique. Dans le contexte de ce document, il s'agit d'une carte à puce à microprocesseur.
Native	Qualifie une carte dont l'application billettique est intégrée à l'OS.
Operating System	Logiciel assurant les fonctions de base d'un équipement (carte native, Java Card, mobile NFC, etc.), et permettant éventuellement le fonctionnement de logiciels (applications) supplémentaires.
Opérateur billettique	Opérateur en charge de l'exploitation de tout ou partie du système billettique.
Opérateur de transport	Opérateur en charge de l'exploitation du réseau de transport. Dans le contexte de ce document, sauf indication contraire ce terme englobe la fonction d'opérateur billettique , car cela ne modifie pas les besoins techniques des différentes interfaces considérées.
OS	Voir Operating System.
SE	Voir Secure Element.
Secure Element	Élément physique ou logique sécurisé certifié pour héberger et permettre l'exécution d'applications. Par exemple une carte à puce bancaire ou transport, carte SIM. Le module transport est un SE.
SI	*Système d'information* : ensemble des serveurs de données et d'applications (ERP, CRM, etc.) nécessaires à la mise en œuvre d'un service.
SI transport	Système d'information géré par opérateur billettique ou par un opérateur de transport.
SIM GSM	Carte SIM de l'opérateur télécom. Elle peut être le module transport.
SSD	*Supplementary Security Domain* : environnement de sécurité supplémentaire d'une carte GlobalPlatform.
Terminal billettique	Dans le contexte de ce document, est considéré comme terminal billettique tout terminal qui dispose temporairement ou en permanence d'une IHM billettique, à l'exception d'un mobile NFC. Par exemple, l'ordinateur personnel d'un voyageur utilisé pour acheter un titre de transport sur le site Internet de l'opérateur billettique avec un navigateur standard est considéré comme un terminal billettique pour toute la durée de cette opération.

2 PARCOURS CLIENT

Le parcours client décrit ci-dessous, tel que repris du DoFoCo Mobile NFC, rappelle les services offerts par la billettique transport sur mobile NFC :



Pour chaque étape du parcours client, les acteurs potentiellement concernés dans l'écosystème billettique sur Mobile NFC sont :

- l'autorité organisatrice de transport public, en charge de l'organisation des transports sur la zone géographique concernée
- l'opérateur de transport, en charge de l'exploitation du réseau de transport
- l'opérateur billettique, en charge de l'exploitation de tout ou partie du système billettique
- l'opérateur télécom, en charge de l'exploitation du réseau télécom mobile
- le distributeur de mobile, en charge de la vente des mobiles aux voyageurs
- le distributeur de module transport, en charge de la vente du module transport
- le gestionnaire du module transport, en charge de l'administration technique et sécuritaire du module de sécurité hébergeant l'application billettique

3 ENVIRONNEMENT TECHNIQUE ET RECOMMANDATIONS ASSOCIEES

L'objet de ce chapitre est de décrire les contraintes techniques présentant un fort impact sur l'interopérabilité et qu'il est nécessaire de prendre en compte dans le cadre des exigences fonctionnelles et techniques de la billettique NFC en France.

Les choix techniques qui se posent aux Autorités Organisatrices et aux Opérateurs de Transport sont également décrits. Ces choix sont liés aux contraintes imposées par les standards, aux limitations des technologies utilisées, et à la nécessité de prise en compte des systèmes existants.

Un choix technique peut avoir un coût important lié aux évolutions des systèmes existants qu'ils peuvent entrainer. Il est donc important d'appréhender les conséquences fonctionnelles des choix techniques retenus.

Note concernant la propriété intellectuelle
Toutes les technologies sont issues de travaux de recherche et sont, pour la plupart, protégées par des brevets ou des droits d'auteur, soit pour en réserver l'utilisation à leur créateur, soit pour valoriser les travaux de recherche ou encore financer les améliorations apportées à ces technologies. Lorsqu'une technologie est intégrée à un standard, les propriétaires de brevets s'engagent à offrir des licences sur une base raisonnable et non discriminatoire (conditions « RAND »). Ces conditions d'accès comportent souvent une contrepartie financière incluant le versement de royalties aux possesseurs de brevets. La prise en compte de ces licences et des financements qui leur sont associés, sont assurés par les fabricants d'équipements ; les utilisateurs n'étant généralement pas concernés. C'est par exemple le cas des brevets sur la technologie ISO 14443 (brevets gérés par NXP pour le type A et par Innovatron pour le type B/B'), pour la technologie NFC, pour la technologie Calypso, le produit MIFARE Classic (protocole MIFARE Classic), etc. La validité d'un brevet ne peut dépasser vingt ans. La durée de validité d'un droit d'auteur est plus longue (généralement 70 à 120 ans). Lorsque cela est pertinent, le présent chapitre contient des clarifications sur la gestion de la propriété intellectuelle attachée aux technologies mentionnées.

3.1 PROTOCOLE DE COMMUNICATION SANS CONTACT

Les systèmes télébillettiques ont retenu la norme *ISO/IEC 14443* ([5] à [8]) pour les échanges sans contact entre les terminaux et les objets portables. Cette norme comprend deux protocoles de communication, appelés « *Type B* » et « *Type A* ».

La France étant pionnière dans la billettique interopérable, de nombreux systèmes télébillettiques y utilisent un protocole précédant la norme ISO 14443, appelé *protocole Innovatron* [13] (ou « *Type B'* », car il a servi de base au type B de la norme). Ce protocole ne fait pas partie de la norme ISO 14443 et n'est pas utilisée à l'étranger.

Les produits MIFARE Classic, bien que compatibles avec la norme ISO 14443 Type A, utilisent un jeu de commande et une cryptographie propriétaires et non normalisés.

Enfin, les différents types de billets sans contact utilisent des variantes simplifiées de la norme ISO 14443, et non entièrement compatibles avec elle.

Les *terminaux* peuvent communiquer selon un ou plusieurs de ces protocoles. Dans un même système billettique, il est donc possible de traiter différents types d'objets.

Un *objet portable* communique selon l'un de ces protocoles [2].

➔ **Question en cours**	Question en cours auprès de l'AFSCM sur ce point : *La norme ISO 14443 prévoit une détection automatique du type (B/A) de l'objet portable (PICC) présenté dans le champ d'un terminal (PCD).* *Pour cela, le terminal appelle alternativement les différents types d'objets portables.* *Si d'autres protocoles radio sont gérés par le terminal (B'/Innovatron, Protocole MIFARE Classic, billets sans contact, etc.), de même, le terminal appelle alternativement ces différents types d'objets.* *L'esprit de la norme ISO 14443 définit ainsi clairement un fonctionnement dans lequel le terminal est multi-protocole et l'objet portable mono-protocole.* *Toutefois, certains mobiles NFC utilisés en mode carte sont capables de fonctionner également selon plusieurs protocoles radio.* *Si un tel mobile reconnait dynamiquement le type de protocole utilisé par le terminal, plusieurs problèmes peuvent intervenir, tels que :* *- multiples détections du même mobile par le terminal (une fois dans chaque protocole commun).* *- phénomènes de " battements " entre le mobile et le terminal rendant la communication plus difficile.* *De plus, les spécifications EMV exigent que les objets portables EMV ne soient détectables que dans un seul protocole.* *Afin de garantir l'interopérabilité entre les mobiles NFC et les terminaux multi-protocoles, les acteurs du transport publics pourraient donc envisager de recommander que les mobiles NFC soient configurés dans un mode de communication unique lorsqu'ils fonctionnent en mode carte (à un moment donné).* ***Étant donné l'état de la normalisation NFC, et de la normalisation Java Card/GlobalPlatform (en particulier la version 1.0 de l'annexe C de GP 2.2), l'AFSCM a-t-elle émis une recommandation concernant ce fonctionnement en mode carte des mobiles multi-protocoles ?***

Les mobiles NFC utilisent les normes *ISO/IEC 18092* [9] et *ISO/IEC 21481* [9], appelées *NFC* pour « Near Field Communication » (*Communication en Champ Proche*). Ces normes intègrent l'ISO 14443 en tant que sous-ensemble. Certains mobiles NFC prototypes, en particulier lorsqu'ils sont destinés au marché Français, peuvent utiliser les protocoles Innovatron ou MIFARE Classic.

L'application *Calypso* [17] peut être utilisée à travers tout type de protocole de communication (ISO 14443 types B / A, ISO/IEC 7816-3 [11] (contacts) ou autres). Le protocole ISO 14443 doit être possible avec tout objet portable Calypso.

[2] Il est possible de fabriquer un objet portable compatible avec plusieurs protocoles sans contact. Toutefois cela va à l'encontre de l'esprit de la norme ISO 14443 et doit être évité pour des raisons fonctionnelles. En effet, les terminaux qui utilisent plusieurs protocoles sans contact risquent dans ce cas de traiter plusieurs fois le même objet portable.
Les mobiles NFC pouvant traiter plusieurs protocoles n'en activent qu'un en Mode Carte à un instant donné.

Voici les avantages et inconvénients généraux liés à chaque type de transmission pour un mobile NFC utilisé en *Mode Carte* dans un réseau billettique :

Type de protocole (mode Carte)	*Avantages*	*Inconvénients*
ISO 14443 Type B	Normalisé. Présent dans les mobiles NFC.	-
ISO 14443 Type A	Normalisé. Présent dans les mobiles NFC.	N'est encore utilisé par aucun objet portable Calypso déployé en quantité. Certains réseaux Calypso n'activent pas le type A.
Innovatron (« B' »)	Compatibilité avec les terminaux installés et n'utilisant pas encore l'ISO 14443.	Protocole non normalisé. Ce protocole, remplacé par l'ISO 14443 Type B, disparaîtra à terme. Difficulté de trouver des mobiles NFC utilisant ce protocole.
MIFARE Classic	Compatible avec les cartes MIFARE Classic, ce qui peut intéresser certaines applications hors transport (contrôle d'accès physique par exemple).	Protocole non normalisé. Non utilisé pour l'interopérabilité dans les transports publics français. Sécurité insuffisante des cartes MIFARE Classic [3].

Note concernant la propriété intellectuelle
Des brevets existent concernant les technologies mises en œuvre dans la norme ISO 14443. Ces brevets sont décrits dans les premières pages de la norme. Il est à noter que les mêmes brevets s'appliquent de la même façon au type B de l'ISO 14443 et au B', ces deux technologies étant extrêmement proches.

[3] Le gouvernement français recommande de ne plus utiliser la cryptographie des produits MIFARE Classic : *http://www.securite-informatique.gouv.fr/gp_article654.html.*

Note concernant les réseaux existants et non conformes à l'ISO 14443

Il est techniquement possible de disposer d'échantillons de mobiles NFC fonctionnant selon le protocole Innovatron (B') ou MIFARE Classic, en mode *Carte* ou en mode *Lecteur*.

- Est-il alors possible à un réseau existant et n'acceptant que les objets portables au protocole Innovatron (B') ou MIFARE Classic d'utiliser ces mobiles NFC afin d'éviter de mettre à jour son parc de lecteur ?

Non, car il n'est pas possible de maîtriser le parc de mobiles NFC utilisés par les clients du réseau de transport (excepté pour une expérimentation). La plupart des mobiles NFC fonctionneront selon la norme ISO 14443, et n'accepteront pas les protocoles Innovatron (B') et MIFARE Classic, qui ne sont pas normalisés.

Par ailleurs, les possesseurs de mobiles NFC souhaiteront les utiliser pour d'autres applications (autres réseaux de transport, paiement, contrôle d'accès, tags...), ce qui n'est possible que si la norme ISO est utilisée.

Enfin, la gestion de mobiles NFC requiert d'autres modifications fonctionnelles dans les terminaux, sur lesquelles une mise à jour est donc de toute façon nécessaire (gestion de la ratification de fin de transaction, de SELECT APPLICATION, etc.).

Toutefois, il ne faut pas sous estimer les travaux requis pour cette mise à jour (voir le chapitre 5).

- Est-il possible d'utiliser le mobile NFC pour recharger les cartes fonctionnant selon le protocole Innovatron (B') ou MIFARE Classic ?

Oui, toutefois tout le parc de mobiles NFC n'offrira pas ces protocoles obsolètes ou non normalisés, et qui disparaîtront à terme.

Note concernant le standard EMV Contactless

Un mobile approuvé pour le standard *EMV Contactless* et conforme à ISO 14443 est traité normalement par tout terminal billettique [4].

Il est à noter que, comme requis par le standard *EMV Contactless*, les terminaux billettiques doivent utiliser la valeur 00h pour le champ *AFI* de l'ISO 14443 (en effet, certains mobiles pourraient ne pas répondre si d'autres valeurs sont utilisées).

[4] Cette analyse résulte des travaux menés par le groupe de travail 9 (WP9) de Calypso Networks Association.

Recommandations techniques et de sécurité

Recommandation	*Niveau / Objectif*
Les terminaux billettiques *doivent* traiter l'ISO 14443 type B *et* type A.	**Incontournable** **Assurer la pérennité de fonctionnement en se basant sur la norme internationale ISO 14443.** **Accepter un mobile NFC quelque soit le type ISO 14443 qu'il utilise.**
Les terminaux billettiques *peuvent* également traiter d'autres protocoles sans contact comme le protocole Innovatron (B') ou le protocole MIFARE Classic, à condition que cela ne perturbe pas le traitement des objets portables ISO 14443.	**Optionnel** **Assurer la compatibilité avec d'autres objets portables (monomodaux, ou préexistants sur le réseau ou bien sur un réseau interopérable).**
Les mobiles NFC *doivent* fonctionner selon la norme ISO 14443. **Avant une utilisation en mode Carte avec des équipements billettiques, le mobile NFC doit fonctionner dans un seul des deux types B ou A (et non les deux simultanément)[5].**	**Incontournable** **Permettre l'utilisation de tout mobile NFC et pour d'autres applications sans contact.**
Dans les trames REQB et WUPB (cf. ISO 14443-3), les terminaux billettiques doivent fixer le champ AFI à la valeur 00h.	**Fortement recommandé** **Permettre l'utilisation de tout mobile NFC indiquant un domaine d'activité quelconque.**

Ces recommandations peuvent être assouplies dans le cadre d'expérimentations et de test pilotes.

[5] Voir note encadrée page 15, qui décrit la question posée à l'AFSCM concernant cette contrainte.

3.2 CALYPSO : TYPES DE CLES CRYPTOGRAPHIQUES

La sécurité des systèmes télébillettiques[6] est basée sur l'utilisation d'informations secrètes, les *clés cryptographiques*, permettant aux objets portables et aux terminaux de s'authentifier. Ces clés sont enfermées dans des composants de sécurité (puces de sécurité utilisées pour les cartes, les SIM des mobiles NFC, les SAM des terminaux) qui en assurent la confidentialité.

Il existe différents types de clés, correspondant à différents types d'usages : DES, DESX, Triple-DES, AES, RSA, ECC, ainsi que des types propriétaires tels que Crypto-1 (MIFARE Classic).

La technologie Calypso, largement utilisée pour permettre l'interopérabilité en France, permet actuellement l'utilisation de clés Triple-DES, DESX et DES :

Type	*Taille des clés*[7]	*Remarques*
Triple-DES	112 bits	Haut niveau de sécurité. Disponible seulement sur les objets portables Calypso à partir de la révision 3 du standard. Mieux standardisé que DESX, donc potentiellement disponible dans les OS génériques, ce qui simplifie les développements et peut améliorer les performances. Par exemple, pour un terminal de validation typique[8], une transaction TDES est de 10 à 20% plus rapide avec des objets *Java Card* [16] tels que les mobiles NFC.
DESX	120 bits	Très bon niveau de sécurité. Utilisé par la plupart des réseaux Calypso déployés à mi-2010. Possible sur une plateforme Java Card standard, avec une transaction un peu plus lente qu'avec du Triple-DES.
DES	56 bits	Obsolète, ne doit plus être utilisé pour de nouveaux déploiements.

Note concernant la propriété intellectuelle
Les brevets concernant les algorithmes DES, DESX et Triple-DES et leur mise en œuvre ont expiré. Il n'y a pas de différence dans la mise en œuvre de ces différents algorithmes d'un point de vue de la propriété intellectuelle[9].

[6] Cf. le livre blanc Calypso sur la sécurité ([19]).

[7] La résistance aux attaques cryptographiques est principalement fonction de la taille de la clé.

[8] Pour un terminal de validation moyen. Plus le terminal est performant, plus le ralentissement relatif de la transaction est perceptible.

[9] Le « hash Innovatron » utilisé avec le DES et le DESX n'est pas attaché à une licence spécifique.

Note concernant les réseaux existants (DES simple ou DESX)

Continuer à utiliser des clés DESX avec des mobiles NFC est possible et évite de remplacer les SAM installés dans les équipements.

Utiliser des clés Triple-DES présente les avantages suivants :
- accélérer la transaction avec les objets portables Java Card (10 à 20%),
- améliorer le niveau de sécurité par l'utilisation des mécanismes de sécurité standard Java Card.

Attention : une mise à jour logicielle des terminaux est requise pour traiter les objets portables Java Card, dont les mobiles NFC (voir le chapitre 5).

Un système billettique évolue avec le temps, et il est important de prévoir et de maîtriser ces évolutions. Lors de la mise à jour des SAM (par exemple en fin de vie du produit, ou lors d'extensions du système), il est donc fortement recommandé de profiter du remplacement ou de l'extension pour ajouter des clés Triple-DES (et DESX le cas échéant), afin de permettre :
- l'utilisation de clés Triple-DES, en particulier pour les mobiles NFC, lorsque tous les SAM du ou des réseaux concernés auront été remplacés.
- l'abandon des clés DES simple (lorsque tous les SAM du ou des réseaux concernés auront été remplacés et que les cartes ayant des clés DES simple seront arrivées en fin de vie).

Note concernant les temps de transaction

Les mobiles NFC, comme tous les objets Java Card, sont plus lents que les cartes natives. Cette différence s'amenuise toutefois avec les améliorations des composants électroniques. Le temps total de transaction dépend également des temps de traitement des terminaux (valideur, SAM).

Typiquement, les durées de traitement peuvent varier de 1 à 5 selon la plateforme utilisée (natif, Java) et le temps de traitement des terminaux, par exemple moins de 100 ms à plus de 500 ms pour une transaction simple [10].

Ces durées sont données à titre indicatif. Les performances peuvent être dégradées dans certains cas (mobile éteint, transaction complexe, etc.).

Dans tous les cas, le type de clé a une influence *non prépondérante* sur la durée de la transaction (par rapport aux autres paramètres : composant, logiciel[11], traitements du terminal, etc.), y compris pour une implémentation de la cryptographie DESX sur une plateforme Java Card standard (système d'opération Java Card non modifié pour accélérer le traitement en DESX : pas de « patch de l'OS »).

[10] Définie comme suit : anticollision ISO 14443, sélection d'application Calypso, ouverture de session avec lecture, trois lectures, une modification, fermeture de session, ratification par commande.

[11] Pour une carte Java, le logiciel se compose du système d'opération et de l'applet.

Recommandations techniques et de sécurité

Recommandation	*Niveau / Objectif*
La mise en service d'un *nouveau* système billettique doit définir des SAM : **- comportant des clés DESX et Triple-DES,** **- ne comportant PAS de clés DES simple.**	**Incontournable** **Assurer la compatibilité avec tous les supports Calypso, et permettre une vitesse de transaction optimale avec les supports Calypso Java Card, dont les mobiles NFC (la création initiale de clés DESX et Triple-DES ne présente aucun inconvénient pour un nouveau système).** **Éviter des fraudes possibles par attaque des clés DES simple.**
Les systèmes billettiques Calypso *existants peuvent* déployer des clés Triple-DES lors d'une mise à jour des SAM.	**Fortement recommandé** **Permettre à terme une vitesse de transaction optimale avec les supports Calypso Java Card, dont les mobiles NFC.**
Les systèmes billettiques Calypso utilisant des clés DES simples devraient prévoir leur fin de vie.	**Fortement recommandé** **Améliorer le niveau de sécurité et éviter des fraudes possibles par attaque des clés DES simple.**

3.3 MODULE TRANSPORT

Les logiciels qui stockent et manipulent les secrets de l'application billettique (clés cryptographiques) doivent s'exécuter dans un environnement physique assurant un niveau de sécurité suffisant (par exemple le niveau d'évaluation VLA.4/VAN.5 définit par les critères communs, cf. ISO 15408). Actuellement, seules les cartes à puce à microprocesseur répondent à cette exigence[12].

L'application billettique peut donc être traitée soit par la carte SIM de l'opérateur télécom (SIM GSM), soit par une carte à puce tierce.

Recommandations techniques et de sécurité

Recommandation	*Niveau / Objectif*
Les clés et le logiciel du module transport *doivent* être présents dans une carte à puce à microprocesseur.	**Incontournable** **Assurer un niveau de sécurité suffisant contre les attaques de fraudeurs.**
La carte à puce hôte du module transport *peut* être la SIM GSM du mobile.	**Optionnel** **Compatibilité avec la plupart des mobiles.**
La carte à puce hôte du module transport *peut* être une carte à puce tierce (par exemple une seconde carte SIM, une carte enfichable ou un composant fixé au mobile).	**Optionnel** **Indépendance vis-à-vis de l'émetteur de la SIM GSM.**

Note :

Actuellement les Java Cards sont significativement plus lentes que les cartes dédiées. De plus, elles présentent de grandes disparités de temps de transaction, principalement liées :

- aux capacités du composant ;
- à son système d'exploitation, en particulier pour les fonctions Java ;
- au package (cardlet) utilisé.

Afin de minimiser les ralentissements, en particulier lors de la validation, il est recommandé de :

- s'assurer que les transactions ne comportent aucune opération superflue ;
- donner aux critères de performances une importance majeure dans le cahier des charges des valideurs, des mobiles, des cartes et des cardlets ;
- limiter le nombre et la complexité des titres chargés dans les supports lents.

[12] En particulier, pour des raisons de sécurité, il n'est pas possible de traiter l'application billettique à l'aide d'un module logiciel exécuté par le processeur du mobile (« midlet »). La possibilité de cette solution, évoquée dans le DoFoCo (§4.4, §7.1.2.5, §7.7.1.2 et §7.7.2), doit donc être écartée.

3.4 GESTION DE PLUSIEURS APPLICATIONS SANS CONTACT

Il est possible d'utiliser un mobile NFC pour différentes applications sans contact, telles que :

- plusieurs applications de transports publics correspondant à différents réseaux,
- moyen de paiement,
- application de contrôle d'accès,
- autres.

Afin que le terminal puisse sélectionner l'application qui lui correspond, le mobile NFC doit être conforme à la norme ISO 14443 (voir section 3.1), et à la norme ISO/IEC 7816-4 [12] concernant la sélection d'application (gestion de la commande SELECT APPLICATION).

Comme le spécifie la norme ISO/IEC 7816, chaque application doit être identifiée de façon unique par son identifiant d'application (« AID » ou « Application Identifier »).

Pour les applications de transport public en France, la règle de gestion des AID est définie dans la norme Intercode.

3.5 IDENTIFIANT TRANSPORT

L'identifiant transport, tel que défini dans le DoFoCo Mobile NFC (§7.2.2.3, page 58), est géré par le Domaine Transport et permet d'identifier sans ambigüité l'application billettique d'un mobile NFC donné.

Cet identifiant peut être :

- un numéro de support unique (par exemple le ***numéro de série Calypso***), ou
- un numéro applicatif unique (donnée de l'application billettique, tel qu'un numéro d'émission)

Il doit être lié au nom de l'application (***AID***), de façon à faciliter la sélection parmi la pluralité d'applications portées par le module transport (tel qu'une carte SIM GSM).

Lorsque le gestionnaire de l'application billettique n'est pas le gestionnaire du module transport, ce dernier définit un *identifiant technique du module*, qu'il fournit au gestionnaire de l'application billettique qui établit la correspondance entre *l'identifiant transport* et *l'identifiant technique*.

Dans le cas de l'utilisation de la SIM GSM, la *Spécification Technique Ulysse* ([3], §11.1) définit l'identifiant technique « ID_TECH » unique, choisi par l'opérateur télécom, qui permet de fournir à l'opérateur de transport un identifiant sans lui communiquer le numéro de mobile associé.

Dans les autres cas, il n'existe pas de spécification de référence pour le choix et l'implémentation (codage, mode de transmission, etc.) de l'identifiant technique ; cette identification sera donc à réaliser au cas par cas. Néanmoins, pour toutes les fonctions où le mobile doit recevoir un SMS, le numéro de mobile doit être utilisé (avec l'accord de l'utilisateur).

