Annexe 3 -

Contrat de délivrance des Produits Tarifaires des Services de Mobilité du réseau TBM par les Fournisseurs de Services Numériques Multimodaux

Avril 2025

NOMS ET COORDONNEES DES CONTACTS KB2M	marie.saint-martin@keolis.com frederic.turcant@keolis.com

Annexe 3 –

Accès au Service Numérique de Vente (SNV) :

Charte d'intégration et Guide d'implémentation

La présente Annexe 3 présente au Fournisseur de Service Numérique Multimodal (FSNM) la charte d'intégration des parcours clients et les modalités techniques d'accès au SNV, en complément des stipulations de l'Article 5 du Contrat.

1. CHARTE D'INTEGRATION

Les principes énoncés dans ce document font foi pour tous types de Produits Tarifaires dématérialisés, générés via un téléphone Android ou iOs.

PARCOURS DE DÉLIVRANCE DE PRODUITS TARIFAIRES

Le FSNM doit présenter l'ensemble des éléments descriptifs des Produits Tarifaires, leurs conditions et restrictions d'usage éventuelles, ainsi que le tarif unitaire.

Ces éléments sont exposés par l'API Catalogue de l'API Mticket :
GET /networks/{id}/catalog

La variable {id} correspond à l'identifiant du réseau TBM dans l'API et permet avec les accès dédiés au FSNM d'obtenir la liste des Produits Tarifaires disponibles à la délivrance. A chaque titre nommé "Product" dans l'API est associé :

- Un ID technique unique
- Un nom
- Une description
- Des dates de début et de fin de période de vente
- Un prix TTC

Lors de son achat, le client peut choisir une quantité et doit explicitement valider les conditions générales de ventes du réseau TBM avant paiement.

Le FSNM doit explicitement indiquer au client que le titre acheté doit être validé lors de chaque montée à bord du véhicule, en sélectionnant le titre et en approchant son téléphone du valideur, en ayant au préalable activé l'interface bluetooth et la géolocalisation de celui-ci.

La séquence de commande avec l'API Mticket se fait en plusieurs étapes :

- Tout d'abord l'initialisation d'une commande sur l'API Mticket avec l'API : POST /orders
- Puis il est à la Charge du FSNM d'initier et de finaliser sa séquence de paiement

avec son PSP (Prestataire de services de Paiement).

- Enfin et une fois que le FSNM a la certitude d'avoir perçu ou refusé le paiement de l'utilisateur (Via une notification instantanée de paiement (IPN) par exemple) il doit confirmer ou annuler la commande initiée. C'est cette étape qui déclenche la génération du titre dans le portefeuille de l'utilisateur. Cela se fait via l'API Mticket : POST /payments/{id}/transaction
- L'id correspond à l'identifiant généré renvoyé par l'API à l'étape d'initialisation de la commande. Un « Statut » doit obligatoirement être renvoyé pour informer de l'état de la transaction :
    - SUCCESS (pour confirmer la commande après réception du paiement)
    - ERROR (à notifier en cas d'erreurs technique de paiement)
    - CANCELLED (en cas d'annulation et donc d'abandon du paiement)

PARCOURS DE VALIDATION

L'ensemble des Produits Tarifaires achetés et en cours de validité doit être affichés au client. Les modalités d'activation, la date de fin de validité et/ou le nombre de voyages restants doivent être affichés.

Ces éléments sont exposés par l'API Wallet Tickets :
GET /customers/{id}/wallet/tickets

Le paramètre ID correspond ici à l'identifiant du compte de l'utilisateur dans le système Mticket. Cet ID peut être récupéré lors de la création du compte client dans le système Mticket par le FSNM doit obligatoirement être transmis pour récupérer les Produits Tarifaires de l'utilisateur connecté.

L'API Wallet Tickets ne contient pas à elle seule toutes les informations nécessaires au bon affichage des Produits Tarifaires à l'utilisateur. Chaque ticket contient une référence à un ID d'objet unique nommé "Blueprint".

