Système Billettique Central

Politique générale de sécurité des services du SBC

Contrat spécifique sécurité

Version 1.3

30/03/2021

îledeFrance mobilités

Historique

Version	Date	Auteur	Entité	Statut / Suivi des modifications
1.0	23/11/2020	IdFM	MB	Première version diffusée.
1.1	02/03/2021	IdFM	MB	Version pour contractualisation avec les Partenaires.
1.2	18/03/2021	IdFM	MB	Distinction Textes de référence / Directives sécurité.
1.3	30/03/2021	IdFM	MB	Mise à jour nommage directives sécurité

Sommaire

1. Introduction

1.1 Objet du document

IdFM coordonne le développement et la maintenance de services franciliens de télé-billettique pour les transports en commun en Ile-de-France déployés sur le Système Billettique Central (SBC) au travers du Programme de Modernisation de la Billettique (PMB).

La sécurité de l'information vise à protéger ce Système Billettique Central, et les systèmes d'information s'y raccordant, contre les risques inutiles ou inacceptables. Elle se manifeste par des contrôles et des contre-mesures qui protègent la confidentialité et l'intégrité des données des services du Système Billettique Central et la disponibilité des systèmes, via des défenses en couches de contre-mesures physiques, procédurales, personnelles et techniques.

Le but de ce document est de fournir une politique de sécurité de haut niveau pour les systèmes billettiques franciliens, une déclaration publique d'intention afin de délimiter ce qui est attendu dans le domaine de la sécurité de l'information, et sert de base à l'adoption de procédures, plans, mesures et normes communes convenues. Celles-ci comprendront des concepts d'emploi, le contrôle de l'accès à l'information, le contrôle de l'utilisation et de la diffusion de l'information, le contrôle de l'utilisation légitime, un mandat stipulant que les systèmes doivent rester disponibles et des dispositions pour la continuité des activités en cas de problèmes liés à la sécurité.

La définition de la politique de sécurité est également la première étape de la mise en place d'une organisation contractuelle ou conventionnelle des acteurs de l'écosystème et au rôle que chaque acteur du système est appelé à jouer, tout au long du déploiement et de la vie courante du PMB et au-delà du programme.

La politique de sécurité est applicable à toutes les activités fonctionnelles et techniques contribuant à l'ouverture des différents services du Système Billettique Central.

1.2 Structure du document

Ce document définit la politique générale de sécurité pour les services du SBC. Il fournit un cadre de sécurité pour les services du SBC, notamment :

- La définition des objectifs de sécurité (Quoi).
- La définition des domaines de sécurité (Où).
- La définition des parties prenantes et des responsabilités (Qui).
- La description du système de gestion et de management de la sécurité de l'information (Comment).
- La base de référence de la documentation de sécurité SBC, c'est-à-dire la liste des références aux documents portant sur la sécurité du SBC.

1.3 Champs d'application

Le présent document est applicable à l'utilisation opérationnelle du système d'information portant les services du SBC par IdFM et ses partenaires de mobilité s'y raccordant : opérateurs de transport, exploitants d'infrastructures de réseau ferroviaire, délégataires de service public, services numériques multimodaux, etc.

1.4 Principes de base

Cette politique décrit les principes et règles essentiels de la sécurité des services du SBC, dont l'objectif est de faciliter l'atteinte des objectifs métiers du PMB. Il est à noter que la base de cette politique de sécurité de l'information est constituée par des règlements, référentiels, directives générales et démarches de sécurité émises par l'ANSSI et par la Commission Européenne.

Ses principes et règles, ainsi que les instructions et directives qui en découlent, sont recommandés dans l'ensemble du PMB en tant qu'exigences de sécurité minimale.

Les propriétaires de systèmes billettiques peuvent, en fonction des risques encourus, mettre en place des exigences et des solutions de sécurité plus strictes.

Les informations sur l'état de conformité de cette politique et les plans pour son amélioration sont disponibles auprès du propriétaire du document.

Ce document est sensible et ne doit être diffusé qu'en cas de besoin, à la discrétion d'IdFM.