Recommandations techniques et de sécurité

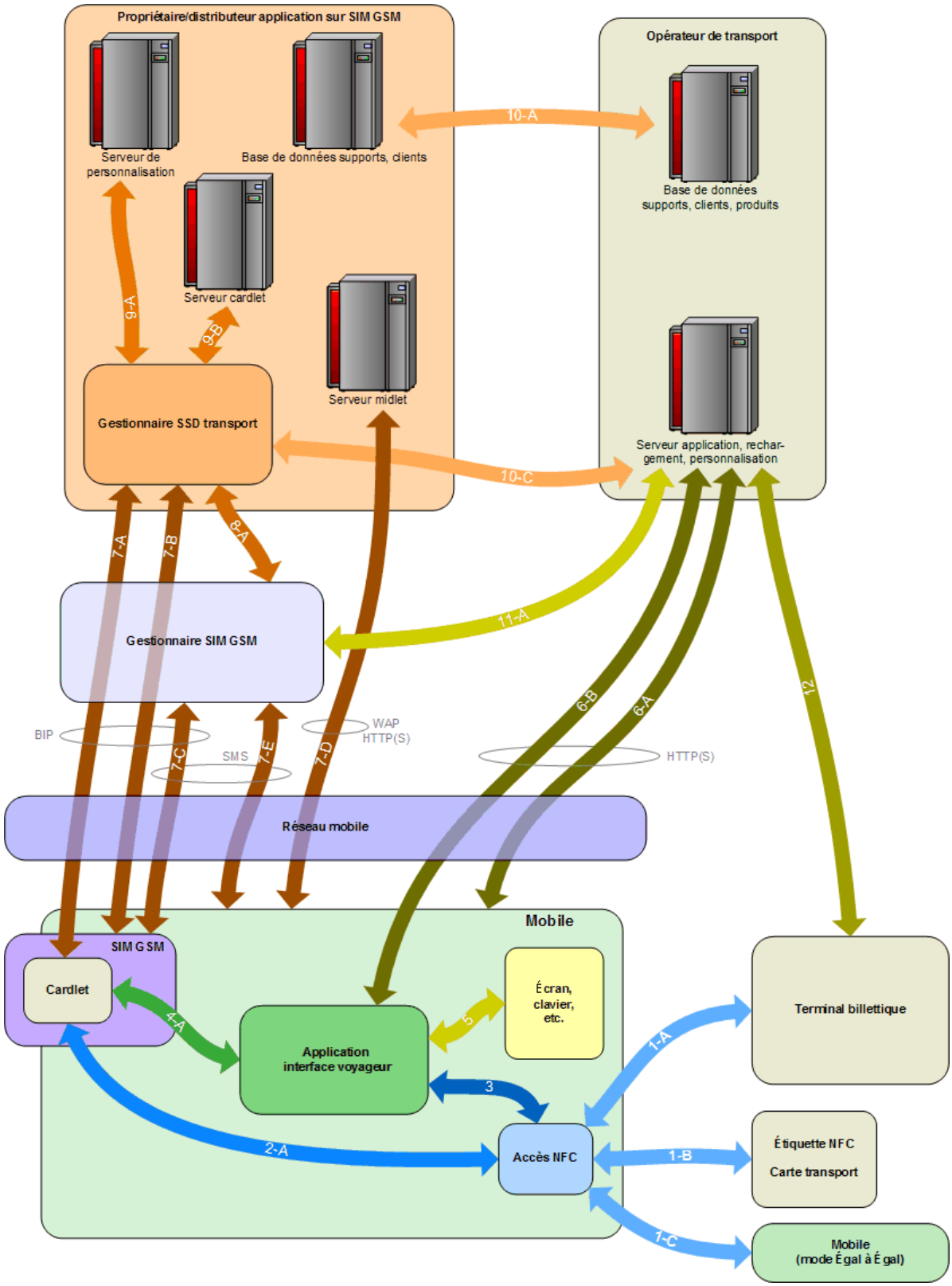
Recommandation		*Niveau / Objectif*
L'identifiant transport doit **être un numéro unique géré par le Domaine Transport.** **Il *doit* être associé au nom de l'application (AID).** **Il *doit* être défini selon des règles communes à tous les opérateurs de transport d'un même réseau interopérable.**		**Incontournable** **Identification simple et unique de l'application billettique.**
Le module transport est la SIM GSM.	***L'identifiant technique*** **du module transport défini par les spécifications Ulysse doit être utilisé.**	**Incontournable** **Indépendance de gestion, interopérabilité.**
	Le gestionnaire transport *doit* gérer la correspondance entre l'identifiant transport et l'identifiant technique du module.	**Incontournable** **Identifier le module transport, dans le respect de la gestion des données personnelles.**

<table>
<tr><td rowspan="5">Le module transport n'est pas la SIM GSM.</td><td rowspan="2">Le module transport n'est pas géré par le gestionnaire transport</td><td>L'identifiant technique du module transport doit être défini par le gestionnaire du module transport, selon des principes standard ou non.</td><td>Incontournable
Indépendance de gestion.</td></tr>
<tr><td>Le gestionnaire transport doit gérer la correspondance entre l'identifiant transport et l'identifiant technique du module.</td><td>Incontournable
Identifier le module transport, dans le respect de la gestion des données personnelles.</td></tr>
<tr><td rowspan="2">Le module transport est géré par le gestionnaire transport</td><td>L'identifiant technique du module transport peut être défini par le gestionnaire transport, selon des principes standard ou non.</td><td>Optionnel
Indépendance de gestion.</td></tr>
<tr><td>Le gestionnaire transport peut gérer la correspondance entre l'identifiant transport et l'identifiant technique du module.</td><td>Optionnel
Identifier le module transport, dans le respect de la gestion des données personnelles.</td></tr>
<tr><td colspan="2">Le numéro de téléphone du mobile peut être connu du gestionnaire de l'application billettique pour la durée de l'opération en cours.</td><td>Optionnel
Identifier temporairement le mobile (par exemple pour un voyageur anonyme).</td></tr>
<tr><td colspan="2">Le numéro de téléphone du mobile peut être connu du gestionnaire de l'application billettique, qui l'associe au voyageur (au moins pour la durée de vie de son application transport).</td><td>Optionnel
Associer un mobile à un voyageur référencé.</td></tr>
</table>

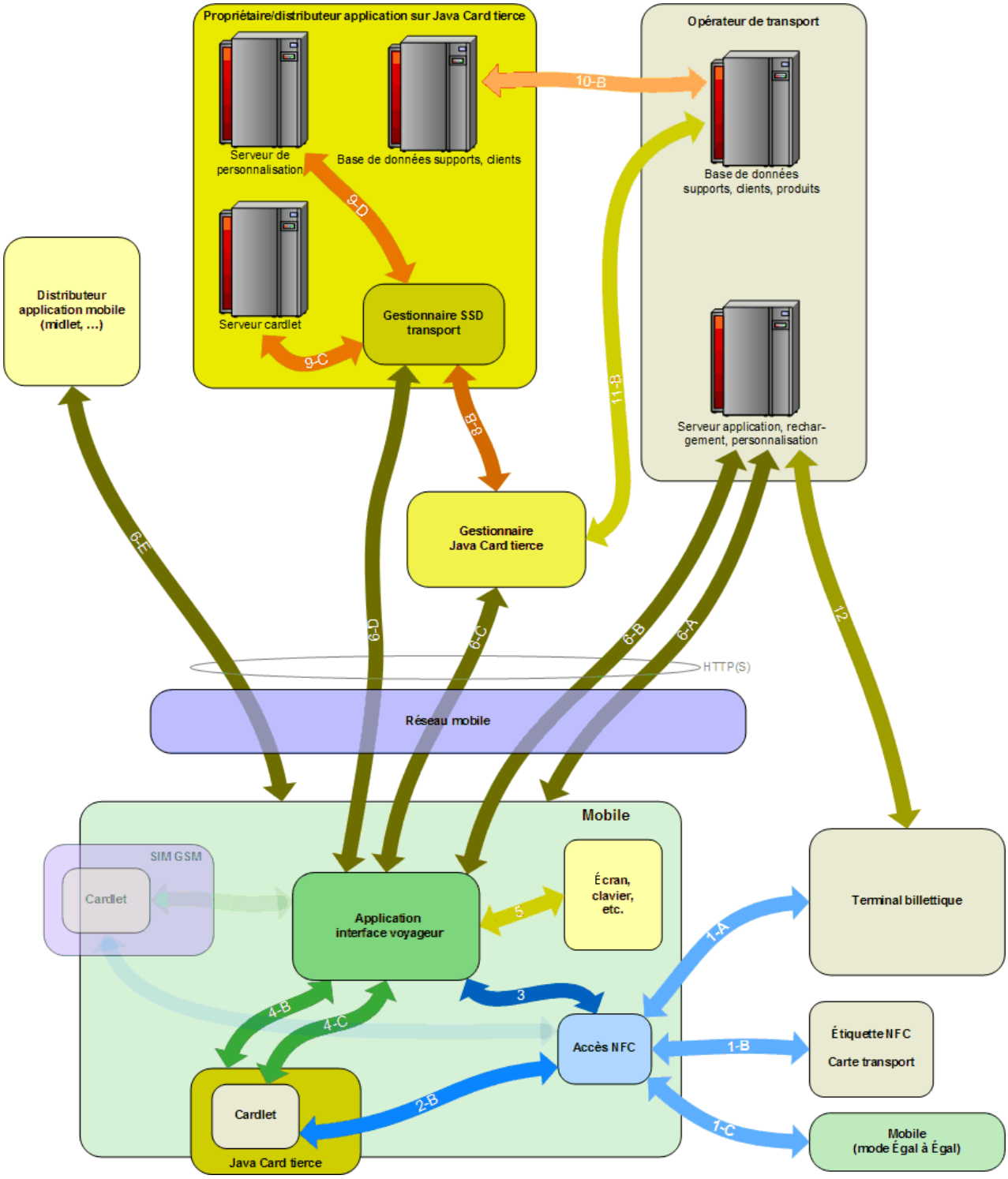
3.6 INTERFACES

Les diagrammes ci-dessous sont une description simplifiée des éléments potentiellement mis en œuvre dans un système billettique utilisant des mobiles NFC, et de celles de leurs interfaces qui sont couvertes par le présent document.

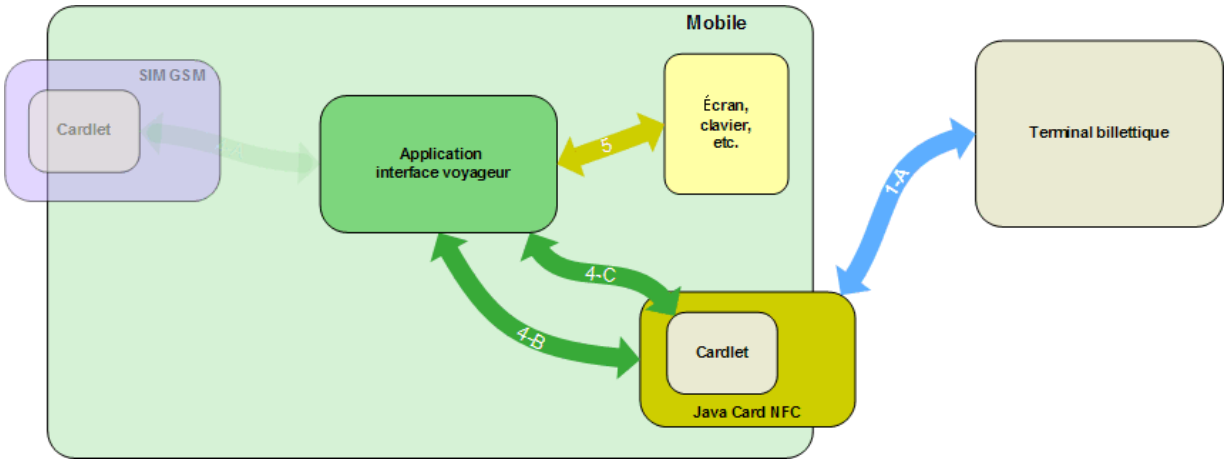
Utilisation de la SIM GSM :



Utilisation d'une carte tierce :



Cas d'une carte tierce intégrant l'interface NFC :



Pour les interfaces décrites dans ces diagrammes, le tableau ci-dessous indique les normes ou les standards qui peuvent s'appliquer :

Interface		Normes et standards applicables
1	**Interface NFC externes (protocole sans contact, voir chapitre 3.1)**	NFC : [9] et [10] ISO 14443 : [5] à [8]
1-A	Mode Carte : mobile / terminal billettique	-
1-B	Mode Terminal : mobile / carte ou billet sans contact, tag NFC	B', MIFARE Classic, CTS512, SRT512, etc. Tags NFC : [30] à [35]
1-C	Mode Égal à Égal : mobile / mobile	-
2	**Interface NFC du module transport (échanges internes au mobile, entre le module d'interface NFC et le module transport)**	ISO 7816 : [11] et [12] SWP : [22] HCI : [23]
2-A	Cardlet SIM GSM / accès NFC	
2-B	Application carte tierce / accès NFC	
3	**Interface logiciel du mobile / accès NFC (échanges internes au mobile, entre l'application billettique du mobile et le module d'interface NFC)**	HCI : [23] JSR 257 : [28] SD/SDIO Bluetooth JSR 82 : [26]
4	**Interface module transport / logiciel du mobile (échanges internes au mobile, entre le module transport ou la carte à puce hôte et l'application billettique)**	ISO 7816 : [11] et [12] USB JSR 177 : [27] Calypso Product Remote Loading : [17]
4-A	Cardlet SIM GSM / logiciel du mobile	Support de BIP : [36]
4-B	Carte tierce / logiciel du mobile	SD/SDIO Bluetooth JSR 82 : [26]
4-C	Application carte tierce / logiciel du mobile	
5	**Dispositifs d'IHM (interface homme-machine) du mobile**	Java ME JSR 118

6	**Interface mobile / SI non télécom (via le lien http(s) du mobile)**	SSL
6-A	Mobile / SI transport (serveur d'applications d'interface voyageur)	-
6-B	Logiciel du mobile / SI transport (serveur de rechargement, personnalisation)	Calypso Product Remote Loading : [17]
6-C	Logiciel du mobile / gestionnaire Java Card tierce	Calypso Application Downloading : [16]
6-D	Logiciel du mobile / gestionnaire SSD transport Java Card tierce	Calypso Application Downloading : [16]
6-E	Mobile / fournisseur d'application mobile	-
7	**Interface OTA via l'opérateur télécom**	Ulysse : [2] et [3]
7-A	BIP : Cardlet SIM GSM / gestionnaire SSD transport SIM GSM	Calypso Product Remote Loading : [17]
7-B	BIP : SIM GSM / gestionnaire SSD transport SIM GSM	Calypso Application Downloading : [16]
7-C	BIP ou SMS : SIM GSM / gestionnaire SIM GSM	Calypso Application Downloading : [16]
7-D	WAP ou http(s) : Mobile / gestionnaire module transport SIM GSM (serveur midlet)	-
7-E	SMS : Mobile / gestionnaire SIM GSM	-
8	**Interface gestionnaire SIM / gestionnaire SSD transport**	-
8-A	Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM	Ulysse : [2] et [3]
8-B	Gestionnaire Java Card tierce / gestionnaire SSD transport Java Card tierce	-
9	**Interface gestionnaire SSD / serveurs internes**	Calypso Application Downloading : [16]
9-A	Gestionnaire SSD transport SIM GSM / serveur de personnalisation	-
9-B	Gestionnaire SSD transport SIM GSM / serveur cardlet	-
9-C	Gestionnaire SSD transport Java Card tierce / serveur cardlet	-
9-D	Gestionnaire SSD transport Java Card tierce / serveur de personnalisation	-
10	**Interface SI transport / SI gestionnaire de modules transport**	-
10-A	Base de données supports, clients : SI transport / propriétaire/distributeur application SIM GSM	-
10-B	Base de données supports, clients : SI transport / propriétaire/distributeur application Java Card tierce	-
10-C	SI transport (serveur de rechargement, personnalisation) / gestionnaire SSD transport SIM GSM	Calypso Product Remote Loading : [17]
11	**Interface SI transport / gestionnaire Java Card**	-
11-A	SI transport (base de données supports, clients) / gestionnaire SIM GSM	Ulysse : [2] et [3]
11-B	SI transport (base de données supports, clients) / gestionnaire Java Card tierce	-
12	**Interface terminal billettique / SI transport (serveur de rechargement, personnalisation)**	Calypso Product Remote Loading : [17] SSL

Carte tierce non Java Card

Par simplification, dans le diagramme et les interfaces décrites ci-dessus, la solution technique avec une carte tierce non Java Card est omise. Ce cas est néanmoins traité lorsque nécessaire.

Par ailleurs, dans le cas d'une carte tierce native, les échanges entre le logiciel du mobile et la carte sont tous considérés comme portés par l'interface 4-C.

Interfaces internes aux SI

Dans les SI décrits, les relations entre les différents sous-systèmes sont hors du périmètre de ce document.

Utilisation de la SIM GSM

Les interfaces relatives à l'utilisation d'une SIM GSM comme hôte du module transport sont décrites dans les spécifications *Ulysse* ([2] et [3]). Cela concerne en particulier tout ou partie des interfaces suivantes : 1-A à 1-C, 2-A, 3, 4-A, 5, 7-A à 7-E, 8-A, 9-A, 9-B, 10-A et 11-A.

3.6.1 INTERFACE 1 : COMMUNICATIONS NFC

Ce chapitre traite les échanges en mode sans contact entre le module d'interface NFC du mobile et les terminaux billettiques, les cartes sans contact billettiques, et les tags NFC. Il reprend les recommandations du chapitre 3.1, en les détaillant lorsque nécessaire.

Note : Dans certaines solutions techniques, le module d'interface NFC pourrait être intégré au module transport accès au sans contact soit directement et les interfaces 2 et 3 pourraient être absentes.

Recommandations techniques et de sécurité

Recommandation			*Niveau / Objectif*
NFC du terminal billettique.		**ISO 14443 B *et* A.**	**Incontournable (cf. §3.1)** **Utilisation de tous types de supports normalisés**
		Autre protocole (Innovatron, MIFARE Classic, etc.).	**Optionnel (cf. §3.1)** **Compatibilité**
		AFI=00h dans REQB et WUPB.	**Fortement recommandé** **Utilisation de tous types de supports multi-application**
NFC du mobile.	**Mode Carte.**	**ISO 14443 B *ou* A.**	**Incontournable (cf. §3.1)** **Interopérabilité**
		Avant une utilisation en Mode Carte avec des équipements billettiques, le mobile NFC doit fonctionner dans un seul protocole.	**Incontournable (cf. §3.1)** **Éviter les risques de traitements inappropriés par les terminaux billettiques.**
	Mode Lecteur (ISO 14443 B *et* A).		**Fortement recommandé** **Lecture de *tags NFC* ([30] à [35]).**
			Optionnel **Transfert de titres vers une carte.** **Lorsque cette fonction est disponible, les recommandations pour l'interface NFC du terminal billettique (ci-dessus) s'appliquent également.**
	Mode Égal à Égal.		**Optionnel** **Transfert de titres entre mobiles.**
	Sélection automatique du mode de fonctionnement (Mode Lecteur ou Mode Égal à Égal).		**Optionnel** **Simplification du transfert de titres.**

Note concernant la sélection automatique du mode de fonctionnement

Lorsque le mobile est utilisé comme un « automate portable » (cf. §4.4.2.4), il peut fonctionner soit en Mode Terminal (par exemple pour communiquer avec une carte) soit en Mode Égal à Égal (par exemple pour communiquer avec un autre mobile).

La norme NFC indique que l'application initie la communication soit en « mode actif » (pour fonctionner en Mode Égal à Égal) soit en « mode passif » (pour fonctionner en Mode Terminal), ce qui correspond au choix du mode de fonctionnement par l'utilisateur décrit dans le DoFoCo (§7.4.3.7).

Il est néanmoins possible de définir un scénario de sélection automatique du mode de fonctionnement, où le mobile initiateur teste alternativement la présence d'une cible dans le mode actif et dans le mode passif. Dès qu'une cible répond dans le mode actif alors la communication est réalisée en Mode Égal à Égal. Si une cible répond en mode passif alors le mobile teste à nouveau le mode actif comme confirmation que la cible ne peut pas traiter le mode actif (pour détecter le cas où la cible a été présentée entre le test du mode actif et le test du mode passif), et ne réalise la communication en mode Terminal que si la confirmation ne détecte pas de cible en mode actif.

3.6.2 INTERFACE 2 : MODULE TRANSPORT / MODULE D'INTERFACE NFC

Ce chapitre traite les échanges entre le module transport et le module d'interface NFC du mobile.

Recommandations techniques et de sécurité		
Recommandation		*Niveau / Objectif*
Utilisation de la SIM GSM.	**Interface *SWP* [22] et protocole *HCI* [23], pour le module transport et pour le module d'interface NFC.**	**Incontournable** **Conformité Ulysse.**
Utilisation d'une carte tierce.	**Interface SWP et protocole HCI, pour le module transport et pour le module d'interface NFC.**	**Optionnel** **Interopérabilité des composants.**
	Interface ISO 7816, pour le module transport et pour le module d'interface NFC.	**Optionnel** **Norme par défaut lorsque SWP n'est pas disponible.**
	Autres types d'interface.	**Optionnel** **Acceptation de mobiles d'architecture quelconque.**
	Interface non disponible.	**Optionnel** **Utilisation d'une carte tierce qui intègre le module d'interface NFC.**

Note : Dans certaines solutions techniques basées sur un module transport porté par une carte tierce, il est possible que cette interface ne soit pas réalisée par une liaison électrique dédiée. Dans ce cas, le module transport est relié au module d'interface NFC via les interfaces 3 et 4, ce qui peut augmenter les temps de transaction.

Note concernant l'utilisation d'une carte tierce avec un mobile intégrant le module d'interface NFC
Actuellement, lorsque le module d'accès NFC est interne au mobile et utilise le standard HCI, tous les échanges NFC en mode Carte sont aiguillés vers la SIM GSM. Dans ce cas, l'utilisation d'une carte tierce requiert la disponibilité de mécanismes spécifiques à chaque mobile. Les détails d'une telle utilisation sortent donc du périmètre du présent document.

Note concernant l'utilisation d'un dispositif NFC externe au mobile
Actuellement, lorsque le module d'accès NFC est externe au mobile (carte sans contact, carte microSD, module Bluetooth, etc.), la mise en œuvre de l'interface NFC est spécifique à chaque produit. Elle peut être basée sur des standards existant, ou non. Les détails d'une telle utilisation sortent donc du périmètre du présent document.

3.6.3 INTERFACE 3 : LOGICIEL DU MOBILE / MODULE D'INTERFACE NFC

Ce chapitre traite les échanges entre le logiciel du mobile (midlet ou autre) et le module d'interface NFC.

Recommandations techniques et de sécurité

Recommandation		*Niveau / Objectif*
Utilisation de la SIM GSM.	**Protocole HCI, pour le logiciel du mobile et pour le module d'interface NFC.**	**Incontournable** **Conformité Ulysse.**
	Bibliothèque *JSR 257* [28] avec « Appendix B (Contactless API) », pour le logiciel du mobile.	**Fortement recommandé** **Choix du titre de transport via un tag NFC.** **Activation de l'IHM du mobile suite à une transaction sans contact.**
Utilisation d'une carte tierce.	**Protocole HCI, pour le logiciel du mobile et pour le module d'interface NFC.**	**Optionnel** **Interopérabilité des composants.**
	Bibliothèque JSR 257 avec « Appendix B (Contactless API) », pour le logiciel du mobile.	**Optionnel** **Choix du titre de transport via un tag NFC.** **Activation de l'IHM du mobile suite à une transaction sans contact.**
	Standard SD/SDIO pour le logiciel du mobile et pour le module d'interface NFC.	**Optionnel** **Support des modules d'accès NFC au format SD, miniSD ou microSD.**
	Standard Bluetooth pour le logiciel du mobile et pour le module d'interface NFC.	**Optionnel** **Support des « stickers » NFC.**
	Spécification *JSR 82* [26] (Bluetooth API), pour le logiciel du mobile.	**Optionnel** **Support des « stickers » NFC.**
	Autres types d'interfaces, éventuellement non standard.	**Optionnel** **Acceptation de mobiles d'architecture quelconque.**

Notes :

- Dans certaines solutions techniques basées sur un module transport porté par une carte tierce, il est possible que cette interface ne soit pas réalisée par une liaison électrique dédiée, par exemple lorsque le module d'interface NFC est intégré à la carte tierce ou à dispositif externe au mobile. Dans ce cas, la liaison entre le logiciel du mobile et le module d'interface NFC peut être impossible (dans ce cas l'interface 3 est indisponible) ou assurée par l'interface entre le mobile et le dispositif externe. Cette interface peut être réalisée par liaison électrique ou sans fil standard (par exemple SD/SDIO ou Bluetooth) ou propriétaire.
- Lorsque cette interface est indisponible, certaines fonctions ne peuvent pas être assurées : Mode Lecteur, Mode Égal à Égal, activation de l'IHM du mobile suite à une transaction sans contact, etc.

Note concernant l'accès du logiciel du mobile à l'interface NFC
Actuellement il n'existe ni standard, ni norme, ni spécification, ni produit permettant au logiciel du mobile d'utiliser l'interface 2 pour communiquer via le canal NFC (interface 1). Certaines fonctions décrites dans el DoFoCo ne sont donc pas disponibles (voir au chapitre 4).

Note concernant l'activation de l'IHM du mobile suite à une validation ou à un contrôle

Comme l'indique le DoFoCo Mobile NFC §7.5.2.4 page 85), l'activation de l'IHM du mobile suite à une transaction sans contact n'est pas possible avec les standards existants.

D'une part, une évolution des spécifications Intercode et / ou Calypso peut être nécessaire pour décrire comment le terminal billettique demande au module transport d'interagir avec le mobile (IHM, conditions de déclenchement, etc.).

D'autre part :

1/ Pour la SIM GSM : une API Java Card standard est nécessaire pour permettre à un cardlet de déclencher une action vers le mobile (envoi de messages HCI, en particulier pour envoyer l'événement EVT_TRANSACTION au mobile). NB : Actuellement, certains fournisseurs de JCRE (OS Java Card) ont défini une API propriétaire.

2/ Pour une carte tierce : la disponibilité de cette fonction est spécifique à chaque solution, et dépend du mobile, du module transport, et de leur interconnexion.

Concernant Intercode et / ou Calypso, le groupe de travail préconise une solution externe à l'application Calypso (donc sans impact sur les spécifications Calypso).

Par exemple, les données de l'application Calypso pourraient simplement indiquer au terminal billettique que le mobile supporte le déclenchement d'actions d'IHM. Ainsi, immédiatement à la suite de la transaction Calypso (avant de libérer la connexion sans contact), le terminal pourrait sélectionner une autre application (non Calypso) du mobile ayant la capacité de déclencher l'IHM (son AID pouvant être lu dans les données de l'application Calypso).

Pour un mobile et un module d'accès NFC capables de gérer plusieurs SE (routage de la commande Select vers le bon SE selon l'AID reçu), on pourrait envisager que le mobile soit intégré à la liste des destinataires potentiels des APDU NFC en allouant des AID à certaines applications du mobile. Le terminal traiterait d'abord l'application billettique, puis l'application d'interface voyageur. Un tel mécanisme assurait les fonctions d'activation de l'IHM du mobile sans contrainte supplémentaire sur l'application billettique et sur le module transport.

3.6.4 INTERFACE 4 : MODULE TRANSPORT / LOGICIEL DU MOBILE

Ce chapitre traite les échanges entre le module transport et le logiciel du mobile.

Recommandations techniques et de sécurité

Recommandation			*Niveau / Objectif*
Utilisation de la SIM GSM.	**Bibliothèque *JSR 177* [27], comprenant le module SATSA-APDU.**		**Incontournable** **Envoi de commandes à la SIM GSM par le logiciel du mobile.**
	Support de BIP (avec commandes proactives définies par Ulysse [13]).		**Incontournable** **Envoi de commandes au SSD de la SIM GSM en mode OTA (cf. interface 7, §3.6.7).**
	GlobalPlatform v2.2 et Amendments A & C [24].		**Incontournable** **Gestion des cardlets de la SIM GSM ; conformité Ulysse ; conformité Calypso Specification - Application Downloading.**
	Autres types d'interfaces, éventuellement non standard.		**Optionnel** **Envoi de commandes ISO7816-4 en mode OTA à l'application billettique de la SIM GSM.**
Utilisation d'une carte tierce.	**Bibliothèque JSR 177, comprenant le module SATSA-APDU.**		**Optionnel** **Interopérabilité des composants.**
	Standard SD/SDIO pour le logiciel du mobile et pour le module transport.		**Optionnel** **Support des modules transport au format SD, miniSD ou microSD.**
	Standard Bluetooth pour le logiciel du mobile et pour le module transport.		**Optionnel** **Support des « stickers » NFC contenant le module transport.**
	Spécification JSR 82 (Bluetooth API), pour le logiciel du mobile.		**Optionnel** **Support des « stickers » NFC contenant le module transport.**
	Autres types d'interfaces, éventuellement non standard.		**Optionnel** **Acceptation de mobiles d'architecture quelconque.**
	Java Card	**GlobalPlatform v2.2 avec son Amendment A.**	**Fortement recommandé** **Gestion des cardlets d'une Java Card tierce ; conformité Calypso Specification - Application Downloading.**
		GlobalPlatform v2.1.1.	**Optionnel** **Gestion des cardlets d'une Java Card tierce ; conformité Calypso Specification - Application Downloading.**

[13] Chapitre 9.3.1, pages 57-58.

Notes :

- Il n'existe pour l'instant pas de standard décrivant la possibilité pour le navigateur d'un mobile d'accéder à une carte à puce du mobile. Néanmoins, on peut signaler que le projet BONDI (de « Open Mobile Terminal Platform », association de fabricants de mobiles) vise à fournir en 2010 une librairie javascript extension de WebKit [14] spécifique aux navigateurs de mobiles, et disposant d'une interface d'accès SIM. Des versions de BONDI sont disponibles en téléchargement, pour Android entre autres.
- Certains produits Java Card disposent d'un serveur http au standard *SCWS* ([29]) qui permet au navigateur web du mobile d'accéder directement à la carte. Cette possibilité n'est pas prise en compte dans cette version du document.
- Dans certaines solutions techniques, la carte tierce est contenue dans un dispositif externe. Dans ce cas, l'interface entre le logiciel du mobile et le module transport est portée par l'interface entre le mobile et le dispositif externe, qui peut être réalisée par liaison électrique ou sans fil standard (par exemple SD/SDIO [15] ou Bluetooth) ou propriétaire.
- Le cas d'une Java Card où la communication entre l'application billettique et l'extérieur de la carte se fait par l'intermédiaire d'un autre cardlet de la carte n'est pas pris en compte dans cette version du document car aucun standard ne le décrit. Néanmoins, on peut signaler que dans ce type d'interface l'application billettique est sélectionnée par le cardlet d'interface et échange avec lui des commandes (au format ISO7816-4) en interne, le cardlet d'interface de son côté échangeant des commandes avec l'extérieur selon un autre protocole (par exemple SIMToolkit, DGI GlobalPlatform, BIP, SCWS, etc.). Cette méthode est donc une des solutions possibles pour les échanges OTA de commandes ISO 7816-4 (actuellement non disponibles, voir chapitre 3.6.7).
- Pour la SIM GSM seul l'Amendment A de GlobalPlatform v2.2 peut être utilisé. Pour une Java Card tierce, le processus de chargement d'une application Calypso est également possible avec GlobalPlatform v2.1.1, mais il est alors plus complexe.

[14] Bibliothèque de fonctions permettant d'intégrer facilement un moteur de rendu de pages Web dans un logiciel, disponible sous licences libres BSD et GNU LGPL.

[15] Le protocole SDIO n'étant pas toujours disponible, le dialogue entre le mobile et la carte SD peut être réalisé par lecture/écriture dans des zones mémoires non utilisées (mode « Mass Storage »).

3.6.5 INTERFACE 5 : DISPOSITIFS D'INTERFACE HOMME MACHINE (IHM)

L'accès aux dispositifs d'interface homme machine dépend de l'environnement logiciel fourni par le système d'exploitation du mobile, et des capacités d'affichage et de saisie. Afin de faciliter la portabilité de l'application d'interface voyageur d'un modèle de mobile à l'autre, seuls les dispositifs les plus usuels ou qui font l'objet d'interfaces standardisées sont recommandés.

