Profil de Protection
pour Carte à puce Billettique Avec et Sans Contact

Version : **1.2**

Date : 02/02/99

Enregistré par l'Organisme de Certification français sous la référence PP/9903

SOMMAIRE

1. Introduction

1.1. Identification du profil de protection

Titre : Profil de Protection pour Carte à puce Billettique Avec et Sans Contact

Enregistrement : PP/9903

Mots clés : Carte à puce, billettique, sans contact

Un glossaire des termes employés dans ce profil de protection figure en annexe.

Ce profil de protection a été rédigé à l'aide de la version 2.0 des Critères Communs pour l'Évaluation et la Certification de la Sécurité des Technologies de l'Information.

1.2. Présentation du profil de protection

Ce profil de protection est l'oeuvre de deux opérateurs de transports français :

- la Régie Autonome des Transports Parisiens,
- et la Société Nationale des Chemins de Fer Français.

L'objet de ce profil de protection est de spécifier les **exigences de sécurité minimales** qui doivent être satisfaites par les **cartes à puce** utilisées en **billettique multimodale** par les deux entreprises ci-dessus.

Les cartes à puce visées par le profil de protection :

- doivent pouvoir fonctionner
  - soit **en insertion** — mode à contact,
  - soit **en téléalimentation** — mode sans contact où la carte ne contient pas de pile : l'énergie qui lui est nécessaire pour fonctionner lui est fournie par le dispositif d'interface,
- peuvent posséder un microprocesseur, mais ce n'est pas a priori nécessaire (c'est peut-être une contrainte issue de la prise en compte des exigences de sécurité définies dans ce profil de protection).

Par "billettique", on entend ici la gestion de l'accès aux moyens de transport.

Les cartes à puce billettiques peuvent comporter d'autres "applications" que l'application billettique multimodale, comme par exemple une application de porte-monnaie électronique et une ou plusieurs applications de fidélisation. À une "application" correspond toujours une zone mémoire dédiée, employée pour stocker des informations voire des traitements spécifiques à l'application.

Ce profil de protection peut s'appliquer aux cartes à puce permettant le téléchargement d'applications constituées d'informations et de traitements, c'est-à-dire des cartes à puce avec machine virtuelle (exemple : les JavaCard).

Le niveau d'assurance visé pour ce profil de protection est : **EAL 4 augmenté**.

Le niveau de robustesse des fonctions de sécurité demandé est : **fort,** c'est-à-dire **SOF-high**.

Optique d'élaboration et caractéristiques principales du profil de protection :

Les trois points ci-dessous résument l'optique qui a été adoptée pour l'élaboration de ce profil de protection :

- volonté de prendre en compte une cible d'évaluation la plus large possible. Or, la sécurité d'une carte à puce est grandement liée à la façon dont les composants matériels et logiciels coopèrent,
- volonté de la part des auteurs de ne formuler des exigences de sécurité que pour ce qui est de leur ressort (phase opérationnelle),
- volonté de s'inscrire dans la démarche adoptée pour le profil de protection pour circuit intégré encartable, [SIC], et consistant à élaborer un profil de protection pour chaque phase du cycle de vie d'une carte à puce.

Du fait de l'optique retenue, les principales caractéristiques de ce profil de protection sont :

- La cible d'évaluation choisie pour ce profil de protection est la carte à puce billettique multimodale de laquelle on retire les applications non billettiques. En effet, les cartes à puce utilisées en billettique peuvent contenir des applications qui ne sont pas de la responsabilité des opérateurs de transport.

  La cible d'évaluation est donc constitué de composants matériels et de logiciels. La cible d'évaluation n'est pas seulement la composante logicielle de l'application billettique.
- Ce profil de protection concerne la phase de spécification de la carte. C'est en effet à ce stade que le profil doit être utilisé.
- Néanmoins, les menaces considérées couvrent tout le cycle de vie de la carte, et surtout la phase opérationnelle (quand la carte a été délivrée à son porteur). Les menaces concernant les phases qui précèdent la phase opérationnelle (phase 7) sont peu détaillées car ces phases sont pour la plupart en dehors du métier des auteurs de ce profil de protection.
- Les objectifs de sécurité sur la cible d'évaluation ne concernent que les menaces identifiées pour la phase opérationnelle. Il en découle que :
  - les menaces identifiées pour les phases précédentes sont couvertes par les objectifs de sécurité portant sur l'environnement de la cible d'évaluation,
  - les exigences fonctionnelles de sécurité portant sur la cible d'évaluation ne concernent que la phase opérationnelle.

1.3. Références

[CC-1] Common Criteria for Information Technology Security Evaluation
Part 1 : Introduction and general model
CCIB-98-026, version 2.0 de mai 1998

[CC-2] Common Criteria for Information Technology Security Evaluation
Part 2 : Security functional requirements
CCIB-98-027, version 2.0 de mai 1998

[CC-2B] Common Criteria for Information Technology Security Evaluation
Part 2 : Annexes
CCIB-98-027A, version 2.0 de mai 1998

[CC-3] Common Criteria for Information Technology Security Evaluation
Part 3 : Security assurance requirements
CCIB-98-028, version 2.0 de mai 1998

[SIC] Smartcard Integrated Circuit Protection Profile, version 2.0
Enregistré au SCSSI sous la référence PP/9806

2. Description de la TOE

Ce chapitre présente de façon détaillée la TOE, en insistant sur son environnement opérationnel.

2.1. Nature de la TOE

La TOE est une carte à puce utilisée en billettique, pouvant fonctionner soit en insertion soit en téléalimentation (combi-carte), et dont on ne prend pas en compte les éventuelles applications non billettiques.

Du fait de l'optique retenue pour ce profil de protection — positionnement en phase de spécification de la carte, mais menaces exprimées pour toutes les phases de leur cycle de vie — la TOE considérée est à la fois :

- la carte à puce en devenir, au cours de son développement,
- la carte à puce opérationnelle.

La TOE opérationnelle est constituée des éléments suivants d'une carte à puce combi :

- la partie du circuit intégré, comportant :
  - **l'application billettique** multimodale,
  - les composants matériels et les **composants** logiciels **de base** (système d'exploitation et firmware),
- **l'antenne** et les composants associés (pour les communications sans contact).

Le circuit intégré ne comporte pas forcément de microprocesseur : il peut être conçu en logique câblée.

2.2. Cycle de vie de la TOE

Le cycle de vie d'une TOE considéré dans ce profil de protection et rapporté dans le tableau ci-dessous est conforme à celui pris en compte dans [SIC]. La phase 1 est cependant ici constituée de deux sous-phases :

- une première sous-phase de spécification de la carte — les acteurs principaux sont les utilisateurs de la carte opérationnelle, et notamment les opérateurs de transport,
- une seconde sous-phase de conception et développement du logiciel embarqué ainsi que de spécification des exigences de pré-personnalisation du circuit intégré — l'acteur principal est le concepteur/développeur du logiciel embarqué .

Ce profil de protection porte sur la sous-phase de spécification de la carte de la phase 1.

Phase 1	Spécification de la TOE	Le spécificateur de la TOE a en charge la spécification de la TOE et notamment du logiciel embarqué.
	Développement du masque	Le concepteur du masque a en charge : • le développement du masque, • la spécification des exigences de pré-personnalisation du CI.
Phase 2	Conception et développement du CI	Le concepteur du CI a en charge : • la conception du CI, • le développement du logiciel dédié au CI (firmware) • la fourniture, au concepteur du masque, d'informations, de logiciels et/ou d'outils, • la réception du masque, via des procédures de livraison et de vérification de confiance, • la construction de la base de données du CI, nécessaire à la fabrication du photomasque, • la fabrication du photomasque.
Phase 3	Fabrication et test du CI	Le fabricant du CI a en charge la production du CI, ce qui inclut : • la fabrication du CI, • le test du CI, • la pré-personnalisation du CI.
Phase 4	Collage et test du CI	L'entreprise qui réalise le collage du CI a en charge : • le collage du CI, • le test du CI.
Phase 5	Encartage du CI	Réalisée par l'encarteur.
Phase 6	Personnalisation de la carte	Le personnalisateur de la carte a en charge : • la personnalisation de la carte, qui peut inclure le chargement d'un autre logiciel embarqué ou d'une autre partie de logiciel embarqué. • les tests finaux.
Phase 7	Utilisation opérationnelle de la carte	L'émetteur de la carte est responsable : • de la délivrance de la carte au porteur, • de la fin de vie de la carte.

Cycle de vie de la TOE

La phase 7 est appelée phase "opérationnelle" par la suite.

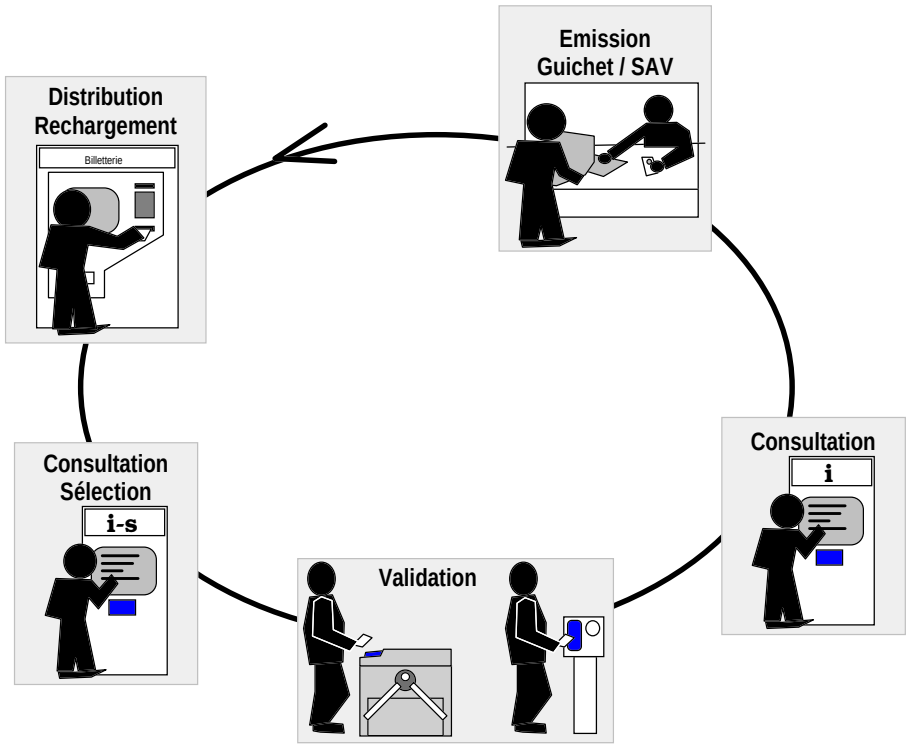
2.3. Utilisation de la TOE, en phase opérationnelle

Ce paragraphe précise l'utilisation attendue de la TOE par l'utilisateur final, le porteur. Il concerne la phase opérationnelle (phase 7).

