Ministère de l'Equipement, des Transports et du Logement

Direction des Transports Terrestres

Sous-direction des Transports Collectifs

DTT/TC2

Affaire suivie par :
Jean-Jacques FAURE
Tél. : 01 40 81 16 29
Télécopie : 01 40 81 16 40

Mission des Transports Intelligents

DTT/MTI

Affaire suivie par :
Jean-François JANIN
Tél. : 01 40 81 82 69

La Défense, le 7 février 2002

Le ministre de l'équipement, des transports et du logement

A

Monsieur le préfet de région d'Ile-de-France
Direction régionale de l'équipement d'Ile-de-France

Madame et messieurs les préfets de région (pour information)
Directions régionales de l'équipement (pour information)

Mesdames et Messieurs les préfets de département

Directions départementales de l'équipement

Objet : Sécurité des systèmes d'information liés à la billetterie électronique

P.J. : Guide pour l'élaboration d'une politique de sécurité pour un système billettique interopérable.

La mise en oeuvre de la politique de développement des transports publics fait une large place à la notion d'intermodalité et aux accords à conclure entre autorités organisatrices de transport et opérateurs pour l'amélioration des services.

La création d'un système de billetterie électronique fait partie des outils dont disposent les collectivités pour prendre mieux en compte les besoins des usagers, maîtriser la fraude et réduire les coûts de maintenance des matériels. Afin de rendre plus attractif le transport public, les systèmes de billettique doivent être conçus pour faciliter le passage d'un réseau à un autre (concept d'intéropérabilité)

Cette facilité nouvelle donnée aux usagers a une contrepartie en terme de sécurité, puisque chacun des systèmes peut faire courir des risques aux autres s'il ne prend pas les mesures adéquates pour assurer la protection des données, la fiabilité des traitements et une information pertinente en cas d'incident.

On notera d'ailleurs que même en l'absence d'intéropérabilité effective, la diffusion de cartes de transport à plusieurs millions d'usagers va rendre crédibles des menaces « ludiques » ou « médiatiques » auxquelles les responsables devraient se préparer à apporter des réponses coordonnées.

Dans la situation actuelle, les autorités organisatrices mettent en place ces systèmes, le plus souvent sous la forme de contrats « clef en main », sans formalisation d'une politique de sécurité.

Il convient de rappeler à ces maîtres d'ouvrage le dispositif mis en place par l'Etat pour leur apporter l'appui méthodologique nécessaire à la définition de ces politiques, en particulier la recommandation 901 et la documentation disponible auprès de la Direction Centrale de la Sécurité des systèmes d'information.

Compte tenu du contexte particulier dans lequel se mettent en place ces systèmes, l'idée a été émise de constituer, sur la base du volontariat, un groupement des maîtres d'ouvrage qui pourraient mettre au point et appliquer de bonnes pratiques professionnelles dans ce domaine.

En transmettant aux autorités organisatrices responsables des projets concernés les éléments ci-joints qui résultent des réflexions conduites au plan national dans le cadre de la Charte Billettique Monétique, je vous serais obligé de leur demander s'ils seraient disposés à participer à un tel groupement et de me faire connaître leurs réponses avant le 8 mai 2002.

GUIDE POUR L'ÉLABORATION D'UNE POLITIQUE DE SÉCURITE POUR UN SYSTÈME BILLETTIQUE INTEROPERABLE

La sécurité des systèmes interopérables présente une difficulté particulière du fait du partage des responsabilités entre les différents maîtres d'ouvrage. En l'absence de règles précises et de procédures permettant d'assurer leur mise en œuvre, il existe des risques que des événements qui n'ont pas de conséquence immédiate pour l'un des partenaires passe inaperçu alors qu'il pourrait avoir de graves conséquences pour un autre ou pour le système dans son ensemble.

Il est nécessaire, au moment où l'on décide de mettre en exploitation des systèmes billettiques interopérables de formaliser une politique de sécurité d'ensemble et des politiques pour chacun des systèmes et de prévoir un mécanisme permanent pour vérifier l'application de ces politiques et tirer les conséquences des incidents constatés et de l'évolution de l'environnement.