Recommandations techniques et de sécurité

Recommandation		*Niveau / Objectif*
Utilisation de la SIM GSM.	**Environnement logiciel Java Micro Edition (Java ME [16]).**	**Fortement recommandé** **Interopérabilité des composants, conformité Ulysse.**
	Bibliothèque JSR 118 (affichage graphique).	**Fortement recommandé** **Interopérabilité des composants, conformité Ulysse.**
Utilisation d'une carte tierce.	**Environnement logiciel Java Micro Edition (Java ME [16]).**	**Fortement recommandé** **Interopérabilité des composants.**
	Bibliothèque JSR 118 (affichage graphique).	**Fortement recommandé** **Interopérabilité des composants.**
Autres types d'environnements logiciels ou d'interfaces, éventuellement non standard.		**Optionnel** **Acceptation de mobiles d'architecture quelconque.**
Stockage de la photo dans la mémoire du mobile.		**Déconseillé** **Limitation de la mémoire utilisée dans le module transport.** **Utilisation de modules transport qui ne permettent pas le stockage de la photo.** **Risque de suppression de la photo.**

Notes :

- Le stockage de la photo dans la mémoire du mobile est décrite dans le DoFoCo Mobile NFC (§7.5.2.5, page 85). Mais il serait assez facile de modifier la photographie affichée par le mobile. Le stockage de la photo dans la mémoire du mobile est donc déconseillé.
- Le contrôle du titre sur l'écran du mobile est décrit dans le DoFoCo Mobile NFC (§7.5.2.5, page 85). Mais il serait assez facile de modifier le titre affiché par le mobile. Par conséquent il est recommandé aux gestionnaires transport qui autorisent le contrôle du titre sur l'écran du mobile (lorsque l'interface NFC est indisponible) :
  - de mette en place un système de surveillance de la fréquence de ces contrôles pour un mobile donné ;
  - de prévoir la possibilité de l'arrêt de ce mode de contrôle en cas de fraude trop fréquente.

[16] « Java Micro Edition », également appelé « J2ME » et « JME ».

Note concernant l'affichage de la photo sur le mobile

L'affichage de la photo sur le mobile est déconseillé. Il présente des problèmes de sécurité, et le contrôle de l'identité du voyageur n'étant pas spécifique à la billettique sur mobile NFC, il devrait être traité par une méthode générale (qui s'applique à tout type de support anonyme).

Le groupe de travail recommande le stockage de la photo dans l'application billettique, et son affichage sur le terminal de contrôle, qui est compatible avec tous les types de support de titre.

3.6.6 INTERFACE 6 : MOBILE / SI NON TELECOM

Ce chapitre traite les échanges entre le mobile (système d'exploitation ou logiciel) et les systèmes d'information non gérés par l'opérateur télécom ou le propriétaire/gestionnaire de la SIM GSM, via un canal de type http ou https (hors WAP).

Recommandations techniques et de sécurité		
Recommandation		*Niveau / Objectif*
Toutes interfaces 6	**Protocoles http et https.**	**Incontournable** **Échange (éventuellement sécurisé) de données quelconques entre un client (le mobile) et un serveur (un SI).**
Interface 6-A : mobile / serveur d'applications d'interface voyageur du SI transport.	**Mécanisme non standard de téléchargement d'application de mobile [17].**	**Optionnel** **Acceptation de systèmes non standard.**
Interface 6-B : Logiciel du mobile / SI transport (serveur de rechargement, personnalisation).	**Capacité à traiter et à transporter des fichiers XML tels que décrits par la spécification Calypso Specifications - Product Remote Loading [18].**	**Fortement recommandé** **Indépendance vis-à-vis du canal de communication.**
	Protocole propriétaire pour le transport des APDU entre le SI transport et le mobile.	**Optionnel** **Acceptation de systèmes non standard.**
	Protection des échanges par utilisation de méthodes non standard.	**Optionnel** **Acceptation de systèmes non standard.**
Interface 6-C : Logiciel du mobile / gestionnaire Java Card tierce.	**Protocole Calypso Specification - Application Downloading (téléchargement de cardlet Calypso).**	**Incontournable** **Utilisation d'un cardlet Calypso.**
Interface 6-D : Logiciel du mobile / gestionnaire SSD transport Java Card tierce.	**Protocole Calypso Specification - Application Downloading (téléchargement de cardlet Calypso).**	**Incontournable** **Utilisation d'un cardlet Calypso.**

[17] Un tel mécanisme est porté par http(s), qui est incontournable.

[18] Ce standard Calypso permet d'échanger des APDU avec tous types de modules transport, Calypso ou non.

Interface 6-E : Mobile / fournisseur d'application mobile.	**Protocole non standard de téléchargement d'application de mobile [17].**	**Optionnel** **Acceptation de systèmes non standard.**

Notes :

- Les interfaces 6-C à 6-E ne sont pas mises en œuvre dans le cas de l'utilisation de la SIM GSM.
- À l'heure actuelle, il n'existe aucun standard relatif au téléchargement d'applications de mobile (interfaces 6-A et 6-E).
- Dans le cas de l'utilisation d'une carte tierce, le mode push (interfaces 6-C, 6-D et 6-E) nécessite la présence dans le mobile d'un processus assurant la connexion permanente (ou périodique [19]) entre le module transport et le SI concerné. S'il est disponible, ce processus est mis en place par l'application d'interface voyageur du mobile. À l'heure actuelle, il n'existe aucun standard pour de tels processus, en particulier pour la méthode d'identification du module transport par les SI concernés (assignation d'un identifiant, diffusion, etc.). Pour certains mobiles cette fonction ne peut pas être mise en œuvre (par exemple, seul le fournisseur du système d'exploitation peut activer et utiliser des processus en tâche de fond).
- Les transmissions entre le mobile et le SI transport étant facturées au voyageur par l'opérateur mobile, le système mis en œuvre doit limiter ces transmissions autant que possible, et elles doivent être autorisées par le voyageur.

[19] La période de connexion doit être compatible avec les exigences de délai de chargement du DoFoCo, tout en préservant l'autonomie du mobile.

3.6.7 INTERFACE 7 : OTA VIA L'OPERATEUR TELECOM

Ce chapitre traite tous les échanges OTA réalisés avec (ou via) le système d'information du gestionnaire télécom (y compris le canal WAP). Il ne concerne que le cas de l'utilisation de la SIM GSM.

Recommandations techniques et de sécurité		
Recommandation		*Niveau / Objectif*
Protocole BIP, tel que spécifiée par Ulysse et amendé par Calypso Specification - Application Downloading.		**Incontournable** **Conformité Ulysse, et personnalisation de cardlet.**
Protocoles SMS et WAP, tels que spécifiés par Ulysse.		**Incontournable** **Conformité Ulysse.**
« Interface [1] » telle que spécifiée par Ulysse.		**Incontournable** **Conformité Ulysse.**
Interface 7-D : **Mobile / gestionnaire module transport SIM GSM (serveur midlet).**	**Protocoles http et https.**	**Incontournable** **Échange (éventuellement sécurisé) de données quelconques entre un client (le mobile) et un serveur (serveur midlet).**

Notes :

- Le protocole BIP est complété par *Calypso Specification – Application Downloading* car contrairement à ce qui est indiqué dans les spécifications Ulysse, les standards actuels ne définissent pas de méthode pour échanger OTA [20] des commandes ISO7816-4 arbitraires avec une application Java Card standard d'une SIM GSM (cf. Calypso Specifications - Product Remote Loading, §5.3.2.2, p. 37). Pour la phase de personnalisation d'un cardlet, la méthode recommandée est celle décrite par Calypso (également utilisable pour d'autres types d'applications). Pour la réalisation OTA de transactions billettiques (par exemple un chargement de profil ou de contrat) avec une SIM GSM (interface 7-A), actuellement (et à court terme) aucune solution technique n'est disponible.
- Les transmissions OTA étant facturées au voyageur par l'opérateur mobile, le système mis en œuvre doit limiter ces transmissions autant que possible, et elles doivent être autorisées par le voyageur.

[20] Il s'agit ici uniquement du cas OTA via l'opérateur télécom. En configuration SIM GSM, il reste en effet possible via la JSR177 (SATSA-APDU) et le lien http(s) du mobile de faire transiter des APDU ISO7816-4 entre la SIM GSM et un serveur distant.

3.6.8 INTERFACE 8 : GESTIONNAIRE JAVA CARD / GESTIONNAIRE SSD TRANSPORT

Ce chapitre ne s'applique que pour les cas où le module transport est conforme aux spécifications *GlobalPlatform* [24] et Java Card. Il traite les échanges entre le système d'information du gestionnaire du domaine de sécurité GlobalPlatform du cardlet et ce même domaine dans la carte.

Recommandations techniques et de sécurité

Recommandation		*Niveau / Objectif*
Utilisation de la SIM GSM.	**« Interface [1] » telle que spécifiée par Ulysse.**	**Incontournable** **Conformité Ulysse.**
Utilisation d'une Java Card tierce.	**Mécanismes standards ou non pour la gestion du cardlet via le gestionnaire Java Card tierce.**	**Optionnel** **Acceptation de systèmes existant.**

3.6.9 INTERFACE 9 : GESTIONNAIRE SSD / SERVEURS INTERNES

Ce chapitre traite les échanges internes aux systèmes d'information.

Recommandations techniques et de sécurité

Recommandation		*Niveau / Objectif*
Protocole Calypso Specification - Application Downloading (téléchargement de cardlet Calypso).		**Fortement recommandé** **Indépendance vis-à-vis du canal de communication.**

3.6.10 INTERFACE 10 : SI TRANSPORT / SI GESTIONNAIRE DE MODULES TRANSPORT

Ce chapitre traite les échanges entre le système d'information du domaine transport et les systèmes d'information de gestion du SSD transport des Java Cards.

Recommandations techniques et de sécurité

Recommandation		*Niveau / Objectif*
Interface 10-A : **SI transport / propriétaire/distributeur application SIM GSM.**	**Hors périmètre.**	-
Interface 10-B : **SI transport / propriétaire/distributeur application Java Card tierce.**	**Hors périmètre.**	-
Interface 10-C : **SI transport (serveur de rechargement) / gestionnaire SSD SIM GSM).**	**Capacité à transporter des fichiers XML tels que décrits par la spécification Calypso Specifications - Product Remote Loading [18].**	**Fortement recommandé** **Indépendance vis-à-vis du canal de communication.**

3.6.11 INTERFACE 11 : SI TRANSPORT / GESTIONNAIRE JAVA CARD

Ce chapitre traite les échanges entre le système d'information du domaine transport et le système d'information du gestionnaire de la SIM GSM ou d'une Java Card tierce.

Recommandations techniques et de sécurité		
Recommandation		*Niveau / Objectif*
11-A : SI transport (base de données supports, clients) / gestionnaire SIM GSM	**Mécanismes de gestion de l'identifiant ID_TECH (« Interface [2] »), tel que spécifiés par Ulysse.**	**Incontournable** **Conformité Ulysse.**
11-B : SI transport (base de données supports, clients) / gestionnaire Java Card tierce	**Mécanismes non standard d'identification commune du module transport entre le SI transport et le gestionnaire Java Card tierce (identifiant technique).**	**Optionnel** **Acceptation de systèmes existant.**

Note : Il n'existe actuellement aucun mécanisme standard d'identification commune du module transport entre le SI transport et le gestionnaire Java Card tierce (identifiant technique).

3.6.12 INTERFACE 12 : TERMINAL BILLETTIQUE / SI TRANSPORT (SERVEUR DE RECHARGEMENT, PERSONNALISATION)

Ce chapitre traite les échanges entre le système d'information du domaine transport et un terminal billettique.

Recommandations techniques et de sécurité		
Recommandation		*Niveau / Objectif*
Protocole de rechargement distant.	**Spécification Calypso Specifications – Product Remote Loading [18].**	**Fortement recommandé** **Indépendance vis-à-vis du canal de communication.**
	Autres protocoles.	**Optionnel** **Acceptation de systèmes existant.**
Protection des échanges par utilisation de méthodes standard de type SSL.		**Fortement recommandé** **Confidentialité des échanges.**

3.6.13 PAIEMENT

Aucune interface spécifique à la billettique sur mobile NFC n'étant mise en œuvre pour le paiement, il n'entre pas dans le périmètre de ce document.

Les cas envisagés pour le paiement d'un titre de transport sont néanmoins indiqués au chapitre 4.4.2.2.

4 MISE EN ŒUVRE

Pour chaque fonction liée à la mise en œuvre et au fonctionnement de la billettique sur mobile NFC, telles que définies dans le DoFoCo Mobile NFC, ce chapitre décrit des exemples de cas d'utilisation qui illustrent les actions à effectuer et les interfaces utilisées.

Tableau synthétique fonctions/interfaces :

Fonction	Cas d'utilisation					Interfaces											
						1	2	3	4	5	6	7	8	9	10	11	12
Accès au service	*(Non spécifique à la billettique sur mobile NFC)*																
Chargement de l'application transport	Requête de chargement	Depuis un mobile NFC															12
		Depuis Internet															12
		Via un tag NFC	Url			1B		3		5							12
			N° court SMS	Url		1B		3		5							12
				Application du mobile		1B		3		5							12
			Application du mobile			1B		3		5							12
		Via un numéro SMS	Url														12
			Application du mobile														12
		Depuis les équipements transport															12
	Chargement de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull							6E						
				Mode push *(non disponible)*													
			Via l'opérateur télécom	Mode pull								7D					
				Mode push								7D 7E	8A				
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)						4B	5	6B 6C 6D		8B	9C 9D	10 B	11 B	
			Via l'opérateur télécom (SIM GSM)									7C 7B	8A		10 A 10 B	11 A	
		Depuis les équipements transport *(non disponible)*															
Personnalisation	Attribution de profil *(non spécifique à la billettique sur mobile NFC)*																
	Signalement d'événement *(non spécifique à la billettique sur mobile NFC)*																
	Mise à jour	Depuis les équipements transport				1A	2										
		Mode pull : via l'application d'interface voyageur							4	5	6B						
		Mode push	Via l'opérateur télécom *(non disponible)*														
			Via l'application d'interface voyageur						4		6B						
Distribution de titres	Sélection	Depuis le mobile	Sans connexion						4	5							
			Avec connexion						4	5	6B						
		Depuis Internet	Identification manuelle														12
			Identification OTA mode pull						4	5	6B						12
			Identification OTA mode push	Via l'opérateur télécom *(non disponible)*													
				Via l'application d'interface voyageur					4		6B						12
		Depuis les équipements transport				1A	2										
		Depuis un tag	Url			1B		3		5							12

		NFC	N° court SMS	Url	1B		3		5						12											
				Application du mobile	1B		3	4	5	6B																
			Application du mobile		1B		3	4	5	6B																
		Par saisie de n° court SMS	Url												12											
			Application du mobile					4	5	6B																
	Paiement *(non spécifique à la billettique sur mobile NFC)*																									
	Chargement	OTA mode pull						4	5	6B																
		OTA mode push	Via l'opérateur télécom *(non disponible)*																							
			Via l'application d'interface voyageur					4		6B																
		Depuis les équipements transport			1A	2																				
	Transfert de titres	Vers/depuis un support sans contact, en Mode Lecteur			1B		3	4	5																	
		Vers un autre mobile, en Mode Égal à Égal			1C		3	4	5	6B																
	Interface de vente	Avec un support sans contact, en Mode Lecteur			1B		3		5	6B																
		Avec un autre mobile, en Mode Égal à Égal			1C		3		5	6B																
Validation et contrôle	Validation simple				1A	2																				
	Conflit à la validation	Sélection préalable	Sur le terminal de validation		1A	2																				
			Sur le mobile		1A	2		4	5	6B																
		Sélection sur mobile après une validation			1A	2	3	4	5	6B																
	Validation multi-voyageurs, titre unique	Validation unique simple			1A	2																				
		Sélection préalable sur mobile			1A	2		4	5	6B																
		Sélection sur terminal après une validation			1A	2	3	4	5	6B																
		Validations multiples	Simples		1A	2																				
			Avec confirmation sur le mobile		1A	2	3	4	5	6B																
	Validation multi-voyageurs, titres multiples : voir gestion des données																									
	Contrôle	Simple			1A	2																				
		Avec affichage de la photo	Sur le terminal de contrôle		1A	2																				
			Sur le mobile		1A	2	3	4	5																	
		Avec NFC défectueux						4	5																	
Gestion des données par le voyageur	Consultation sur le mobile							4	5																	
	Pré-sélection de données avant validation	OTA						4	5	6B																
		Depuis les équipements transport			1A	2																				
	Pré-sélection d'application (*non disponible*)																									
	Sauvegarde, restauration ou suppression des données billettiques	OTA	Via l'application d'interface voyageur					4	5	6B																
			Via l'opérateur télécom *(non disponible)*																							
		Depuis les équipements transport			1A	2									12											
	Suppression de l'application transport	OTA , Carte tierce						4B 4C	5	6B 6C 6D		8B		10 B	11 B											
		OTA , SIM GSM	Via l'application d'interface voyageur					4A	5	6B	7B 7C	8A		10 A	11 A											
			Via l'opérateur télécom *(non disponible)*																							
		Depuis les équipements transport *(non disponible)*																								
	Restauration de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull					6E																	
				Mode push *(non disponible)*																						
			Via	Mode pull						7D																

			l'opérateur télécom	Mode push								7D 7E	8A										
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)								4B	5	6B 6C 6D		8B	9C 9D	10 B	11 B					
			Via l'opérateur télécom (SIM GSM)											7C 7B	8A		10 A 10 B	11 A					
		Depuis les équipements transport *(non disponible)*																					
Service après-vente	Diagnostic ou sauvegarde	OTA	Via l'application d'interface voyageur								4	5	6B										
			Via l'opérateur télécom *(non disponible)*																				
		Depuis les équipements transport			1A	2																	12
	Reconstitution de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull									6E										
				Mode push *(non disponible)*																			
			Via l'opérateur télécom	Mode pull										7D									
				Mode push										7D 7E	8A								
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)								4B	5	6B 6C 6D		8B	9C 9D	10 B	11 B					
			Via l'opérateur télécom (SIM GSM)											7C 7B	8A		10 A 10 B	11 A					
		Depuis les équipements transport *(non disponible)*																					
	Reconstitution des données de l'application billettique	OTA	Via l'application d'interface voyageur								4	5	6B										
			Via l'opérateur télécom *(non disponible)*																				
		Depuis les équipements transport			1A	2																	12
	Blocage du module transport (*non défini*)																						

4.1 FONCTION - ACCES AU SERVICE

L'accès au service, tel que décrit dans le DoFoCo Mobile NFC, ne met en œuvre aucune interface technique qui soit dans le périmètre de ce document.

4.2 FONCTION - CHARGEMENT DE L'APPLICATION TRANSPORT

4.2.1 CAS D'UTILISATION

L'*application transport* est constituée de deux parties, possédant chacune leur propre cycle de vie :

- l'*application billettique* : logiciel chargé dans le module transport (cardlet dans le cas d'une Java Card) ;
- l'*application d'interface voyageur* : logiciel chargé dans le mobile (midlet dans le cas d'un mobile Java ME).

Les cas d'utilisation du chargement de l'application recouvrent les fonctionnalités suivantes :

- assistance au chargement de l'application transport ;
- requête de chargement de l'application transport :
  - à distance (via le mobile, via Internet, à partir d'un tag NFC ou à partir d'un numéro SMS) ;
  - depuis un équipement du bassin de transport ;

- identifiant transport ;
- chargement de l'application d'interface voyageur :
    - à distance (via le mobile, via Internet, à partir d'un tag NFC ou à partir d'un numéro SMS) ;

Note concernant le chargement de l'application d'interface voyageur OTA, mode push
À notre connaissance, les OS des mobiles existant ne permettent pas de charger une application d'interface voyageur en mode push (sans aucune interaction avec l'utilisateur du mobile) sans passer par l'opérateur télécom. Par conséquent, ce chargement n'est pas considéré dans ce chapitre.

    - par pré-personnalisation en volume (hors périmètre, car ne met en œuvre aucune interface spécifique à la billettique sur mobile NFC) ;

- chargement de l'application billettique :
    - à distance (via le mobile, via Internet, à partir d'un tag NFC ou à partir d'un numéro SMS) ;

Note concernant le chargement de l'application billettique en mode push, cas d'une carte tierce
Le chargement de l'application billettique en mode push dans le cas d'une carte tierce n'est pas traité car une interaction avec le voyageur et la connexion avec le SI transport sont toujours nécessaires. La connexion avec le SI transport est alors disponible pour réaliser également les échanges d'APDU avec le module transport (et pour déclencher les traitements nécessaires avec le gestionnaire de SSD transport et le propriétaire/distributeur d'application Java Card tierce).

    - par pré-personnalisation en volume (hors périmètre, car ne met en œuvre aucune interface spécifique à la billettique sur mobile NFC).

Note concernant le chargement de l'application transport via un terminal du bassin de transport
Actuellement le logiciel du mobile ne peut pas communiquer via le canal NFC (cf. note au chapitre 3.6.3). Le chargement de l'application d'interface voyageur via un terminal du bassin de transport décrit dans le DoFoCo (§7.2.2.4, page 59) n'est donc pas disponible à court terme. Par conséquent, le chargement de l'application transport par l'interface NFC n'est pas considéré dans ce chapitre. Lorsque cette limitation sera levée : • Dans le cas de la SIM GSM le chargement de l'application billettique via l'interface NFC ne sera toujours pas possible, un cardlet pouvant être chargé dans la SIM uniquement en usine ou OTA via l'opérateur télécom. • Pour le chargement de l'application billettique d'une carte tierce, et pour le chargement de l'application d'interface voyageur, ou pourra par exemple envisager que l'équipement du bassin de transport et le SI transport se comportent comme de simples passerelles vers les distributeurs de l'application d'interface voyageur et de l'application billettique (pour les mobiles NFC et les modules transport qui le permettront).

La compatibilité des deux parties de l'application transport avec le mobile et avec le module transport est supposée avoir été vérifiée en amont.

Lorsqu'aucune des deux parties d'une application transport n'est déjà présente dans le mobile, elles sont si possible chargées simultanément et de manière transparente pour le voyageur.

Pour le cas d'une carte tierce amovible, le chargement de l'application transport peut être réalisé avant distribution au voyageur, selon des procédures proches de celles des cartes sans contact. Cette fonction est hors du périmètre du présent document.

Note concernant le chargement de l'application d'interface voyageur via un module transport amovible
Actuellement il n'existe ni standard ni norme relatif à l'installation automatique d'une application dans un mobile depuis un support amovible. La méthode utilisée (lorsqu'elle est disponible) pour installer automatiquement une application d'interface voyageur depuis un support amovible dépend donc du mobile et du support amovible utilisés.

Notes concernant le chargement de l'application billettique
Lorsqu'une application billettique doit être chargée dans une Java Card, l'ergonomie serait améliorée si l'application d'interface voyageur pouvait énumérer les Java Card disponibles et éligibles, et proposer à l'utilisateur de choisir laquelle utiliser. Actuellement cette énumération n'est pas disponible (voir la note concernant la pré-sélection d'application, au chapitre 4.6.1).

4.2.2 DESCRIPTION DES ECHANGES

4.2.2.1 ASSISTANCE AU CHARGEMENT DE L'APPLICATION TRANSPORT

L'assistance au chargement de l'application transport est hors du périmètre de ce document car elle ne met en œuvre aucun mécanisme spécifique à la billettique sur mobile NFC.

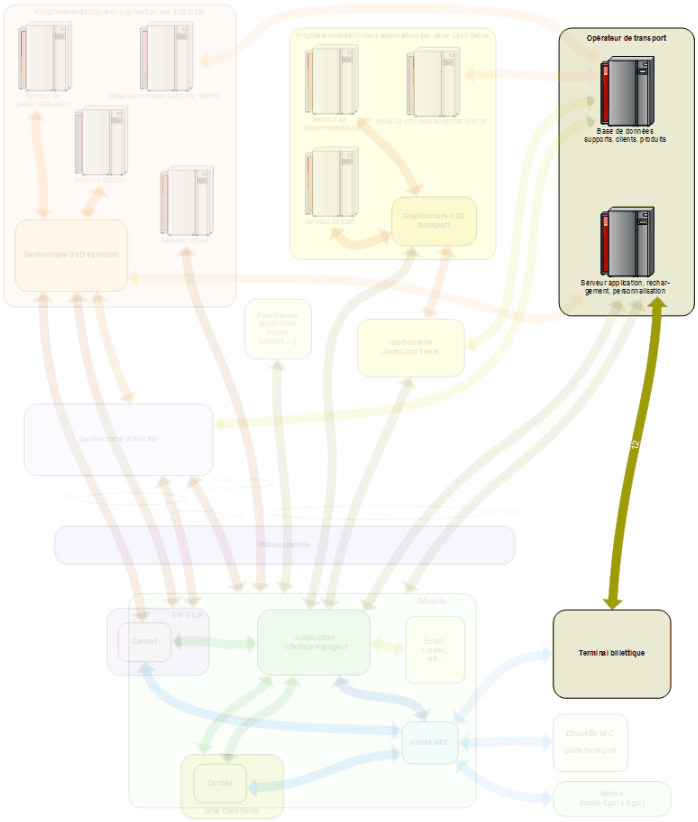
4.2.2.2 REQUETE DE CHARGEMENT

Les différents canaux envisagés pour une requête de chargement de l'application transport sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mises en œuvre.

Seuls les scénarios où ni l'application billettique ni l'application d'interface voyageur ne sont présentes sont décrits, les scénarios intermédiaires ne mettant en œuvre aucune interface supplémentaire.

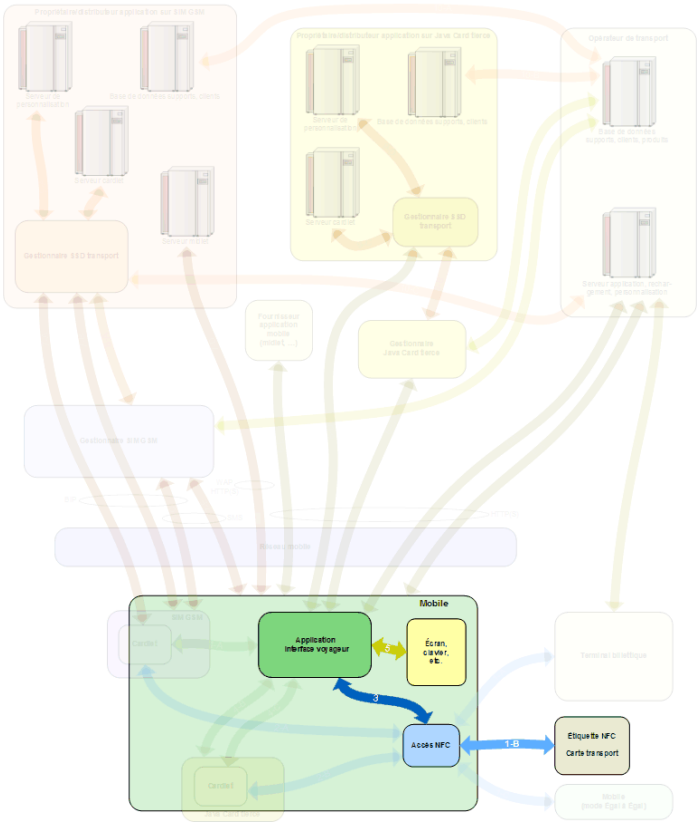
Requête de chargement	Action	Interfaces
Depuis un mobile NFC	Le mobile est utilisé comme un terminal Internet.	Cf. requête de chargement depuis Internet (ci-dessous)

Requête de chargement	Action	Interfaces
Depuis Internet	Connexion au site Internet de vente des titres du bassin de transport, et demande de chargement de l'application billettique. Le voyageur indique son numéro de mobile, qui ne sera conservé par le SI transport qu'avec son accord.	12 : Terminal billettique / SI transport



Note : Dans ce cas d'usage le terminal billettique est un terminal Internet.