La politique de sécurité des services du SBC fournit un ensemble de principes et d'objectifs de haut niveau pour la sécurité des services du SBC ainsi que les déclarations de bonnes pratiques associées. Ils peuvent être utilisés pour améliorer le niveau de sécurité des manières suivantes :

- Maximiser le niveau de sécurité des systèmes d'information.
- Garantir le niveau de sécurité de l'information billettique.
- Compléter et renforcer les processus d'intégration de la sécurité dans les projets.
- Garantir le Maintien en Conditions de Sécurité.
- Évaluer les performances en matière de sécurité de l'information.
- Soutenir les audits de sécurité.
- Vérifier la conformité aux normes de l'industrie.

La mise en œuvre de la politique doit contribuer à :

- Gérer la surface d'exposition et la profondeur des risques de sécurité associés.
- Progresser vers les meilleures pratiques.
- Renforcer la confiance au sein des partenaires dans le fait que la sécurité est traitée de manière professionnelle.
- Réduire la probabilité d'interruption des services suite à des incidents critiques ou majeurs liés à la sécurité.
- Maintenir l'intégrité commerciale.

Cette politique de sécurité du SBC appartient à IdFM. Elle est amenée à évoluer dans le temps et pourra ainsi être revue par IdFM afin de prendre en compte :

- Les évolutions des menaces et les retours d'expérience des traitements d'incidents.
- Les résultats d'analyses de risques complémentaires ainsi que les actions découlant de contrôles ou d'inspections.
- Les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

Toute évolution sera alors communiquée aux correspondants SSI des Partenaires.

1.5 Sécurité billettique et des SI

L'information billettique est un actif commercial qui est précieux dans le cadre des services du SBC et qui doit donc être suffisamment protégé.

Les besoins en protection sécuritaire reposent sur les caractéristiques suivantes :

- Disponibilité
    - La disponibilité doit être maximale afin de garantir la possibilité de créer un espace porteur, d'acheter et d'utiliser des droits au déplacement et d'accéder au SAV afin d'éviter un manque à gagner et une perte de confiance des usagers dans les services.
    - La disponibilité doit également être maximale pour assurer des cinématiques, non visibles des usagers, de contrôle, de validation, de gestion de la fraude, etc.
- Intégrité
    - Maîtrisée : les altérations, notamment sur les droits au transport, doivent être détectées et pouvoir être corrigées.
- Confidentialité
    - Le système traitant de données à caractère personnel et sensibles (DCPS), formant télétraitement de l'administration vis-à-vis du public, le système disposera d'une conformité au RGS et d'un avis conforme CNIL, avant toute mise en service. Le RGPD renforce cet objectif notamment avec la nécessité de mettre à disposition des utilisateurs finaux un service garantissant leurs droits à l'information sur la manière dont sont gérées leurs données personnelles, dans le cadre du SAV.
- Imputabilité
    - Le système doit fournir toutes les traces nécessaires pour implémenter les pistes d'audit tant techniques que métiers (contrôle interne, suspicion de fraude).

2. Objectifs de sécurité

Les services du SBC doivent fournir aux systèmes tiers que sont :

- Applications mobiles clientes,
- Sites Web,
- Briques de paiement,
- Equipements de validation et SI Exploitant Equipements,
- SI Gestion de Fraude,
- SI Commerçants,

Un ensemble cohérent de mécanismes de sécurité génériques, adaptés à chaque typologie de raccordement :

- Appel d'API Web Services.
- Intégration de sous-systèmes de services SBC aux systèmes tiers
    - SDK billettique pour les applications mobiles Android
    - SDK billettique pour les applications mobiles iOS
    - SI embarqué
- Echanges de fichiers.

Les mécanismes de sécurité proposés doivent prendre en compte différentes dimensions : architecture logique, adhérence, imbrication, technologie, volume de l'information échangée, etc.

Ces mécanismes visent aussi à aider ces systèmes tiers à atteindre leurs propres objectifs de sécurité.