Ces Blueprints contiennent les descriptions techniques et marketings des types de Produits Tarifaires. La liste des Blueprints se récupère via cette API :

GET : /wallet/blueprints

Cette API permet notamment d'identifier s'il s'agit d'un titre "à Voyages" ou d'un titre "à durée" selon ces critères :

Titre "n voyages" :

- Le titre dispose d'un nombre de validations restantes limité (le champ ticketDto.state.validationRemainingPunches n'est pas null)

Titre "a durée" :

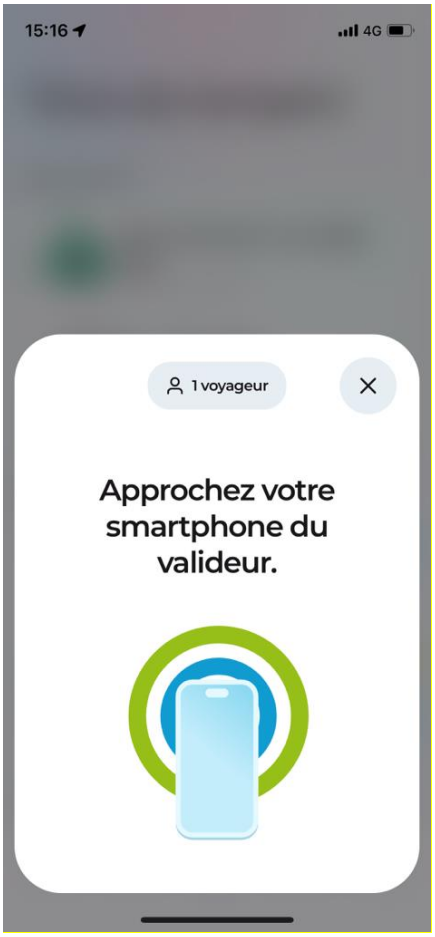
- Le blueprint du titre a une durée (le champ config.settings.contractDuration ou config.settings.ticketDurationDefinition n'est pas null)

En raison du caractère "statique" des blueprints une mise en cache est appréciable.

Celle-ci peut être d'une durée de 1h.

Le client doit pouvoir sélectionner le titre à valider et ajuster le nombre de voyageurs (pour les Produits Tarifaires dits « Multi validables » : 2 Voyages, 10 Voyages et 10 voyages réduit)

Un écran doit alors lui indiquer et illustrer le « geste de validation » à réaliser, consistant à approcher le téléphone à moins de 5 cm du valideur.



Après détection de la trame BLE par le SDK, le client doit constater qu'une tentative de validation est en cours (une animation doit être affichée le temps de l'échange avec le web service de validation) : API POST /wallet/validate

La validation se fait via l'API POST /wallet/validate.

L'id du Ticket validé (ContactID) et le contexte de validation récupérés au travers de la trame bluetooth du valideur doivent être envoyés obligatoirement lors de la validation.

La liste des variables devant obligatoirement être envoyées dans le corps de la requête, dans le cadre de chaque validation, est la suivante :

```
"context": {
  "locationLineCode": "61",
  "locationLineName": "Tram C",
  "locationMediaCode": "29EE28BC-B059-4F65-907F-3B4836F7682C",
  "locationMediaType": "APP",
```

```
  "locationStationCode": "3765",
  "locationStationName": "Gare Saint-Jean (Bordeaux)",
  "locationTripDirection": "BACK",
  "locationVehicleCode": "2219",
  "locationVehicleType": "TRAM",
  "passengers": 1
}
```

Dans l'utilisation d'un titre Mticket pour valider on distingue 2 cas :

- La "PrimoValidation" première validation qui déclenche l'utilisation d'un titre.
- La "Correspondance" qui permet de valider un titre en cours d'utilisation en correspondance sur une autre ligne du réseau TBM et pendant l'heure qui suit la "PrimoValidation".

Afin d'éviter la fraude et qu'un utilisateur utilise en "Correspondance" et à distance un même titre déjà "PrimoValidé" sur un autre téléphone : Un contrôle de continuité d'usage d'un même smartphone pour un même voyage avec un même titre de transport doit être intégré.

Pour ce faire un identifiant unique associé au téléphone initiateur de la "PrimoValidation" doit être transmis à chaque validation (Variable locationMediaCode) et vérifié avant chaque validation en correspondance.