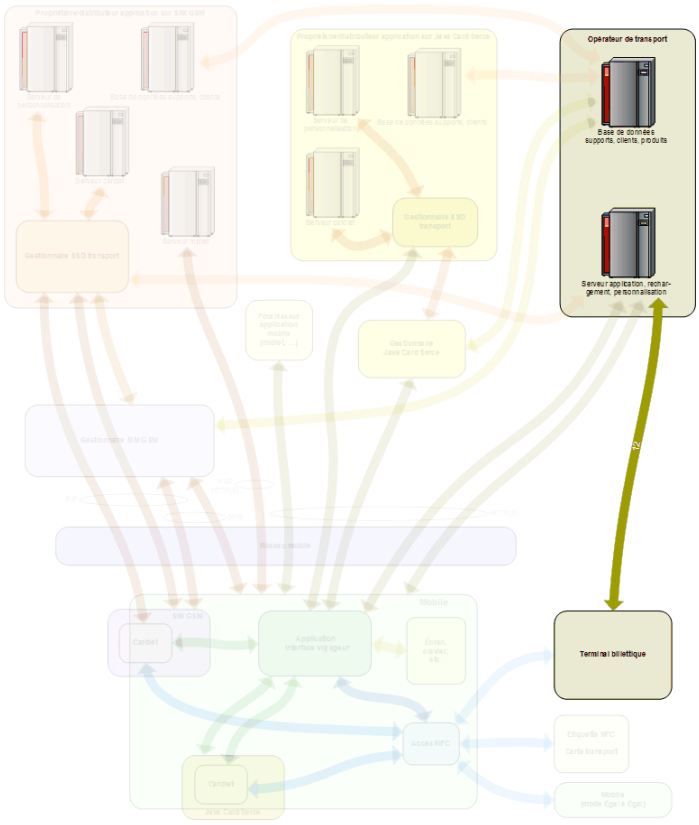
Requête de chargement	Action	Interfaces
Via un tag NFC	Lecture du tag NFC et activation de l'IHM du mobile (fonctions intrinsèques de son OS.	1-B : NFC externe, Mode Lecteur 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile
	Option : Affichage d'une URL, validation de cette URL par le voyageur, lancement du navigateur web du mobile.	Cf. requête de chargement depuis Internet
	Option : Affichage d'un numéro, validation par le voyageur de l'envoi d'un SMS à ce numéro.	Cf. requête de chargement via un numéro SMS
	Option : Affichage d'une invite à lancer une application, validation de cette invite par le voyageur.	Cf. requête de chargement depuis le mobile NFC



Note : Dans ce diagramme l'application mise en œuvre dans le mobile n'est pas l'application d'interface voyageur mais une fonction intrinsèque de l'OS du mobile.

Requête de chargement	Action	Interfaces
Via un numéro SMS	Envoi par le voyageur d'un SMS au numéro indiqué par l'opérateur de transport.	-
	Option : Réception et affichage d'un SMS contenant une URL, validation de cette URL par le voyageur.	Cf. requête de chargement depuis Internet
	Option : Réception et affichage d'un SMS contenant une invite à lancer une application, validation de cette invite par le voyageur.	Cf. requête de chargement depuis le mobile NFC

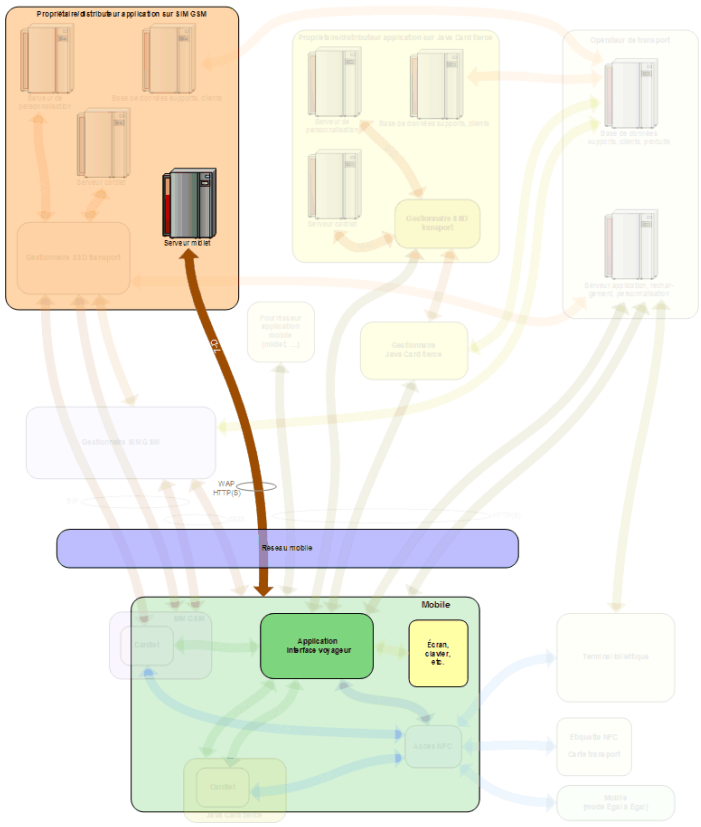
Requête de chargement	Action	Interfaces
Depuis les équipements d'un bassin de transport	Utilisation de l'IHM du terminal billettique pour demande de chargement de l'application billettique. Le voyageur indique son numéro de mobile, qui ne sera conservé par le SI transport qu'avec son accord.	12 : Terminal billettique / SI transport



4.2.2.3 CHARGEMENT DE L'APPLICATION D'INTERFACE VOYAGEUR

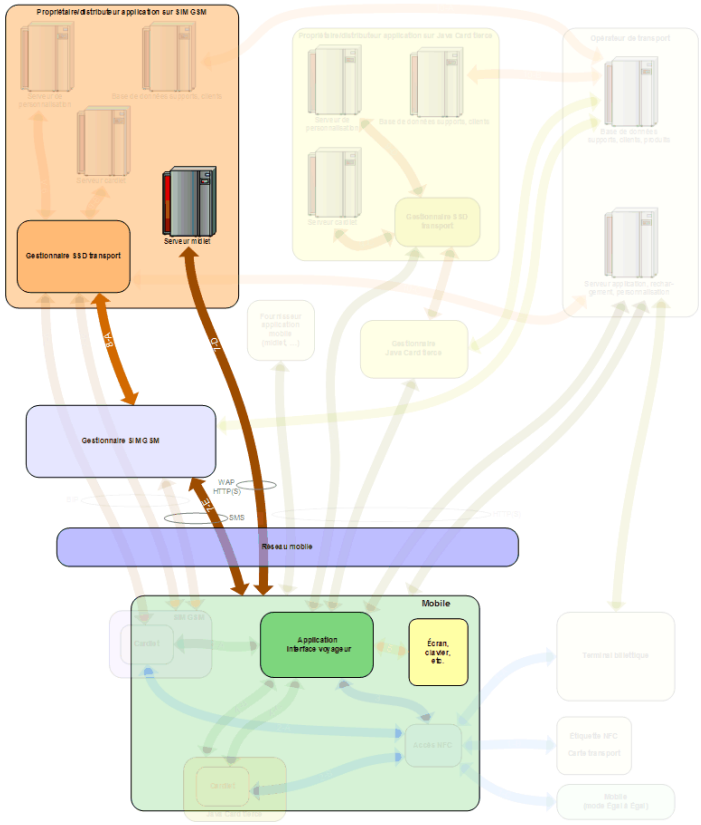
Les différents canaux envisagés pour le chargement de l'application d'interface voyageur sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Chargement de l'application d'interface voyageur	Action	Interfaces
OTA via l'opérateur télécom, mode pull	L'application billettique doit être déjà chargée (cf. Spécifications Générales Ulysse, §9.7.4).	-
	En utilisant les fonctionnalités intrinsèques de son mobile, le voyageur se connecte au serveur midlet du gestionnaire module transport SIM GSM et télécharge l'application d'interface voyageur qui correspond au réseau d'interopérabilité et à l'opérateur souhaités.	7-D : Mobile / gestionnaire module transport SIM GSM (serveur midlet)



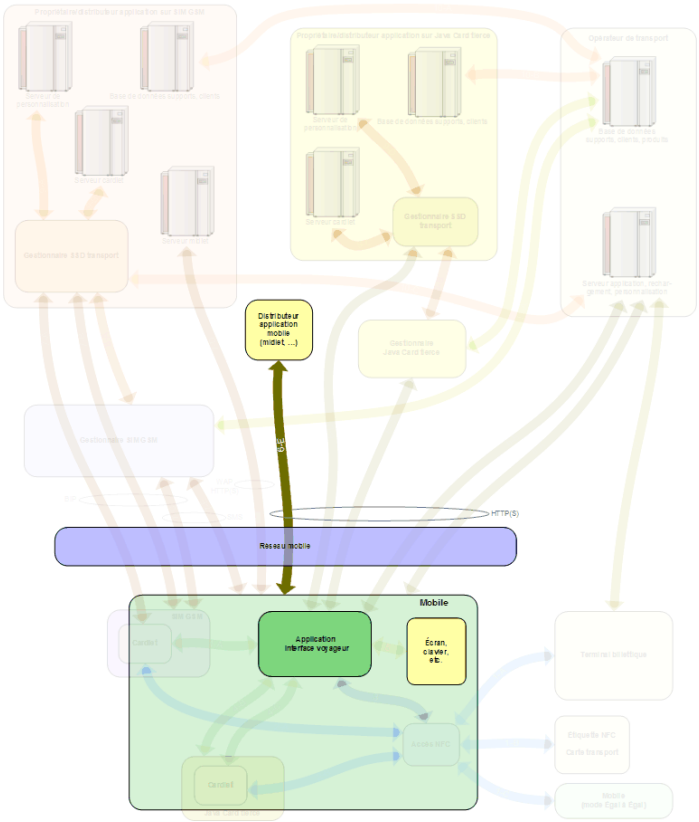
Note : Dans ce diagramme l'application mise en œuvre dans le mobile n'est pas l'application d'interface voyageur mais une fonction intrinsèque de l'OS du mobile.

Chargement de l'application d'interface voyageur	Action	Interfaces
OTA via l'opérateur télécom, mode push	L'application billettique doit être déjà chargée (cf. Spécifications Générales Ulysse, §9.7.4).	-
	Le gestionnaire module transport SIM GSM envoie au mobile une demande de connexion en mode données (« SMS push WAP »), via le gestionnaire de SIM GSM.	7-E : Mobile / gestionnaire SIM GSM 8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM
	En utilisant les fonctionnalités intrinsèques de son mobile, le voyageur se connecte au serveur midlet du gestionnaire module transport SIM GSM et télécharge l'application d'interface voyageur qui correspond au réseau d'interopérabilité et à l'opérateur souhaités.	7-D : Mobile / gestionnaire module transport SIM GSM (serveur midlet)



Note : Dans ce diagramme l'application mise en œuvre dans le mobile n'est pas l'application d'interface voyageur mais une fonction intrinsèque de l'OS du mobile.

Chargement de l'application d'interface voyageur	Action	Interfaces
OTA via l'OS du mobile (mode pull)	En utilisant les fonctionnalités intrinsèques de l'OS du mobile, le voyageur se connecte au SI du fournisseur d'application mobile et télécharge l'application d'interface voyageur qui correspond au bassin de transport et à l'opérateur souhaités.	6-E : Mobile / fournisseur d'application mobile



Notes :

- Selon les capacités de l'OS du mobile, l'application d'interface voyageur peut également être chargée par connexion du mobile à un ordinateur personnel.
- Dans ce diagramme l'application mise en œuvre dans le mobile n'est pas l'application d'interface voyageur mais une fonction intrinsèque de l'OS du mobile.

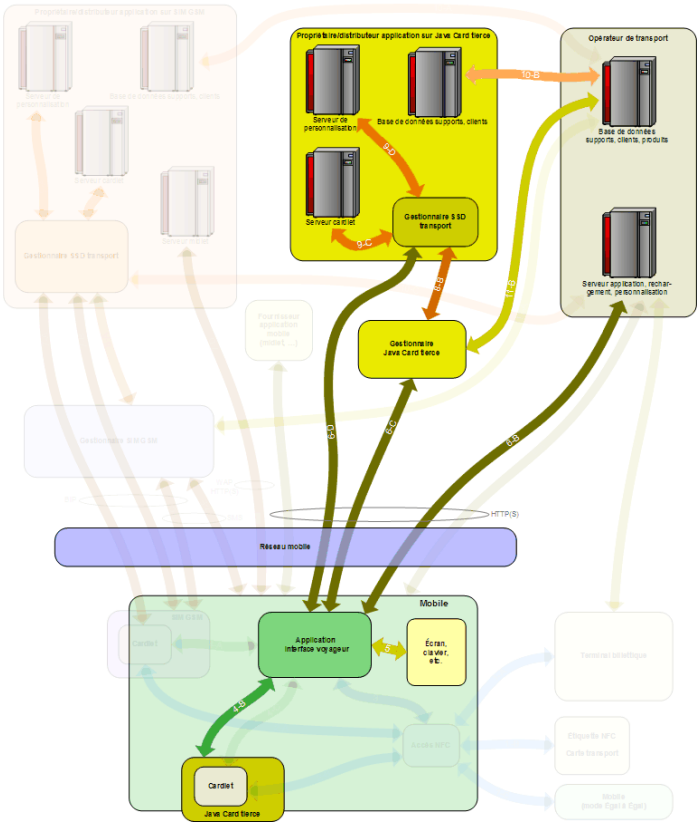
4.2.2.4 CHARGEMENT DE L'APPLICATION BILLETTIQUE

Les différents canaux envisagés pour le chargement de l'application billettique sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre. L'application d'interface voyageur est supposée présente.

Chargement de l'application billettique	Action	Interfaces
OTA, cas d'une carte tierce [21]	Activation de l'application d'interface voyageur, précédemment chargée, et connexion au SI transport.	5 : IHM du mobile 6-B : Logiciel du mobile / SI transport
	L'application d'interface voyageur identifie le type de module transport, et en déduit quel est le gestionnaire de modules transport Java Card tierce correspondant (dont son url). Cette opération peut nécessiter des échanges avec le SI transport.	4-B : Carte tierce / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Le SI transport choisit temporairement un identifiant de support de titre, et le communique à l'application d'interface voyageur.	6-B : Logiciel du mobile / SI transport
	L'application d'interface voyageur se connecte au gestionnaire Java Card tierce, lui communique l'identifiant de support de titre et l'AID de l'application billettique, et le met en relation avec le module transport. Le gestionnaire Java Card tierce obtient du module transport son identifiant d'ISD, et l'associe à l'identifiant de support de titre. Si nécessaire, le gestionnaire Java Card tierce réalise toutes les opérations de préparation de la Java Card tierce pour qu'elle puisse recevoir l'application billettique.	4-B : Carte tierce / logiciel du mobile 6-C : Logiciel du mobile / gestionnaire Java Card tierce
	Le gestionnaire Java Card tierce fournit au SI transport un identifiant technique du module transport.	11-B : SI transport (base de données supports, clients) / gestionnaire Java Card tierce
	Chargement de l'application billettique (chargement du package, instanciation et activation de l'application) en mode « single SD with DAP » ou en mode « Delegated Management ».	9-C : Gestionnaire SSD transport Java Card tierce / serveur cardlet 8-B : Gestionnaire Java Card tierce / gestionnaire SSD transport Java Card tierce 6-C : Logiciel du mobile / gestionnaire Java Card tierce 6-D : Logiciel du mobile / gestionnaire SSD transport Java Card tierce 4-B : Carte tierce / logiciel du mobile

[21] Pour une carte tierce, le mode push ne mettant pas en œuvre d'interface spécifique (mêmes interfaces qu'en mode pull, il n'est pas décrit.

	Personnalisation de l'application billettique, en obtenant un numéro de série Calypso d'un module d'activation Calypso, et en obtenant d'un CSM Calypso les clés diversifiées (en mode « single SD with DAP » ou en mode « Delegated Management »).	9-D : Gestionnaire SSD transport Java Card tierce / serveur de personnalisation 8-B : Gestionnaire Java Card tierce / gestionnaire SSD transport Java Card tierce 6-C : Logiciel du mobile / gestionnaire Java Card tierce 6-D : Logiciel du mobile / gestionnaire SSD transport Java Card tierce 4-B : Carte tierce / logiciel du mobile
	Le propriétaire/distributeur application Java Card tierce fournit au SI transport les paramètres de l'application billettique chargée (identifiant technique du module transport, numéro de série Calypso, etc.).	10-B : SI transport / propriétaire/distributeur application Java Card tierce
	Le SI transport assigne un identifiant transport à l'application billettique (qui remplace l'identifiant de support de titre).	-



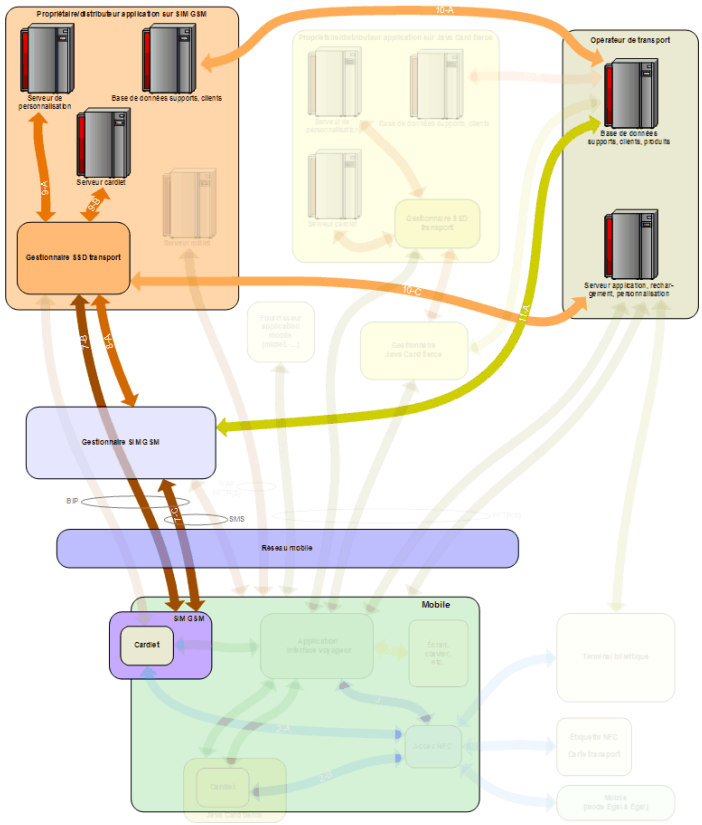
Notes :

- Ces échanges ne s'appliquent que lorsque la carte tierce est conforme aux spécifications GlobalPlatform et Java Card. Ils peuvent néanmoins être transposés à d'autres cas de carte tierce dans laquelle une application billettique est téléchargeable. Par ailleurs, ils sont décrits uniquement pour le cas où le module transport ne contient pas encore le package de l'application billettique.

- D'autres scénarios sont possibles. Par exemple, les échanges sur les interfaces 6-C/6-D pourraient être remplacés par des échanges via le SI transport (interfaces 10-C/11-B + 6-A).

Chargement de l'application billettique	Action	Interfaces
OTA, mode push, cas de la SIM GSM [22]	Le SI transport obtient de l'opérateur télécom l'ID_TECH correspondant au numéro de mobile.	11-A : SI transport (base de données supports, clients) / gestionnaire SIM GSM
	Le SI transport demande au propriétaire/distributeur application SIM GSM le chargement de l'application billettique (cible identifiée par son ID_TECH).	10-A : SI transport / propriétaire/distributeur application SIM GSM
	Établissement d'une session BIP (mode « single SD with DAP » ou mode « Delegated Management », cf. spécifications Ulysse).	8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM 7-C : SIM GSM / gestionnaire SIM GSM 7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP)
	Chargement de l'application billettique (chargement du package, instanciation et activation de l'application).	8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM 7-C : SIM GSM / gestionnaire SIM GSM 7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP)
	Personnalisation de l'application billettique, en obtenant un numéro de série Calypso d'un module d'activation Calypso, et en obtenant d'un CSM Calypso les clés diversifiées.	8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM 7-C : SIM GSM / gestionnaire SIM GSM 7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP)
	Fermeture de session BIP.	7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP)
	Le propriétaire/distributeur application SIM GSM fournit au SI transport les paramètres de l'application billettique chargée (numéro de série Calypso, etc.).	10-A : SI transport / propriétaire/distributeur application SIM GSM
	Le SI transport assigne un identifiant transport à l'application billettique (associé à l'ID_TECH).	-

[22] Le mode pull n'est pas disponible pour le cas de la SIM GSM (cf. spécifications Ulysse).



4.3 FONCTION - PERSONNALISATION

Ce chapitre présume que le mobile NFC contient une application transport prête à être personnalisée. Dans le cas contraire, le déroulement des opérations de personnalisation peut inclure le chargement de l'application transport (cf. chapitre précédent), sans incidence sur les recommandations du présent chapitre.

4.3.1 CAS D'UTILISATION

Un mobile NFC utilisé pour la billettique peut contenir des informations propres au voyageur, telles que des droits spécifiques (appelés « profils » [23]), ou d'une photographie pour l'identification du porteur en cas d'utilisation de titres de transport non cessibles d'un support nominatif.

La modification des profils du voyageur se déroule comme suit :

- attribution d'un profil, selon les cas :
  - par le voyageur, via Internet ou via l'IHM du mobile ;
  - par le SI Transport ;
- si l'inscription n'est pas réalisée en mode push, le voyageur est informé (par mail, SMS ou autre) que son nouveau profil est prêt à être installé dans le mobile ;
- inscription des nouveaux profils dans le module transport, selon les cas :
  - via un terminal billettique ;
  - en mode pull, avec utilisation l'IHM du mobile ;

[23] Un profil peut parfois être géré comme un titre de transport. Le chargement de ce type de profil correspond à une opération de distribution (voir chapitre 4.4).

- en mode push (sans activation de l'IHM du mobile) ;

Note concernant la personnalisation OTA via l'opérateur télécom
La personnalisation OTA via l'opérateur télécom n'est pas disponible actuellement (interface 7-A indisponible, voir notes du chapitre 3.6.7). Par conséquent, cette méthode n'est pas considérée dans ce chapitre.

- suppression de profils (avec accord éventuel du voyageur), pouvant également se produire avant l'inscription de nouveaux profils en cas d'espace de stockage insuffisant.
- si l'inscription a été réalisée en mode push, le voyageur est informé (par mail, SMS ou autre) que son mobile a été mis à jour avec les nouveaux profils.

Les cas de gestion d'une photographie du voyageur sont :

- inscription de la photographie dans le module transport ;
- inscription de la photographie dans la mémoire du mobile [24] ;
- émission d'une contre-carte portant la photographie et l'identifiant transport, traité au chapitre 3.5.

4.3.2 DESCRIPTION DES ECHANGES

4.3.2.1 ATTRIBUTION D'UN PROFIL

L'attribution de profil est hors du périmètre de ce document car elle ne met en œuvre aucun mécanisme spécifique à la billettique sur mobile NFC.

4.3.2.2 SIGNALEMENT D'EVENEMENT PROFILS OU PHOTOGRAPHIE

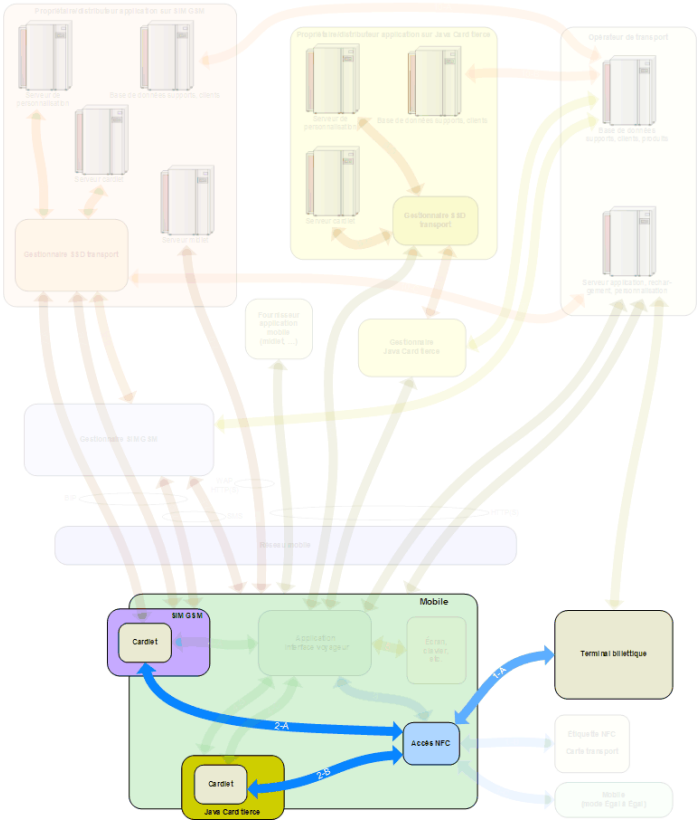
Le signalement d'événement profils ou photographie n'est dans le périmètre de ce document que cet avertissement est réalisé par SMS.

Signalement d'événement	Action	Interfaces
Par SMS	Réception et affichage d'un SMS indiquant l'événement profil ou photographie.	-
	Option : Si le chargement des données de personnalisation a été réalisé en mode push, ce SMS indique que les données ont été automatiquement mises à jour.	-
	Option : Si le chargement des données de personnalisation n'a pas été réalisé en mode push, ce SMS contient une invite à effectuer la mise à jour du module transport en lançant l'application d'interface voyageur du mobile ou en utilisant un terminal billettique.	-

[24] Le DoFoCo Mobile NFC n'évoque pas la possibilité de stocker la photographie dans la mémoire du mobile au chapitre sur la personnalisation (§7.3.3, p. 64/65), mais il l'indique au chapitre sur le contrôle (§7.5.2.5, p. 85).

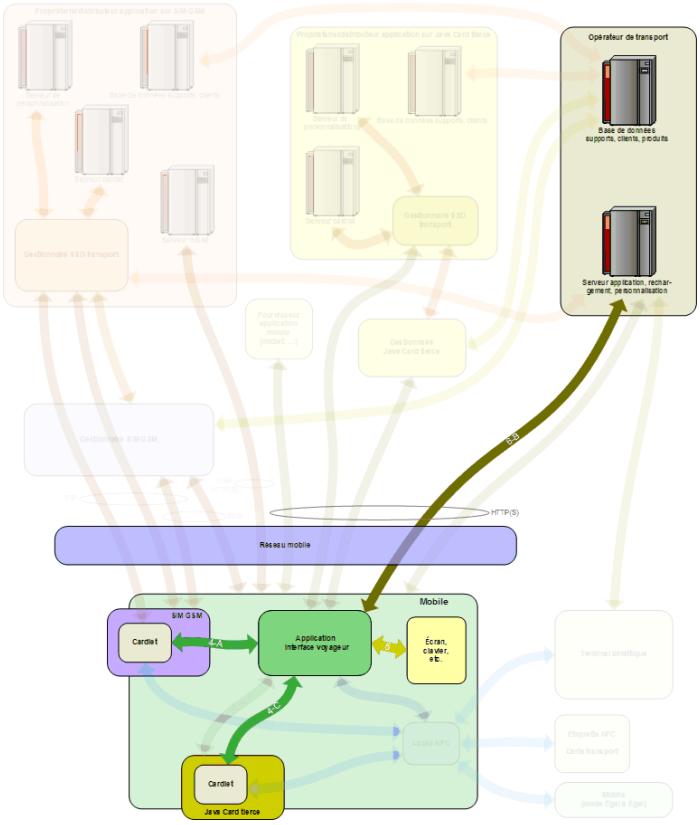
4.3.2.3 MISE A JOUR DES PROFILS OU CHARGEMENT DE LA PHOTOGRAPHIE

Mise à jour profils / photo	Action	Interfaces
Via interface NFC	Le processus détaillé, identique à celui d'une carte sans contact, est hors du périmètre de ce document. Ce processus doit être possible sans fourniture d'énergie par le mobile.	1-A : NFC externe, Mode Carte 2 : NFC du module transport

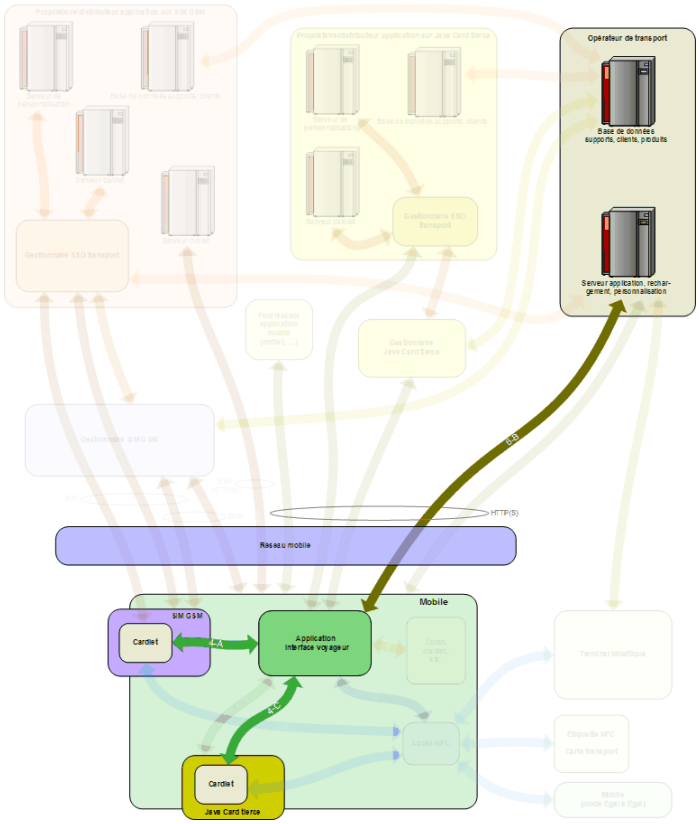


Note : Les scénarios de traitement des échecs de chargement ne mettent en œuvre aucune interface spécifique. Ils correspondent uniquement à des cas particulier d'utilisation des interfaces déjà définies dans ce document.