En corollaire :

- Les services du SBC, aussi bien pour leurs parties frontales aux usagers que pour les parties back-end accessibles aux administrateurs et opérateurs, doivent présenter intrinsèquement le niveau de sécurité le plus satisfaisant possible. A cet effet, les services du SBC reposeront sur des solutions logicielles présentant les certifications reconnues du marché (PCI-DSS, Calypso, critères communs, etc.).
- Les services du SBC doivent fournir des sous-systèmes sûrs et fiables aux systèmes tiers.
- Les applications clientes de commercialisation des services du SBC ne doivent pas introduire de failles de sécurité.
- Réciproquement les services du SBC ne doivent pas introduire de failles de sécurité dans les systèmes tiers.

La méthode utilisée pour atteindre ces objectifs sera décrite en détail dans le chapitre Processus de management de la sécurité.

3. Domaines de sécurité

3.1 Principes

Ce chapitre définit les composants et la juridiction de la politique (frontières logiques et physiques).

Chaque service du SBC est défini par des périmètres :

- Physique
  - Infrastructures d'hébergement
  - Terminaux mobiles des usagers
- Technique
  - Briques applicatives
- Fonctionnel
  - Données billettiques et DCPS portées par le service
  - Cas d'usage portés par le service.

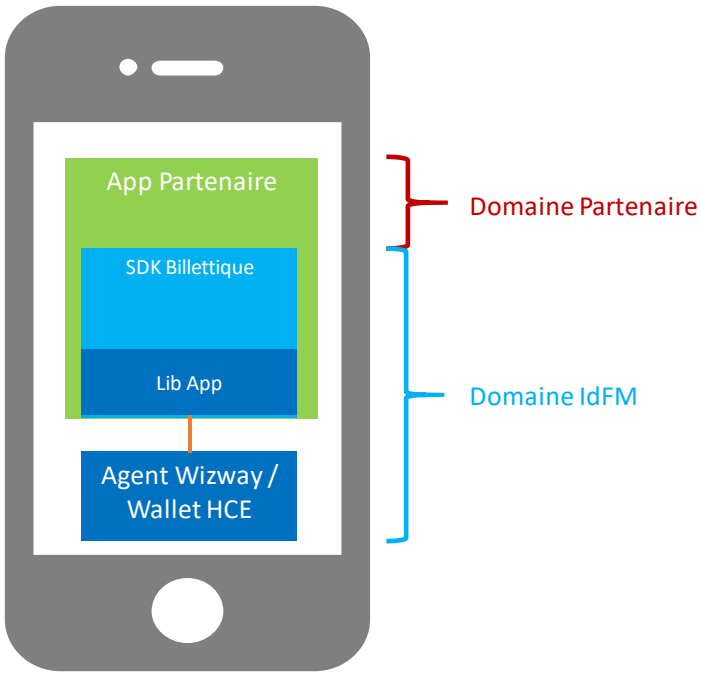
Dans les détails de l'architecture logique, on retrouve quelques typologies génériques, ou patterns d'architecture, qui permettent de définir les domaines de sécurité et donc les responsabilités associées.

