Table des Matières de l'annexe 5

Facteurs de risques

Document d'analyse des risques d'un système billettique interopérable

I. OBJET

Le but de ce document est d'ébaucher une liste des risques encourus par différents acteurs d'un système billettique interopérable, comme les clients, les exploitants et les industriels.

Cette liste devrait permettre aux exploitants de se positionner face à ces risques.

Ils devront choisir :

- de mettre des moyens pour en éviter certains
- d'en accepter d'autres dont la probabilité d'occurrence semble moins importante que les coûts et délais des moyens à mettre en place pour les pallier.

Il est d'autant plus important de faire ces choix lorsque plusieurs exploitants doivent collaborer au sein de systèmes interopérables car le degré de sécurité du système doit être homogène dans tous les réseaux. Il ne s'agit pas qu'un exploitant qui n'a pas voulu mettre les moyens pour pallier un risque fasse courir ce risque aux autres exploitants.

L'objet de cette note n'est pas de tenter d'établir un tableau des risques associant une ou plusieurs réponses à chaque risque mais bien de lancer des pistes de réflexion pour les exploitants désireux d'effectuer une analyse des risques exhaustive concernant leur système et leur interopérabilité.

En complément de cette approche des risques systémiques, les exploitants devront s'interroger en premier lieu sur une approche Qualité cohérente de leurs systèmes.

II. APPROCHE QUALITE

Afin d'adopter une démarche qualité homogène dans les systèmes interopérables, il est essentiel de s'accorder sur l'établissement des exigences qualité : les facteurs et critères Qualité du système projeté pour répondre aux besoins et aux attentes de tous les acteurs de la billettique.

II.1 FACTEURS QUALITE

FQ1 : Confidentialité	Aptitude à être protégé contre tout accès par des personnes non autorisées.
FQ2 : Efficacité	Aptitude à minimiser l'utilisation des ressources disponibles
FQ3 : Maniabilité	Aptitude à la convivialité, à la facilité d'emploi
FQ4 : Robustesse	Aptitude à conserver un comportement conforme aux besoins exprimés en présence d'événements non souhaités ou non prévus
FQ5 : Maintenabilité	Aptitude à faciliter la localisation et la correction des erreurs résiduelles
FQ6 : Adaptabilité / évolutivité	Aptitude à faciliter la suppression, l'évolution ou l'ajout de tout élément fonctionnel et technique du système avec une minimisation des coûts d'évolution
FQ7 : Portabilité	Aptitude à minimiser les répercussions d'un changement d'environnement logiciel et matériel

II.2 CRITERES QUALITE

Les critères Qualité permettent de s'assurer que le système répond bien aux facteurs Qualité. Bien évidemment, il est nécessaire de quantifier ces critères et d'identifier les seuils à partir desquels on peut dire que le critère est atteint.

On peut citer :

- La communicabilité
- La facilité d'apprentissage (notamment pour le client)
- La modularité
- La simplicité
- La lisibilité (pour pallier l'opacité du support par exemple)
- …

III. IDENTIFICATION DES FACTEURS DE RISQUES, DES RISQUES ET DES CONSEQUENCES

Notations :

- Fx désigne un facteur de risque
- Rx désigne un risque
- Cx désigne une conséquence
- CEx désigne une conséquence élémentaire (une conséquence qui découle d'une autre conséquence)

En général, un facteur de risque induit un risque qui induit une conséquence qui peut induire une conséquence élémentaire :

$$\mathbf{Fx \rightarrow Rx \rightarrow Cx \rightarrow CEx}$$

III.1 FACTEURS DE RISQUES

F1 : Fraude Clientèle	Elle peut se traduire par la non validation d'un titre de transport pour accéder au service, par la cessibilité de la carte personnelle, …
F2 : Fraude Exploitant	Il s'agit de fraude interne qui peut se traduire de nombreuses manières comme la reproduction de carte (en utilisant par exemple un processus utilisé pour la reconstitution de cartes), la reproduction de transactions, …
F3 : Fraude Industriel	Elle peut se traduire par la communication de secrets sur la sécurité du système comme les algorithmes cryptographiques ou les clés de sécurité.
F4 : Manque de fiabilité du matériel	
F5 : Vol d'équipement de vente	Cela peut entraîner des risques de reproduction de cartes, de reproduction de transactions, de modifications des données sur la carte, ...