Mise à jour profils / photo	Action	Interfaces
Via l'application d'interface voyageur du mobile (mode pull)	Activation par le voyageur de l'application d'interface voyageur du mobile, affichage de la disponibilité d'une mise à jour des profils ou de la photographie, et validation par le voyageur.	5 : IHM du mobile 6-B : Logiciel du mobile / SI transport
	Mise à jour du contenu du module transport par le SI transport.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport



Mise à jour profils / photo	Action	Interfaces
En mode push	Le SI transport envoie au module transport les commandes relatives à la mise à jour des profils, et reçoit en retour les réponses du module transport.	4 : Application carte / logiciel du mobile 6-B : Logiciel du mobile / SI transport



4.4 FONCTION - DISTRIBUTION DE TITRES

Ce chapitre présume que le mobile NFC contient un module transport prêt à recevoir des titres pour le réseau considéré. Dans le cas contraire, le déroulement des opérations de distribution de titre peut inclure le chargement de l'application et sa personnalisation (cf. chapitres précédents), sans incidence sur les recommandations du présent chapitre[25].

4.4.1 CAS D'UTILISATION

Les cas d'utilisation envisagés pour le chargement de titres dans un mobile NFC sont les suivants (DoFoCo Mobile NFC, §7.4.3) :

- Achat et chargement de titres depuis le mobile.
- Achat et chargement de titres depuis Internet.
- Achat et chargement de titres depuis les équipements d'un bassin de transport.
- Achat et chargement de titres depuis un tag ou un numéro SMS.
- Paiement du montant des achats.
- Transfert des titres d'un mobile NFC vers un autre en Mode Égal à Égal.

[25] Dans ce cas le chargement de l'application transport est intégré au processus de chargement du titre, tout en le signalant au voyageur.

- Transfert des titres d'un mobile NFC (en Mode Lecteur) vers un support sans contact.
- Transfert des titres d'un support sans contact vers un mobile NFC (en Mode Lecteur).
- Mobile comme interface de vente.

Note concernant la distribution de titres OTA via l'opérateur télécom
La distribution de titres OTA via l'opérateur télécom n'est pas disponible actuellement (interface 7-A indisponible, voir notes du chapitre 3.6.7). Par conséquent, cette méthode n'est pas considérée dans ce chapitre.

Note concernant les transferts de titres :

Dans les applications billettiques existantes, l'inscription d'un titre de transport dans un support sans contact nécessite la génération de signatures cryptographiques par un SAM. Pour des raisons de sécurité, cette fonction « SAM » ne peut être présente dans un mobile NFC.

Par conséquent, le transfert doit se faire via le SI transport, qui dispose de SAM permettant ces opérations.

Cela restera nécessaire jusqu'à une future évolution des technologies billettiques (par exemple par la mise en œuvre d'une infrastructure à clés publiques).

4.4.2 DESCRIPTION DES ECHANGES

Toute distribution de titres de transport se décompose en trois étapes :

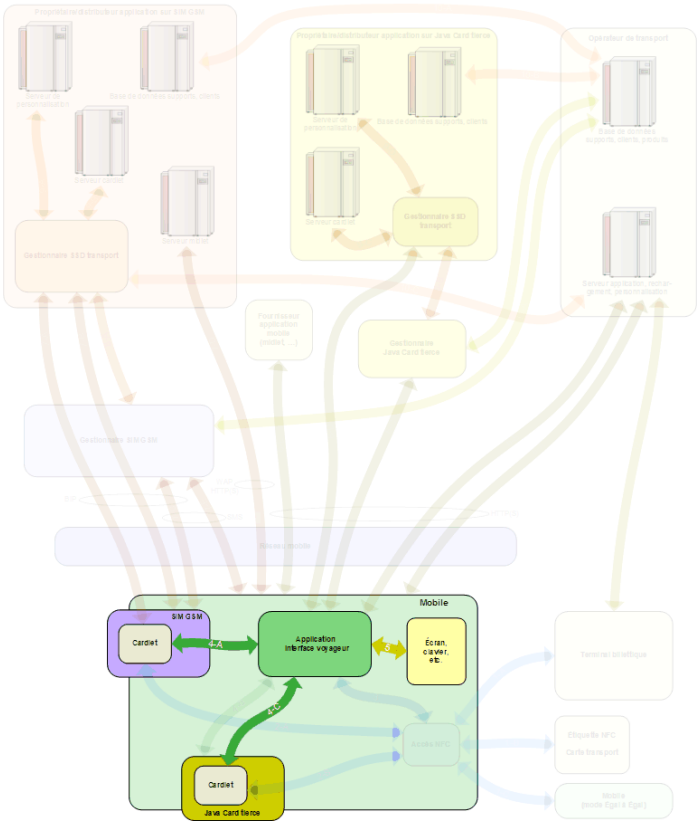
- choix du titre ;
- paiement du titre, et facturation ;
- chargement du titre sur le support.

Dans la suite de ce chapitre, pour chaque étape sont présentées les actions réalisées et les interfaces mises en œuvre pour tous les cas d'utilisation envisagés.

4.4.2.1 CHOIX DU (DES) TITRE(S)

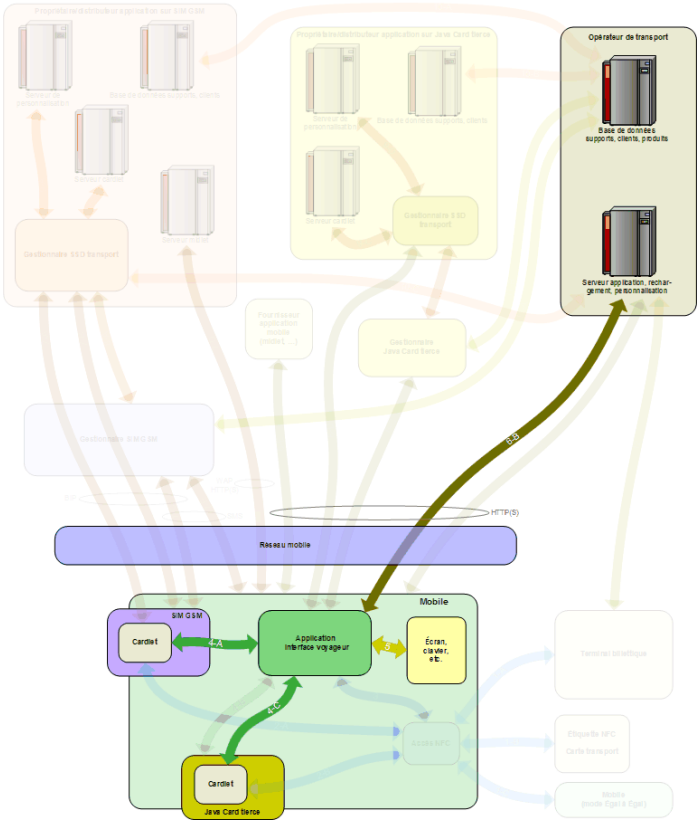
Les différents canaux envisagés pour le choix des titres sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Choix du titre	Action	Interfaces
Depuis un mobile NFC, sans connexion au SI transport	Activation par le voyageur de l'application d'interface voyageur du mobile, et demande des titres disponibles à l'achat.	5 : IHM du mobile
	Option : Optimisation de la liste des titres proposés à la vente sur mobile, par lecture des données relatives au voyageur (profil, contrats, etc.) dans le module transport.	4 : Module transport / logiciel du mobile
	Présentation des titres proposés à la vente sur mobile, et choix par le voyageur.	5 : IHM du mobile

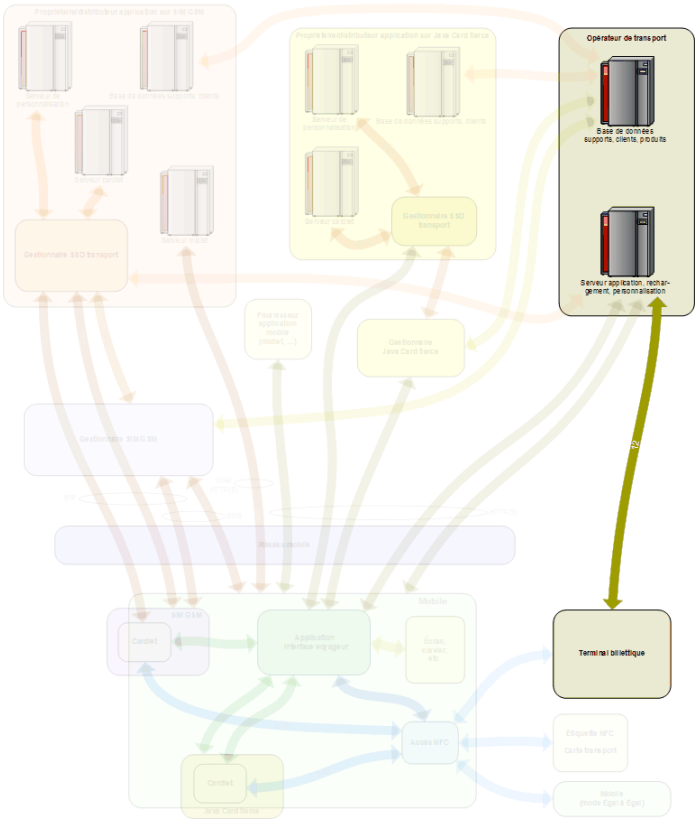


Note : Pour ce cas, l'application d'interface voyageur du mobile contient tous les paramètres de tarification à jour. Ces paramètres pourront être vérifiés au début de la phase de chargement des titres acquis, si nécessaire avec annulation du paiement au cas où ils s'avéreraient obsolètes.

Choix du titre	Action	Interfaces
Depuis un mobile NFC, avec connexion au SI transport	Activation par le voyageur de l'application d'interface voyageur du mobile, et demande des titres disponibles à l'achat.	5 : IHM du mobile
	Connexion au site Internet mobile de vente des titres du bassin de transport.	6-B : Logiciel du mobile / SI transport
	Option : Identification du voyageur par le SI transport, par lecture de son identifiant transport tel qu'inscrit dans le module transport.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Option : Optimisation de la liste des titres proposés à la vente sur mobile, par lecture des données relatives au voyageur (profil, contrats, etc.) dans le module transport.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Présentation des titres proposés à la vente sur mobile, et choix par le voyageur.	5 : IHM du mobile 6-B : Logiciel du mobile / SI transport



Choix du titre	Action	Interfaces
Depuis Internet, sans accès au module transport	Connexion au site Internet de vente des titres du bassin de transport.	12 : Terminal billettique / SI transport
	Option : Identification du mobile (n° de mobile) ou de l'application billettique (identifiant transport) à recharger, par saisie manuelle.	12 : Terminal billettique / SI transport
	Présentation des titres proposés à la vente par Internet, et choix par le voyageur.	12 : Terminal billettique / SI transport



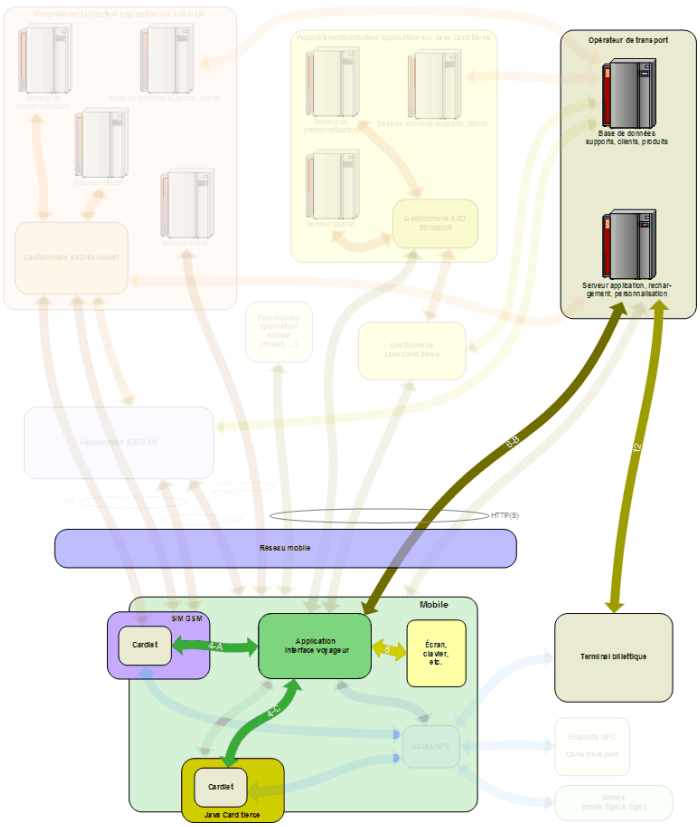
Note : Dans ce cas d'usage le terminal billettique est un terminal Internet.

Choix du titre	Action		Interfaces
Depuis Internet, avec accès OTA au module transport [26]	Connexion au site Internet de vente des titres du bassin de transport.		12 : Terminal billettique / SI transport
	Identification du mobile (n° de mobile) ou de l'application billettique (identifiant transport) à recharger, par saisie manuelle.		12 : Terminal billettique / SI transport
	Option : Lecture du module transport en mode pull.	Option : Sur le mobile cible, activation manuelle de l'application du mobile.	5 : IHM du mobile
		Option : Sur le mobile cible, réception et affichage d'un SMS contenant une invite à lancer une application, validation de cette invite par le voyageur.	-
		Connexion au SI transport et lecture du module transport en mode pull.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Option : Lecture du module transport en mode push.		Idem chargement du titre en OTA en mode push (§4.4.2.3) : 4, 6-B
	Présentation des titres proposés à la vente par Internet, et choix par le voyageur.		12 : Terminal billettique / SI transport

Note : Dans ce cas d'usage le terminal billettique est un terminal Internet.

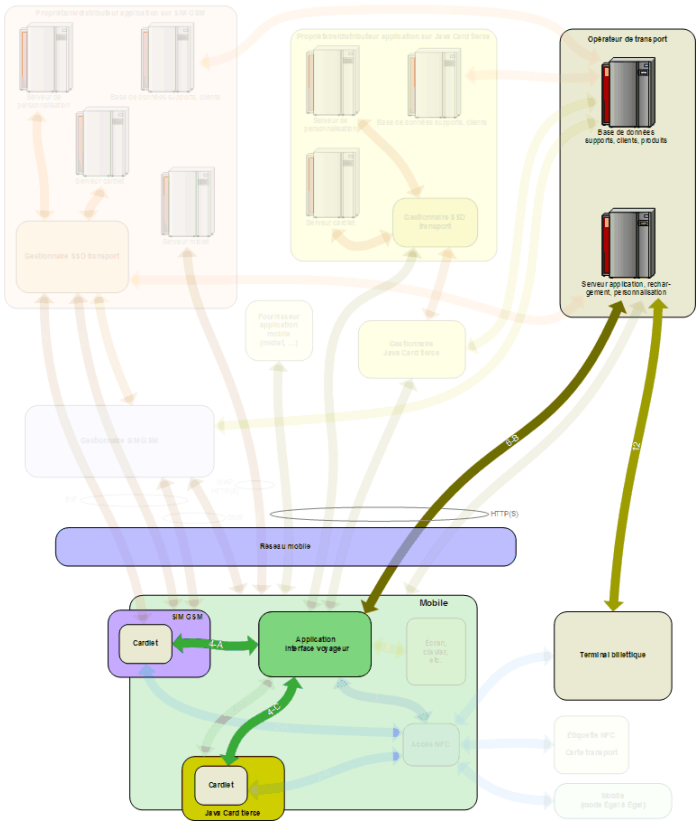
[26] Par exemple lorsque le choix du titre est effectué avec le navigateur d'un ordinateur personnel (faisant fonction de terminal billettique) et si l'utilisateur a la possibilité de saisir un identifiant de la cible à recharger, de sorte que le SI transport puisse lire cette cible et proposer à l'utilisateur une offre commerciale adaptée.

Pull :

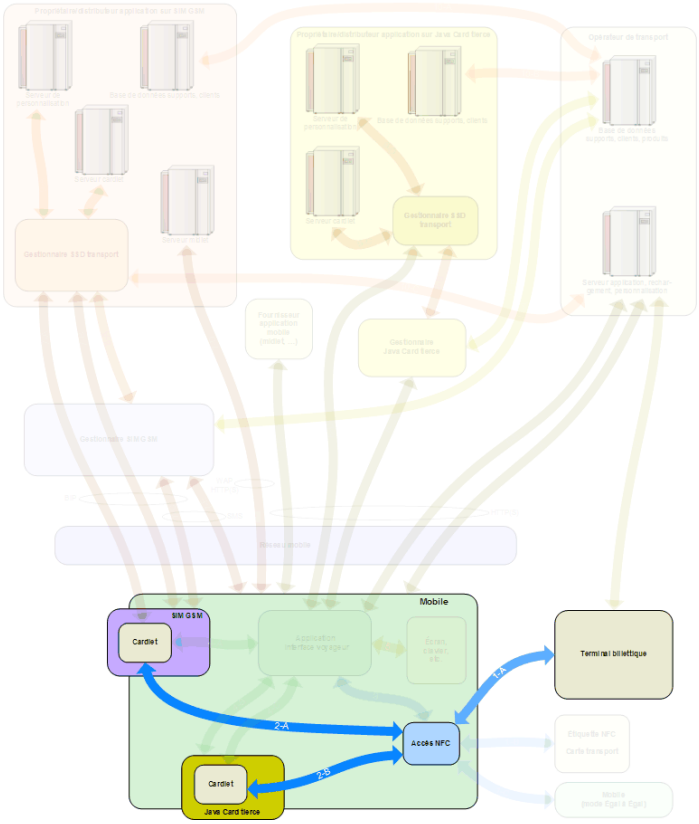


Note : Pour le mode pull, l'application du mobile est activée soit manuellement soit par réception d'un SMS.

Mode push :

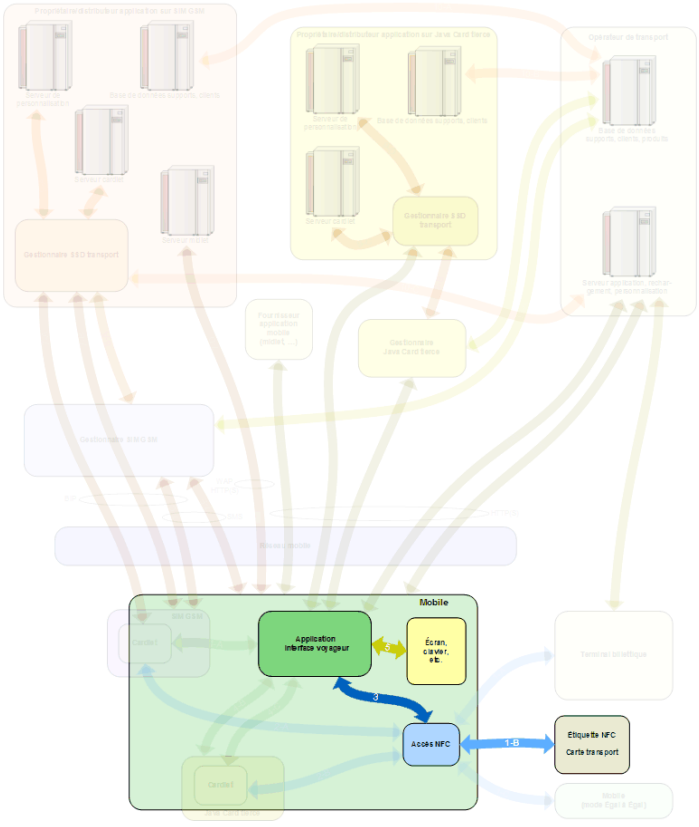


Choix du titre	Action	Interfaces
Depuis les équipements d'un bassin de transport	Le processus détaillé, identique à celui d'une carte sans contact, est hors du périmètre de ce document. Ce processus doit être possible sans fourniture d'énergie par le mobile.	1-A : NFC externe, Mode Carte 2 : NFC du module transport



Note : Le terminal billettique peut être en relation avec le SI transport, selon les procédures mises en place par l'opérateur de transport. De tels échanges sont hors du périmètre de ce document.

Choix du titre	Action	Interfaces
Via un tag NFC	Lecture du tag NFC et activation de l'IHM du mobile.	1-B : NFC externe, Mode Lecteur 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile
	Option : Affichage d'une URL, validation de cette URL par le voyageur, lancement du navigateur web du mobile.	Cf. choix d'un titre par terminal billettique (sans accès au module transport [27])
	Option : Affichage d'un numéro, validation par le voyageur de l'envoi d'un SMS à ce numéro.	Cf. choix d'un titre par numéro SMS
	Option : Affichage d'une invite à lancer une application, validation de cette invite par le voyageur.	Cf. choix d'un titre par le mobile NFC



[27] Il n'existe pour l'instant pas de standard décrivant la possibilité pour le navigateur d'un mobile d'accéder à une carte à puce du mobile (voir notes du chapitre 3.6.4).

Choix du titre	Action	Interfaces
Via un numéro SMS	Envoi par le voyageur d'un SMS au numéro indiqué par l'opérateur de transport.	-
	Option : Réception et affichage d'un SMS contenant une URL, validation de cette URL par le voyageur.	Cf. choix d'un titre par terminal billettique (sans accès au module transport [28])
	Option : Réception et affichage d'un SMS contenant une invite à lancer une application, validation de cette invite par le voyageur.	Cf. choix d'un titre par le mobile NFC

4.4.2.2 PAIEMENT DU MONTANT DES ACHATS

Aucune interface spécifique à la billettique sur mobile NFC n'est mise en œuvre pour le paiement des titres, qui peut être effectué selon les méthodes décrites dans le DoFoCo Mobile NFC (§7.4.3.5) :

- Sur l'équipement de vente lorsque l'achat est opéré sur un équipement billettique, comme pour l'utilisation d'une carte sans contact :
  - espèces ;
  - chèque ;
  - carte bancaire ;
  - mobile NFC si ce dernier est équipé d'une application bancaire de paiement de proximité. Dans ce cadre, le processus doit prendre en compte le fait que le mobile doit opérer en même temps deux transactions, le chargement du titre d'une part et le paiement d'autre part, et en sachant que :
    - le chargement n'est confirmé que si le paiement est réalisé,
    - si le chargement subit un échec un remboursement doit avoir lieu.
- À distance lors de l'achat via le mobile ou Internet :
  - service de paiement à distance fourni par l'opérateur mobile ;
  - service de paiement à distance fourni par un prestataire spécialisé ;
  - service de paiement à distance choisi et mis à disposition par le service transport ;
  - utilisation d'une application bancaire embarquée dans le mobile.
- A posteriori, via une facture :
  - établissement d'une facture par l'opérateur du service billettique ;
  - répercussion des achats sur la facture télécom mobile.

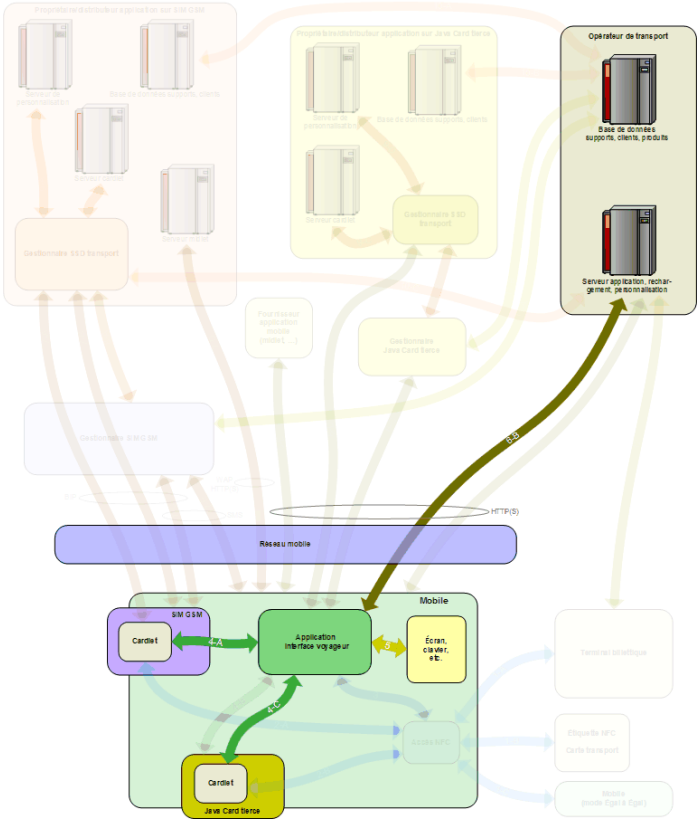
Dans tous les cas ou un paiement est nécessaire, le chargement des titres n'est effectué qu'après réception par le système de chargement (SI transport ou terminal billettique) de la confirmation du paiement.

[28] Il n'existe pour l'instant pas de standard décrivant la possibilité pour le navigateur d'un mobile d'accéder à une carte à puce du mobile.

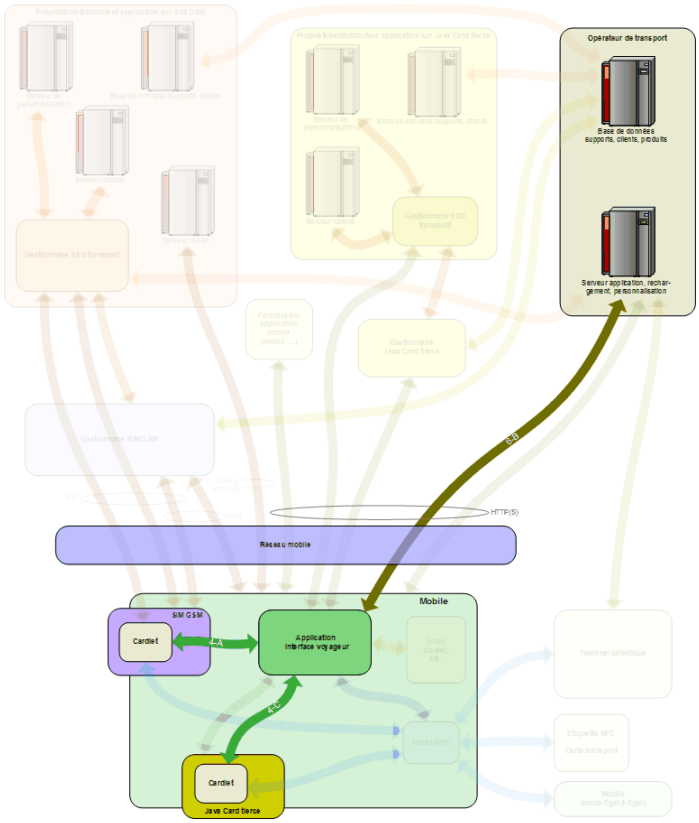
4.4.2.3 CHARGEMENT DU (DES) TITRE(S) DE TRANSPORT

Les différents canaux envisagés pour le chargement du (ou des) titre(s) sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Chargement du titre	Action	Interfaces
OTA mode pull	Mise à jour du contenu du module transport, suite à la demande (ou à l'accord explicite) du voyageur via l'IHM du mobile.	4 : Module transport / logiciel du mobile 5 : IHM du mobile 6-B : Logiciel du mobile / SI transport

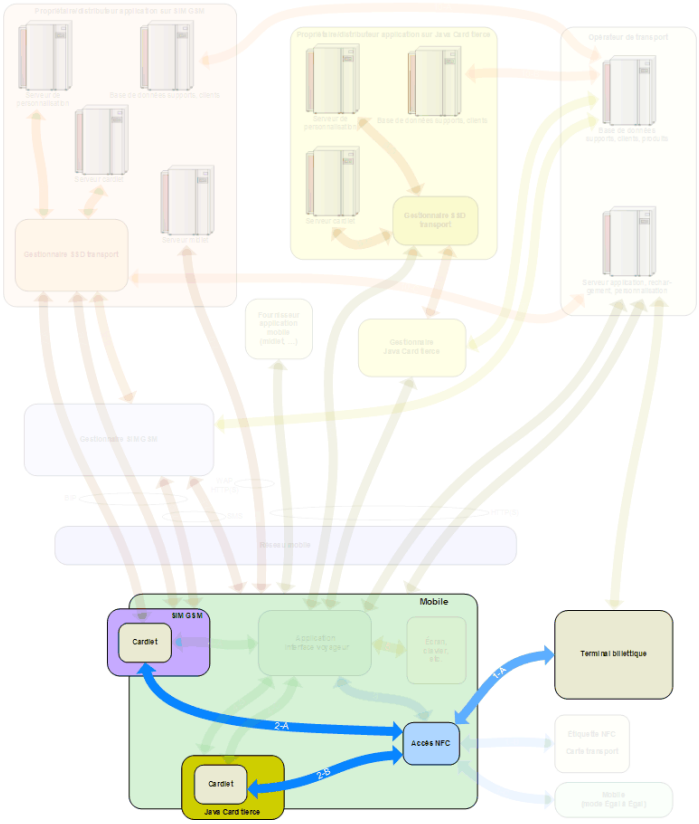


Chargement du titre	Action	Interfaces
OTA mode push [29]	Le SI transport envoie au module transport les commandes relatives au chargement du titre, et reçoit en retour les réponses du module transport.	4 : Application carte tierce / logiciel du mobile 6-B : Logiciel du mobile / SI transport



[29] Le processus se déroule sans mettre en œuvre l'IHM du mobile.