3.2 Domaine par typologie

3.2.1 Intégration d'un sous-système SBC

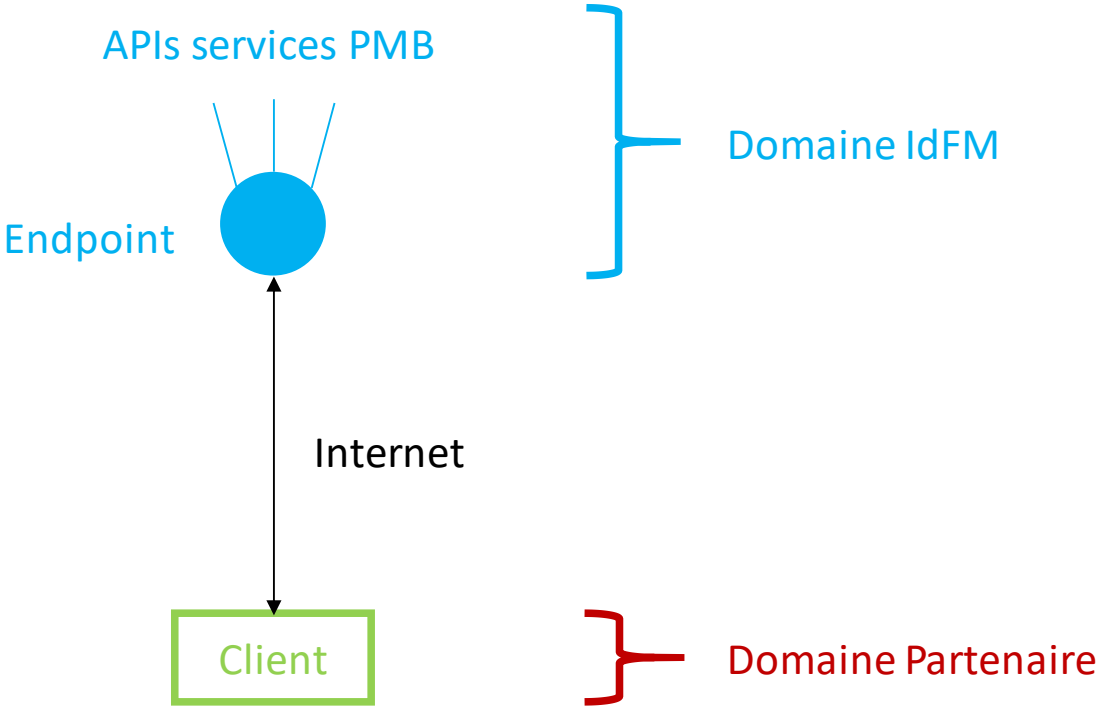
Cette intégration correspond à l'intégration d'un SDK dans une application mobile ou à un SI Embarqué.

Pour un SDK, la segmentation des domaines est la suivante :



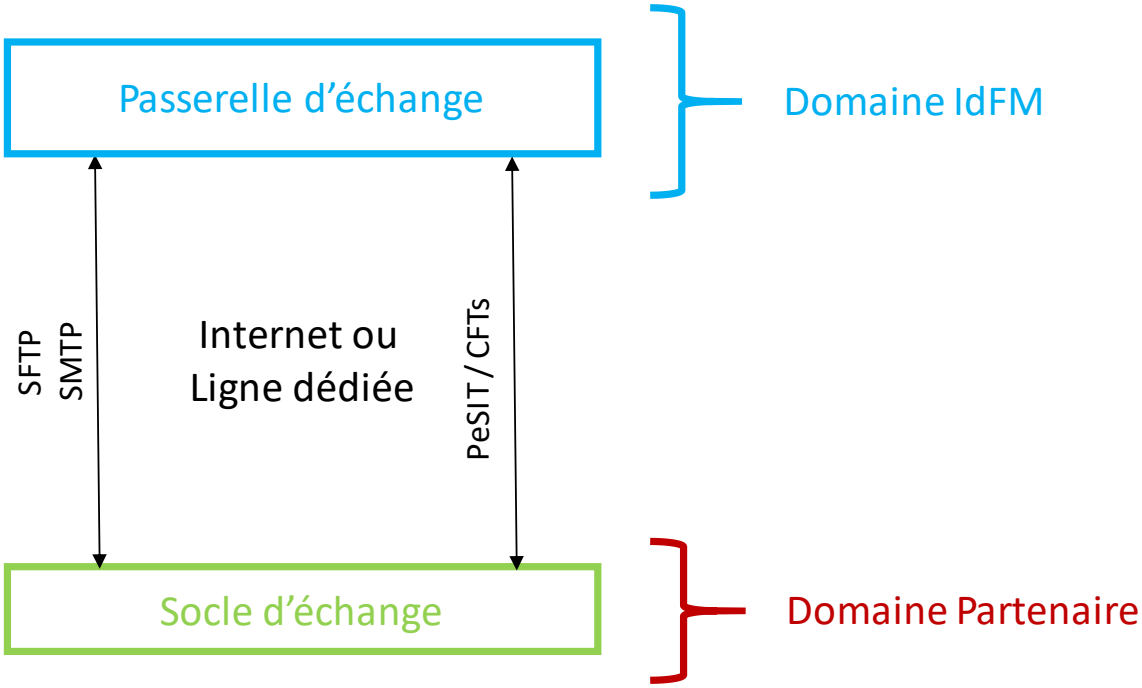
3.2.2 Appel API Web Service

Les appels sont initiés depuis un client qui peut être une application mobile, un frontal web, un SI, un équipement, etc.