Dans ce but, si un titre est déjà en cours d'utilisation un appel à l'API suivante doit être effectué :

GET /customers/<m-ticket-id>/wallet/contracts/<contract-id>/events

Cet appel API va renvoyer la liste des événements de validation d'un titre et si la variable "LocationMediaCode" transmise à la primoValidation ne correspond pas à l'identifiant unique du téléphone de l'utilisateur alors on doit lui refuser la validation en correspondance et l'affichage du QR Code de Contrôle.

Une fois la validation acquittée par l'API, un écran de succès de validation doit être affiché.

Le client doit pouvoir valider un titre alors qu'un autre titre est déjà validé.
(Ex : Validation d'un titre 10 Voyages pour soi, puis validation d'un titre 10 Voyages réduit pour un enfant accompagnant).

EXIGENCES DE CONTROLE

Principes généraux

Les agents désignés par le Concessionnaire peuvent à tout moment du déplacement, vérifier les titres de transport des voyageurs, que ce soit dans les bus, les tramways, les navettes fluviales ou de manière générale sur l'ensemble du réseau TBM.

Les voyageurs sont tenus de présenter leur titre en bon état à toute réquisition des agents assermentés par le Concessionnaire. Le voyageur devra présenter son titre de

transport validé et l'éventuelle justification requise pour son utilisation.

Pour le contrôle d'un M-ticket dématérialisé, l'application du voyageur devra permettre l'affichage d'un QR code de contrôle standardisé, afin de permettre la vérification automatisée de la validité du titre et de sa validation, par lecture optique à l'aide du terminal de contrôle des agents TBM.

Le titre dématérialisé devra également être contrôlable à vue, grâce à l'affichage clair des informations de validation.

Parcours de contrôle

Les voyages en cours doivent être affichés au client, depuis chaque titre validé ou depuis une vue dédiée.

Une vue de contrôle doit pouvoir être affichée depuis le voyage en cours.

Cette vue doit afficher :

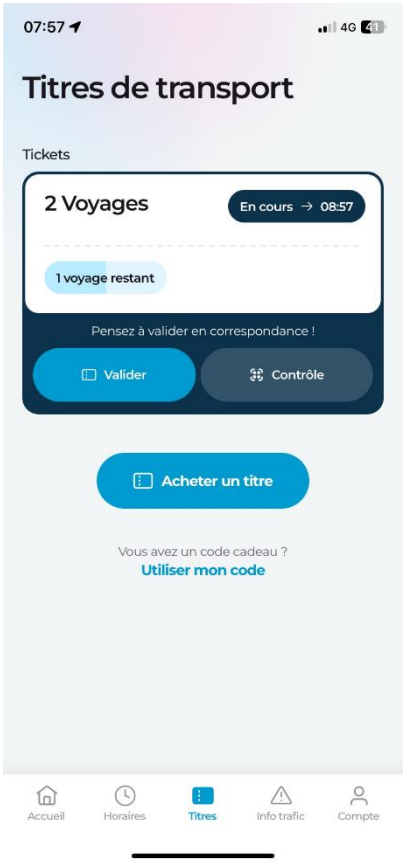
- Un QR code affiché sur au moins la moitié de la largeur de l'écran :

    2. Pour le contrôle à vue, une animation dynamique doit être affichée pour permettre aux contrôleurs de vérifier qu'il s'agit réellement d'un titre et non d'une capture d'écran. Cette animation doit pouvoir s'arrêter lorsque l'on clique sur le QR Code de contrôle pour s'assurer qu'il s'agit réellement d'un titre et non d'une vidéo.