Dès qu'une TOE sera délivrée à un porteur, celui-ci pourra s'en servir pour effectuer les opérations billettiques suivantes :

- Chargement d'un titre de transport — cette opération consiste à stocker dans la TOE un titre de transport après que le porteur l'a payé,
- Rechargement de la réserve d'argent — cette opération consiste à approvisionner la réserve d'argent stockée par la carte après que le porteur a payé la somme correspondante,
- Sélection d'un titre de transport — la TOE peut contenir plusieurs titres de transport. La sélection est l'opération qui permet à un porteur d'indiquer quel titre il compte utiliser. Elle est à effectuer avant de rentrer sur un réseau de transport (géré par un opérateur de transport),
- Validation d'un titre de transport (avec éventuellement paiement du titre à l'aide de la réserve d'argent) — cette opération consiste, à l'entrée voire à la sortie d'un réseau de transport, à inscrire l'information dans la TOE. Dans les gares de trains, la validation s'effectue typiquement au passage des tourniquets. Dans certains cas, la validation est accompagné d'un débit de la réserve d'argent,
- Contrôle embarqué — cette opération consiste à vérifier à bord d'un moyen de transport (train, bus ...) que le porteur est en règle, c'est-à-dire que le titre de transport validé est valide,
- Consultation d'informations billettiques — cette opération permet au porteur d'obtenir un certain nombre d'informations sur le contenu de sa carte. Comme par exemple la liste des titres de transport,
- Chargement d'informations billettiques — cette opération permet d'inscrire, modifier ou supprimer dans la TOE des informations utiles pour les autres opérations (exemple : modification des droits à réduction),
- Service après-vente — le service après-ventre regroupe les opérations effectuées à un guichet et concernant :
  - l'échange et le remboursement d'un titre de transport,
  - la gestion des problèmes d'accès aux trains (réclamations).

Le schéma ci-dessous récapitule les opérations de ce qui est communément appelé la "chaîne du voyage" .



Chaîne du voyage

2.4. Principes des échanges entre la TOE et un équipement billettique, en phase opérationnelle

NOTA BENE : Dans la suite du profil de protection, est appelé "équipement billettique" tout équipement utilisé par un système billettique pour dialoguer avec la TOE.

Lors d'une opération avec un équipement billettique, la TOE est toujours pilotée par l'équipement. Une opération est ainsi formée d'une succession d'échanges, chacun de ceux-ci étant constitués d'une commande envoyée par l'équipement à la TOE et de la réponse de celle-ci.

La réponse de la TOE comporte toujours un code d'erreur permettant à l'équipement billettique de savoir si une erreur est survenue.

La nature et le nombre des échanges varient suivant le type d'opération (chargement d'un titre de transport, service après-vente ...) et la situation (le chargement d'un abonnement diffèrera de celui d'un titre unitaire).

Du point de vue de la sécurité, il y a deux principaux types de commande :

- les commandes de lecture dans la TOE,
- les commandes d'écriture dans la TOE, plus sensibles puisque modifiant le contenu et donc potentiellement la valeur de la carte.

2.5. Types d'utilisateur de la TOE, en phase opérationnelle

Les types d'utilisateur de la TOE considérés dans ce profil de protection, au sens des Critères Communs (cf. [CC-2]) sont les suivants, pour la phase opérationnelle :

- porteur : remote human user (pour la saisie du PIN uniquement),
- équipement billettique : remote untrusted IT product.

Dans ce profil de protection, il a été décidé de ne pas considérer que les équipements billettiques utilisés en phase opérationnelle sont des équipements de confiance, c'est-à-dire des "remote trusted IT products" au sens de [CC-2]. Cela permet en effet :

- de faire en sorte que l'évaluateur de la TOE n'utilisera pas ces équipements billettiques dans ses tests de la TOE, et de rendre ainsi la démarche d'évaluation de la TOE complètement indépendante du développement et de la sécurité des équipements billettiques,
- ne pas rendre nécessaire l'évaluation de tous les équipements billettiques,
- de prendre en compte le cas des équipements non billettiques (dans le cas où la carte contient plusieurs applications).

Remarque : il est cependant bien clair que la démarche d'analyse de la sécurité qu'appellent les Critères Communs et adoptée pour la carte à puce billettique multimodale pourra être complétée par des démarches similaires sur les équipements billettiques.

2.6. Fonctionnalités de la TOE

Afin de remplir ses missions, la TOE doit disposer de fonctionnalités :

- de stockage de données,
- et de traitement. La TOE doit notamment :
  - effectuer des calculs arithmétiques (incrémentation de compteurs ...),
  - effectuer des calculs cryptographiques (calcul et vérification de signatures électroniques ...),
  - gérer ses communications avec l'extérieur,
  - gérer l'accès à sa mémoire (écriture / lecture suivants droits d'accès ...).

3. Environnement de sécurité de la TOE

3.1. Typologie des attaques

Les motivations prévisibles sont surtout :

- **avides** : appât du gain ou envie de moins dépenser,
- **ludiques** (y compris avec de gros moyens, en université par exemple),
- **stratégiques** — on range dans cette catégorie les velléités d'un organisme désireux d'obtenir des informations sur un porteur (pour un usage marketing par exemple) auxquelles il ne devrait pas avoir accès. La motivation stratégique peut conduire à une atteinte à la vie privée des porteurs,
- rancunières,
- voire terroristes — on range sous cette appellation les motivations d'individus ou de groupes désirant semer le désordre dans les systèmes billettiques sans vouloir en retirer un avantage financier ou concurrentiel.

Compte tenu du haut niveau technologique des cartes à puce billettiques, il est estimé que les attaques seront surtout le fait d'entités disposant de moyens financiers et techniques considérables, qui seront surtout motivées par l'appât du gain ou des raisons stratégiques.

Un attaquant motivé par l'appât du gain va par exemple chercher à :

- charger des titres de transport sans les payer,
- créditer sa réserve d'argent sans payer la contre-partie financière.

Il convient de ne pas écarter les attaques d'individus isolés, motivés principalement par l'aspect ludique ou l'envie de moins dépenser. Les moyens de communications (Internet) permettent de diffuser très facilement et très largement une attaque réussie. Cependant ces attaques sont surtout cantonnées aux phases d'utilisation et de fin de vie : la motivation ludique est plus pertinente quand la personne n'appartient pas au personnel d'une entité jouant un rôle dans les phases précédant la phase opérationnelle.

Les attaques de nature rancurières ne semblent pas aussi probables. En effet, elles seront réalisées par des personnes ayant accès au système billettique et viseront celui-ci bien plus que la carte.

Les attaques de nature terroriste sont peu probables.

3.2. Biens

Le tableau suivant précise les types de bien identifiés pour la TOE, et donne des exemples de biens pour chaque type, ainsi que le besoin de sécurité de chaque type ('C' = Confidentialité, 'I' = Intégrité).

Types de biens				Précisions / Exemples	Besoin de sécurité
Biens intermédiaires	Ayant un besoin de confidentialité et d'intégrité			Le photomasque (fabriqué en phase 2), le logiciel dédié du circuit intégré.	C + I
	Ayant un besoin d'intégrité seul			Les spécifications de la carte.	I
Biens finaux	Traitements	De niveau TOE		Les traitements de niveau TOE sont les traitements que chaque application peut utiliser.	I[1]
		Billettiques		Les traitements billettiques sont spécifiques à l'application billettique.	I[1]
	Informations	De niveau TOE	Eléments secrets	Exemples possibles : la clé permettant de créer l'application billettique, un code (PIN) permettant au porteur d'être authentifié.	C + I
			Informations de gestion et de structure	Exemples d'informations de gestion : l'identifiant de la TOE, les informations relatives à l'encarteur.	I[2]
		Billettiques	Eléments secrets	Les clés (différentes) utilisées par les équipements de vente et de validation pour authentifier la TOE.	C + I
			Informations applicatives ayant un besoin de confidentialité et d'intégrité	Ce sont des informations applicatives liées au porteur. Exemples possibles : • les voyages (on n'accèderait par exemple sans présentation du PIN qu'au dernier événement de transport) • des informations personnelles (donnant par exemple droit à des réductions)	C + I
			Informations applicatives et de structure ayant un besoin d'intégrité seul	Informations applicatives représentant notamment : • une valeur, comme un contrat de transport, • un droit à réduction, c'est-à-dire liées au porteur (mais n'ayant pas de besoin de confidentialité), • l'état de la TOE, comme l'information indiquant son blocage : un attaquant sachant que sa carte est repérée et bloquée pourrait échapper aux systèmes billettiques s'il sait effectuer la modification inverse.	I[2]

Biens identifiés pour la TOE

En outre, **la TOE elle-même est un bien**.

[1] Les traitements sensibles mis en oeuvre dans la TOE n'ont pas de besoin de confidentialité : en cryptologie, on suppose toujours que l'ennemi connaît l'algorithme de chiffrement, et que la sécurité du cryptosystème repose avant tout sur le secret des clés.

[2] Les informations de structure, de niveau TOE ou billettiques, sont décrites dans des documents de spécification ou de conception et sont donc supposées connues d'un attaquant potentiel : elles n'ont pas de besoin de confidentialité.

NOTA BENE :

- tous les traitements de la TOE sont sensibles (besoin d'intégrité)
- toutes les informations de la TOE (de niveau TOE et billettiques) sont sensibles : elles ont toutes un besoin d'intégrité, et certaines ont en plus un besoin de confidentialité
- tous les biens ont un besoin d'intégrité
- aucun bien n'a un besoin de disponibilité

Précisions :

- Les biens intermédiaires sont ceux qui n'existent pas dans la TOE à l'état opérationnel, mais qui sont transformés en d'autres biens intermédiaires ou en biens finaux.
- Les biens finaux existent tous dans la TOE à l'état opérationnel mais certains peuvent exister avant (exemple : les traitements sensibles de niveau TOE existent à l'issue de la phase 3 de fabrication et de test du circuit intégré).
- Les éléments secrets sont des clés, codes, valeurs initiales (intervenant dans des calculs cryptographiques) ...
- Les informations de structure, qu'elles soient billettiques ou de niveau TOE, sont relatives à l'organisation des données dans les fichiers (nombre de fichiers, taille et mode d'accès des fichiers ...).
- Les traitements sont mis en oeuvre à l'aide de composants matériels et logiciels.

3.3. Acteurs de la TOE

Trois types d'acteur sont considérés dans ce profil de protection :

1. les acteurs qui spécifient la TOE,
2. les acteurs qui agissent sur la TOE, y compris en phase opérationnelle,
3. les acteurs qui utilisent la TOE opérationnelle, les porteurs.