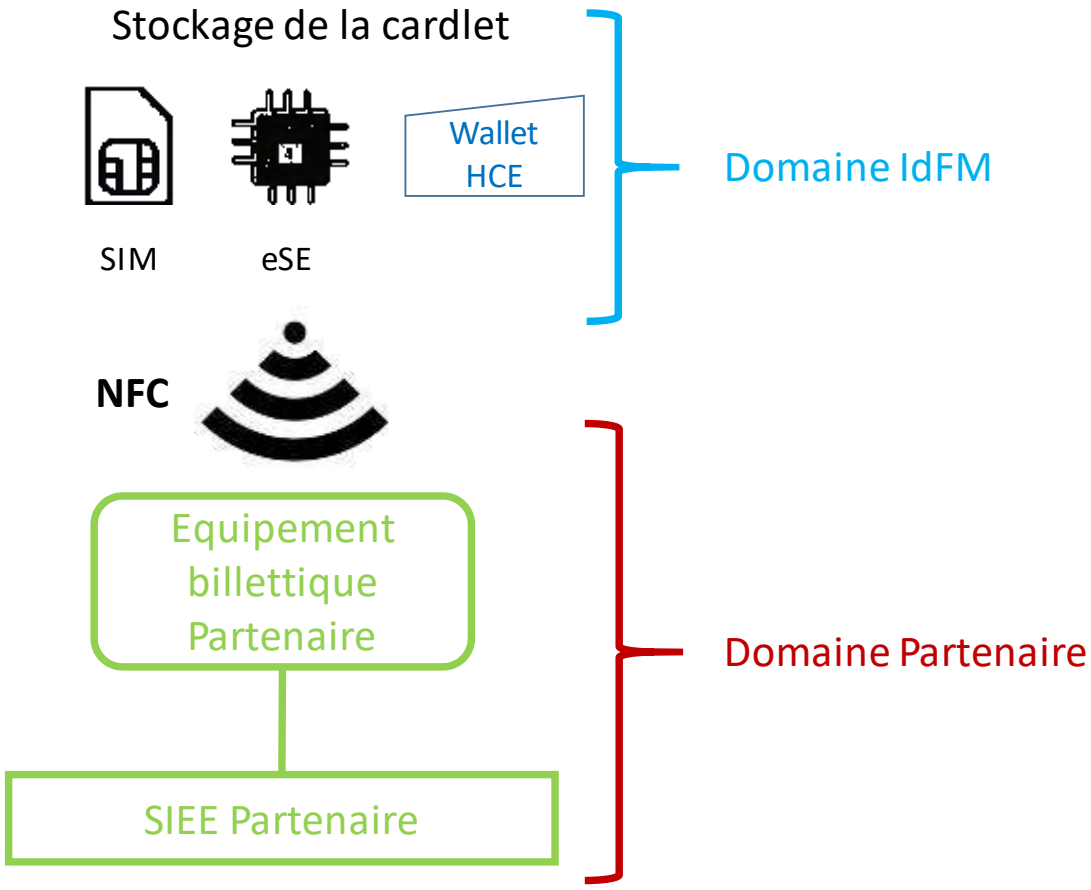
3.2.3 Echange de fichiers

Les transferts asynchrones de fichiers reposent sur l'architecture suivante :



3.2.4 Liaison NFC Smartphone / Equipements de validation

Les services Canaux Digitaux du SBC intègrent un liaison NFC entre les smartphones et les équipements de validation ou de contrôle :



3.2.5 Hors domaines

Il est à noter que la définition périmétrique n'inclut pas les terminaux mobiles des usagers, directement sous leur propre responsabilité. Les exigences de sécurité pour le smartphone, en tant que support physique de titres dématérialisés, sont limitées : version minimale de l'OS, téléphone non rooté, etc.

Les terminaux mobiles, comme Internet, font partie du domaine public, et sont vus comme un domaine hors de toute responsabilité.

3.3 Domaine global de sécurité de l'information

L'information billettique est gérée et traitée sur l'ensemble des briques d'architecture des services du SBC dont les typologies ont été présentées dans le chapitre précédent.

