

ETUDE SÉCURITÉ BILLETTEQUE POUR LES AO DE TAILLES INTERMÉDIAIRES

Présentation du 12 Mai 2016

La sécurité et la billettique

- **La billettique** recouvre l'ensemble des procédés et outils de gestion des titres de transport. Elle sert donc en particulier à assurer la collecte des revenus d'exploitation par les réseaux de transports publics et à leur apporter des statistiques permettant de suivre les usages.
- **La sécurité billettique** recouvre l'ensemble des mesures prises pour garantir la confidentialité, l'intégrité et la disponibilité des données nécessaires au bon fonctionnement du système billettique. Il s'agit en particulier de :
 - Garantir la collecte des revenus des réseaux
 - Assurer la fiabilité des données d'exploitation
 - Prévenir les incidents d'exploitation potentiels relatifs à la billettique
 - Dissuader et détecter la fraude
- **La fraude** consiste à ne pas payer le tarif approprié pour réaliser un voyage
- **NB** la notion de sécurité est différente de la notion de sûreté qui concerne notamment les risques d'agressions physiques des voyageurs et/ou agents des réseaux.

Généralités sur la sécurité billettique

- Acquérir un système billettique permet avant tout de collecter les revenus du réseau de transport. La sécurité billettique est un outil qui permet au réseau de protéger cette collecte de revenus :
 - En offrant un moyen de lutter contre la fraude technologique potentiellement organisée
 - En permettant de détecter des comportements frauduleux et d'intervenir sur certains (e.g mise en liste noire)
- Il s'agit d'un ensemble d'exigences applicables au SI billettique dans sa globalité :
 - A l'ensemble des éléments impliqués dans le traitement billettique : supports, équipements, serveurs
 - Complétées par des mesures permettant de lutter contre la fraude : règles d'usages et procédures d'exploitation
- La sécurité billettique est un sujet évolutif qu'il faut adapter à son contexte
 - La sécurité n'est pas un acquis figé : les mesures doivent être revues et mises à jour régulièrement
 - Le coût de la sécurité doit être évalué et comparé au bénéfice apporté par la lutte contre la fraude

La fraude dans les transports en commun

- Différentes situations d'infraction :
 - Infraction tarifaire : payer son titre à un tarif auquel on n'est pas éligible
 - Infraction d'accès au moyen de transport : ne pas valider son titre lors de la montée
 - Infraction de contrôle : ne pas être en mesure de présenter un titre valide ou un justificatif exigible
- Différents types de fraude :
 - Fraude contrainte
 - « Je n'ai pas eu le temps d'acheter un billet, le tram est à quai, je monte »
 - « Je n'ai pas trouvé de point de vente et ai besoin de prendre le bus »
 - Fraude intentionnelle individuelle ou organisée
 - « Je n'achète pas de ticket et prends le bus quand même »
 - « J'ai un ticket mais ne le valide pas pour pouvoir le réutiliser »
 - Associations d'utilisateurs qui prennent les amendes à leur charge contre une cotisation mensuelle moins chère que l'abonnement
 - Contrefaçon ou clonage de titres
 - Fraude interne
 - Paiement en liquide au chauffeur qui conserve l'argent et laisse le voyageur monter sans fournir de ticket
 - Arrangement similaire entre un contrôleur et un fraudeur
 - Détournement de stock de titres prêts à l'usage

Quels outils pour lutter contre la fraude

- Les AOTs disposent de deux outils pour lutter contre la fraude :
 - Des exigences fonctionnelles portant sur la sécurité apportée par leurs solutions billettiques
 - Des mesures et procédures institutionnelles
- Les slides qui suivent donnent des exemples d'exigences fonctionnelles pour les solutions billettiques et de mesures complémentaires.
- Le document de restitution de l'étude présentera les réponses fonctionnelles et institutionnelles aux différents types de fraude :

	Types de fraudes	Réponses en terme d'exigences sur la solution billettique	Mesures complémentaires
Fraude interne	Détournement de recettes		
	Détournement de titres		
Fraude contrainte	Absence de titre		
	Titre invalide		
Fraude intentionnelle individuelle	Absence de titre		
	Titre non consommé		
	Titre invalide		
	Titre contrefait		
Fraude organisée	Absence de titre		
	Dégradation des équipements		