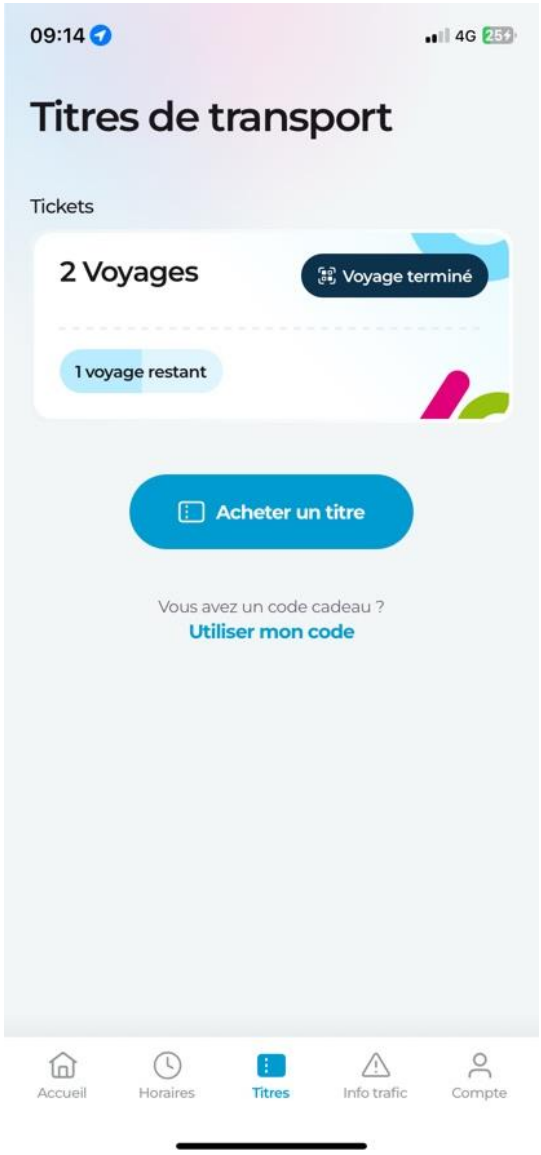
- Pour chaque validation (primo validation et correspondances) :

    3. Date et heure de validation du titre (primo validation et correspondances) ;
        - N° du véhicule dans lequel la validation a été effectuée ;
        - Nom de la ligne dans laquelle la validation a été effectuée ;
        - Nom de l'arrêt où la validation a été effectuée.

- Pour le titre validé / en cours d'utilisation :
    - Libellé du titre ;
    - Nombre de voyageurs ;
    4. Date et heure de fin de validité (60 minutes après la 1ère validation) ;
        - Le titre reste en « voyage en cours » jusqu'à 2h après la validation ;
    5. Entre 0 et 1h : « Valider » et « Contrôle » sont visibles et cliquables sur l'app TBM ;



- Entre 1h et 2h : la mention "en cours" est remplacée par "voyage terminé" et le titre est cliquable. Au clic, on a le choix entre générer une nouvelle validation ou accéder au QR code de contrôle de la précédente validation ;



- Après 2h, le titre reprend son statut "non utilisé" ou disparaît s'il est expiré (date de fin de validité atteinte).

Le QR Code doit pouvoir être lu par les portables de contrôle des agents TBM.

La récupération de la chaine de caractères Hexadécimale qui permet l'affichage du QRcode de contrôle se récupère via l'API suivante :

GET /customers/{id}/wallet/contracts/{contractId}/attestation

La variable "id" correspond à l'id Mticket de l'utilisateur.
La variable "contractId" correspond à l'id du contrat (titre mticket) sur lequel la validation est en cours.

La réponse de l'API au format suivant :

```
{
  "payload":
"b7b6e3c7d8e7a3d26127fc7a3e91c1217486b440767be20a4add5de9bcb363afe137ad0956c8f
515e98367d890f52039ebd40f4998d1117f0942e2221baeda14",
  "format": "QR:HEX"
}
```

C'est le contenu de la variable Payload qui doit être récupéré et affiché au format QR Code.
Attention il ne faut pas convertir la chaîne Hexadécimal en QR Code au format “text” mais bien au format “Hexadécimal”.

2. REGLES D’IMPLEMENTATION

Avant-propos

Cette documentation a pour objectif de permettre à un nouveau FSNM de pouvoir rapidement intégrer l’API et le SDK du Service Numérique de Vente.

Pour pouvoir utiliser l’API, il est nécessaire de s’authentifier préalablement à l’aide de credentials fournis par Airweb.

L’authentification, décrite dans le premier scénario ci-dessous, permet au FSNM d’obtenir un token d’accès (Bearer) utilisable pour l’ensemble des scénarios.

Les données renvoyées par l’API correspondent uniquement à celles que le FSNM est autorisé à récupérer.