Les qualifications sécuritaires de chacune de ces briques constituent la base d'une analyse globale et consolidée de la sécurité de l'information, soit la sécurité billettique et la gestion de la fraude technologique des services du SBC.

4. Parties prenantes et responsabilités

.

IdFM est pilote et responsable des services du SBC, propriétaire d'une partie des systèmes d'information et responsable de traitement des données au sens RGPD.

Les principales responsabilités de sécurité du propriétaire sont :

- Définition et approbation des exigences de sécurité pour l'information et le système.
- Décisions sur le niveau et le coût de la protection du système et de l'information qui réduisent le risque d'information à un niveau acceptable.

Chaque partenaire est responsable de son domaine, tel que décrit ci-avant.

4.1 Organisation sécurité SBC d'IdFM

4.1.1 Autorité Qualifiée (AQ)

L'autorité qualifiée de sécurité des systèmes d'information est chargée de :

- S'assurer que les dispositions réglementaires et, le cas échéant, contractuelles sur la sécurité des systèmes d'information sont appliquées,
- Faire appliquer les consignes et les directives internes,
- Désigner l'autorité d'homologation des systèmes relevant de sa responsabilité,
- S'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes et pour l'agrément des dispositifs de sécurité,
- Faire appliquer aux sous-traitants IdFM sa politique de sécurité et ses exigences pour la construction du Système Billettique Central,
- S'assurer que des contrôles internes de sécurité sont régulièrement effectués.

Les AQSSI étant les responsables juridiques du périmètre concerné, c'est à leur niveau que s'exerce :

- La maîtrise d'ouvrage (définition des enjeux de sécurité liés aux systèmes d'information), la responsabilité de passer des actes contractuels (marchés publics)
- La responsabilité de mettre en place des organisations (comité de pilotage de la SSI, logistique de crise)
- Les arbitrages budgétaires
- La possibilité, le cas échéant, d'intenter une action en justice.

4.1.2 Autorité d'Homologation (AH)

L'autorité d'homologation (AH) s'engage sur la capacité du système d'information portant les services du SBC à traiter les informations conformément à la législation et la règlementation en vigueur relatives à la SSI, conformément aux mécanismes de sécurité prévus et décrits dans les différents documents qui constituent le dossier d'homologation.

La décision d'homologation est l'engagement par lequel l'autorité d'homologation atteste, au nom de l'autorité qualifiée, que les projets ont bien pris en compte les contraintes opérationnelles de sécurité, que les exigences de sécurité sont déterminées et satisfaites, que les risques résiduels sont maitrisés et acceptés, et que les services du SBC sont donc aptes à entrer en service.

4.1.3 Responsable SSI Projets (RSSI-P)

Le responsable de la sécurité du système d'information projets (RSSI-P) est désigné au sein de l'entité responsable du programme, c'est l'adjoint en matière de SSI du directeur de programme ou de projet.

Il est responsable de tous les aspects relevant de la sécurité pour le système durant la phase de BUILD.

Il est plus particulièrement chargé de :

- Piloter la mise en œuvre **transverse** des mesures de sécurité nécessaires à la couverture des exigences de sécurité et à l'atteinte des objectifs de sécurité
- Coordonner les travaux des RSSI des MOE / groupements
- Coordonner les actions SSI au sein des projets de BUILD
- Valider les procédures d'exploitation de sécurité (PES) fournies par les RSSI des MOE / groupements
- Définir et piloter les audits de sécurité à mener sur les points clés du système d'information
- Conduire la démarche jusqu'à la décision d'homologation des services du SBC.

4.1.4 Responsable SSI Aval du système (RSSI-A)

Le RSSI-A, pour RSSI aval, est désigné pour assurer le suivi SSI du système en service, jusqu'à son retrait. Le RSSI-A est notamment chargé d'instruire les renouvellements d'homologation.

Pour le système dont il a la charge, il conseille, recommande et propose au responsable fonctionnel et au responsable technique du système des règles spécifiques. Il est le garant de la cohérence des mécanismes et des procédures de sécurité (MCS).

4.2 Organisation sécurité du partenaire

Cette politique ne préjuge pas de l'organisation sécurité mise en place au sein des partenaires mais elle requiert, a minima, un Correspondant SSI SBC pour chaque partenaire et désigné par celui-ci.