Chargement du titre	Action	Interfaces
Via interface NFC	Le processus détaillé, identique à celui d'une carte sans contact, est hors du périmètre de ce document. Ce processus doit être possible sans fourniture d'énergie par le mobile.	1-A : NFC externe, Mode Carte 2 : NFC du module transport



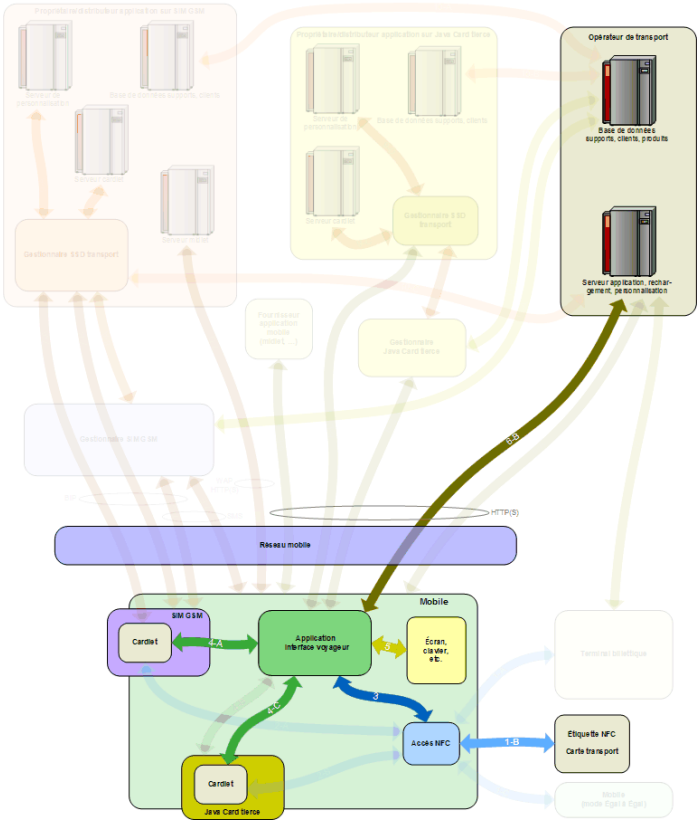
Note : Les scénarios de traitement des échecs de chargement ne mettent en œuvre aucune interface spécifique. Ils correspondent uniquement à des cas particulier d'utilisation des interfaces déjà définies dans ce document.

4.4.2.4 LE MOBILE UTILISE COMME « AUTOMATE PORTABLE »

Les différents canaux envisagés pour le transfert de titres cessibles préalablement chargés dans le module transport, et pour le cas du mobile utilisé comme interface de vente, sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

<table>
<tr><th>Mobile comme automate portable</th><th colspan="2">Action</th><th>Interfaces</th></tr>
<tr><td rowspan="8">Transfert de titres en Mode Lecteur</td><td colspan="2">Avec l'application d'interface voyageur du mobile, l'utilisateur sélectionne les titres à transférer.</td><td>4 : Module transport / logiciel du mobile
5 : IHM du mobile</td></tr>
<tr><td colspan="2">Option :
Si le mobile ne peut pas détecter automatiquement le mode de fonctionnement, l'utilisateur sélectionne le Mode Lecteur.
(NB : Peut avoir été effectué précédemment.)</td><td>3 : Logiciel du mobile / accès NFC</td></tr>
<tr><td rowspan="3">Mobile vers carte [30]</td><td>La carte où transférer les titres est présentée à proximité de l'interface NFC du mobile, qui établit la communication en Mode Lecteur et avertit l'utilisateur de ne pas interrompre la communication.</td><td>1-B : NFC externe, Mode Lecteur
3 : Logiciel du mobile / accès NFC
5 : IHM du mobile</td></tr>
<tr><td>À l'aide du SI transport, le mobile supprime les titres à transférer de son module transport.</td><td>4 : Module transport / logiciel du mobile
6-B : Logiciel du mobile / SI transport</td></tr>
<tr><td>À l'aide du SI transport, le mobile charge les titres à transférer dans la carte.</td><td>1-B : NFC externe, Mode Lecteur
3 : Logiciel du mobile / accès NFC
6-B : Logiciel du mobile / SI transport</td></tr>
<tr><td rowspan="3">Carte [30] vers mobile</td><td>La carte d'où extraire les titres est présentée à proximité de l'interface NFC du mobile, qui établit la communication en Mode Lecteur et avertit l'utilisateur de ne pas interrompre la communication.</td><td>1-B : NFC externe, Mode Lecteur
3 : Logiciel du mobile / accès NFC
5 : IHM du mobile</td></tr>
<tr><td>À l'aide du SI transport, le mobile supprime de la carte les titres à transférer.</td><td>1-B : NFC externe, Mode Lecteur
3 : Logiciel du mobile / accès NFC
6-B : Logiciel du mobile / SI transport</td></tr>
<tr><td>À l'aide du SI transport, le mobile charge les titres à transférer dans le module transport du mobile.</td><td>4 : Module transport / logiciel du mobile
6-B : Logiciel du mobile / SI transport</td></tr>
<tr><td colspan="2">L'IHM du mobile informe l'utilisateur du bon déroulement du transfert.</td><td>5 : IHM du mobile</td></tr>
</table>

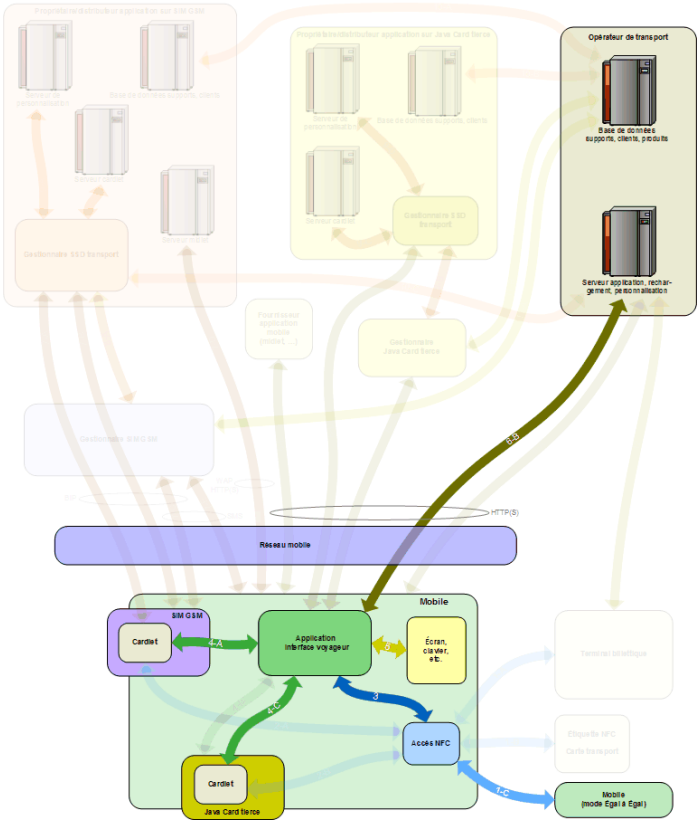
[30] Ou tout autre type d'objet portable compatible et fonctionnant conformément à ISO/IEC 14443.



Note : En cas d'interruption de la communication entre le mobile et la carte après la suppression des titres et avant leur chargement dans la carte, le SI transport pourra restituer les titres à l'utilisateur du mobile, comme pour un chargement OTA (cf. §4.4.2.3).

Mobile comme automate portable	Action	Interfaces
Transfert de titres en Mode Égal à Égal	Avec l'application d'interface voyageur du mobile fournisseur, l'utilisateur sélectionne les titres à transférer.	4 : Module transport / logiciel du mobile 5 : IHM du mobile
	Option : Si le mobile ne peut pas détecter automatiquement le mode de fonctionnement, l'utilisateur sélectionne le Mode Égal à Égal. (NB : Peut avoir été effectué précédemment.)	3 : Logiciel du mobile / accès NFC
	Le mobile [31] récepteur des titres est présenté à proximité de l'interface NFC du mobile fournisseur. Ayant établi la communication en Mode Égal à Égal, les deux mobiles avertissent leur utilisateur respectif de ne pas interrompre la communication.	1-C : NFC externe, Mode Égal à Égal 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile
	À l'aide du SI transport, le mobile fournisseur supprime les titres à transférer de son module transport.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	À l'aide du SI transport, le mobile fournisseur charge les titres à transférer dans le mobile récepteur.	1-C : NFC externe, Mode Égal à Égal 3 : Logiciel du mobile / accès NFC 6-B : Logiciel du mobile / SI transport
	Les deux mobiles avertissent leur utilisateur respectif du bon déroulement du transfert.	5 : IHM du mobile

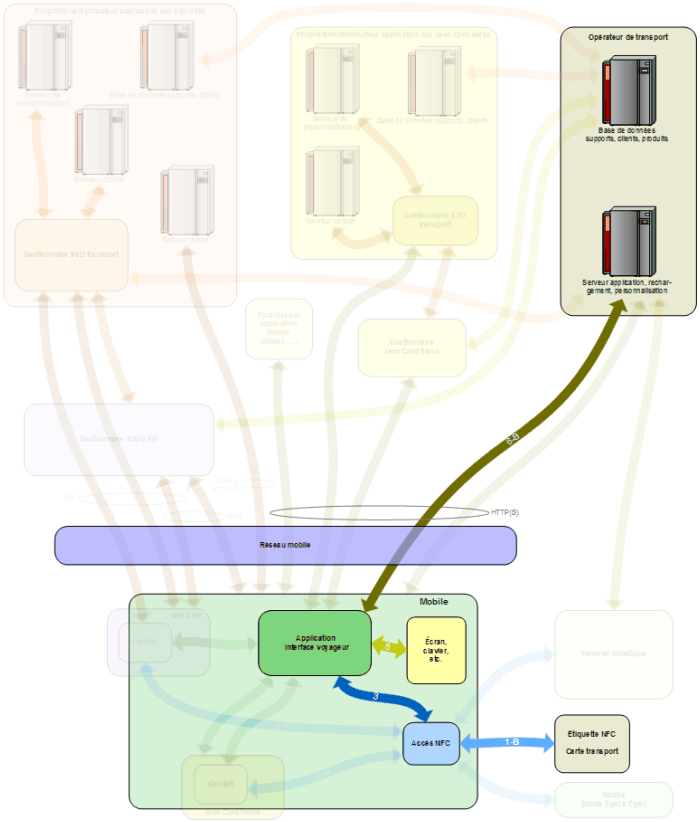
[31] Ou tout autre type d'objet portable compatible et fonctionnant en Mode à Égal à Égal.



Note : En cas d'interruption de la communication entre les mobiles après la suppression des titres et avant réception par le mobile fournisseur de l'acquittement de chargement dans le mobile récepteur, le SI transport pourra si nécessaire charger les titres dans le mobile récepteur, comme pour un chargement OTA (cf. §4.4.2.3).

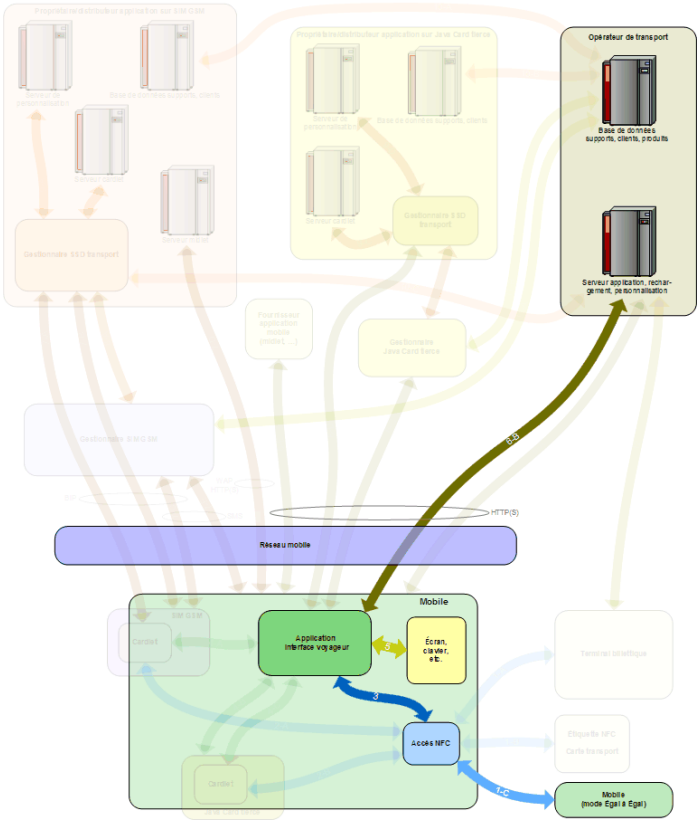
Mobile comme automate portable	Action	Interfaces
Interface de vente en Mode Lecteur	Activation par le voyageur de l'application d'interface voyageur du mobile, et demande des titres disponibles à l'achat pour un autre support.	5 : IHM du mobile
	Connexion au site Internet mobile de vente des titres du bassin de transport.	6-B : Logiciel du mobile / SI transport
	Option : Si le mobile ne peut détecter automatiquement le mode de fonctionnement, l'utilisateur sélectionne le Mode Lecteur. (NB : Peut avoir été effectué précédemment.)	3 : Logiciel du mobile / accès NFC
	La carte [32] où transférer les titres est présentée à proximité de l'interface NFC du mobile, établit la communication en Mode Lecteur, et avertit l'utilisateur de ne pas interrompre la communication.	1-B : NFC externe, Mode Lecteur 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile
	Le SI transport lit le contenu de la carte cible, présente sur l'IHM du mobile la liste optimisée des titres proposés à la vente, puis l'utilisateur du mobile sélectionne les titres à charger.	1-B : NFC externe, Mode Lecteur 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile 6-B : Logiciel du mobile / SI transport
	Paiement du montant des achats via le mobile (cf. §4.4.2.2)	-
	Via le mobile, le SI transport charge les titres dans la carte.	1-B : NFC externe, Mode Lecteur 3 : Logiciel du mobile / accès NFC 6-B : Logiciel du mobile / SI transport
	L'IHM du mobile informe l'utilisateur du bon déroulement du chargement.	5 : IHM du mobile

[32] Ou tout autre type d'objet portable compatible et fonctionnant conformément à ISO/IEC 14443.


Opérateur de transport
Base de données supports, clients, produits
Serveur application, rechargement, personnalisation
3-S
HTTP(S)
Réseau mobile
Mobile
Application interface voyageur
Écran, clavier, etc.
Accès NFC
1-S
Étiquette NFC
Carte transport

Mobile comme automate portable	Action	Interfaces
Interface de vente en Mode Égal à Égal	Activation par le voyageur de l'application d'interface voyageur du mobile, et demande des titres disponibles à l'achat pour un autre support.	5 : IHM du mobile
	Connexion au site Internet mobile de vente des titres du bassin de transport.	6-B : Logiciel du mobile / SI transport
	Option : Si le mobile ne peut détecter automatiquement le mode de fonctionnement, l'utilisateur sélectionne le Mode Égal à Égal. (NB : Peut avoir été effectué précédemment.)	3 : Logiciel du mobile / accès NFC
	Le mobile [33] récepteur des titres est présenté à proximité de l'interface NFC du mobile fournisseur. Ayant établi la communication en Mode Égal à Égal, les deux mobiles avertissent leur utilisateur respectif de ne pas interrompre la communication.	1-C : NFC externe, Mode Égal à Égal 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile
	Le SI transport lit le contenu de la carte cible, présente sur l'IHM du mobile la liste optimisée des titres proposés à la vente, puis l'utilisateur du mobile sélectionne les titres à charger.	1-C : NFC externe, Mode Égal à Égal 3 : Logiciel du mobile / accès NFC 5 : IHM du mobile 6-B : Logiciel du mobile / SI transport
	Paiement du montant des achats via le mobile (cf. §4.4.2.2)	-
	Via le mobile, le SI transport charge les titres dans la carte.	1-C : NFC externe, Mode Égal à Égal 3 : Logiciel du mobile / accès NFC 6-B : Logiciel du mobile / SI transport
	L'IHM du mobile informe l'utilisateur du bon déroulement du chargement.	5 : IHM du mobile

[33] Ou tout autre type d'objet portable compatible et fonctionnant en Mode à Égal à Égal.



Note : La fonction « interface de vente en Mode Égal à Égal » ne s'applique que lorsque le mobile cible est dans l'impossibilité de réaliser lui-même l'opération.

4.5 FONCTION - VALIDATION ET CONTROLE DES TITRES

4.5.1 CAS D'UTILISATION

Validation

La validation du titre de transport correspond à la confirmation de l'acceptation du contrat de transport par le voyageur et l'opérateur de transport, et à son enregistrement dans le support. Les cas d'utilisation envisagés sont les suivants :

- Validation simple, comme pour une carte
- Conflit à la validation :
    - Validation avec sélection préalable via l'IHM du terminal billettique, comme pour une carte.
    - Validation avec sélection préalable via l'IHM du mobile.
    - Activation automatique de l'IHM du mobile suite à une action de validation avec conflit.

➔ **Note pour le groupe**	Le DoFoCo Mobile NFC indique (§7.5.2.2, p. 83) à propos de l'activation automatique de l'IHM du mobile (en cas de conflit à la validation, pour permettre au voyageur de sélectionner le titre à valider) : *« La sélection du titre à valider en priorité nécessite aujourd'hui de se connecter à un serveur distant au travers du réseau GSM pour pouvoir opérer la sélection du titre pour des raisons de sécurité. »* et *« Un chantier doit être lancé au niveau de Calypso (ou entité équivalente) et d'Intercode pour définir une solution qui permette de sélectionner son titre de transport sans avoir à se connecter à un serveur distant. »* Il s'agit ici que le logiciel du mobile inscrive dans le module transport une information à destination du terminal de validation. Or dans les structures de fichiers Calypso définies par Intercode, toute modification nécessite l'utilisation d'un SAM, donc la connexion du mobile à un serveur billettique. Une solution simple serait de modifier uniquement Intercode afin d'ajouter aux structures de fichiers Calypso un fichier modifiable sans SAM (ce qui est autorisé par Calypso Rev.2 et Rev.3). **Cette solution ne protège pas contre le risque qu'un logiciel malveillant installé dans le mobile tente de nuire au système en altérant les informations de sélection**, mais la connexion à un serveur ne protège pas non plus contre ce type d'attaque (le résultat de la sélection effectuée par le voyageur sur le clavier du mobile pouvant être altéré avant son envoi au serveur et son inscription dans le module transport).

- Voyage à plusieurs avec un seul titre de transport, prévu pour plusieurs voyageurs :
    - Validation globale :
        - Sans IHM du terminal billettique ni du mobile, comme pour une carte.
        - Avec sélection préalable du nombre de voyageurs via l'IHM du mobile, comme indiqué au chapitre 4.5.2.4.
        - Avec sélection du nombre de voyageurs via l'IHM du terminal billettique, suite à une première action de validation, comme pour une carte.
    - Validations multiples, qui correspondent au nombre effectif de voyageurs :
        - Sans IHM du mobile, comme pour une carte.
        - Avec confirmation de chaque validation via l'IHM du mobile.
- Voyage à plusieurs avec plusieurs titres de transport, avec configuration préalable du voyage via l'IHM du mobile, comme indiqué au chapitre 4.5.2.4

Affichage d'informations ou de requêtes sur le mobile, suite à une action de validation

L'IHM du mobile NFC peut être activée par le terminal billettique lors d'une opération de validation ou de contrôle, afin d'afficher :

- des informations concernant le contenu du module transport, par exemple :
    - présence de conflits entre titres (ou entre application) et demande de choix ;
    - attente de confirmation avant chaque voyageur supplémentaire ;

- solde du titre validé et proposition de rechargement si ce solde est proche de zéro ;
- date fin de validité d'un titre X jours avant la fin de validité, avec X paramétrable et proposition de rechargement du titre.

- des informations personnalisées concernant le voyage, par exemple :
  - perturbations ;
  - calcul d'itinéraire alternatif ;
  - temps de parcours restant.

Contrôle

Lors d'un contrôle du titre de transport, le contrôleur vérifie la situation du voyageur à partir des informations lues en mode NFC et affichées sur l'appareil de contrôle.

Quand le contrôle de l'identité du voyageur est nécessaire et que sa photo est stockée dans le mobile, elle est affichée :

- Sur l'appareil de contrôle (lors de la lecture de l'application billettique), si la photo est hébergée par le module transport.
- Sur le mobile, si la photo est hébergée dans un espace mémoire du mobile :
  - avec activation manuelle de l'IHM du mobile par le voyageur ;
  - avec activation automatique de l'IHM du mobile suite à l'opération de contrôle.

En cas de lecture sans contact impossible sur le mobile, le voyageur peut prouver sa bonne foi via l'IHM du mobile en montrant au contrôleur le contenu du module transport.

4.5.2 DESCRIPTION DES ECHANGES

La validation d'un titre de transport se déroule selon le processus général suivant :

- Éventuellement, sélection via l'IHM du mobile du titre à valider ou du nombre de voyageurs.
- Présentation du mobile au terminal de validation :
  - lecture, analyse et vérification des données billettiques contenues dans le mobile ;
  - si les données lues sont suffisantes, inscription dans le mobile des données de validation et achèvement de la procédure de validation (par exemple signal vert et déblocage du tripode) ;
- Si une interaction avec le voyageur est requise, mise en œuvre de l'IHM du mobile ou du terminal de validation.
- Si une validation supplémentaire est requise, reprise du processus à la présentation du mobile au terminal de validation.

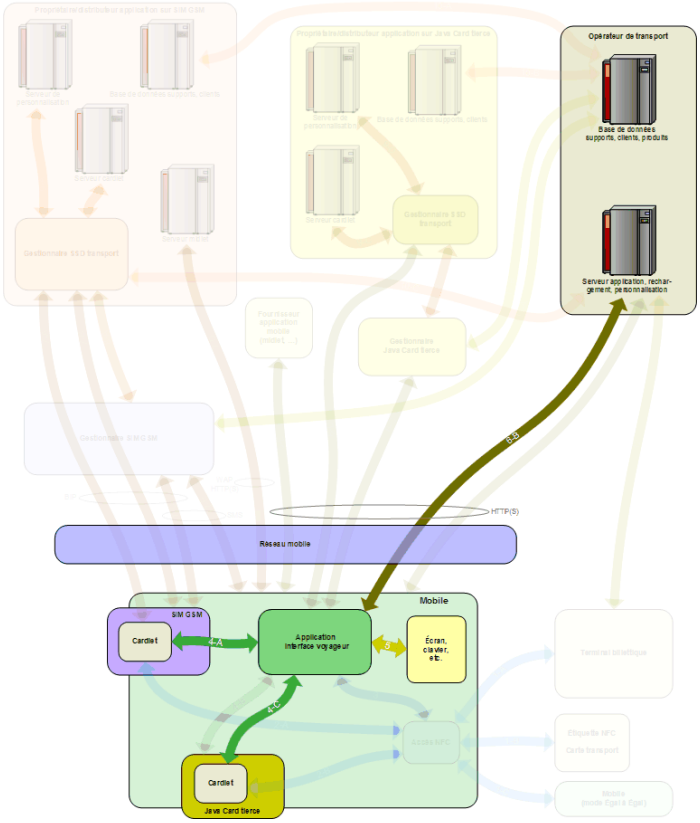
Le contrôle d'un titre de transport se décompose ainsi :

- Présentation de la carte au terminal de contrôle :
  - lecture, analyse et vérification des données billettiques contenues dans le mobile ;
  - affichage (et saisie éventuelle) via l'IHM du terminal de contrôle ;
  - éventuellement, inscription dans le mobile de données de contrôle.
- Éventuellement, actions de contrôle supplémentaires (affichage de la photo sur le mobile, présentation d'une contre-carte, etc.).

4.5.2.1 VALIDATION : SELECTION PREALABLE VIA L'IHM DU MOBILE

La sélection via l'IHM du mobile, préalablement à la validation, du titre à valider parmi ceux chargés dans le module transport est décrite dans le tableau et le diagramme ci-dessous, avec indication des actions et des interfaces mis en œuvre.

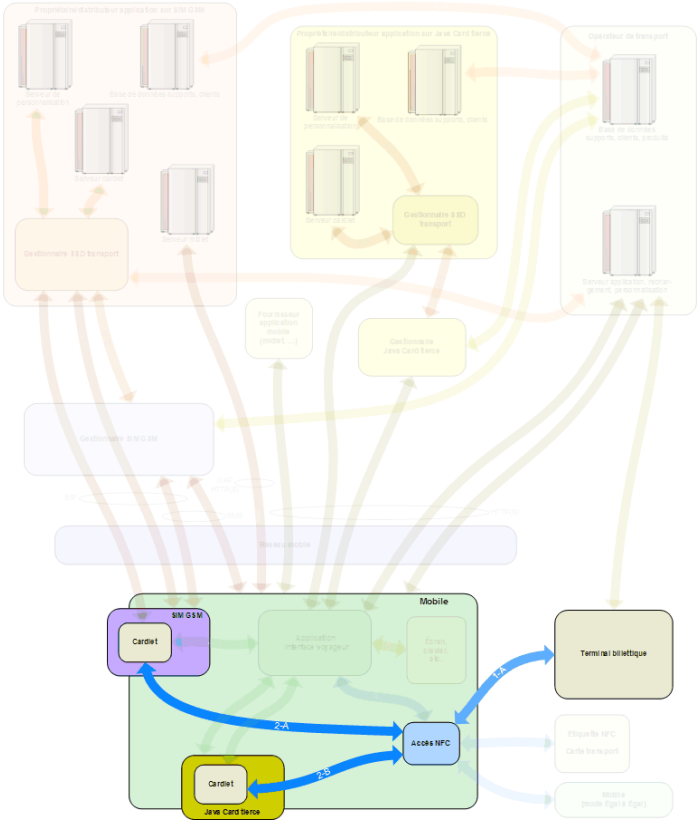
Action	Interfaces
Activation manuelle de l'application d'interface voyageur.	5 : IHM du mobile
Lecture du module transport par le logiciel du mobile, et affichage via l'IHM du mobile du choix du titre à valider ou du nombre de voyageurs.	4 : Module transport / logiciel du mobile 5 : IHM du mobile
Saisie via l'IHM du mobile du titre à valider ou du nombre de voyageurs.	5 : IHM du mobile
Inscription dans le module transport par le logiciel du mobile des données correspondant au choix effectué, éventuellement avec connexion au SI transport (serveur de rechargement ou de personnalisation) pour sécurisation de cette inscription.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport



4.5.2.2 VALIDATION OU CONTROLE : TRANSACTION SANS CONTACT

La transaction sans contact réalisée lors d'une validation ou d'un contrôle est décrit dans le tableau et le diagramme ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Action	Interfaces
Le processus détaillé, identique à celui d'une carte sans contact, est hors du périmètre de ce document. Ce processus doit être possible sans fourniture d'énergie par le mobile.	1-A : NFC externe, Mode Carte 2 : NFC du module transport



Notes :

- La transaction peut inclure l'inscription dans le module transport d'un scénario d'interaction avec l'utilisateur, qui sera mis en œuvre par le logiciel du mobile à l'issue d'une communication sans contact.
- Le terminal billettique peut être en relation avec le SI transport, selon les procédures mises en place par l'opérateur de transport. De tels échanges sont hors du périmètre de ce document.