Dans le cas où la carte billettique n'héberge aucune autre application, les acteurs de la sous-phase de spécification de la carte de la phase 1 sont :

- des organismes impliqués dans la billettique (opérateurs de transports notamment), qui spécifient entièrement la carte — acteurs de type 1,
- l'organisme chargé de concevoir et de développer le logiciel embarqué — acteur de type 2.

Dans le cas où la carte billettique héberge une ou plusieurs autres applications, les acteurs de la sous-phase de spécification de la carte de la phase 1 sont :

- des organismes impliqués dans la billettique (opérateurs de transports notamment), qui spécifient l'application billettique de la carte et participent aux spécifications du reste de la TOE — acteurs de type 1,
- des organismes spécifiant les applications non billettiques, qui participent également aux spécifications de la partie de la TOE commune à toutes les applications — acteurs de type 1,
- l'organisme chargé de concevoir et de développer le logiciel embarqué — acteur de type 2.

Dans les menaces ci-dessous, un certain nombre ont pour libellé "modification non autorisée" ou "divulgation non autorisée", libellé accompagné de la mention des biens concernés.

Une modification ou une divulgation sont considérées comme non autorisées quand :

- l'utilisateur d'un document ou équipement employé au titre de la phase est non autorisé — tout utilisateur autre que celui désigné pour effectuer cette tache est non autorisé ; un utilisateur autorisé fait partie du personnel d'un acteur de la TOE chargé de la spécifier (acteur de type 1) ou d'agir dessus (acteur de type 2),
- un utilisateur autorisé effectue une action qui ne lui est pas autorisée, à la suite d'une erreur ou d'une malveillance.

3.4. Hypothèses

3.4.1. Hypothèses sur l'usage attendu de la TOE

Aucune.

3.4.2. Hypothèses sur l'environnement de la TOE pendant tout son cycle de vie

NOTA BENE : Le titre proposé par les Critères Communs (cf. [CC-2]) pour ce paragraphe est "Hypothèses sur l'environnement d'utilisation de la TOE". Or, dans ce profil de protection la TOE est à la fois une carte à puce en devenir, au cours de son développement, que la carte à puce opérationnelle de la phase 7. Il a ainsi paru judicieux de rebaptiser le titre de ce paragraphe afin de pouvoir formuler des hypothèses sur la phase d'utilisation de la TOE, la phase opérationnelle, mais également sur les phases où la TOE n'est pas encore opérationnelle, les phases de développement.

A.QUAL : Il est supposé que les acteurs de la TOE, quelle que soit la phase, connaissent les responsabilités financières, civiles et pénales associées au développement ou à l'utilisation de la TOE.

A.EQPT_DVPT : Il est supposé que tous les équipements utilisés pour agir sur les biens intermédiaires et finaux, avant que la TOE ne soit à l'état opérationnel, sont de confiance (conception, réalisation, installation, maintenance).

3.5. Menaces

Remarques :

- Les menaces ci-dessous font référence à des attaques physiques aussi bien que logiques.
- Pour les menaces portant sur des biens finaux, des exemples sont donnés afin d'éclairer le lecteur. Ce n'est pas le cas pour celles qui portent sur des biens intermédiaires car cela amènerait à citer donner des exemples de tels biens. Ce qui n'est pas l'optique choisie pour ce profil de protection.

3.5.1. Menaces portant sur les biens intermédiaires

T.INTER_MOD : Modification non autorisée de biens intermédiaires

- ayant un besoin d'intégrité seul,
- ayant un besoin de confidentialité et d'intégrité.

Remarques :

Les attaques sont de nature soit accidentelle soit malveillante : les modifications sont erronées ou illicites (respectivement). Dans le second cas, les attaquants sont essentiellement des groupes organisés, dont la motivation est soit avide soit stratégique, et susceptibles de bénéficier de complicités en interne à l'un des acteurs de la TOE, de type 1 ou 2. Mais ce peut être des individus isolés, faisant partie du personnel de l'un des acteurs de la TOE, poussés par la rancune.

Les connaissances techniques et cryptographiques ainsi que les moyens financiers peuvent être importants, mais ce n'est pas nécessaire.

T.INTER_DIV : Divulgation non autorisée de biens intermédiaires

- ayant un besoin de confidentialité et d'intégrité.

Remarques :

Les attaques sont de nature accidentelle ou malveillante (surtout). Dans le second cas, les attaquants sont essentiellement des groupes organisés, dont la motivation est soit avide soit stratégique, et susceptibles de bénéficier de complicités en interne à l'un des acteurs de la TOE, de type 2. Mais ce peut être des individus isolés, faisant partie du personnel de l'un des acteurs de la TOE, poussés par la rancune.

Les connaissances techniques et cryptographiques ainsi que les moyens financiers peuvent être importants, mais ce n'est pas nécessaire.

T.INTER_VOL : Vol de biens intermédiaires

Remarques :

Cette attaque, de nature malveillante, est avant tout le fait de groupes organisés, bénéficiant ou non de complicités au sein du personnel de l'un des acteurs de la TOE, de type 2.

Les moyens financiers ne sont pas forcément importants. Aucune connaissance technique ou cryptographique n'est requise.

3.5.2. Menaces portant sur les biens finaux

Rappel : Un bien est considéré comme final dès qu'il existe dans la TOE, même si son existence dans la TOE commence avant la phase opérationnelle.

T.FIN_MOD_TRAIT : Modification non autorisée de traitements sensibles

- traitements de niveau TOE,
- traitements billettiques.

Remarques :

Les attaques sont uniquement malveillantes et a priori le fait de groupes organisés disposant de connaissances techniques et cryptographiques et de moyens financiers importants.

Exemple(s) de menace :

– modification des traitements effectués par la TOE quand elle reçoit la commande de débit de la réserve d'argent afin d'éviter de la débiter ou de limiter le montant du débit.

T.FIN_MOD_INFO : Modification non autorisée d'informations sensibles, à savoir

- d'éléments secrets billettiques,
- d'informations billettiques applicatives ayant un besoin de confidentialité et d'intégrité,
- d'informations billettiques applicatives et de structure ayant un besoin d'intégrité seul,
- d'éléments secrets de niveau TOE,
- d'informations de gestion et de structure de niveau TOE.

Remarques :

Les attaques peuvent être accidentelles mais sont surtout malveillantes. Les motivations des attaquants sont alors principalement avides, ludiques et stratégiques.

Cette menace prend toute son ampleur en phase opérationnelle, quand la TOE est la plupart du temps non maîtrisée car en possession de son porteur. Il est donc très facile de se procurer des TOE et de se livrer sur elles à toutes sortes de manipulations.

La mise en oeuvre de cette menace nécessite a priori des connaissances techniques et cryptographiques et des moyens financiers importants.

Exemple(s) de menace :

- modification des informations relatives à un titre de transport afin d'en élargir la portée (transformation par exemple d'un abonnement hebdomadaire en abonnement mensuel),
- inscription illicite dans la TOE du droit à réduction "famille nombreuse 30%".

T.FIN_DIV_I : Divulgation interdite

- d'éléments secrets billettiques,
- d'éléments secrets de niveau TOE.

Remarques :

Les informations susmentionnées ne doivent pas être accessibles à qui que ce soit.

La menace s'applique notamment pendant toutes les opérations billettiques possibles en phase opérationnelle, et en dehors.

Les attaques sont malveillantes, pas accidentelles. Elles doivent demander des connaissances techniques et cryptographiques ainsi que des moyens financiers importants. Les motivations sont avides, stratégiques voire ludiques.

Exemple(s) de menace :

- lecture dans le silicium de la clé permettant de charger un titre de transport. La réalisation de cette menace permet ensuite d'être en mesure d'en mettre d'autres en application, par exemple le chargement de titres de transport sans les payer (T_FIN_MOD_INFO).

T.FIN_DIV_NA : Divulgation non autorisée

- d'informations billettiques applicatives ayant un besoin de confidentialité et d'intégrité.

Remarques :

La menace s'applique surtout pendant la phase opérationnelle.

Les attaques sont malveillantes, pas accidentelles. Dans ce cas, les attaques ne nécessitent pas forcément des connaissances techniques et cryptographiques ni des moyens financiers importants. Les motivations sont avant tout stratégiques, et visent notamment l'atteinte à la vie privée du porteur.

Exemple(s) de menace :

- lecture des références bancaires du porteur utilisées pour le paiement du chargement des titres.

T.FIN_CLONE : Clonage de la TOE

Remarques :

Cette menace consiste en la reproduction de la TOE par copie de son support physique, ou en la simulation logique permettant à l'attaquant de reproduire tout ou partie des fonctions de la TOE.

Cette attaque, de nature uniquement malveillante, est avide, voire ludique.

Selon le mode de reproduction, les moyens financiers peuvent être conséquents et de bonnes connaissances techniques et cryptographiques nécessaires. Dans le cas où la reproduction consiste en une simulation logique, l'attaque nécessite au préalable l'obtention des éléments secrets concernés.

Cette menace n'est pas prise en compte pour les biens intermédiaires : le clonage de ces biens est certes possible, mais le clone obtenu n'est pas opérationnel. Il faut donc réaliser au moins une autre menace sur le clone avant de pouvoir l'utiliser.

Exemple(s) de menace :

- sans objet.

T.FIN_VOL : Vol de la TOE

Remarques :

Cette menace est toujours d'origine malveillante, pas accidentelle. Elle prend toute son ampleur lors de la phase opérationnelle, car la TOE y est très souvent non maîtrisée : son vol est bien plus aisé à réaliser que lors des phases précédentes.

Le vol peut donc être le fait d'individus isolés voire de groupes désirant seulement utiliser la carte volée, sans chercher à la trafiquer. Outre le fait que la TOE est considérée elle-même comme un bien, le vol de TOE peut avoir des retombées sur l'image et l'acceptation des systèmes billettiques, notamment s'il permet de léser des clients/porteurs.

Exemple(s) de menace :

- vol de la TOE d'un porteur alors qu'il l'utilise pour charger un titre de transport.

3.6. Règles organisationnelles de sécurité

Les règles organisationnelles ci-dessous sont issues de la prise en compte de menaces portant non pas sur la TOE mais sur le reste du système billettique. Ces menaces engendrent néanmoins des exigences fonctionnelles concernant la TOE.

P.GEN_AUTH : La TOE doit, en phase opérationnelle, pouvoir s'authentifier auprès d'un équipement billettique à la demande de celui-ci.

P.VERIF_SIGN : La TOE doit, en phase opérationnelle, pouvoir vérifier l'intégrité de certaines informations qui lui sont transmises.