Les correspondants SSI SBC du partenaire peuvent être, sans exhaustivité :

- RSSI Projet (BUILD)
- RSSI Aval (RUN)
- RSSI SI
- RSSI Entité
- Officier de Sécurité
- Directeur de Projets PMB du partenaire

Chaque partenaire peut désigner des rôles miroir à ceux de l'organisation sécurité SBC d'IdFM.

Le Correspondant SSI SBC du partenaire constituera le point de contact privilégié d'IdFM pour les processus de management de la sécurité décrits dans le chapitre suivant.

5. Processus de management de la sécurité

5.1 Principes

Pour aborder le problème de la sécurité de l'information billettique des services du SBC de manière cohérente, il faut développer un cadre structuré couvrant les aspects de Security By Design en phase de construction, de maintien des services du SBC en condition de sécurité et de contrôle continu de la sécurité.

L'évaluation des risques de sécurité constitue l'étape préliminaire dans l'établissement et la mise en œuvre d'un programme logique et systématique de gestion de la sécurité de l'information billettique portée par les services du SBC.

Elle vise à identifier quels sont les vrais risques de sécurité pesant sur les actifs SBC, et particulièrement les titres dématérialisés et les DCPS, et quelles mesures de sécurité, techniques ou procédurales sont appropriées pour éliminer, ou pour le moins réduire les risques identifiés, afin d'assurer la continuité des activités des services du SBC.

Les mesures de sécurité exigées sont ensuite détaillées au travers de check-lists sécurité adaptées aux différentes briques constituant les services du SBC.

Des audits de conformité sont systématiquement menés afin de s'assurer de la bonne couverture des différentes briques à ces exigences de sécurité.

Ces audits de conformité sont complétés d'audits techniques de sécurité de type audit de code, audit de configuration et test d'intrusion.

Si l'ensemble de ces audits sont exigés avant toute première mise en service, le niveau de sécurité initialement évalué doit être maintenu tout au long du cycle de vie des services du SBC et des systèmes s'y raccordant.

Les processus d'intégration de la sécurité dans la construction des services du SBC, détaillés dans les chapitres suivants, précisent, pour chacun, les fréquences de renouvellement de la qualification sécuritaire.

5.2 Intégration de la sécurité dans la construction des services du SBC

5.2.1 Démarche d'homologation des services du SBC

IdFM mène une démarche d'homologation de sécurité des services du SBC sur son périmètre de responsabilité.

La démarche d'homologation est un processus d'information et de responsabilisation qui aboutit à une décision prise par l'autorité d'homologation, après avis de la commission d'homologation. Cette décision constitue un acte formel par lequel le responsable :

- atteste de sa connaissance du système d'information et des mesures de sécurité techniques, organisationnelles et juridiques mises en œuvre,
- accepte les risques qui demeurent, appelés risques résiduels.

En particulier, l'homologation atteste de la capacité d'un système d'information à traiter des informations sensibles au vu des mesures mises en œuvre pour les protéger.

La décision, prononcée par l'autorité d'homologation et valable pour une durée fixée, est communiquée aux partenaires.

La démarche d'homologation est maintenue tout le long du cycle de vie du système d'information et prend fin avec le retrait de services du SBC.

La démarche est détaillée en référence [HOMOL].

Il est à noter que la démarche d'homologation initiale d'un service intègre la rédaction d'une note sur la sécurité billettique et la gestion de la fraude technologique couvrant l'intégralité du service concerné.

5.2.2 Procédure d'agrément des applications mobiles

Toute application mobile étant interfacée avec les composants critiques des services du SBC, intégrant des sous-systèmes SBC et reposant sur un support physique non maitrisé, peut par là-même induire des vulnérabilités sur l'ensemble de la solution et sur le niveau de service.

A ce titre, IdFM met en place une procédure d'agrément des applications mobiles qui répond à plusieurs objectifs :

- Pour IdFM, de maintenir le niveau global de sécurité des services SBC.
- Pour les propriétaires d'applications mobiles, de leur faciliter le respect des exigences contractuelles qui s'imposent à leurs activités de vente de titres de transport en Ile-de-France.
- Pour les usagers, de leur apporter des garanties concernant la sécurité de l'application mobile.