Authentification

1. Récupération d’un token d’accès

Pour pouvoir utiliser l’API, il est nécessaire d’avoir un token d’accès à mettre dans le header Authorization en tant que Bearer token.
Ce token est obtenu en fournissant un couple identifiant / secret, délivré par Airweb.

Cet échange se fait sur la route POST /auth/token.

Voici un exemple de curl à utiliser pour générer un token d’accès à partir de son couple identifiant / secret :

```
<https://XXXXXXXXXX/auth/token>" \\
 -H "Content-Type: application/x-www-form-urlencoded" \\
 -H "User-Agent: <userAgent>" \\
 -H "Accept: */*" \\
 -H "Cache-Control: no-cache" \\
 -H "Host: v1-14---staging-proxy-ra6rh2jj5a-ew.a.run.app" \\
 -H "Accept-Encoding: gzip, deflate, br" \\
 -H "Connection: keep-alive" \\
 --data-urlencode "grant_type=client_credentials" \\
 --data-urlencode "client_id=<clientId>" \\
```

```
--data-urlencode "client_secret=<clientSecret>"
```

Gestion des clients

L'API Partenaire ne permet de gérer l'authentification des utilisateurs finaux (il ne s'agit pas d'un IAM fédérateur d'identité).

il appartient au FSNM d'intégrer son propre système de gestion de comptes clients et d'identification.

Cependant, pour pouvoir utiliser les services Mtickets de l'API partenaire chaque client final du FSNM devra bénéficier d'un compte « technique » qui lui sera créé au travers de l'API sur le Service Numérique de Vente.

Pour ce faire le FSNM devra créer un compte pour chaque client via l'API `POST /users`.

Le FSNM pourra s'il le souhaite enregistrer un code Externe qui lui est propre dans le système Airweb mais devra obligatoirement transmettre les informations personnelles suivantes à la création de compte :

Prénom
Nom
Date de Naissance
Email
NetworkIds : (Le numéro de réseau technique transmis au FSNM pour Bordeaux)

Dans chaque séquence d'appels avec l'API Partenaire nécessitant l'identification d'un client c'est l'ID de compte de l'API Partenaire qui devra être utilisé.

Bien qu'il existe une API permettant de faire de la recherche de compte sur plusieurs critères il est vivement recommandé de stocker dans la base du client du FSNM les IDs de comptes technique mticket afin d'optimiser l'ensemble des appels à l'API.

Contraintes

• L'API Partenaire ne peut en aucun cas être contactée directement depuis un front. Toutes les requêtes doivent être effectuées depuis un serveur afin de ne pas rendre publiques les identifiants de connexion privés.

• Les tokens d'accès ne doivent être récupérés que toutes les heures et doivent être mis en cache ce temps-là pour ne pas générer un volume abusif de tokens.

• Le catalogue peut lui aussi être mis en cache pendant la durée d'utilisation du token d'accès car c'est à travers ce token que l'on récupère la liste des produits qu'un FSNM peut afficher.

• L'API Partenaire doit être obligatoirement intégrée au travers de l'APIM (API Manageur) de Keolis Bordeaux Metropole Mobilité. Celui-ci permet d'assurer la supervision des interfaces et de garantir leur sécurité.

• Un paramètre dans le Header HTTP permettant d'authentifier l'intégrateur de l'API sur l'APIM devra obligatoirement être transmis.

Limitation de requêtes sur l'API

Afin de garantir une qualité de service optimale et d'assurer une utilisation équitable des ressources, nous appliquons les règles suivantes concernant le nombre de requêtes autorisées par seconde :

1. Limite standard :

- Chaque client est limité à 30 requêtes par seconde (req/s) en temps normal.

2. Blocage temporaire :

- Si un client dépasse 50 req/s en moyenne sur une minute, l'accès à l'API sera temporairement bloqué pendant 5 minutes.

3. Blocage prolongé et déblocage manuel :

- Si le dépassement de 50 req/s en moyenne persiste pendant 10 minutes, l'accès restera bloqué.
- Déblocage uniquement sur demande :
    - Le client devra contacter le support@airweb.fr pour expliquer la raison du dépassement.
    - Il devra confirmer avoir pris les mesures nécessaires pour éviter un nouvel excès.
    - Une fois ces éléments validés, nous procéderons manuellement au déblocage de l'accès.