Remarques :

- ces informations ne sont pas forcément billettiques : ce peut être des informations de niveau TOE,
- ces informations ne sont pas sensibles : une information doit être stockée dans la TOE pour être sensible,
- ces informations peuvent devenir, une fois stockées, des traitements billettiques (le téléchargement en phase opérationnelle de traitements de niveau TOE est exclu).

P.CALC_SIGN : La TOE doit, en phase opérationnelle, pouvoir donner à l'équipement billettique avec lequel elle dialogue, quel qu'il soit, la possibilité de vérifier l'intégrité de certaines informations billettiques sensibles qu'elle lui transmet.

P.DECHIF_CLE : La TOE doit, en phase opérationnelle, déchiffrer les clés qui lui sont transmises avant de les stocker dans la TOE.

4. Objectifs de sécurité

La justification de ce que les objectifs de sécurité définis dans ce chapitre couvrent effectivement les menaces, hypothèses et règles organisationnelles du chapitre précédent est fournie au chapitre 7 "Justifications".

4.1. Objectifs de sécurité pour la TOE

NOTA BENE : Les objectifs pour la TOE présentés dans ce paragraphe ne concernent que la **phase opérationnelle**, donc que des **biens finaux**. Les menaces pesant sur les biens intermédiaires sont couvertes par les objectifs portant sur l'environnement de la TOE.

O.AUTH : La TOE doit pouvoir s'identifier et s'authentifier auprès d'un équipement billettique.

O.AUTH_REC : La TOE doit pouvoir authentifier un équipement billettique. En cas d'échec de l'authentification d'un équipement billettique, la TOE doit avertir celui-ci.

Remarque : l'identification d'un équipement billettique n'est pas indispensable. Seule son authentification est nécessaire, dans certains cas.

O.PORTEUR : La TOE doit pouvoir authentifier son porteur. Elle doit n'accepter qu'un nombre limité de tentatives infructueuses d'authentification. A chaque tentative infructueuse, la TOE doit avertir l'équipement billettique avec lequel elle dialogue.

O.ACCES : La TOE doit contrôler l'accès à tous ses biens finaux afin d'en protéger la confidentialité et/ou l'intégrité.

O.INTEG_STOCK : La TOE doit pouvoir vérifier l'intégrité de ses traitements et informations sensibles, et réagir à tout défaut d'intégrité en avertissant l'équipement billettique avec lequel elle dialogue.

O.INTEG_RECP : La TOE doit pouvoir vérifier l'intégrité des informations qu'elle reçoit. Cela inclut les informations qui deviendront des traitements billettiques sensibles une fois stockées dans la TOE (cas d'une carte à puce avec machine virtuelle). En cas de vérification négative, la TOE doit avertir l'équipement billettique avec lequel elle dialogue.

Rappel : les informations concernées par cet objectif ne sont pas considérées comme sensibles. Un sous-ensemble seulement deviendra sensible, une fois stocké dans la TOE.

O.INTEG_EMIS : La TOE doit pouvoir permettre aux équipements billettiques de vérifier l'intégrité des informations sensibles qu'elle leur transmet.

O.DECHIF_CLE : La TOE doit savoir déchiffrer les clés qui lui sont transmises durant la phase opérationnelle.

O.PHYSIQUE : La TOE doit posséder des dispositifs de protection contre les attaques physiques (physical tampering), ainsi que des dispositifs de détection. En cas de détection d'une attaque physique, elle doit réagir en avertissant l'équipement billettique avec lequel elle dialogue.

O.DYSFONC : La TOE doit pouvoir détecter tout dysfonctionnement, accidentel ou provoqué, rester dans un état sûr, et avertir l'équipement billettique avec lequel elle dialogue.

Remarque : On appelle "dysfonctionnement" toute exécution d'un traitement qui rencontre un problème, dû par exemple à un défaut d'intégrité dans le code du traitement ou dans les données stockées qu'il utilise.

4.2. Objectifs de sécurité pour l'environnement de la TOE

O.ACCES_PHY : Lorsque la TOE n'est pas entre les mains d'un porteur, l'accès physique à la TOE doit être contrôlé, quelle que soit la phase.

O.LIVRAISON : Durant ses transferts entre acteurs l'intégrité et la confidentialité de la TOE doivent être préservées, quelle que soit la phase.

O.SENSIB_FORM : Les acteurs de la TOE hormis les porteurs, et quelle que soit la phase, connaissent les responsabilités financières, civiles et pénales associées à l'usage de la TOE.

O.OUTILS : Les méthodes et les outils (équipements, documents) de développement employés dans les phases précédant la phase opérationnelle de la TOE doivent garantir :

- l'intégrité de tous les biens, y compris les biens intermédiaires,
- la confidentialité des biens, y compris intermédiaires, qui en ont besoin.

O.PROP_SECU : En début de phase opérationnelle, les propriétés de sécurité de la TOE doivent être conformes à ce qui est attendu.

5. Exigences de sécurité

5.1. Exigences de sécurité sur la TOE

5.1.1. Exigences fonctionnelles de sécurité portant sur la TOE

Remarques générales :

- Il est rappelé que les exigences fonctionnelles de sécurité portant sur la TOE ne concernent que la phase opérationnelle, et donc que les biens finaux.
- Quand des précisions relatives aux opérations sur les éléments des composants (affectation, sélection ...) ne sont pas fournies, c'est qu'elles seront à fournir dans la/les cible(s) de sécurité à venir.
- Les précisions sur les opérations des éléments des composants sont fournies de la façon suivante :
  - les précisions relatives à un élément sont données juste après le texte de cet élément (et pas après le texte de l'ensemble des éléments),
  - les précisions sont données opération par opération, en précisant le type d'opération, voire le numéro d'ordre de l'opération quand il y en a plusieurs du même type dans le texte d'un élément. Exemple : après "Affectation n°2 : " les informations apportées portent sur la seconde affectation du texte de l'élément concerné.
- La TOE ne contient qu'un seul "sujet" au sens de [CC-2], c'est-à-dire qu'une seule entité active : la TOE est mono-processeur et mono-tâche.
- Correspondance entre les biens identifiés pour la TOE et les types de données pris en compte dans les exigences fonctionnelles de [CC-2] :

  Les exigences fonctionnelles fournies par les Critères Communs, dans [CC-2], ne distinguent que deux types de données :

  - les données utilisateur ("user data"),
  - les données de la TSF[3] ("TSF data").

[3] TSF = TOE Security Functions — c'est-à-dire que la TSF est le sous-ensemble de la TOE qui met en oeuvre les fonctions de sécurité.

La correspondance entre les biens identifiés pour la TOE et ces deux types de données est la suivante, en ce qui concerne la phase opérationnelle, les traitements étant considérés ici comme des données stockées en mémoire :

Biens	Données de la TSF	Données utilisateur
Traitements de niveau TOE	X	
Traitements billettiques	X	
Eléments secrets de niveau TOE	X	
Informations de gestion et de structure de niveau TOE	X Certaines informations de structure sont des attributs de sécurité, et donc des données de la TSF (ex. : informations de contrôle d'accès)	X
Eléments secrets billettiques	X	
Informations billettiques applicatives et de structure ayant un besoin de confidentialité et d'intégrité		X
Informations billetiques applicatives ayant un besoin d'intégrité seul	X Certaines informations de structure sont des attributs de sécurité, et donc des données de la TSF (ex. : informations de contrôle d'accès)	X

Correspondance entre biens et données utilisateur et de la TSF

Classe FAU — Security audit

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.

Affectation : En cas de détection d'une violation potentielle de la sécurité (tout traitement carte qui échoue ; cf. l'exigence suivante), la TSF doit en avertir l'équipement billettique avec lequel elle dialogue.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b) [assignment: *any other rules*].

Affectation n°1 : La TSF doit être capable de détecter qu'un traitement initié à la réception d'une commande en provenance d'un équipement billettique a échoué. Tout traitement carte qui échoue est en effet considéré dans ce profil de protection comme une violation potentielle de la sécurité, puisque tous les éléments de la TOE (traitements ou informations) sont sensibles (cf. le § 3.2.).

Dans ce document, on considère qu'un traitement qui échoue a pour cause :

- soit un dysfonctionnement de la TOE,
- soit une vérification négative. C'est le cas par exemple de données envoyées à la TOE par un équipement billettique et modifiées au cours de la transmission. La vérification de la signature qui accompagne ces données va être négative alors que le traitement de vérification n'est sujet à aucun dysfonctionnement.

Classe FCO — Communication

FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the [selection: *originator, recipient,* [assignment: *list of third parties*]].

Affectation n°1 : Les informations concernées par cette exigence sont au moins des informations sensibles de gestion et de structure de niveau TOE (dont : l'identifiant de la TOE).

Sélection : La génération de la preuve par la TOE est effectuée suite à une requête d'un équipement billettique, destinataire de la preuve.

FCO_NRO.1.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].

Classe FCS — Cryptographic support

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Affectation n°1 : Les opérations cryptographiques consistent au moins en :

- calcul de signatures électroniques (pour protéger l'intégrité d'informations transmises par la TOE et pour authentifier la TOE auprès d'un équipement billettique),
- vérification de signatures électroniques (pour vérifier l'intégrité d'informations reçues par la TOE et authentifier un équipement billettique),
- génération de nombres pseudo-aléatoires (permet d'authentifier un équipement billettique à l'aide d'un procédé de challenge/response évitant le rejeu),
- déchiffrement de clés.

Affectation n°2 : La TOE doit donc disposer d'au moins un algorithme de chiffrement, symétrique ou asymétrique

Remarques :

- dans ce document, l'expression "signature électronique" est utilisée dans le cas des algorithmes symétriques et asymétriques.
- dans la suite de ce profil de protection, les authentifications qui utilisent une signature électronique sont appelées "authentifications par clé".
- dans ce document, il est considéré qu'une signature électronique n'est pas un attribut de sécurité. En effet :
  - des informations peuvent être signées pour plusieurs raisons : pour en protéger l'intégrité, ou pour authentifier la TOE ou un équipement billettique,
  - deux informations d'une même catégorie de biens peuvent ne pas avoir le même besoin d'intégrité,
  - une information peut ne pas avoir le même besoin d'intégrité selon la situation, et donc ne pas avoir besoin d'une signature dans certains cas.

  L'adjonction d'une signature électronique à une information doit être vue comme le résultat d'une fonction visant la protection de l'intégrité de cette information, fonction qui peut être déclenchée par un équipement billettique si besoin est.

Classe FDP — User data protection

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] and all operations among subjects and objects covered by the SFP.

Affectation n°1 : La TOE doit distinguer les accès en lecture et les accès en écriture/effacement à un objet (conteneur d'informations, au sens de [CC-2]). La TOE doit mettre en oeuvre les trois types d'accès en lecture suivants, au minimum :

1. libre,
2. soumis à authentification par code confidentiel (PIN),
3. interdit.