III.2 RISQUES

- R1 : Détérioration physique de la carte
- R2 : Faillibilité des algorithmes cryptographiques
- R3 : Reproduction de cartes (clonage)
- R4 : Atteinte à l'intégrité des données des cartes (il s'agit de la modification non autorisée des données d'une carte)
- R5 : Reproduction de transactions
- R6 : Altération de la communication entre le sol et les cartes
- R7 : Vol de carte
- R8 : Réclamation client
- R9 : Accès au système sans validation client
- R10 : Exploitation des données d'exploitation d'un transporteur par une organisation susceptible d'être concurrente

III.3 PRINCIPALES CONSEQUENCES IDENTIFIEES

Risque	Conséquences	Conséquences élémentaires
R1. Détérioration physique de la carte	C1 : Impossibilité d'effectuer une transaction (composant + support)	
	C2 : Envoi d'informations incorrectes aux équipements (composant)	⇒ CE1. Préjudice porté au client ⇒ CE2. Pertes financières d'exploitation ⇒ CE3. Statistiques erronées
R2. Faillibilité des algorithmes cryptographiques	C3 : Atteinte à la confidentialité des données	⇒ R10. Exploitation des données d'exploitation d'un transporteur par une organisation susceptible d'être concurrente ⇒ CE4. Atteinte à la liberté des clients
	R4 : Atteinte à l'intégrité des données des cartes	Cf. Conséquences R4
R3. Reproduction de cartes	C4 : Transactions fictives	⇒ CE2. Pertes financières d'exploitation (transactions de vente) ⇒ CE3. Statistiques erronées (transactions de vente et de validation)
R4. Atteinte à l'intégrité des données des cartes	C5 : Accroissement des droits sur une carte : profil, dates de validité, titres, ...	⇒ CE2. Pertes financières d'exploitation ⇒ CE3. Statistiques erronées
	C6 : Carte rendue inutilisable	⇒ CE5. Terrorisme
R5. Reproduction de transactions	C4 : Transactions fictives	⇒ CE2. Pertes financières d'exploitation ⇒ CE3. Statistiques erronées
R6. Altération de la communication entre le sol et les cartes	C7 : Suppression d'une partie de la transaction	*Suppression/diminution du paiement* ⇒ CE2. Pertes financières d'exploitation *Suppression/diminution d'un débit de validation* ⇒ CE2. Pertes financières d'exploitation ⇒ CE3. Statistiques erronées (transactions de vente et de validation)

Risque	Conséquences	Conséquences élémentaires
R7. Vol de carte	C3 : Atteinte à la confidentialité des données	⇒ R10. Exploitation des données d'exploitation d'un transporteur par une organisation susceptible d'être concurrente ⇒ CE4. Atteinte à la liberté des clients
	C4 : Transactions fictives	⇒ CE2. Pertes financières d'exploitation ⇒ CE3. Statistiques erronées
	C6 : Carte rendue inutilisable	⇒ CE5. Terrorisme
R8. Réclamation client	C8 : Insatisfaction client	⇒ CE6. Baisse du taux de fréquentation ⇒ CE2. Pertes financières d'exploitation
R9. Accès au système sans validation client		⇒ CE2. Pertes financières d'exploitation
R10. Exploitation des données d'exploitation d'un transporteur par une organisation susceptible d'être concurrente	C10 : Mise en place de services concurrents	⇒ CE6. Baisse du taux de fréquentation ⇒ CE2. Pertes financières d'exploitation
	C11 : Utilisation des données clients pour les capter	⇒ CE4. Atteinte à la liberté des clients ⇒ CE6. Baisse du taux de fréquentation ⇒ CE2. Pertes financières d'exploitation

IV. MOYENS PREVENTIFS ET CURATIFS A METTRE EN ŒUVRE

Il s'agit ici de citer de grandes classes de moyens à mettre en œuvre (inspirées pour certaines des ITSEC "Critères harmonisés pour l'évaluation de la sécurité des systèmes et produits informatiques") et non d'une liste exhaustives de solutions techniques.

M1 : Authentification des utilisateurs avec contrôle d'accès	Fonctions destinées à vérifier l'identité d'un utilisateur et à contrôler l'utilisation des ressources et des flux d'informations.
M2 : Audit	Fonctions concourant à détecter et investiguer les événements qui peuvent constituer une menace pour la sécurité.
M3 : Fidélité	Fonctions destinées à s'assurer que les données n'ont pas été modifiées indûment.
M4. Échange de données sécurisé	Fonctions qui garantissent la sécurité des données sur les voies de transmission
M5. Non répudiation	Fonctions destinées à disposer des moyens de répondre à toute réclamation sur l'utilisation du système. Il s'agit entre autre de certifier et d'archiver les transactions de vente et de validation dans le cas de réclamations clients.
M6. Gestion de listes noires	Fonctions destinées à répertorier les éléments d'un réseau pour lesquels a été détectée une anomalie. Elles visent notamment à interdire l'usage de cartes volées ou perdues.
M7. Contrôle	Fonctions destinées à vérifier la validité des titres de transport des usagers.