4.5.2.3 VALIDATION OU CONTROLE : ACTIVATION AUTOMATIQUE DU LOGICIEL DU MOBILE

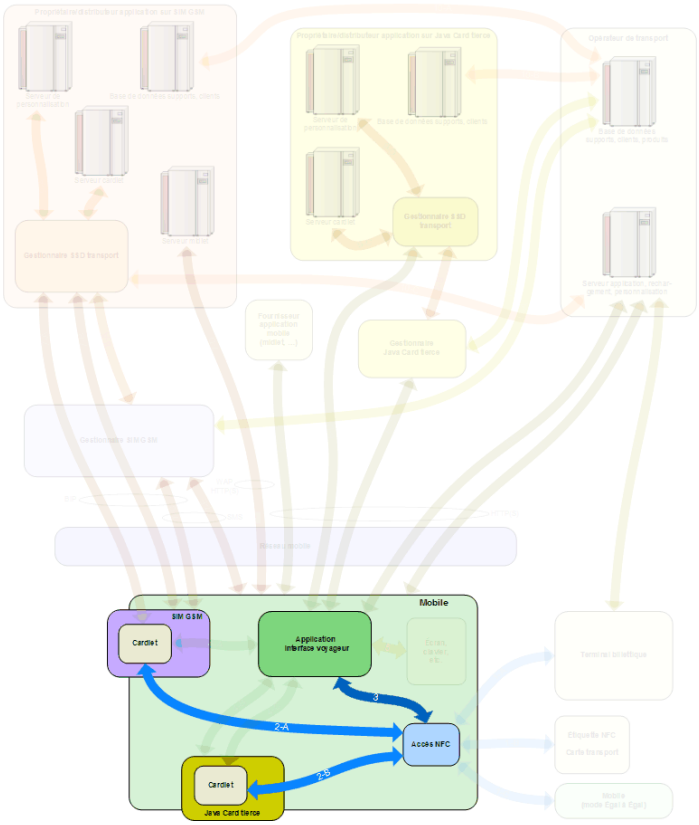
Les différents canaux envisagés pour l'activation automatique à l'issue d'une communication sans contact lors d'une validation ou d'un contrôle sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Notes :

- Le module transport doit contenir toutes les informations nécessaires à l'IHM du mobile pour la gestion des interactions qui découlent de son activation. Elles peuvent y avoir été inscrites par exemple lors du chargement, de la personnalisation, de la gestion du module transport, ou lors de la transaction sans contact qui a déclenché l'activation de l'IHM du mobile.

- Selon les circonstances, cette activation, et les interactions avec l'IHM du mobile qui en découlent, peuvent être remplacées par des interactions via l'IHM du terminal billettique, hors du périmètre de ce document.

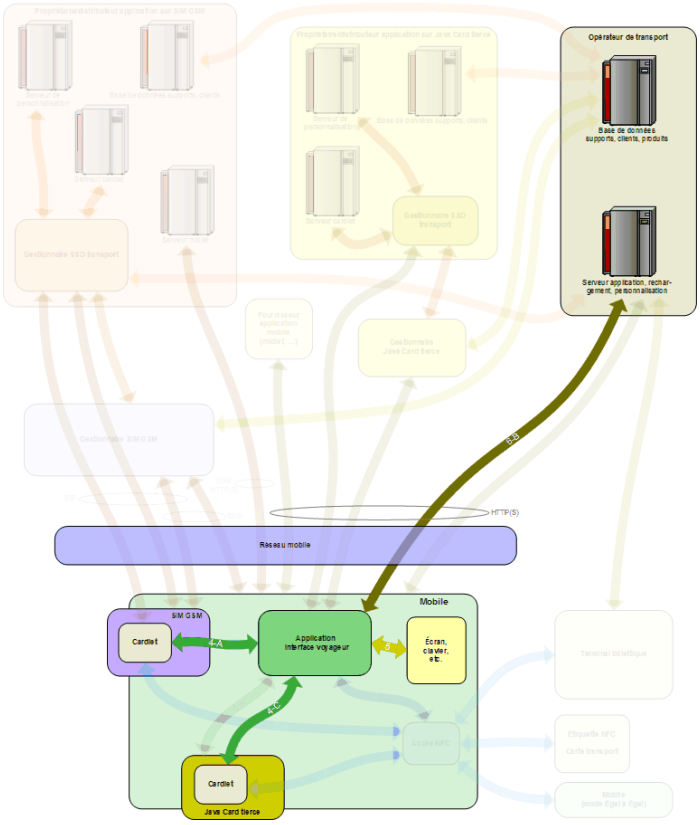
Action	Interfaces
À l'issue d'une action de validation ou de contrôle, le module transport demande au module d'interface NFC l'activation du logiciel du mobile afin qu'il puisse ensuite procéder à des interactions via l'IHM du mobile.	2 : NFC du module transport 3 : Logiciel du mobile / accès NFC



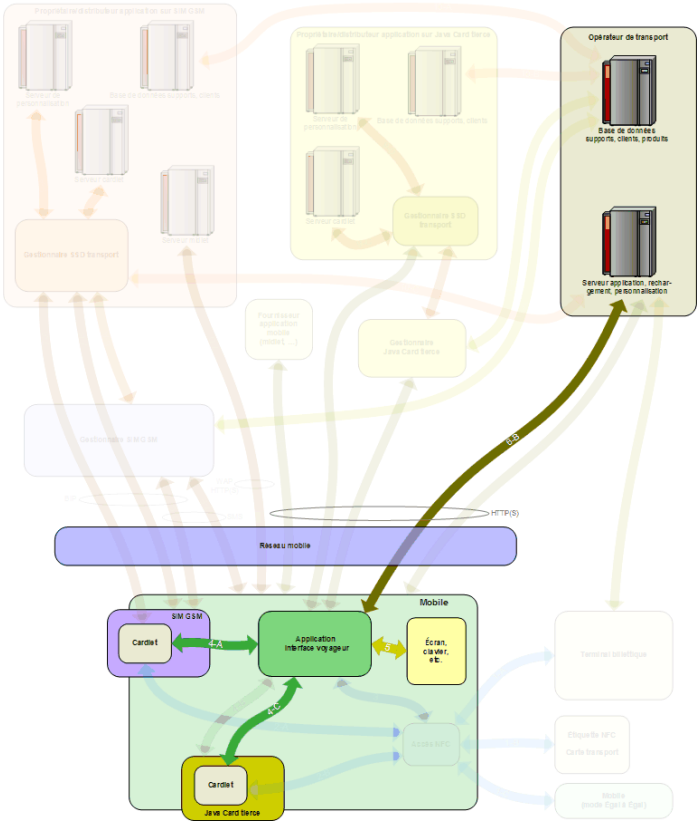
4.5.2.4 VALIDATION OU CONTROLE : INTERACTIONS INTERMEDIAIRES OU FINALES AVEC LE VOYAGEUR VIA L'IHM DU MOBILE

Les différents canaux envisagés pour les interactions via l'IHM du mobile consécutives à une activation automatique à l'issue d'une communication sans contact lors d'une validation ou d'un contrôle sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

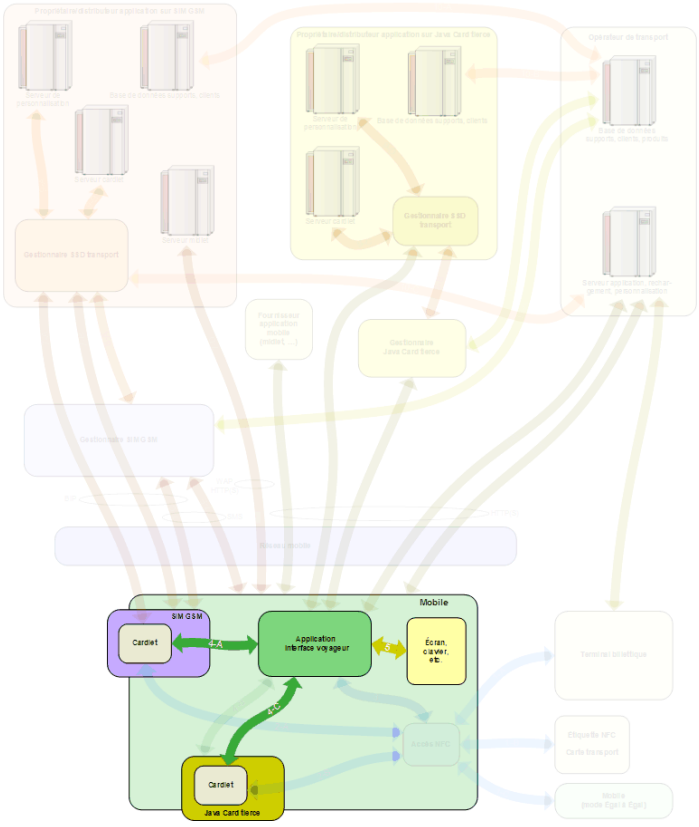
Interactions intermédiaires ou finales via l'IHM du mobile	Action	Interfaces
Validation avec conflit	Lecture du module transport par le logiciel du mobile, pour prendre connaissance du scénario à traiter et des informations à afficher (description des titres éligibles).	4 : Module transport / logiciel du mobile
	Affichage via l'IHM du mobile des choix de résolution du conflit	5 : IHM du mobile
	Saisie via l'IHM du mobile du titre à valider.	5 : IHM du mobile
	Inscription dans le module transport par le logiciel du mobile des données correspondant au choix effectué, éventuellement avec connexion au SI transport (serveur de rechargement ou de personnalisation) pour sécurisation de cette inscription.	4 : Module transport / logiciel du mobile 5 : IHM du mobile 6-B : Logiciel du mobile / SI transport



Interactions intermédiaires ou finales via l'IHM du mobile	Action	Interfaces
Confirmation d'une nouvelle validation pour un voyage à plusieurs	Lecture du module transport par le logiciel du mobile, pour prendre connaissance du scénario à traiter et des éventuelles informations à afficher (description du titre à valider).	4 : Module transport / logiciel du mobile
	Éventuellement, affichage du titre à valider ou de la demande de confirmation.	5 : IHM du mobile
	Saisie de la confirmation par le voyageur.	5 : IHM du mobile
	Inscription dans le module transport par le logiciel du mobile des données correspondant à la confirmation, éventuellement avec connexion au SI transport (serveur de rechargement ou de personnalisation) pour sécurisation de cette inscription.	4 : Module transport / logiciel du mobile 5 : IHM du mobile 6-B : Logiciel du mobile / SI transport



Interactions intermédiaires ou finales via l'IHM du mobile	Action	Interfaces
Affichage de la photo, d'informations ou de requêtes	Lecture du module transport par le logiciel du mobile, pour prendre connaissance du scénario à traiter et des éventuelles informations à afficher (photo, etc.).	4 : Module transport / logiciel du mobile
	Éventuellement, affichage d'informations ou de requêtes.	5 : IHM du mobile
	Éventuellement, saisie d'un choix par le voyageur.	5 : IHM du mobile
	Éventuellement, tout traitement déterminé par les étapes précédentes (par exemple la gestion des données transport par le voyageur), hors du périmètre de ce chapitre.	-



4.6 FONCTION - GESTION DES DONNEES TRANSPORT PAR LE VOYAGEUR

4.6.1 CAS D'UTILISATION

L'application d'interface voyageur du mobile NFC permet d'accéder aux informations présentes dans l'application billettique, pour :

- consulter ses données personnelles (numéro de client, âge, sexe, photo, etc.), ses droits (profils et titres) et ses derniers trajets (événements) ;
- inscrire une pré-sélection d'utilisation d'un titre (nombre de zones, distance, etc.), pour la prochaine validation ;
- inscrire une pré-sélection de titre ou de nombre de voyageurs, pour la prochaine validation ;
- effectuer une sauvegarde du contenu de l'application billettique, OTA ou via les équipements d'un bassin de transport ;

- supprimer tout ou partie du contenu de l'application billettique, OTA ou via les équipements d'un bassin de transport ;
- supprimer l'application transport (application d'interface voyageur et application billettique) ;
- restaurer une sauvegarde, OTA ou via les équipements d'un bassin de transport.

De plus, lorsque qu'un mobile contient plusieurs applications billettiques (éventuellement dans des modules transport différents) correspondant à l'AID utilisé par les valideurs, l'utilisateur peut choisir celle qui sera sélectionnée à la prochaine validation, si le mobile et le (ou les) module transport le permettent. Cette fonction ne mettant pas en œuvre d'interface spécifique à la billettique, elle n'est pas traitée dans la description des échanges (chapitre 4.6.2).

Note concernant la pré-sélection d'application
La pré-sélection d'application nécessite la capacité pour le mobile NFC à recenser les applications billettiques de tous ses modules transport, et à fixer des priorités entre celles en conflit potentiel d'AID (applications dont au moins les 5 premiers octets d'AID sont identiques). À notre connaissance, actuellement aucun standard, mobile NFC ni module transport ne permet cette fonction, elle n'est donc pas considérée dans ce chapitre. Toutefois, GlobalPlatform étudie cette possibilité (cf. *GlobalPlatform Mobile Task Force – Requirements for NFC Mobile: Management of Multiple Secure Elements – Version 1.0*, [25]), mais les spécifications correspondantes ne sont pas publiées.

Note concernant la pré-sélection et la suppression des données billettiques en mode push
La pré-sélection et la suppression des données billettiques en mode push ne sont pas considérées dans ce chapitre car elles mettent toujours en œuvre une interaction avec le voyageur et la connexion avec le SI transport, qui est alors disponible pour réaliser également les échanges d'APDU avec le module transport.

Note concernant la gestion des données billettiques via l'opérateur télécom
La gestion des données billettiques via l'opérateur télécom n'est pas disponible actuellement (interface 7-A indisponible, voir notes du chapitre 3.6.7). Par conséquent, cette méthode n'est pas considérée dans ce chapitre.

Notes :

- La suppression d'une application transport ne doit être possible que par le voyageur, dûment authentifié par le SI transport. C'est également le cas pour une demande de restauration nécessitant une suppression préalable.
- La suppression (et la restauration) de l'application billettique n'est possible que lorsque le module transport est une Java Card.
- La suppression d'une application transport doit être signifiée au SI transport, afin qu'il puisse entreprendre les opérations techniques et commerciales nécessaires. En particulier, il peut être nécessaire d'en informer le gestionnaire du SSD transport et le gestionnaire du module transport.
- La suppression est réalisée par communication OTA avec le gestionnaire SSD transport et si nécessaire le gestionnaire du module transport, qui en informent le SI transport.

- Lors de la suppression du dernier cardlet d'un package, le gestionnaire SSD transport supprime également le package.
- Lors de la suppression du dernier package d'un SSD transport, le gestionnaire SSD transport en informe le gestionnaire du module transport, qui le supprime.
- La restauration de l'application transport mettant en œuvre les mêmes mécanismes que son chargement initial, décrit au chapitre 4.2, elle n'est pas détaillée dans ce chapitre.

Note concernant la suppression de l'application billettique suite à la demande de suppression de l'application transport

Dans certains OS de mobiles (par exemple Java ME), il est possible pour une application du mobile d'être avertie qu'elle va être supprimée. Une telle application d'interface voyageur pourrait alors tenter d'avertir le SI transport de sa suppression, le SI transport pouvant alors demander au gestionnaire SSD transport de supprimer le cardlet associé (nécessite qu'avant d'être effectivement supprimée l'application d'interface voyageur reste disponible le temps nécessaire à la suppression du cardlet, et si nécessaire du package et du SSD transport).

Comme il y aura forcément des cas où la suppression du cardlet au moment de la suppression de l'application d'interface voyageur ne sera pas possible – parce que le mobile ne le permet pas, ou parce que la tentative a échoué (par exemple s'il n'y a pas de connexion GSM possible à ce moment) et que l'application d'interface voyageur a été malgré tout supprimée – une procédure de suppression a posteriori des applications billettiques « orphelines » doit être mise en place.

Par exemple, lors d'une tentative de chargement d'un nouveau cardlet il serait demandé à l'utilisateur de choisir les cardlets inutiles (éventuellement avec sauvegarde avant suppression). Pour aider le voyageur, l'application d'interface voyageur utilisée pour charger la nouvelle application billettique pourrait recenser les applications billettiques déjà présentes dans le module transport, et grâce à leur AID indiquer au voyageur à quel réseau de transport elles sont associées.

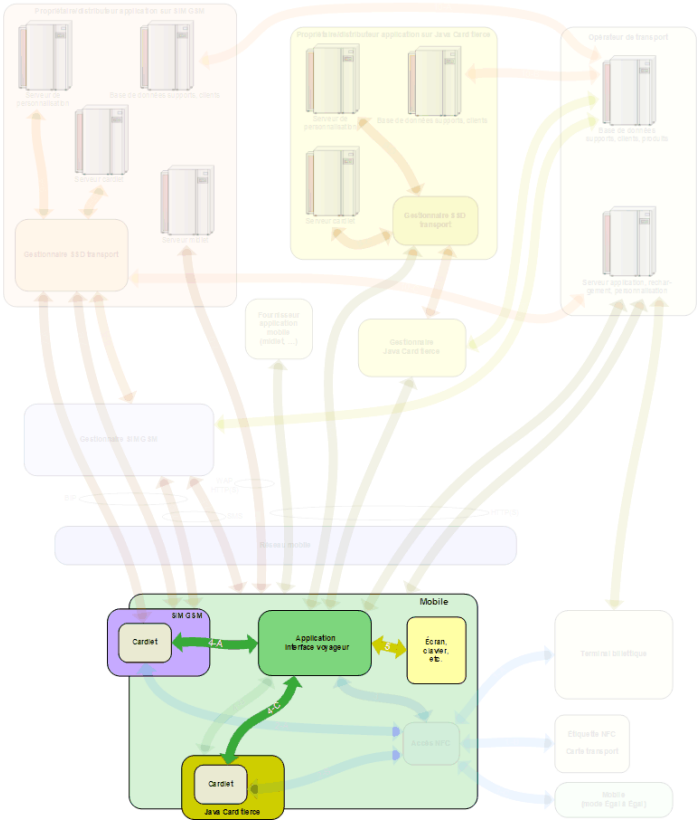
Note concernant la suppression de l'application transport via un terminal du bassin de transport
Actuellement il n'existe ni standard, ni norme, ni spécification, ni produit permettant au logiciel du mobile de communiquer via le canal NFC (cf. §3.6.2). La suppression de l'application d'interface voyageur via un terminal du bassin de transport décrit dans le DoFoCo (§7.2.2.4, page 59) n'est donc pas disponible à court terme. Par conséquent, la suppression de l'application transport par l'interface NFC n'est pas considérée dans ce chapitre.

4.6.2 DESCRIPTION DES ECHANGES

4.6.2.1 CONSULTATION SUR LE MOBILE NFC

Les actions réalisées et interfaces mises en œuvre lors de la consultation des données de l'application billettique sur le mobile NFC sont décrits dans le tableau et le diagramme ci-dessous.

Action	Interfaces
Activation par le voyageur de l'application d'interface voyageur du mobile, et demande de consultation de données de l'application billettique : données personnelles (numéro de client, âge, sexe, photo, etc.), droits (profils et titres) et derniers trajets (événements).	5 : IHM du mobile
Lecture des données de l'application billettique.	4 : Module transport / logiciel du mobile
Présentation des données sur mobile.	5 : IHM du mobile

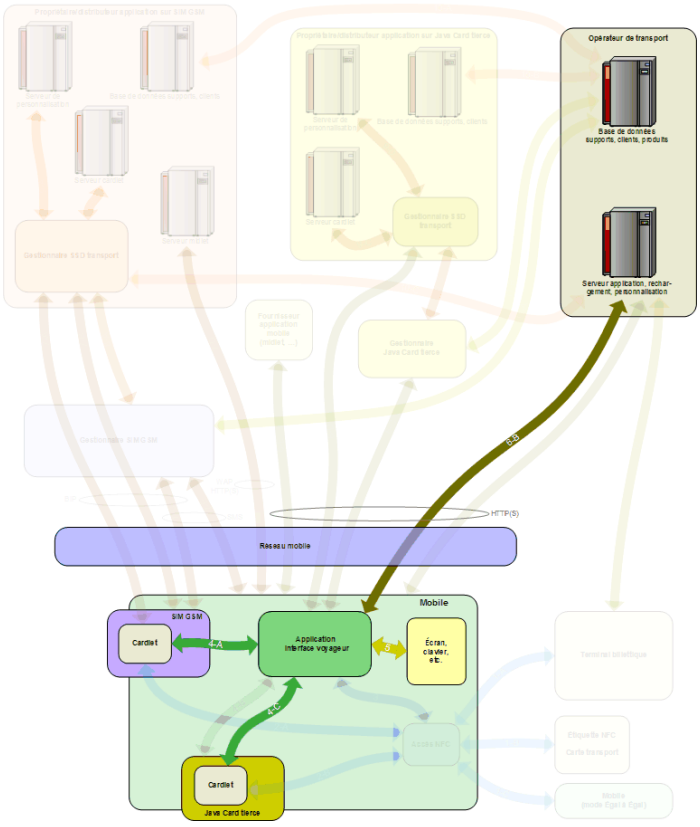


Note : Pour ce cas, l'application d'interface voyageur du mobile contient tous les paramètres de tarification à jour.

4.6.2.2 PRE-SELECTION DE DONNEES AVANT VALIDATION

Les actions réalisées et les interfaces mises en œuvre lors d'une une pré-sélection d'utilisation d'un titre, et d'une pré-sélection de titre ou de nombre de voyageurs sont décrites dans le tableau et le diagramme ci-dessous.

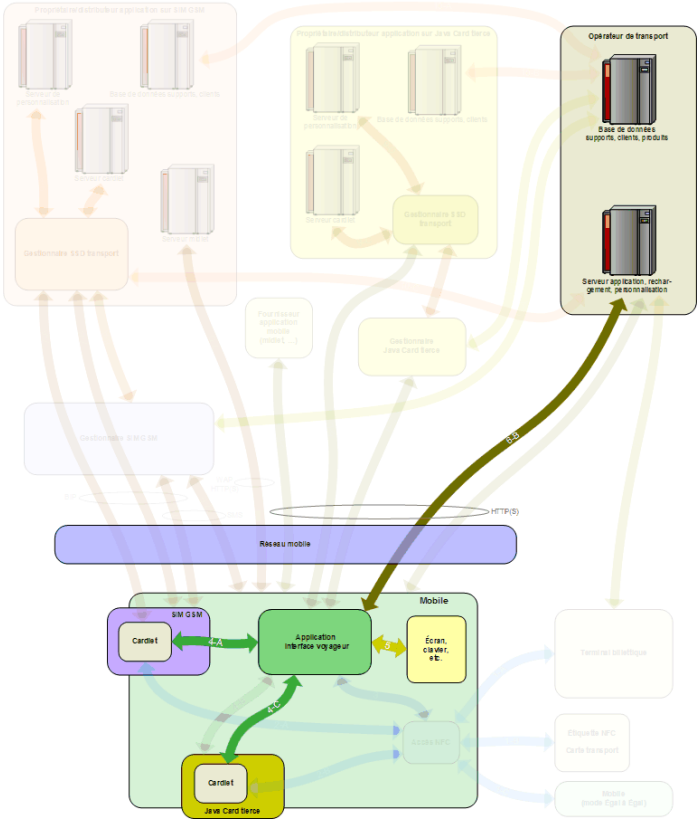
Action	Interfaces
Activation par le voyageur de l'application d'interface voyageur du mobile, et choix de l'action souhaitée.	5 : IHM du mobile
Si nécessaire, lecture des données de l'application billettique à traiter, et présentation au voyageur.	4 : Module transport / logiciel du mobile 5 : IHM du mobile
Si nécessaire, confirmation par le voyageur des actions à effectuer.	5 : IHM du mobile
Modification des données de l'application billettique.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport



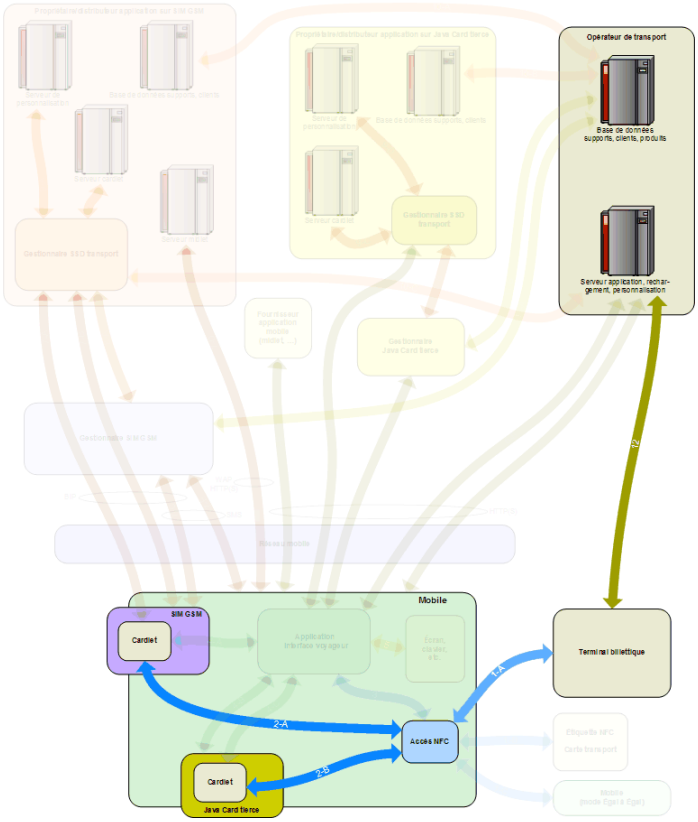
4.6.2.3 SAUVEGARDE, RESTAURATION OU SUPPRESSION DE DONNEES DE L'APPLICATION BILLETTIQUE

Les actions réalisées et les interfaces mises en œuvre lors d'une sauvegarde, d'une suppression ou d'une restauration des données de l'application billettique sont décrites dans les tableaux et diagrammes ci-dessous.

Sauvegarde, restauration, suppression de données	Action	Interfaces
OTA mode pull	Activation par le voyageur de l'application d'interface voyageur du mobile, et choix de l'action souhaitée.	5 : IHM du mobile
	Identification du voyageur par le SI transport, par exemple par présentation d'un mot de passe.	5 : IHM du mobile 6-B : Logiciel du mobile / SI transport
	Modification (restauration, suppression) ou lecture (sauvegarde) sécurisée dans le module transport des données de l'application billettique.	4 : Module transport / logiciel du mobile 6-B : Logiciel du mobile / SI transport



Sauvegarde, restauration, suppression de données	Action	Interfaces
Via interface NFC	Le processus détaillé, identique à celui d'une carte sans contact, est hors du périmètre de ce document. Ce processus doit être possible sans fourniture d'énergie par le mobile.	1-A : NFC externe, Mode Carte 2 : NFC du module transport 12 : Terminal billettique / SI transport



4.6.2.4 SUPPRESSION D'APPLICATION TRANSPORT

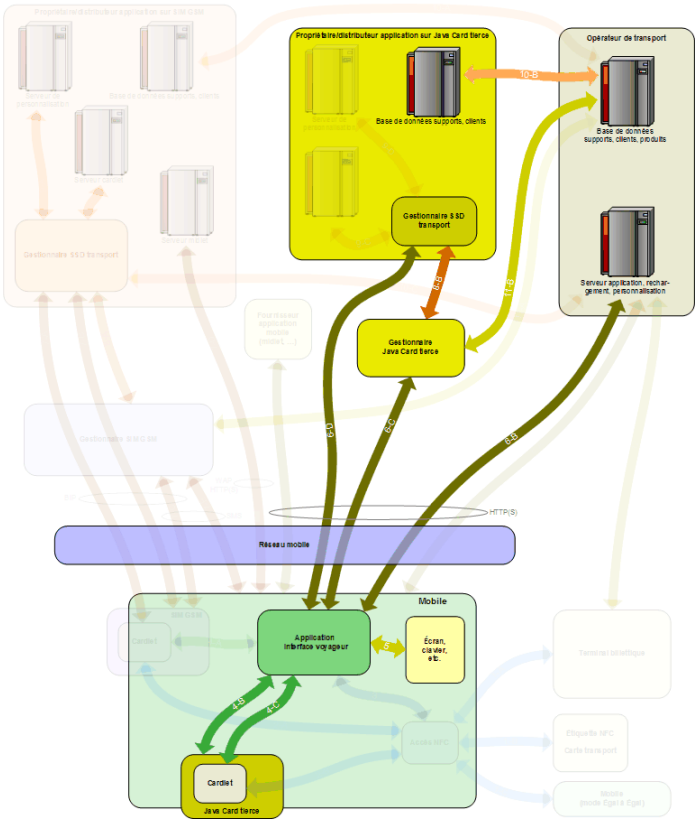
Les différents canaux envisagés pour la suppression de l'application transport sont décrits dans les tableaux et diagrammes ci-dessous, avec indication des actions et des interfaces mis en œuvre.