Les accès en écriture/effacement doivent être toujours soumis à une authentification par clé, utilisant une signature électronique.

Affectation n°2 : Les règles de contrôle d'accès doivent pouvoir s'appliquer à tous les objets de la TOE.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes, named groups of security attributes*].

Affectation n°2 : La TSF doit employer au moins deux attributs de sécurité liés à un objet, (c'est-à-dire à un élément contenant de l'information — typiquement un fichier, pour une carte à puce) :

- son/ses modes d'accès — il doit au minimum y avoir deux modes : un mode d'accès en lecture seule, et un mode d'accès en écriture/effacement.
- pour chaque mode, les conditions d'accès — il doit au minimum y avoir quatre conditions d'accès : accès libre (non valable pour le mode d'accès en écriture/effacement), accès soumis à authentification par clé (non valable pour le mode d'accès en lecture), accès soumis à authentification par PIN (non valable pour le mode d'accès en écriture/effacement), accès interdit.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules based on security attributes, that explicitly deny access of subjects to objects*].

FDP_IFC.1 Subset information flow control

FDP_IFC.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

Classe FIA — Identification and authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

Affectations : Le tableau suivant récapitule le comportement que la TOE doit avoir en matière de tentatives infructueuses d'authentification :

Affectation n°2	Affectation n°1
Authentification par PIN	3
Authentification par clé	Pas de limite imposée par la TOE

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].

Affectation : Quand le nombre de tentatives infructueuses de connexions accepté pour le mécanisme d'authentification concerné est atteint, la TOE doit :

- refuser toute nouvelle tentative d'authentification,
- refuser d'exécuter les traitements soumis à cette authentification.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.

Affectation : La TSF doit posséder les deux mécanismes suivants :

- authentification par mot de passe (ou PIN) — utilisé pour authentifier un porteur,
- authentification par clé — utilisé pour authentifier un équipement billettique qui doit dialoguer avec la TOE.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Rafinement : Ce composant (FIA_UID.1.1 + FIA_UID1.2) ne concerne que les utilisateurs que sont les porteurs. La TOE doit constituer un identifiant de son porteur, préalable indispensable à l'authentification par PIN de celui-ci.

Remarque : l'identification de l'autre type d'utilisateur que sont les équipements billettiques n'est pas exigée. En effet, l'authentification par clé d'un équipement billettique ne nécessite pas d'identification.

Classe FPT — Protection of the TOE Security Functions

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

FPT_PHP.2 Notification of physical attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.

Affectation n°2 : Tout équipement billettique dialoguant avec la TOE doit être averti.

Remarque : les éléments de la TSF qui ont un besoin de détection active ne sont pas précisés pour la raison suivante : leur liste est très dépendante de l'état de l'art, qui évolue avec le temps. Les auteurs du présent profil préfèrent se reposer sur les compétences d'une part des industriels de la carte et d'autre part des organismes impliqués dans l'évaluation sécuritaire.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self tests should occur*]] to demonstrate the correct operation of the TSF.

Affectation dans la sélection : Les tests doivent pouvoir être effectués à la demande de tous les utilisateurs autorisés que sont les équipements billettiques. Chaque traitement exécuté par la TOE

en réponse à une commande envoyée par un équipement billettique doit inclure des tests concernant la partie de la TSF concernée.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of the TSF data.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.

5.1.2. Exigences d'assurance portant sur la TOE

Le niveau d'assurance visé est : **EAL 4 augmenté**.

EAL 4 a été préféré à EAL 3 car il procure un niveau d'assurance sur la sécurité de la TOE jugé sensiblement plus important que dans le cas d'EAL 3, du fait d'un contrôle plus important sur le travail des acteurs agissants sur la TOE (acteurs de type 2).

Les niveaux d'assurance EAL 5 et au-dessus ont été rejetés car ils sont jugés trop contraignants (descriptions semi-formelles voire formelles ...) pour les acteurs agissant sur la TOE au regard du surcroît d'assurance sur la sécurité par rapport à EAL 4 augmenté.

Les exigences d'assurance venant compléter celles qui sont inhérentes à EAL 4 ont pour but de **renforcer la confiance dans la robustesse** de la TOE (efficacité des fonctions de sécurité).

Les deux exigences ci-dessous, tirées de [CC-3], sont donc hiérarchiques par rapport à des exigences requises en standard pour le niveau EAL 4.

Rappel : Le niveau de robustesse des fonctions de sécurité demandé est : **fort,** c'est-à-dire **SOF-high**. La justification est donné au chapitre 7 "Justifications".

ADV_IMP.2 Implementation of the TSF

Developer action elements:

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

Content and presentation of evidence elements:

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

ADV_IMP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

AVA_VLA.4 Highly resistant

Developer action elements:

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements:

AVA_VLA.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.4.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.4.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

5.2. Exigences de sécurité portant sur l'environnement de la TOE

Aucune.

6. Notes d'application

Le choix de la solution de sécurité, c'est-à-dire des mécanismes qui permettront de mettre en oeuvre les fonctions de sécurité, doit être effectué :

- **en conformité avec les normes** en vigueur en matière de sécurité et de cartes à puce, et notamment :
  - ISO 7816 " Technologies de l'information — Cartes d'identification — Cartes à circuit(s) intégré(s) à contacts (norme ISO)", parties 1 à 6
  - EN 726 " Identification Card Systems — Telecommunications Integrated Circuit Cards and Terminals ", parties 2 et 3
- en tenant compte de la **contrainte de performance** importante auxquelles sont soumises certaines transactions billettiques : elles doivent s'effectuer en moins de 200 ms. C'est notamment le cas des transactions sans contact de validation dans les gares. De ce fait, l'exécution des mécanismes de sécurité mis en oeuvre lors de ces transactions est en pratique limitée à 50 ms.

Ce profil de protection présente des exigences fonctionnelles **minimales**. Leur définition a tenu compte des points suivants :

- il a été jugé préférable en cas de doute sur la pertinence d'un composant de [CC-2] de ne pas l'exiger afin de **laisser une liberté aux industriels développeurs**.

  C'est le cas par exemple de FDP_ITC.2 "Import of user data with security attributes". Cette exigence pourrait s'avérer nécessaire pour sécuriser le téléchargement d'application.
- certains composants de [CC-2] sont peu aisément interprétables dans le cas d'une carte à puce.

7. Justifications

7.1. Justification des objectifs de sécurité

7.1.1. Justification de la couverture des menaces, des hypothèse et des règles organisationnelles de sécurité par les objectifs de sécurité

Le tableau ci-dessous indique les objectifs auxquels chaque menace ou hypothèse ou règle orgnisationnelle de sécurité est rattaché, en fournissant à chaque fois les explications nécessaires.

Il démontre que chaque menace, chaque hypothèse, et chaque règle organisationnelle de sécurité

- est prise en compte par au moins un objectif de sécurité,
- est entièrement prise en compte par l'ensemble des objectifs qui lui sont rattachés.

Hypothèse / Menace / Règle	Objectif	Justification / Remarques
A.QUAL	O.SENSIB_FORM	O.SENSIB_FORM couvre entièrement l'hypothèse d'utilisation sûre A.QUAL.
A.EQPT_DVPT	O.OUTILS	O.OUTILS couvre entièrement l'hypothèse d'utilisation sûre A.EQPT_DVPT.
T.INTER_MOD	O.ACCES_PHY O.LIVRAISON O.SENSIB_FORM O.OUTILS O.PROP_SECU	O.ACCES_PHY, en limitant les accès physiques aux biens intermédiaires et aux équipements qui agissent sur eux, permet la prévention de modifications illicites plus qu'erronées. O.LIVRAISON, en imposant des règles strictes lors du transfert de biens intermédiaires, permet la prévention et la détection de modifications illicites. O.SENSIB_FORM, en formant et en responsabilisant les acteurs de la TOE, permet la prévention de modifications erronées ou illicites. O.OUTILS, en imposant des règles et méthodes de développement strictes et rigoureuses, permet la prévention, la détection de modifications erronées ou illicites, ainsi que la réaction et la reprise en cas de réalisation de la menace (correction de la modification). O.PROP_SECU, en imposant que les propriétés de sécurité de la TOE en début de phase opérationnelle soient conformes à ce qui est attendu, permet la détection (peut-être tardive) d'une modification erronée ou illicite de biens intermédiaires. Ces objectifs couvrent entièrement T.INTER_MOD.
T.INTER_DIV	O.ACCES_PHY O.LIVRAISON O.SENSIB_FORM O.OUTILS O.PROP_SECU	O.ACCES_PHY, en limitant les accès physiques aux biens intermédiaires et aux équipements qui agissent sur eux, permet la prévention de divulgations illicites plus qu'erronées. O.LIVRAISON, en imposant des règles strictes lors du transfert de biens intermédiaires, permet la prévention et la détection de divulgations illicites. O.SENSIB_FORM, en formant et en responsabilisant les acteurs de la TOE, permet la prévention de divulgations erronées ou illicites. O.OUTILS, en imposant des règles et méthodes de développement strictes et rigoureuses, permet la prévention, voire la détection de divulgations erronées ou illicites. O.PROP_SECU, en imposant que les propriétés de sécurité de la TOE en début de phase opérationnelle soient conformes à ce qui est attendu, permet la prévention, voire la détection et la réaction à, d'une divulgation erronée ou illicite de biens intermédiaires. Ces objectifs couvrent entièrement T.INTER_DIV.