Exemples d'exigences fonctionnelles pour les SI billettiques

- Back-office
 - Mise à disposition de rapports statistiques fins permettant de détecter des anomalies (par exemple un nombre de validations anormalement faible pour une ligne, ...)
 - Gestion de listes d'opposition
 - Détection des fraudeurs récidivistes (si une même personne reçoit plusieurs PVs)
- Distribution
 - Information sur les profils et droits associés lors des opérations de vente
 - Mise à disposition de canaux de vente permettant un achat immédiat et acceptant différents moyens de paiement
 - Activation des titres ou supports suite à la vente (les stocks ne sont pas utilisables avant la vente)
- Supports et équipements
 - Equipements de contrôle capables de vérifier les profils des usagers, de différencier un titre validé d'un titre non consommé et de détecter des titres contrefaits
 - Installation d'équipements de validation dans les véhicules
 - Mise en œuvre de schémas de sécurité mis en œuvre au niveau des supports et des équipements
 - Emission et règlement des amendes directement via les terminaux de contrôle

Exemples de mesures complémentaires à la sécurité billettique

- Distribution
 - Réduction ou suppression de la vente au casier, limitation de l'usage des paiements en espèces
 - Analyse comptable des statistiques de ventes par canal.
 - Communication sur la gamme tarifaire et les conditions d'éligibilité à certains titres
 - Dématérialisation des titres à usage non immédiat : élimination des stocks et des risques de détournement associés.
- Validation
 - Validation systématique à la montée
 - Institution d'un comportement responsable des usagers : « contrôle social »
- Contrôle
 - Contrôles fréquents et visibles
 - Présentation de justificatifs pour bénéficier de titres d'ayants droits
 - Suivi du recouvrement des amendes
 - Poursuites judiciaires
 - Renforcement de l'arsenal législatif contre la fraude organisée

Ces mesures sont indispensables pour lutter contre la fraude en complément du déploiement d'un système billettique.

Lutte contre la contrefaçon de titres :

Mise en œuvre d'un schéma de sécurité billettique

- Objectif : prévenir la fraude technologique permettant la contrefaçon ou le clonage de titres
- Comment : bonnes pratiques usuelles dans l'IT
 - Authentification des supports et des usagers, chiffrement des échanges de données sensibles, vérification de l'intégrité des données transmises ...
 - Utilisation d'algorithmes cryptographiques éprouvés : DES, 3DES, DESX, AES, RSA, ...
 - Stockage des secrets dans des dispositifs apportant une sécurité physique (et pas simplement logicielle) :
 - Supports: Secure Element (carte à puce), carte SIM ou SE embarqué (mobile NFC)
 - Equipements front office : SAM
 - Serveurs : HSM ou serveur de SAMs

Une implémentation grandement dépendante du type de technologies et de supports déployés.

Tendances billettiques observées lors des interviews

Ticket papier



Carte à puce sans contact



Mobile NFC

1900

2000

2010- 2014

Tout sans contact



Media based ticketing :
Billettique centrée sur le support



Jeton métallique



Ticket magnétique



Billet Sans Contact (BSC)

+ QR Code

+ EMV sans contact



Account based ticketing :
Billettique centrée sur le compte usager

Deux tendances fortes :

- Une capitalisation autour de la technologie sans contact
- Une migration vers des solutions centrées sur le compte usager