Suppression d'application transport	Action	Interfaces
OTA, mode pull avec une Java Card tierce [34]	En utilisant les fonctions de base de l'OS du mobile NFC, le voyageur demande la suppression ou la mise à jour de l'application d'interface voyageur [35].	5 : IHM du mobile
	Si possible, l'OS du mobile informe l'application d'interface voyageur qu'elle va être supprimée : l'application d'interface voyageur se connecte au SI transport et l'informe de sa suppression. Sinon, passer directement à la dernière étape.	6-B : Logiciel du mobile / SI transport
	Par l'intermédiaire de l'application d'interface voyageur, le SI transport invalide l'application billettique.	4-C : Cardlet carte tierce / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Le SI transport met l'application d'interface voyageur en relation avec le gestionnaire de SSD transport pour suppression de cardlet. Le gestionnaire SSD transport supprime l'application billettique et si nécessaire son package, puis il en informe le SI transport.	4-B : Carte tierce / logiciel du mobile 6-B : Logiciel du mobile / SI transport 6-D : Logiciel du mobile / gestionnaire SSD transport Java Card tierce 10-B : SI transport / prop./distrib. application Java Card tierce
	Option (si suppression du SSD transport) : Le gestionnaire SSD transport met l'application d'interface voyageur en relation avec le gestionnaire du module transport pour suppression de SSD, et en informe le SI transport. Le gestionnaire du module transport supprime le SSD transport, et en informe le SI transport.	4-B : Carte tierce / logiciel du mobile 6-C : Logiciel du mobile / gestionnaire Java Card tierce 6-D : Logiciel du mobile / gestionnaire SSD transport Java Card tierce 8-B : Gestionnaire Java Card tierce / gestionnaire SSD transport Java Card tierce 10-B : SI transport / prop./distrib. application Java Card tierce 11-B : SI transport (base de données supports, clients) / gestionnaire Java Card tierce

[34] Non disponible pour le cas de la SIM GSM (cf. spécifications Ulysse).

[35] Cette action du voyageur peut être consécutive à un message de l'opérateur de transport demandant par exemple de procéder à la mise à jour pour correction de problèmes.

	L'application d'interface voyageur accepte sa demande de suppression, et l'OS du mobile la supprime. Les différents systèmes impliqués ont enregistré la suppression de l'application billettique, éventuellement du package et du SSD, et l'entérinent par une gestion ad hoc de l'identifiant technique du module et de l'identifiant transport de l'application supprimée.	-



Notes :

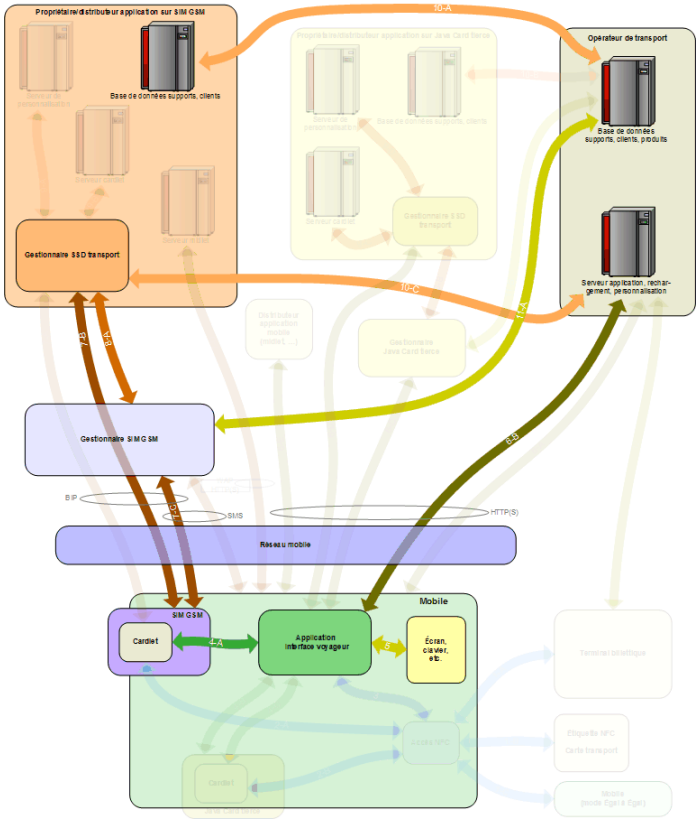
- Ces échanges ne s'appliquent que lorsque la carte tierce est conforme aux spécifications GlobalPlatform et Java Card. Ils peuvent néanmoins être transposés à d'autres cas de carte tierce dans laquelle une application billettique est téléchargeable.
- D'autres scénarios sont possibles. Par exemple :
  - Le déroulement pourrait se faire en deux actions du voyageur, dans un premier temps via l'application d'interface voyageur il déclenche l'invalidation de l'application billettique et sa suppression, puis via l'OS du mobile il supprime l'application d'interface voyageur.
  - Les échanges sur les interfaces 6-C/6-D pourraient être remplacés par des échanges via le SI transport (interfaces 10-C/11-B + 6-A).
- Pour une carte tierce, le mode push ne met pas en œuvre d'interface spécifique (mêmes interfaces qu'en mode pull ci-dessus), il n'est donc pas détaillé.

Suppression d'application transport	Action	Interfaces
OTA, mode push avec une SIM GSM	En utilisant les fonctions de base de l'OS du mobile NFC, le voyageur demande ou la suppression ou la mise à jour de l'application d'interface voyageur [36].	5 : IHM du mobile
	Si possible, l'OS du mobile informe l'application d'interface voyageur qu'elle va être supprimée : l'application d'interface voyageur se connecte au SI transport et l'informe de sa suppression. L'application d'interface voyageur accepte sa demande de suppression, et l'OS du mobile la supprime.	6-B : Logiciel du mobile / SI transport
	Par l'intermédiaire de l'application d'interface voyageur, le SI transport invalide l'application billettique.	4-A :Cardlet SIM GSM / logiciel du mobile 6-B : Logiciel du mobile / SI transport
	Sinon l'application d'interface voyageur a informé le SI transport, il demande au gestionnaire SSD transport SIM GSM la suppression de l'application billettique (cible identifiée par son ID_TECH). Sinon, l'application billettique sera supprimée ultérieurement [37] (la suite de ce tableau s'appliquera à ce moment).	10-A : SI transport / propriétaire/distributeur application SIM GSM
	Établissement d'une session BIP (mode « single SD with DAP » ou mode « Delegated Management », cf. spécifications Ulysse).	7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP) 7-C : SIM GSM / gestionnaire SIM GSM 8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM
	Suppression de l'application billettique, et si nécessaire du package et du SSD.	7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP) 7-C : SIM GSM / gestionnaire SIM GSM 8-A : Gestionnaire SIM GSM / gestionnaire SSD transport SIM GSM
	Fermeture de session BIP.	7-B : SIM GSM / gestionnaire SSD transport SIM GSM (BIP)
	Le propriétaire/distributeur application SIM GSM informe le SI transport de la suppression de l'application. Si nécessaire, le gestionnaire SIM GSM informe le SI transport de la suppression du SSD transport.	10-A : SI transport / prop./distrib. application SIM GSM 11-A : SI transport / gestionnaire SIM GSM

[36] Cette action du voyageur peut être consécutive à un message de l'opérateur de transport demandant par exemple de procéder à la mise à jour pour correction de problèmes.

[37] Lorsqu'une nouvelle application billettique devra être chargée dans la SIM GSM alors que la place disponible y est insuffisante, et que le voyageur aura choisit de supprimer cette application billettique désormais orpheline.

	Les différents systèmes impliqués ont enregistré la suppression de l'application billettique, éventuellement du package et du SSD, et l'entérinent par une gestion ad hoc de l'ID_TECH et de l'identifiant transport de l'application supprimée.	-



Note : D'autres scénarios sont possibles. Par exemple, le déroulement pourrait se faire en deux actions du voyageur (comme décrit dans Ulysse), dans un premier temps via l'application d'interface voyageur il déclenche l'invalidation de l'application billettique et sa suppression, puis via l'OS du mobile il supprime l'application d'interface voyageur.

4.7 FONCTION - SERVICE APRES-VENTE (SAV)

Les fonctions de SAV spécifiques à la billettique et mettant directement en œuvre le mobile NFC sont les suivantes :

- diagnostic à distance ou via les équipements d'un bassin de transport : même interfaces mises en œuvre que la sauvegarde des données billettiques (chapitre 4.6) ;
- sauvegarde : voir le chapitre 4.6 ;
- reconstitution à distance ou via les équipements d'un bassin de transport de l'application transport : même interfaces mises en œuvre que le chargement de l'application transport (chapitre 4.2) ;
- reconstitution à distance ou via les équipements d'un bassin de transport des données de l'application billettique : même interfaces mises en œuvre que la restauration de données billettiques (chapitre 4.6) ;
- blocage du module transport : non défini.

Les autres fonctions de SAV n'entrent pas dans le périmètre du présent document, donc toutes les fonctions du SAV sont couvertes par les chapitres précédents.

Note : Contrairement à ce qu'envisage le DoFoCo (§4.4, §7.1.2.5, §7.7.1.2 et §7.7.2), comme indiqué au chapitre 3.3 le module transport ne peut pas être un module logiciel chargé dans le mobile.

4.8 FONCTION - MODES DEGRADES

Il n'y a pas de mise en œuvre d'interface pour ce chapitre, car dans le DoFoCo (§7.8) il s'agit uniquement d'une liste des fonctions précédemment décrites avec indications de leur possible indisponibilité.

Note : Les modes dégradés liés à l'absence de réseau GSM peuvent dans certains cas être compensés par la présence d'un réseau Wifi, parfois même de manière transparente (le mobile basculant automatiquement les échanges http(s) du GSM au Wifi et réciproquement).

5 MISE A JOUR D'UN SYSTEME BILLETTIQUE EXISTANT POUR LE TRAITEMENT DES MOBILES NFC

5.1 CONTRAINTES TECHNIQUES DE GESTION DES MOBILES NFC

Pour accepter les mobiles NFC, un système télébillettique doit accepter les objets portables conformes à l'ISO 14443.

Pour traiter les applications Calypso, il est recommandé d'être conforme à la révision 3 de Calypso, seule solution assurant l'interopérabilité complète entre les systèmes billettiques :

- Calypso Revision 3, Portable Object Application, réf. : *060708-CalypsoAppli* (documents [14] et [15]).
- Reader Recommendations, ref : *091018-CalypsoReaderRecommendations* (document [18]).

Optionnellement, la mise à jour de tous les SAM du système peut être réalisée afin d'optimiser le fonctionnement avec les mobiles NFC en ajoutant des clés Triple-DES au système billettique.

Dans tous les cas, il est utile de tester les terminaux dans différentes configurations d'objets portables (natif, Java Card, DESX, Triple-DES, etc.).

Utiliser un mode de compatibilité MIFARE Classic ou un protocole B' pour un système billettique donné empêchera d'utiliser le mobile pour d'autres applications NFC, y compris pour d'autres applications billettiques.

5.2 SYSTEME N'ACCEPTANT QUE LES CARTES MIFARE CLASSIC

Pour accepter les mobiles NFC dans un système n'acceptant que des cartes MIFARE Classic, une mise à jour importante des équipements du système billettique est nécessaire car il est nécessaire d'accepter les objets portables normalisés (ISO 14443), de traiter l'application billettique interopérable (par exemple : l'application Intercode instanciée régionalement), et de réaliser les traitements correspondants dans les systèmes centraux.

Les travaux suivants sont nécessaires :

- Mise à jour du logiciel de tous les équipements afin de traiter les exigences applicatives correspondantes (voir section 5.1).
- Mise à jour de tous les SAM du système afin de traiter des clés Triple-DES.

Afin d'assurer la compatibilité avec les mobiles NFC, ces travaux de mise à jour doivent tenir compte des présentes spécifications, ainsi que des documents cités en référence.

Remarque : il est techniquement possible d'utiliser un mode de compatibilité MIFARE Classic offert par certains mobiles NFC pour utiliser le mobile avec le système billettique. Toutefois, cela doit être évité pour la raison suivante :

- Tous les mobiles n'offrent pas un tel fonctionnement non normalisé « MIFARE Classic ».

5.3 SYSTEME N'ACCEPTANT LES CARTES CALYPSO QU'EN PROTOCOLE B'

Pour accepter les mobiles NFC dans un système ne traitant pas l'ISO 14443, les travaux techniques suivants sont nécessaires :

- Mise à jour de tous les terminaux du ou des réseaux concernés afin d'accepter l'ISO 14443. Cette mise à jour peut entrainer une modification matérielle si les équipements en service ne permettent pas la gestion de ce standard.

- Mise à jour du logiciel de tous les équipements afin de traiter les exigences applicatives correspondantes (voir section 5.1).
- Optionnellement : mise à jour de tous les SAM du système afin de traiter des clés Triple-DES.

5.4 SYSTEME ACCEPTANT LES CARTES CALYPSO EN PROTOCOLE ISO 14443

Pour accepter les mobiles NFC, les travaux techniques suivants sont nécessaires :

- Vérification, et mise à jour éventuelle de tous les équipements, afin de traiter les contraintes applicatives correspondantes (voir section 5.1), en particulier :
  - Définir un identifiant d'application unique pour l'application billettique interopérable (cf. Norme Intercode NF P99-405, décembre 2009).
  - Envoyer SELECT APPLICATION avec la classe 00h.
  - Utiliser et transmettre au SAM le numéro de série Calypso retourné par SELECT APPLICATION et non un numéro déduit du processus d'anticollision.
  - Traiter la ratification par envoi de commande et non par la déconnexion radio.
- Optionnellement : mise à jour de tous les SAM du système afin de traiter des clés Triple-DES.

La spécification Calypso Révision 3 intègre ces exigences.

6 ANNEXES

6.1 SYNTHESE

Les services sur mobile NFC sont en phase de développement, et particulièrement pour la billettique. De nombreux standards nécessaires n'existent pas encore.

Pour la mise en œuvre de la billettique sur mobile NFC, il peut donc être inévitable d'utiliser des solutions techniques spécifiques ou propriétaires, comme résumé pour chaque interface dans le tableau ci-dessous :

Interface	Solutions techniques spécifiques ou propriétaires	Fonctions associées
1 : Interface NFC du mobile	Protocole Innovatron ou MIFARE Classic lorsque la compatibilité avec les terminaux installés est nécessaire.	Utilisation d'un terminal billettique.
2 : Module transport / module d'interface NFC	Aiguillage vers une carte tierce des échanges NFC gérés par un module d'interface NFC interne au mobile.	Tous échanges avec l'application billettique via NFC.
	Module d'interface NFC amovible (tous types : microSD, Bluetooth, etc.).	Tous échanges via NFC.
3 : Logiciel du mobile / NFC	Module d'interface NFC interne : aiguillage des échanges NFC vers le logiciel du mobile.	Chargement et gestion de l'application transport via un terminal billettique. Transfert de titres.
	Module d'interface NFC amovible (tous types : microSD, Bluetooth, etc.).	
	Interface non disponible.	Mobile utilisé comme un terminal billettique.
	Gestion de la priorité d'applications billettiques d'AID en conflit.	Pré-sélection d'application
	Activation et gestion de l'IHM du mobile suite à une transaction NFC.	Choix à effectuer par le voyageur après une première validation. Contrôle du titre ou de la photo sur le mobile. Affichage d'informations suite à une validation.
4 : Module transport / logiciel du mobile	JSR177 (SATSA-APDU) non disponible.	Tous échanges entre l'application d'interface voyageur et le module transport ou l'application billettique.
	Carte tierce amovible (tous types : microSD, Bluetooth, etc.).	
5 : Dispositifs d'interface homme machine (IHM)	Java ME non disponible	Toutes fonctions de l'application d'interface voyageur.
	JSR118 non disponible	
6 : Mobile / SI non télécom	Processus de téléchargement d'application du mobile	Chargement et gestion de l'application d'interface voyageur.
	Processus de rechargement à distance non Calypso.	Toutes sessions Calypso réalisées OTA : mise à jour du profil, vente à distance, pré-sélection, transfert de titres, mobile utilisé comme un terminal billettique, etc.
	Mode push.	Toutes fonctions en mode push avec une carte tierce.

7 : OTA via l'opérateur télécom	Échanges ISO 7816-4 avec l'application billettique. Processus de rechargement à distance non Calypso.	Toutes sessions Calypso réalisées OTA : mise à jour du profil, vente à distance, pré-sélection, transfert de titres, mobile utilisé comme un terminal billettique, etc.
8 : gestionnaire SIM / gestionnaire SSD transport	Cas de la carte tierce : mode d'échange des commandes GlobalPlatform entre le gestionnaire de la carte et le gestionnaire du SSD transport.	Chargement et gestion de l'application transport.
9 : Gestionnaire SSD / serveurs internes	-	-
10 : SI transport / SI gestionnaire de modules transport	-	-
11 : SI transport / gestionnaire Java Card	Carte tierce : gestion de l'identifiant technique.	Chargement et gestion de l'application transport.
12 : terminal billettique / SI transport	Processus de rechargement à distance non Calypso.	Toutes sessions Calypso réalisées à on-line sur un terminal billettique : mise à jour du profil, rechargement, etc.

Afin de faciliter l'analyse des solutions techniques proposées par les différents fournisseurs (mobiles, modules transport, etc.), le chapitre suivant (6.2) propose un modèle de tableau permettant d'indiquer pour chaque fonction si elle est disponible pour la solution proposée.

6.2 TABLEAU DE DISPONIBILITE DE FONCTIONS

Lorsque qu'un fournisseur de solution ou de sous-ensemble propose un produit, il indique (sur le modèle du tableau ci-dessous) pour chaque cas d'utilisation de chaque fonction s'il est disponible ou non (date s'il y a lieu), ainsi que les éventuelles références techniques associées (spécifications, standards, etc.).

Fonction	Cas d'utilisation					Disponible ?	Références techniques
Accès au service	*(Non spécifique à la billettique sur mobile NFC.)*						
Chargement de l'application transport	Requête de chargement	Depuis un mobile NFC					
		Depuis Internet					
		Via un tag NFC	Url				
			N° court SMS	Url			
				Application du mobile			
			Application du mobile				
		Via un numéro SMS	Url				
			Application du mobile				
		Depuis les équipements transport					
	Chargement de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull			
				Mode push *(non disponible)*			
			Via l'opérateur télécom	Mode pull			
				Mode push			
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)				
			Via l'opérateur télécom (SIM GSM)				
		Depuis les équipements transport *(non disponible)*					
Personnalisation	Attribution de profil *(non spécifique à la billettique sur mobile NFC)*						
	Signalement d'événement *(non spécifique à la billettique sur mobile NFC)*						
	Mise à jour	Depuis les équipements transport					
		Mode pull : via l'application d'interface voyageur					
		Mode push	Via l'opérateur télécom *(non disponible)*				
			Via l'application d'interface voyageur				
Distribution de titres	Sélection	Depuis le mobile	Sans connexion				
			Avec connexion				
		Depuis Internet	Identification manuelle				
			Identification OTA mode pull				
			Identification OTA mode push	SIM GSM *(non disponible)*			
				Carte tierce			
		Depuis les équipements transport					
		Depuis un tag NFC	Url				
			N° court SMS	Url			
				Application d'interface voyageur			
			Application d'interface voyageur				
		Par saisie de n° court SMS	Url				
			Application d'interface voyageur				
	Paiement *(Non spécifique à la billettique sur mobile NFC.)*						

	Chargement	OTA mode pull				
		OTA mode push	Via l'opérateur télécom *(non disponible)*			
			Via l'application d'interface voyageur			
		Depuis les équipements transport				
	Transfert de titres	Vers un support sans contact, en Mode Carte				
		Vers un autre mobile, en Mode Égal à Égal				
	Interface de vente	Avec un support sans contact, en Mode Carte				
		Avec un autre mobile, en Mode Égal à Égal				
Validation et contrôle	Validation simple					
	Conflit à la validation	Sélection préalable	Sur le terminal de validation			
			Sur le mobile			
		Sélection sur mobile après une validation				
	Validation multi-voyageurs, titre unique	Validation unique simple				
		Sélection préalable sur mobile				
		Sélection sur terminal après une validation				
		Validations multiples	Simples			
			Avec confirmation sur le mobile			
	Validation multi-voyageurs, titres multiples : voir gestion des données					
	Contrôle	Simple				
		Avec affichage de la photo	Sur le terminal de contrôle			
			Sur le mobile			
		Avec NFC défectueux				
Gestion des données par le voyageur	Consultation sur le mobile					
	Pré-sélection de données avant validation	OTA				
		Depuis les équipements transport				
	Pré-sélection d'application (*non disponible*)					
	Sauvegarde, restauration ou suppression des données billettiques	OTA	Via l'application d'interface voyageur			
			Via l'opérateur télécom *(non disponible)*			
		Depuis les équipements transport				
	Suppression de l'application transport	OTA , Carte tierce				
		OTA , SIM GSM	Via l'application d'interface voyageur			
			Via l'opérateur télécom *(non disponible)*			
		Depuis les équipements transport *(non disponible)*				
	Restauration de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull		
				Mode push *(non disponible)*		
			Via l'opérateur télécom	Mode pull		
				Mode push		
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)			
			Via l'opérateur télécom (SIM GSM)			
		Depuis les équipements transport *(non disponible)*				
Service après-vente	Diagnostic ou sauvegarde	OTA	Via l'application d'interface voyageur			
			Via l'opérateur télécom *(non disponible)*			
		Depuis les équipements transport				
	Reconstitution de	OTA,	Via l'OS du	Mode pull		

	l'application transport	application d'interface voyageur	mobile	Mode push *(non disponible)*		
			Via l'opérateur télécom	Mode pull		
				Mode push		
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)			
			Via l'opérateur télécom (SIM GSM)			
		Depuis les équipements transport *(non disponible)*				
	Reconstitution de l'application transport	OTA, application d'interface voyageur	Via l'OS du mobile	Mode pull		
				Mode push *(non disponible)*		
			Via l'opérateur télécom	Mode pull		
				Mode push		
		OTA, application billettique	Via l'application d'interface voyageur (carte tierce)			
			Via l'opérateur télécom (SIM GSM)			
		Depuis les équipements transport *(non disponible)*				
	Reconstitution des données de l'application billettique	OTA	Via l'application d'interface voyageur			
			Via l'opérateur télécom *(non disponible)*			
		Depuis les équipements transport				
	Blocage du module transport (*non défini*)					

6.3 REFERENCES TECHNIQUES

N°	Titre	Référence
[1]	GART – DOcument FOnctionnel COmmun de la billettique sur Mobile NFC – Partie 1 – Définition et Exigences du service	DOFOCO_NFC_V1.0 du 231009 (http://www.gart.org/)
[2]	Groupe de Travail Ulysse : Billettique Transport sur téléphone sans contact – Spécifications Générales	specifications_generales_ulysse_1_1 (http://ulysse.pole-tes.com/)
[3]	Groupe de Travail Ulysse : Billettique Transport sur téléphone sans contact – Spécifications Techniques	specifications_techniques_ulysse_1_1 (http://ulysse.pole-tes.com/)
[4]	AFSCM – NFC Mobile Handset High Level Requirements	090929 - AFSCM TECH - PROC - NFC Mobile Handset High Level Requirements - V3.2 (http://www.afscm.org/)
[5]	Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 1: Caractéristiques physiques	ISO/IEC 14443-1:2008 (http://www.iso.org/)
[6]	Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 2: Interface radiofréquence et des signaux de communication	ISO/IEC 14443-2:2001 ISO/IEC 14443-2:2001/Amd 1:2005 ISO/IEC 14443-2:2001/Amd 1:2005/Cor 1:2007 (http://www.iso.org/)
[7]	Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 3: Initialisation et anticollision	ISO/IEC 14443-3:2001 ISO/IEC 14443-3:2001/Amd 1:2005 ISO/IEC 14443-3:2001/Amd 3:2006 ISO/IEC 14443-3:2001/Amd 1:2005/Cor 1:2006 (http://www.iso.org/)
[8]	Cartes d'identification -- Cartes à circuit(s) intégré(s) sans contact -- Cartes de proximité -- Partie 4: Protocole de transmission	ISO/IEC 14443-4:2008 (http://www.iso.org/)
[9]	Technologies de l'information -- Télécommunications et échange d'information entre systèmes -- Communication de champ proche -- Interface et protocole (NFCIP-1)	ISO/IEC 18092:2004 (http://www.iso.org/)
[10]	Technologies de l'information -- Télécommunications et échange d'information entre systèmes -- Interface et protocole -2 en communication de champ proche (NFCIP-2)	ISO/IEC 21481:2005 (http://www.iso.org/)
[11]	Cartes d'identification -- Cartes à circuit intégré -- Partie 3: Cartes à contacts -- Interface électrique et protocoles de transmission	ISO/IEC 7816-3:2006 (http://www.iso.org/)
[12]	Cartes d'identification -- Cartes à circuit intégré -- Partie 4: Organisation, sécurité et commandes pour les échanges	ISO/IEC 7816-4:2005 ISO/IEC 7816-4:2005/Amd 1:2008 (http://www.iso.org/)
[13]	Validator Batteryless Tag Protocol – Specifications	960613-SE-PMO-ProtBdgSP32 (http://www.CalypsoTechnology.net/)
[14]	Calypso Specification Revision 3 - Portable Object Application	060708-CalypsoAppli v3.1 (http://www.CalypsoTechnology.net/)
[15]	Calypso Specification Revision 3 - Generic Example File Structures	060709-CalypsoFiles v1.1 (http://www.CalypsoTechnology.net/)
[16]	Calypso Specification - Application Downloading	090128-ApplicationDownload v1.0 (http://www.CalypsoTechnology.net/)
[17]	Calypso Specifications - Product Remote Loading	090424-ProductRemoteLoading v1.1 (http://www.CalypsoTechnology.net/)
[18]	Calypso Specification - Reader Recommendations	091018-ReaderRecommendations v1.0 (http://www.CalypsoTechnology.net/)

[19]	Calypso Security – White Paper	080131-CalypsoSecurity v1.0 (http://www.CalypsoTechnology.net/)
[20]	CNA WG1 – WP9 – Analysis of differences between the Calypso specifications and the EMVContactless Communication Protocol Specification	D9.0A-Comparison of Calypso and EMVCo Contactless Level 1 Draft v0.93 (http://www.cnawg.net/)
[21]	EMV Contactless Communication Protocol Specification	EMV Contactless Communication Protocol V2.0.1 (http://www.emvco.com/)
[22]	Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7)	ETSI TS 102 613 V7.0.0 (http://www.etsi.org/)
[23]	Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) Release 7)	ETSI TS 102 622 V7.5.0 (http://www.etsi.org/)
[24]	GlobalPlatform Card – Contactless Services – Card Specification v2.2 - Amendment C	GPC_SPE_025 (http://www.globalplatform.org/)
[25]	GlobalPlatform Mobile Task Force – Requirements for NFC Mobile: Management of Multiple Secure Elements – Version 1.0	GP_REQ_004 (http://www.globalplatform.org/)
[26]	Java™ APIs for Bluetooth™ Wireless Technology (JSR 82) – Java™ 2 Platform, Micro Edition	JSR82-spec_1.1.1 (http://www.globalplatform.org/)
[27]	Security and Trust Services API (SATSA) for Java™ 2 Platform, Micro Edition – JSR 177	j2me_satsa-1_0-fr-spec (http://jcp.org/)
[28]	Contactless Communication API – JSR 257	jsr-257-spec-1.1 (http://jcp.org/)
[29]	Open Mobile Alliance Smartcard Web Server (SCWS)	OMA-TS-Smartcard_Web_Server-V1_0-20080421-A (http://www.openmobilealliance.org/)
[30]	NFC Forum – Type 1 Tag Operation Specification	NFCForum-TS-Type-1-Tag_1.0 (http://www.nfc-forum.org/)
[31]	NFC Forum – Type 2 Tag Operation Specification	NFCForum-TS-Type-2-Tag_1.0 (http://www.nfc-forum.org/)
[32]	NFC Forum – Type 3 Tag Operation Specification	NFCForum-TS-Type-3-Tag_1.0 (http://www.nfc-forum.org/)
[33]	NFC Forum – Type 4 Tag Operation Specification	NFCForum-TS-Type-4-Tag_1.0 (http://www.nfc-forum.org/)
[34]	NFC Forum – Smart Poster Record Type Definition	NFCForum-SmartPoster_RTD_1.0 (http://www.nfc-forum.org/)
[35]	NFC Forum – Generic Control Record Type Definition	NFCForum-TS-GenericControlRTD_1.0 (http://www.nfc-forum.org/)
[36]	Bearer Independant Protocol ; Card Application Toolkit (CAT) Release 7	ETSI TS 102 223 (http://www.etsi.org/)

Note : Les références des normes, standards ou spécifications d'usage général ne sont pas indiquées (USB, Java Card, GlobalPlatform, SD/SDIO, Bluetooth, etc.).