Justification de la couverture des menaces (1/4)

Hypothèse / Menace / Règle	Objectif	Justification / Remarques
T.INTER_VOL	O.ACCES_PHY O.LIVRAISON O.SENSIB_FORM	O.ACCES_PHY, en limitant les accès physiques aux biens intermédiaires et aux équipements qui agissent sur eux, permet la prévention de vols. O.LIVRAISON, en imposant des règles strictes lors du transfert de biens intermédiaires, permet la prévention et la détection de vols. O.SENSIB_FORM, en formant et en responsabilisant les acteurs de la TOE, permet la prévention de vols. Ces trois objectifs couvrent entièrement T.INTER_VOL.
T.FIN_MOD_TRAIT	O.OUTILS, O.ACCES-PHY, O.LIVRAISON et O.SENSIB_FORM O.PROP_SECU O.INTEG_STOCK O.AUTH_REC O.ACCES O.PHYSIQUE O.DYSFONC	O.OUTILS, en imposant aux outils et méthodes de développement de garantir l'intégrité des biens intermédiaires et finaux, et O.ACCES_PHY, O.LIVRAISON et O.SENSIB_FORM, permettent la prévention de modifications erronées ou illicites de traitements installés/chargés. O.PROP_SECU agit aussi en amont, en complément des objectifs ci-dessus, afin de garantir qu'en début de phase opérationnelle la TOE possède les propriétés de sécurité attendues. Il participe donc à la protection contre une modification de traitement, illicite plus qu'erronée. O.INTEG_STOCK, en assurant la vérification de l'intégrité des traitements stockés dans la TOE (notamment), permet la détection de leur modifications, illicites surtout. O.AUTH_REC et O.ACCES, en limitant l'accès aux traitements sensibles de la TOE aux équipements billettiques s'étant dûment authentifiés, permet la prévention de la modification, illicite, de traitements sensibles. O.PHYSIQUE, en imposant une résistance aux attaques physiques, permet la prévention de modifications illicites de traitements. O.DYSFONC permet également la détection de modifications des traitements, erronées autant qu'illicites. Ces objectifs couvrent entièrement T.FIN_MOD_TRAIT.
T.FIN_MOD_INFO	O.OUTILS, O.ACCES-PHY, O.LIVRAISON et O.SENSIB_FORM O.PROP_SECU O.INTEG_STOCK O.AUTH_REC O.ACCES O.PHYSIQUE O.DYSFONC	Justification de O.OUTILS, O.ACCES_PHY, O.LIVRAISON et O.SENSIB_FORM ainsi que de O.PROP_SECU : cf. T.FIN_MOD_TRAIT. O.INTEG_STOCK impose la vérification de l'intégrité des informations sensibles (notamment) et permet ainsi la détection d'une modification non autorisée d'informations sensibles. O.AUTH_REC et O.ACCES, en limitant l'accès aux informations sensibles de la TOE aux équipements billettiques s'étant dûment authentifiés, permet la prévention de la modification, illicite, d'informations sensibles. Justification de O.PHYSIQUE, O.DYSFONC : cf. T.FIN_MOD_TRAIT. Ces objectifs couvrent entièrement T.FIN_MOD_INFO.

Justification de la couverture des menaces (2/4)

Hypothèse / Menace / Règle	Objectif	Justification / Remarques
T.FIN_DIV_I	O.OUTILS, O.ACCES-PHY, O.LIVRAISON et O.SENSIB_FORM O.PROP_SECU O.ACCES O.PHYSIQUE O.DYSFONC	Justification de O.OUTILS, O.ACCES_PHY, O.LIVRAISON, O.SENSIB_FORM et O.PROP_SECU : cf. T.FIN_MOD_TRAIT. O.ACCES, en contrôlant l'accès aux éléments secrets permet la prévention de la divulgation, d'origine malveillante, d'éléments secrets. O.PHYSIQUE, en imposant une résistance de la TOE contre des attaques physiques ainsi qu'une détection de ce type d'attaques, permet d'empêcher la divulgation d'éléments secrets par des moyens physiques. O.DYSFONC, en imposant de protéger la TOE contre des dysfonctionnements, et en agissant notamment en détection de ces dysfonctionnements, permet de limiter les risques de divulgation liés à un dysfonctionnement. Ces objectifs couvrent entièrement T.FIN_DIV_I.
T.FIN_DIV_NA	O.OUTILS, O.ACCES-PHY, O.LIVRAISON et O.SENSIB_FORM O.PROP_SECU O.ACCES O.AUTH_REC O.PORTEUR O.PHYSIQUE O.DYSFONC	Justification de O.OUTILS, O.ACCES_PHY, O.LIVRAISON, O.SENSIB_FORM et O.PROP_SECU : cf. T.FIN_MOD_TRAIT. O.ACCES, en contrôlant l'accès aux éléments secrets, permet la prévention de la divulgation non autorisée, d'origine malveillante, d'informations billettiques applicatives ayant un besoin de confidentialité et d'intégrité. O.AUTH_REC, en imposant l'authentification d'un équipement billettique auprès de la TOE avant l'accès, permet la prévention de la divulgation non autorisée, d'origine malveillante, d'informations billettiques applicatives ayant un besoin de confidentialité et d'intégrité. O.PORTEUR, en permettant d'authentifier un porteur, contribue à limiter l'accès à des informations confidentielles (relatives aux porteurs). O.PHYSIQUE, en imposant la protection de la TOE contre des attaques physiques, permet d'empêcher la divulgation non autorisée d'informations par des moyens physiques. O.DYSFONC, en imposant de protéger la TOE contre des dysfonctionnements, et en agissant notamment en détection de ces dysfonctionnements, permet de limiter les risques de divulgation non autorisée liés à un dysfonctionnement. Ces objectifs couvrent entièrement T.FIN_DIV_NA. Remarque : un objectif requiérant de façon explicite la confidentialité des informations billettiques applicatives ayant un besoin de confidentialité et d'intégrité est inutile : contrôle d'accès et authentification suffisent.
T.FIN_CLONE	O.ACCES-PHY, O.LIVRAISON et O.SENSIB_FORM O.AUTH_REC O.ACCES O.PHYSIQUE	Justification de O.ACCES_PHY, O.LIVRAISON et O.SENSIB_FORM : cf. T.FIN_MOD_TRAIT : les mesures organisationnelles et procédurales qu'appèlent ces objectifs permettent de limiter la divulgation d'informations et le vol d'équipements permettant de faciliter la réalisation de la menace. O.AUTH_REC, en demandant aux équipements (billettiques ou non) de s'authentifier à l'aide d'une clé avant d'accéder à des traitements ou informations sensibles, permet la prévention du clonage. O.ACCES, en contrôlant en phase opérationnelle l'accès aux éléments secrets, permet la prévention du clonage. O.PHYSIQUE, en imposant une résistance aux attaques physiques, permet la prévention d'inspection des couches du circuit intégré et donc de la divulgation illicite d'éléments secrets (nécessaires pour un clonage). Ces objectifs couvrent entièrement la menace T.FIN_CLONE.

Justification de la couverture des menaces (3/4)

Hypothèse / Menace / Règle	Objectif	Justification / Remarques
T.FIN_VOL	O.ACCES_PHY O.LIVRAISON O.SENSIB_FORM O.PORTEUR	O.ACCES_PHY, O.LIVRAISON, O.SENSIB_FORM s'appliquent aussi à la phase opérationnelle, et permettent donc la prévention du vol de TOE par un acteur de la TOE qui n'est pas un porteur. O.PORTEUR, en permettant à la TOE d'authentifier son porteur, contribue à limiter l'impact d'un vol de carte. C'est le cas par exemple si le paiement d'un titre de transport peut être fait en prélevant la somme correspondante directement sur le compte d'un client. Sans vérification de PIN, un voleur pourrait alors charger des titres de transport sans les payer. En phase opérationnelle, la TOE est la plupart du temps non maîtrisée : elle peut être facilement volée. En conséquence, ces objectifs couvrent partiellement la menace (il faut compléter les parades par la mise en oeuvre, côté système, de listes noires).
P. GEN_AUTH	O.AUTH	O.AUTH requiert que la TOE sache s'authentifier auprès d'un équipement. L'objectif couvre entièrement la règle organisationnelle de sécurité.
P.VERIF_SIGN	O.INTEG_RECPT	O.INTEG_RECPT requiert que la TOE sache vérifier l'intégrité de certaines informations qu'elle reçoit. L'objectif couvre entièrement la règle organisationnelle de sécurité.
P.CALC_SIGN	O.INTEG_EMIS	O.INTEG_EMIS requiert que la TOE puisse permettre à un équipement billettique de vérifier l'intégrité des informations sensibles qu'elle lui transmet. L'objectif couvre entièrement la règle organisationnelle de sécurité.
P.DECHIF_CLE	O.DECHIF_CLE	O.DECHIF_CLE requiert que la TOE sache déchiffrer les clés qui lui sont transmises, en phase opérationnelle. L'objectif couvre entièrement la règle organisationnelle de sécurité.

Justification de la couverture des menaces (4/4)

7.1.2. Tableau de couverture des menaces, des hypothèses et des règles organisationnelles de sécurité par les objectifs de sécurité

Le tableau suivant démontre que chaque objectif de sécurité répond au moins à une menace ou à une hypothèse ou encore à une règle organisationnelle de sécurité.

	O.AUTH	O.AUTH_REC	O.PORT.	O.ACCES	O.INTEG_STOCK	O.INTEG_RECP	O.INTEG_EMIS	O.DECHIF_CLE
A.QUAL								
A.EQPT_DVPT								
T.INTER_MOD								
T.INTER_DIV								
T.INTER_VOL								
T.FIN_MOD_TRAIT		X		X	X			
T.FIN_MOD_INFO		X		X	X			
T.FIN_DIV_I				X				
T.FIN_DIV_NA		X	X	X				
T.FIN_CLONE		X		X				
T.FIN_VOL			X					
P.GEN_AUTH	X							
P.VERIF_SIGN						X		
P.CALC_SIGN							X	
P.DECHIF_CLE								X

Couverture des menaces par les objectifs (1/2)

	O.PHYSIQUE	O.DYSFONC	O.ACCES_PHY	O.LIVRAISON	O.SENSIB_FORM	O.OUTILS	O.PROP_SECU
A.QUAL					X		
A.EQPT_DVPT						X	
T.INTER_MOD			X	X	X	X	X
T.INTER_DIV			X	X	X	X	X
T.INTER_VOL			X	X	X		
T.FIN_MOD_TRAIT	X	X	X	X	X	X	X
T.FIN_MOD_INFO	X	X	X	X	X	X	X
T.FIN_DIV_I	X	X	X	X	X	X	X
T.FIN_DIV_NA	X	X	X	X	X	X	X
T.FIN_CLONE	X		X	X	X		
T.FIN_VOL			X	X	X		
P.GEN_AUTH							
P.VERIF_SIGN							
P.CALC_SIGN							
P.DECHIF_CLE							

Couverture des menaces par les objectifs (2/2)

7.2. Justification des exigences de sécurité

7.2.1. Tableau de couverture des objectifs de sécurité portant sur la TOE par les exigences fonctionnelles

Le tableau ci-dessous démontre que :

- chaque objectif de sécurité dispose d'au moins une exigence de sécurité,
- chaque exigence de sécurité contribue à couvrir au moins un objectif.