Tickets code-barres papier ou mobile



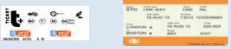





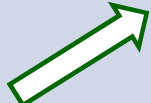




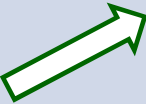

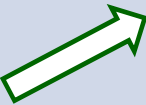


Carte bancaire sans contact

Panorama des supports billettiques

Supports émis par le réseau

Supports émis par des tiers

Supports de titres	Tendances	Commentaires
<p>Ticket papier (thermique)</p> 		<p><u>Ticket papier</u> : solution à bas coût pratique pour la vente à bord mais peu adaptée aux trajets avec correspondances</p>
<p>Carte magnétique / ticket magnétique</p> 		<p><u>Ticket magnétique</u> : support bon marché mais les équipements sont chers à maintenir en raison de l'obsolescence de la technologie et des éléments mécaniques impliqués.</p>
<p>Billet sans contact (BSC) Carte sans contact Clé USB NFC</p> 	 	<p><u>Carte sans contact</u> : solution la plus utilisée pour les voyageurs réguliers</p> <p><u>BSC</u> : permet d'utiliser les mêmes équipements que les cartes sans contact. Supports et distribution sont néanmoins chers</p>
<p>Ticket à code-barres imprimé Ticket à code-barres mobile Smartphone NFC</p> 	 	<p><u>Code-barres</u> : solution bas coût mais sauf titre à usage immédiat, cela nécessite de migrer vers des systèmes Account Based Ticketing (ABT).</p> <p><u>Mobile NFC</u> : L'écosystème NFC est complexe et il n'y a pas de déploiement massif constaté</p>
<p>Carte sans contact EMV</p> 		<p><u>Carte de paiement</u> : solution applicable aux occasionnels. Cependant, tout le monde n'a pas une carte de paiement sans contact (ou ne souhaite pas s'en servir)</p>
<p>Téléphone mobile comme moyen d'authentification : smartphone BLE + Beacons</p> 		<p><u>BLE</u> : L'émergence des smartphones BLE et de beacons bon marché permet de créer une solution intéressante mais encore émergente</p>
<p>Carte comme moyen d'authentification : D'étudiant, D'employé, ...</p> 		<p><u>Cartes tierces</u> : Assez similaire aux cartes sans contact. Cela nécessite de migrer vers des systèmes Account Based Ticketing (ABT).</p>

Présentation des architectures billettiques possibles

- Billettique centrée sur le support :
 - Les titres et données personnelles/de profil sont stockés dans le support
 - Les transactions (validation, vente, contrôle) sont intégralement réalisées localement entre équipement et support
 - Exemple : carte Calypso avec stockage des titres et du profil dans le support, billet sans contact
- Billettique centrée sur le compte usager :
 - Les titres et données personnelles/de profil sont stockés dans des comptes en back-office
 - Le support sert à identifier le porteur auprès des équipements (de vente, validation et contrôle) afin qu'ils réalisent les transactions en back office
 - Exemple : ticket papier avec code-barres, carte Calypso avec stockage d'identifiants dans le support

Schéma de sécurité d'un SI Billettique centré sur le support

Carte à puce Calypso



Support



Équipement



Back-office

Sécurité du support

Sécurité physique de la
carte à puce



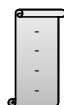
Clés applicatives pour
authentification et
sessions sécurisées

Impression de l'identité et
de la photo du porteur
pour les titres nominatifs

SAM



Clés applicatives pour
authentification et sessions
sécurisées



Listes de supports refusés

Suivi des usages en vue de
reconstitutions de titres



Gestion des listes de supports
refusés (car perdus, volés ou en
opposition)



Signature des titres
(optionnelle)



Vérification de signature des
titres (optionnelle)

Analyse de données pour détecter
des comportements frauduleux
(Gros réseaux uniquement)