La procédure est détaillée en référence [AGR-APPMOB].

5.3 Opération et coordination de la sécurité des services du SBC

Le Maintien en Conditions de Sécurité (MCS) a pour but de maintenir les services du SBC au niveau de sécurité initial évalué au travers du processus d'homologation de sécurité mené préalablement à l'ouverture du service.

L'objectif du MCS est de collecter, agréger et synthétiser les informations traitant des évolutions de la menace et des vulnérabilités. Il s'agit également de qualifier le risque dans le temps et, bien entendu, il faut accompagner le déploiement des correctifs de sécurité.

Le MCS s'impose tout particulièrement aux systèmes interconnectés, à ceux dont la menace liée au contexte extérieur est forte et évolutive, et il faut donc maintenir un bon niveau de sécurité intrinsèque mais aussi cohérent avec l'environnement.

Les services du SBC étant subdivisés en plusieurs sous-systèmes largement indépendants, il est essentiel de dégager une vision globale et coordonnée du MCS du Canal Mobile.

Le dossier de coordination du MCS, référencé [COORD-MCS], détaille les processus de suivi global du MCS, de gestion des incidents de sécurité et d'amélioration continue. Il précise également les acteurs de ces processus, la comitologie et les engagements de service.

5.4 Contrôle de la sécurité billettique des services du SBC

Depuis la mise en service du service Canal Mobile, le RSSI Aval des services du SBC mène les travaux de corrélation des traces de sécurité et d'activité afin de mener les points de contrôle de l'activité billettique qui permettent de détecter des pertes de chiffre d'affaire, pouvant générer des suspicions de fraude.

La politique des contrôles billettiques mise en œuvre au sein des services du SBC est référencée [CTRL-BILL].

6. Annexes

6.1 Textes applicables pour les services SBC

Référence	Libellé	Date
[RGPD]	Règlement (UE) 2016/679 du Parlement Européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.	27/04/2016
[RGS]	Référentiel général de sécurité – V2.0	13/06/2014
[PSSIE]	Politique de Sécurité des Systèmes d'Information de l'Etat	17/07/2014

6.2 Textes de référence pour les services SBC

Référence	Libellé	Date
[HOMOL-CM]	Stratégie d'Homologation de sécurité du Canal Mobile	16/07/2019
[AGR-APPMOB]	Procédure d'Agrément sécurité des applications mobiles	15/06/2020
[COORD-MCS]	Dossier de coordination du Maintien en Condition de Sécurité	01/02/2021
[CTRL-BILL]	Politique des contrôles billettiques des services du SBC	14/09/2020

6.3 Directives sécurité pour les services SBC

IdFM s'engage sur l'application des directives sécurité pour les services SBC détaillant les mesures de sécurité mises en œuvre.

Pour le raccordement des SI Partenaires au SIS, les directives comprennent les « Spécifications d'interconnexion standard au SIS » complétées d'un « Document Architecture des interfaces <Partenaire> avec le SIS » présentant les spécificités sécurité propres à chaque Partenaire.

Pour la mise en œuvre et l'usage de la plateforme de test billettique IdFM, hébergée sur le site Lafayette d'IdFM, le « Dossier sécurité plateforme de test Lafayette » précise les éléments de sécurité physique, l'architecture réseau incluant les modes d'interconnexion, les modalités de protection de l'environnement physique et l'organisation associée.

La « Politique de contrôle d'accès SBC » détaille les modalités de gestion des utilisateurs, et des habilitations associées, se connectant au SBC. Cette politique couvre aussi bien les différents rôles d'opérateurs et de coordonnateurs assurés par la filiale que les utilisateurs Partenaires.

6.4 Glossaire

Sigle	Signification
AH	Autorité d'Homologation
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
DCPS	Données à Caractère Personnel et Sensibles
MCO	Maintien en Condition Opérationnelle
MCS	Maintien en Condition de Sécurité
OWASP	Open Web Application Security Project
PSSI	Politique de Sécurité du Système d'Information
RSSI-A	Responsable de la SSI Aval
RSSI-P	Responsable de la SSI Projets
SSI	Sécurité des Systèmes d'Information