Code	Libellé	O.AUTH	O.AUTH_REC	O.PORTEUR	O.ACCES	O.INTEG_STOCK	O.INTEG_RECP
FAU_ARP.1	Security alarms		X	X		X	X
FAU_SAA.1	Potential violation analysis		X	X		X	X
FCO_NRO.1	Selective proof of origin	X					
FCS_COP.1	Cryptographic operation	X	X				X
FDP_ACC.2	Complete access control				X		
FDP_ACF.1	Security attribute based access control				X		
FDP_IFC.1	Subset information flow control				X		
FDP_IFF.1	Simple security attributes				X		
FDP_SDI.1	Stored data integrity monitoring					X	
FIA_AFL.1	Authentication failure handling		X	X			
FIA_UAU.5	Multiple authentication mechanisms		X	X			
FIA_UID.1	Timing of identification			X			
FPT_FLS.1	Failure with preservation of secure state						
FPT_PHP.2	Notification of physical attack						
FPT_PHP.3	Resistance to physical attack						
FPT_RVM.1	Non-bypassability of the TSP	X	X	X	X	X	X
FPT_TST.1	TSF testing					X	

Couverture des objectifs de sécurité par les exigences fonctionnelles (1/2)

Code	Libellé	O.INTEG_EMIS	O.DECHIF_CLE	O.PHYSIQUE	O.DYSFONC
FAU_ARP.1	Security alarms			X	X
FAU_SAA.1	Potential violation analysis			X	X
FCO_NRO.1	Selective proof of origin				
FCS_COP.1	Cryptographic operation	X	X		
FDP_ACC.2	Complete access control				
FDP_ACF.1	Security attribute based access control				
FDP_IFC.1	Subset information flow control				
FDP_IFF.1	Simple security attributes				
FDP_SDI.1	Stored data integrity monitoring				
FIA_AFL.1	Authentication failure handling				
FIA_UAU.5	Multiple authentication mechanisms				
FIA_UID.1	Timing of identification				
FPT_FLS.1	Failure with preservation of secure state				X
FPT_PHP.2	Notification of physical attack			X	
FPT_PHP.3	Resistance to physical attack			X	
FPT_RVM.1	Non-bypassability of the TSP	X	X	X	X
FPT_TST.1	TSF testing			X	X

Couverture des objectifs de sécurité par les exigences fonctionnelles (2/2)

7.2.2. Justifications de la couverture des objectifs de sécurité portant sur la TOE

Le tableau ci-dessous indique comment chacune des exigences fonctionnelles de sécurité définies contribue à l'atteinte de chacun des objectifs de sécurité portant sur la TOE concernés.

Code	Libellé	Objectif(s) rattaché(s)	Justification / Remarques
FAU_ARP.1	**Security alarms**	O.AUTH_REC O.PORTEUR O.INTEG_STOCK O.INTEG_RECPT O.PHYSIQUE O.DYSFONC	Cf. la justification donnée pour FAU_SAA.1.
FAU_SAA.1	**Potential violation analysis**	O.AUTH_REC O.PORTEUR O.INTEG_STOCK O.INTEG_RECPT O.PHYSIQUE O.DYSFONC	Tout échec dans l'exécution d'un traitement carte est considéré comme une violation potentielle de la sécurité, qui doit en outre être indiquée à l'équipement billettique qui dialogue avec la TOE. De ce fait, les exigences FAU_ARP.1 et FAU_SAA.1 concernent tous les objectifs portant sur la TOE listés.
FCO_NRO.1	**Selective proof of origin**	O.AUTH	Cette exigence de preuve de l'origine d'informations, en l'appliquant aux informations d'identification de la TOE (informations sensibles de gestion et de structure de niveau TOE), permet de couvrir l'objectif O.AUTH.
FCS_COP.1	**Cryptographic operation**	O.AUTH_REC O.AUTH O.INTEG_RECPT O.INTEG_EMIS O.DECHIF_CLE	La TOE nécessite un mécanisme d'authentification fort, basé sur un procédé de challenge/response, que ce soit pour authentifier un équipement (O.AUTH_REC) ou s'authentifier auprès d'un équipement (O.AUTH). Cela nécessite que la TOE puisse chiffrer des données d'identification/authentification. FCS_COP.1 fournit également à la TOE le moyen de calculer et de vérifier des signatures électroniques, contribuant ainsi à l'atteinte de O.INTEG_RECPT et O.INTEG_EMIS. FCS_COP.1 permet aussi le déchiffrement des clés chargées chiffrées dans la TOE, en phase opérationnelle, contribuant ainsi à l'atteinte de O.DECHIF_CLE.
FDP_ACC.2	**Complete access control**	O.ACCES	Cette exigence impose que toutes les informations de la TOE, via les objets qui les contiennent, fassent l'objet d'un contrôle d'accès. FDP_ACC.2 est envisageable au lieu de FDP_ACC.1 du fait que toutes les informations de la TOE sont sensibles. FDP_ACC.2 contribue à l'atteinte de l'objectif O.ACCES. Remarque : le contrôle d'accès à une information dont il est question ici est en fait le contrôle d'accès à l'objet (fichier, enregistrement ...) qui la contient, via un traitement (ou commande, dans le vocabulaire des cartes à puce). Le contrôle d'accès à une information, stricto sensu, fait l'objet des exigences FDP_IFC.1 et FDP_IFF.1.
FDP_ACF.1	**Security attribute based access control**	O.ACCES	Cette exigence permet de préciser les règles de contrôle des accès aux informations et aux traitements sensibles de la TOE, qui sont basées sur des attributs de sécurité. Exemples : le mode d'accès à un fichier (en lecture seule, en lecture et écriture ...), la nécessité d'une authentification préalable (par challenge/response ou par présentation d'un mot de passe). Cette exigence contribue à satisfaire O.ACCES.
FDP_IFC.1	**Subset information flow control**	O.ACCES	Cette exigence impose que certaines informations sensibles de la TOE fassent l'objet d'un contrôle de flux, c'est-à-dire que tout transfert de ces informations soit soumis à contrôle. Cette exigence contribue à satisfaire O.ACCES.

Justification de chaque exigence de sécurité (1/2)

Code	Libellé	Objectif(s) rattaché(s)	Justification / Remarques
FDP_IFF.1	**Simple security attributes**	O.ACCES	Cette exigence permet de préciser les règles de contrôle des flux d'informations, à l'aide d'attributs de sécurité à attacher aux informations. Elle permet ainsi de définir les règles d'accès à une information, quel que soit son contenant. Cette exigence contribue à satisfaire O.ACCES.
FDP_SDI.1	**Stored data integrity monitoring**	O.INTEG_STOCK	Cette exigence ne vise à contrer que les erreurs touchant des données utilisateur stockées, pas les malveillances (dans ce cas, il y a FDP_ACF.1 et FDP_IFC.1). Cette exigence contribue à satisfaire O.INTEG_STOCK.
FIA_AFL.1	**Authentication failure handling**	O.AUTH_REC O.PORTEUR	Cette exigence permet de définir les conditions d'échec de l'authentification d'un équipement et d'un porteur, et contribue donc à satisfaire les objectifs O.AUTH_REC et O.PORTEUR (respectivement).
FIA_UAU.5	**Multiple authentication mechanisms**	O.AUTH_REC O.PORTEUR	La TOE doit disposer de deux mécanismes d'authentification, pour authentifier : – les équipements désirant dialoguer avec elle, à l'aide d'un procédé de challenge/response – les porteurs, à l'aide d'un mot de passe ou PIN (Personal Identification Number). Cette exigence contribue donc à satisfaire les objectifs O.AUTH_REC et O.PORTEUR.
FIA_UID.1	**Timing of identification**	O.PORTEUR	Cette exigence impose l'identification du porteur. Elle constitue donc le préalable indispensable à l'authentification du porteur et contribue à l'atteinte de l'objectif O.PORTEUR.
FPT_FLS.1	**Failure with preservation of a secure state**	O.DYSFONC	Cette exigence requiert que la TSF reste dans un état sûr en cas d'erreur d'origine matérielle ou logicielle. Cela limite les effets d'un dysfonctionnement, et contribue à satisfaire O.DYSFONC.
FPT_PHP.2	**Notification of physical attack**	O.PHYSIQUE	Cette exigence spécifie que la TOE doit être capable de détecter des attaques physiques et d'en avertir l'équipement billettique qui dialogue avec elle. Cette exigence contribue à satisfaire O.PHYSIQUE.
FPT_PHP.3	**Resistance to physical attack**	O.PHYSIQUE	Cette exigence spécifie que la TOE doit être capable de résister à des attaques physiques. Cette exigence contribue à satisfaire O.PHYSIQUE.
FPT_RVM.1	**Non-bypassability of the TSP**	Tous	Cette exigence impose que les fonctions de sécurité de la TOE ne soient pas contournables. Elle s'applique donc à tous les objectifs.
FPT_TST.1	**TSF testing**	O.INTEG_STOCK O.PHYSIQUE O.DYSFONC	Cette exigence permet la détection d'attaques intentionnelles ou non, logiques ou non. Elle porte en outre sur les données de la TSF auxquelles on rattache les traitements sensibles. Cette exigence contribue donc à l'atteinte des objectifs O.INTEG_STOCK, O.PHYSIQUE et O.DYSFONC.

Justification de chaque exigence de sécurité (2/2)

7.2.3. Correspondance entre biens et données utilisateur et de la TSF

Le tableau du paragraphe 5.1.1. indique que les informations de structure, de niveau TOE ou billettiques peuvent être des attributs de sécurité, et donc être des données utilisateur ou des données de la TSF. Cela ne remet pas en cause la couverture de la menace portant sur ces informations, T.FIN_MOD_INFO. En effet, même si certaines exigences fonctionnelles concernent seulement l'un des deux types de données, les deux sont protégés contre la modification non autorisée, quelle soit intentionnelle ou non, d'origine matérielle ou logique :

- en prévention :
  - les deux types de données font l'objet de règles de contrôle d'accès et de flux et leur accès peut/doit être soumis à authentification (FDP_ACC.2, FDP_ACF.1, FDP_IFC.1 et FDP_IFF.1).
  - la TOE doit résister aux attaques physiques (FPT_PHP.3).
- en détection et réaction :
  - la TOE doit savoir détecter des défauts d'intégrité pour les deux types de données (FDP_SDI.1 pour les données utilisateur, FPT_TST.1 pour celles de la TSF).
  - les dysfonctionnements touchant la TSF ont un impact limité du fait de FPT_FLS.1 qui garantit qu'en cas de dysfonctionnement la TSF est mise dans un état sûr.
  - la TOE doit détecter les traitements exécutés par la carte qui échouent (FAU_SAA.1) et en avertir l'équipement avec lequel elle dialogue (FAU_ARP.1)
  - la TOE doit savoir détecter les attaques physiques et en avertir l'équipement avec lequel elle dialogue (FPT_PHP.2).

7.2.4. Dépendances des exigences fonctionnelles

Le tableau vient en complément des précédents pour montrer la pertinence des exigences de sécurité. Pour ce faire, il indique pour chaque exigence fonctionnelle les dépendances fournies par les Critères Communs dans [CC-2], puis précise si la dépendance est respectée ou non. Dans ce dernier cas, la raison de non prise en compte de la dépendance est fournie.