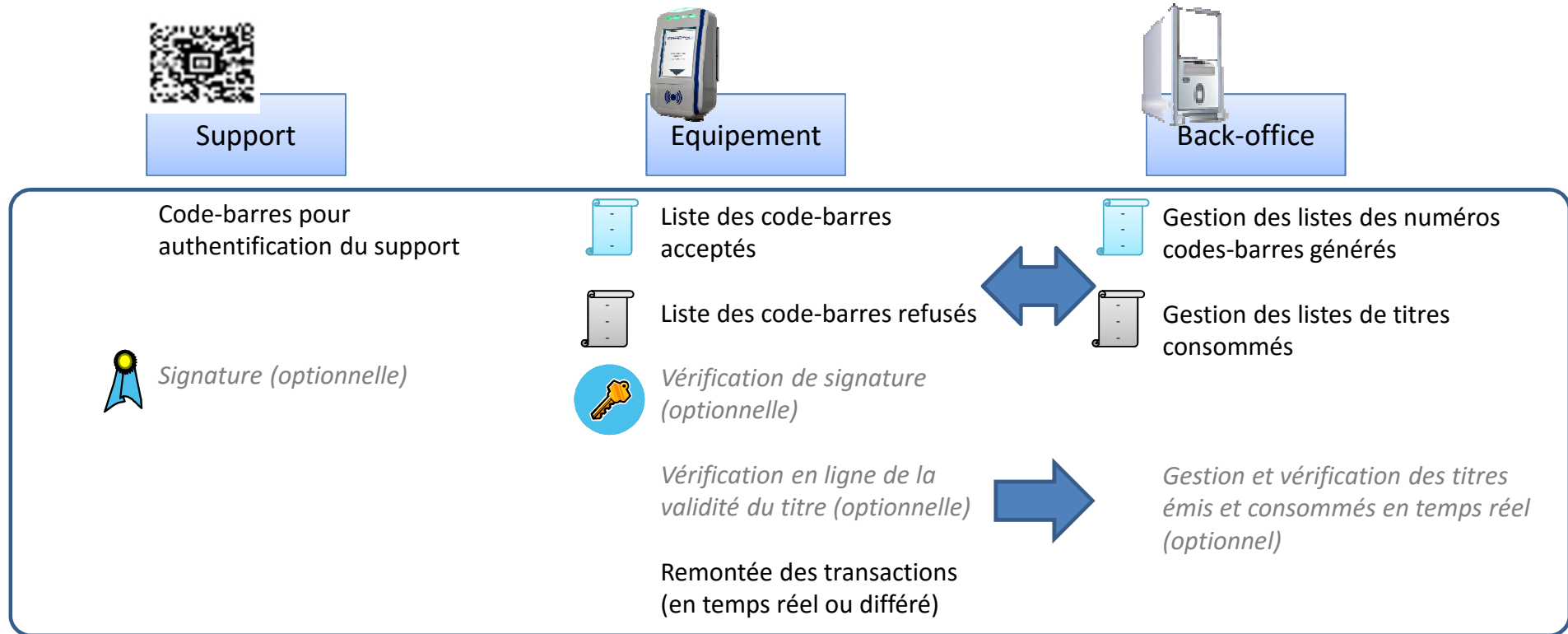
Sécurité des titres

Sécurité en back office

La sécurité du système repose essentiellement sur la sécurité physique du support et de l'équipement.

Schéma de sécurité d'un SI Billettique centré sur le compte usager

Ticket avec code barre



Sécurité du support/titre*

La sécurité du système repose sur une connectivité permanente entre équipements et back-office.

Analyse de données pour détecter des comportements frauduleux (Gros réseaux uniquement)

Sécurité en back office

Conclusions et recommandations

- Pas de « solution » universelle en billettique
 - Il n'y a pas de technologie ou de type de support valable pour tous les usagers
 - Combiner plusieurs supports et technologies pour couvrir toute une gamme tarifaire est en général inévitable
- Pas d'impossibilité à utiliser les différents types de supports et de technologies présentés
 - Dans la mesure où un schéma de sécurité billettique approprié est mis en œuvre.
 - La tendance d'aller vers des équipements connectés permet de déployer des solutions où la sécurité est déportée vers le back office.
- La sécurité billettique ne permet pas seule de lutter contre la fraude
 - La mise en œuvre de procédures d'exploitation et de règles d'usages est indispensable en complément.
- Le défi pour une AOT de taille intermédiaire est de tirer parti des différentes offres existantes et de la connectivité des véhicules pour déployer des solutions billettiques
 - Fiables
 - Apportant aux voyageurs une expérience simple, pratique et de qualité
 - A des coûts maîtrisés
 - Offrant un niveau de sécurité adapté aux titres distribués et aux voyageurs utilisant le réseaux
 - Répondant à ses besoins d'interopérabilité

Prochaines étapes

- Il s'agit aujourd'hui d'un état intermédiaire des travaux portant sur la sécurité billettique.
- Un document détaillant les résultats de l'étude sera produit fin 2016 par le CEREMA
- Puis un événement de restitution finale sera organisé par l'AFIMB et le CEREMA en partenariat avec le GART et AGIR.

Bordeaux:

31 avenue Carnot
33200 Bordeaux – France

Paris:

32 Rue Brancion
75015 Paris – France



Contacts:

Jean Philippe AMIEL

jean-philippe.amiel@nextendis.com

Julien HUYGHE

julien.huyghe@nextendis.com

www.nextendis.com