Dans la colonne "Dépendances indiquées dans [CC-2]", les dépendances non prises en compte apparaissent barrées.

Mnémo. exigence	Libellé	Dépendances indiquées dans [CC-2]	Prise en compte
FAU_ARP.1	Security alarms	FAU_SAA.1 Potential violation analysis	Oui
FAU_SAA.1	Potential violation analysis	~~FAU_GEN.1 Audit data generation~~	La dépendance avec FAU_GEN.1 "Audit data generation" n'a pas lieu d'être : on ne sait pas aujourd'hui faire des cartes à puce satisfaisant à tout ce qu'implique FAU_GEN.1. En revanche, on estime qu'une carte à puce est tout-à-fait capable de détecter des violations potentielles de la sécurité.
FCO_NRO.1	Selective proof of origin	~~FIA_UID.1 Timing of identification~~	La dépendance avec FIA_UID.1 "Timing of identification" n'a pas lieu d'être : une transaction s'effectue entre un équipement billettique et une carte. La TOE n'a donc pas besoin d'identifier l'équipement billettique pour mettre en oeuvre l'exigence. En outre l'identification d'un équipement n'est pas nécessaire : c'est son authentification qui peut l'être, dans certains cas. Remarque : le composant FIA_UID.1 est exigé dans ce profil mais uniquement pour les utilisateurs que sont les porteurs, pas pour les équipements billettiques.
FCS_COP.1	Cryptographic operation	FDP_ITC.1 ~~Import of user data without security attributes~~ ou ~~FCS_CKM.1 Cryptographic key generation~~ ~~FCS.CKM.4 Cryptographic key destruction~~ ~~FMT_MSA.2 Secure security attributes~~	La dépendance avec FCS_CKM.1 "Cryptographic key generation" n'a pas lieu d'être : les clés stockées et utilisées par la TOE lui seront fournies. La dépendance avec FDP_ITC.1 "Import of user data without security attributes" n'a pas lieu d'être : les traitements cryptographiques que la TOE doit effectuer lorsque des éléments secrets lui sont transmis pour y être stockés pourront être définis par les règles de contrôle d'accès du fichier qui va contenir les éléments secrets ou par les règles de contrôle de flux associées aux éléments secrets. La dépendance avec FCS_CKM.4 "Cryptographic key destruction" n'a pas lieu d'être : d'une part les clés dans la TOE seront protégées quelle que soit la phase, d'autre part les TOE seront diffusées en très grand nombre et il est est considéré comme irréaliste de pouvoir détruire les clés dans toutes les TOE. La dépendance avec FMT_MSA.2 n'a pas lieu d'être : les attributs de sécurité sont fixés lors du développement de la TOE et ne peuvent être modifiés durant la phase opérationnelle.
FDP_ACC.2	Complete access control	FDP_ACF.1 Security attribute based access control	Oui

Satisfaction des dépendances des exigences fonctionnelles (1/2)

Mnémo. exigence	Libellé	Dépendances indiquées dans [CC-2]	Prise en compte
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 Subset access control ~~FMT_MSA.3 Static attribute initialisation~~	Oui, car FDP_ACC.2 est hiérarchique à FDP_ACC.1 La dépendance avec FMT_MSA.3 n'a pas lieu d'être : les attributs de sécurité sont fixés lors du développement de la TOE et ne peuvent être modifiés durant la phase opérationnelle. Il n'y a pas d'initialisation.
FDP_IFC.1	Subset information flow control	FDP_IFF.1 Simple security attributes	Oui
FDP_IFF.1	Simple security attributes	FDP_IFC.1 Subset information flow control ~~FMT_MSA.3 Static attribute initialisation~~	La dépendance avec FMT_MSA.3 n'a pas lieu d'être car il n'y a pas d'initialisation.
FDP_SDI.1	Stored data integrity monitoring	Aucune	—
FIA_AFL.1	Authentication failure handling	~~FIA_UAU.1 Timing of authentication~~	La dépendance avec FIA_UAU.1 n'a pas lieu d'être. En effet, le fait que l'accès à certains objets (fichiers) ou informations nécessite une authentification préalable des équipements billettiques est pris en compte par les exigences FDP_ACC.2, FDP_ACF.1, FDP_IFC.1 et FDP_IFF.1. Le fait que la TOE doive disposer de mécanismes d'authentification pour ce faire est pris en compte par l'exigence FIA_UAU.5.
FIA_UAU.5	Multiple authentication mechanisms	Aucune	—
FIA_UID.1	Timing of identification	Aucune	—
FPT_FLS.1	Failure with preservation of secure state	ADV_SPM.1 Informal TOE security policy model	Oui
FPT_PHP.2	Notification of physical attack	~~FMT_MOF.1 Management of security functions behaviour~~	Il est jugé que dans le cas d'une carte à puce, le comportement des fonctions de sécurité ne peut être modifié au cours de la phase opérationnelle.
FPT_PHP.3	Resistance to physical attack	Aucune	—
FPT_RVM.1	Non-bypassability of the TSP	Aucune	—
FPT_TST.1	TSF testing	~~FPT_AMT.1 Abstract machine~~	Dans le cas d'une carte à puce, qui forme un tout, la notion de machine abstraite n'a pas de sens.

Satisfaction des dépendances des exigences fonctionnelles (2/2)

7.2.5. Justification de l'augmentation des exigences d'assurance

Cf. le chapitre 5.1.2.

7.2.6. Dépendance des exigences d'assurance

Les dépendances de chaque exigence d'assurance sont satisfaites. En effet :

- les exigences du niveau EAL 4 forment un tout dont toutes les dépendances sont satisfaites,
- l'augmentation de deux exigences ne remet pas en cause la satisfaction des dépendances du reste des exigences,
- les dépendances des deux exigences augmentées sont satisfaites par le reste des exigences, comme l'indique le tableau suivant :

Mnémo. exigence	Libellé	Dépendances indiquées dans [CC-3]	Prise en compte
ADV_IMP.2	Implementation of the TSF	ADV_LLD.1 Descriptive low-level design ADV_RCR.1 Informal correspondence demonstration ALC_TAT.1 Well-defined development tools	Oui
AVA_VLA.4	Highly resistant	ADV_FSP.1 Informal functional specification ADV_HLD.2 Security enforcing high-level design ADV_IMP.1 Subset of the implementation of the TSF ADV_LLD.1 Descriptive low-level design AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance	Oui

Satisfaction des deux exigences d'assurance augmentées

7.2.7. Cohésion des exigences de sécurité fonctionnelles et d'assurance

Les exigences d'assurance sont cohérentes entre elles car elles correspondent à celles du niveau EAL 4, augmenté de deux exigences. Le fait de remplacer les exigences ADV_IMP.1 et AVA_VLA.2 par ADV_IMP.2 et AVA_VLA.4 (respectivement) ne remet pas en cause la cohésion de l'ensemble des exigences d'assurance, car les secondes sont hiérarchiques des premières.

Les exigences fonctionnelles sont également cohérentes entre elles. En effet :

- toutes les exigences sont tirées de [CC-2], et le seul rafinement effectué (pour FIA_UID.1) ne fait que restreindre le texte du composant concerné

  Cela montre en particulier que les exigences fonctionnelles ne se contredisent pas

- les exigences fonctionnelles ne font pas double emploi

  FDP_SDI.1 "Stored data monitoring" et FPT_TST.1 "Self-testing" peuvent à première vue paraître redondantes. Cependant, la première s'adresse aux données utilisateur, et la seconde aux données de la TSF (cf. le § 7.2.3.)

Enfin, les exigences d'assurance sont par nature cohérentes avec les exigences fonctionnelles, d'autant que le choix du niveau EAL 4 apporte les exigences d'assurance demandées par certaines exigences fonctionnelles (cf. le paragraphe 7.2.4.).

7.2.8. Robustesse des fonctions (SOF) et potentiel d'attaque (AVA_VLA)

Le choix de SOF-high et de AVA_VLA.4 est justifié car cela positionne l'évaluation sécuritaire de la TOE à l'état de l'art. Ce qui est estimé nécessaire parce que :

- la sécurité d'un produit évolue dans le temps, à la baisse. Or, la durée de vie des systèmes billettiques doit dépasser les 10 ans,
- la TOE sera distribuée à des millions d'exemplaires. Il n'est pas question de devoir changer de TOE après leur émission, si une vulnérabilité grave est alors constatée. Les

attaques sur la TOE doivent donc demander des moyens financiers et des compétences techniques et/ou cryptographiques importants.

8. Annexe :Terminologie et glossaire

Application	Ensemble des données et commandes spécifiques à une utilisation de la carte à puce. Les applications viennent donc dans les puces en compléments des composants matériels et des logiciels de base (système d'exploitation carte et firmware). Ex. : application billettique, de porte-monnaie électronique.
CC	Critères Communs pour l'Evaluation et la Certification des Technologies de l'Information, version 2.0 de mai 1998.
CI	Circuit Intégré.
Confidentialité	Propriété d'une information qui ne peut être divulguée aux personnes, entités ou processus non autorisés.
Donnée	Représentation d'une information sous une forme conventionnelle, destinée à faciliter son traitement.
EAL	Evaluation Assurance Level — Ensemble prédéfini d'exigences d'assurance des Critères Communs ([CC-3]), qu'il est possible de compléter.
Equip. de confiance	D'après [CC-2], un équipement est de confiance ("remote trusted IT product") quand il fait l'objet d'une politique de sécurité et a été évalué avec succès.
Firmware	Logiciel développé par le fabricant d'un circuit intégré et consistant en une librairies de fonctions disponibles pour les applications.
Fonction de sécurité	Fonction mettant en oeuvre une partie de la TSP.
Information	Elément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué.
Intégrité	Propriété assurant qu'une info. n'a pas été modifiée de façon non autorisée.
Politique de sécurité	Ensemble des règles qui régissent le traitement des informations sensibles et l'utilisation des ressources par le produit ou système d'information concerné.
PP	Profil de Protection.
Sensible	Un traitement ou une information est sensible dès lors qu'il/elle a un besoin d'intégrité et/ou de confidentialité.
SFP	Security Function Policy — Règles mises en oeuvre par une fonction de sécurité. L'ensemble de ces règles forment la TSP.
SOF	Strength Of Function — Robustesse de la fonction. Ne concerne que les fonctions utilisant des mécanismes probabilistiques et permutationnels.
TOE	Target Of Evaluation — Cible d'évaluation, c'est-à-dire l'ensemble, défini de façon très précise, qui est à évaluer, et sur lequel un profil de protection porte.
TSF	TOE Security Functions — Sous-ensemble de la TOE mettant en oeuvre les fonctions de sécurité.
TSP	TOE Security Policy — Politique de sécurité de la TOE.