Les politiques de sécurité devront prendre en considération l'ensemble des menaces suivantes :

- Indisponibilité des équipements (panne ou dysfonctionnement).
- Menaces liées au paiement (Remboursement de titres acquis illicitement ou inscrits sur une carte acquise illicitement, acceptation de faux titres de transport, …).
- Création de vrais titres sans paiement (détournement des équipements par les utilisateurs ou utilisation d'un cheval de Troie ou d'une faille dans les équipements).
- Contrefaçon de carte (titres de transport, abonnement, statut, droit).
- Falsification de carte (titres de transport, abonnement, statut, droit).
- Contrefaçon d'équipements.
- Utilisation de cartes illisibles (délivrance de titres temporaires).
- Remboursement à tort.
- Fraude aux droits de réduction.
- Acceptation de cartes en listes noires (modification frauduleuse de listes noires ; suppression non autorisée, indisponibilité d'une liste noire).
- Menaces liées au développement, à la maintenance et à la gestion du projet, à l'utilisation de cartes de test ou de jeux d'essai.
- Vol de modules de sécurité, d'équipements et de cartes.
- Intrusion dans les systèmes communautaires ou non-communautaires (accès illicite ou abusif).
- Malversation ou erreur au niveau d'une liste positive.
- Infraction à la loi Informatique et Libertés.

- Détournement de fichiers clientèles à des fins commerciales.

Ces menaces s'ajoutent à celles qui doivent déjà être considérées dans la conception et l'exploitation des systèmes billettiques, même en absence d'interopérabilité :

- Distribution de vraies fausses cartes aux guichets (correspond à un détournement d'équipement).
- Détournement d'équipement, utilisation abusive d'équipement.
- Exploitation des vulnérabilités technologiques de la carte.
- Absence de titre de transport ou titre de transport irrégulier.
- Détournement de paiement.
- Fraudes et erreurs au détriment de l'usager.
- Attaque médiatique.
- Politique discriminatoire d'une entité vis-à-vis d'une autre.

Chaque politique doit être élaborée en fonction du contexte précis de matériel et d'emploi. On ne saurait donc établir une politique de sécurité type. On trouvera cependant ci dessous une liste de parades ou de recommandations correspondant aux menaces citées ci dessus, afin de faciliter la réflexion des concepteurs et des exploitants.

.

Menaces identifiées retenues	**Parades possibles pour contrer ces menaces**
Indisponibilité des équipements (panne ou dysfonctionnement).	Exigences communautaires au niveau du backup, des sauvegardes, de la fiabilité des équipements, … Mise en commun d'équipements.
Menaces liées au paiement.	Politique de remboursement (remboursement par l'émetteur uniquement). Contrôle de la carte et vérification de l'identité de l'usager lors du remboursement. Suivi des remboursements effectués. Suivi des titres émis et des consommations.
Création de vrais titres sans paiement	Procédure de recette des équipements. Politique de sécurité de la sous-traitance.
Contrefaçon de carte (titres de transport, abonnement, statut, droit).	Politique de sécurité au niveau des projets. Gestion des secrets opérationnels et de test. Maîtrise de la sécurité au niveau des sous-traitants.
Falsification de carte (titres de transport, abonnement, statut, droit).	Politique de sécurité au niveau des projets. Gestion des secrets opérationnels et de test. Maîtrise de la sécurité au niveau des sous-traitants.
Contrefaçon d'équipements.	Politique de sécurité au niveau des projets. Gestion des secrets opérationnels et de test. Maîtrise de la sécurité au niveau des sous-traitants.
Utilisation de cartes illisibles (délivrance de titres temporaires).	Confiscation pour analyse des cartes illisibles. Mise en liste d'opposition d'une carte illisible lors de son remplacement. Utilisation d'une BDD commune des images carte comme référence. Suivi des cartes illisibles par un service de détection des fraudes.
Remboursement à tort.	Règles communautaires: remboursement par l'émetteur, …
Fraude aux droits de réduction.	Contrôle rigoureux des demandes de statut.

Menaces identifiées retenues	Parades possibles pour contrer ces menaces
	Politique cohérente entre les bassins au niveau de l'attribution des statuts. BDD communes des statuts et des titulaires de statuts. Suivi de l'utilisation des statuts par un service de détection des fraudes.
Acceptation de cartes en listes noires (modification frauduleuse de listes noires ; suppression non autorisée, indisponibilité d'une liste noire).	Politique commune d'utilisation des listes noires. Gestion des habilitations et contrôle des accès aux systèmes. Imputabilité des actions effectuées par les agents. Utilisation de listes noires et d'opposition communes. Contrôle des transactions effectuées par les agents (identification et authentification des agents ; mémorisation des transactions ; analyse par un service de détection des fraudes). Justificatifs nécessaires pour les modifications et mémorisation de ces justificatifs.
Menaces liées au développement, à la maintenance et à la gestion du projet, à l'utilisation de cartes de test ou de jeux d'essai.	Politique d'assurance qualité - sécurité. Contrôle des équipes de développement. Contrôle des équipes de maintenance. Utilisation d'un environnement, d'équipements et de jeux de test identifiables, séparés et différents du contexte opérationnel. Réalisation d'une analyse des risques au niveau de chaque entité concernée par l'interopérabilité de la TB.
Vol de modules de sécurité, d'équipements et de cartes.	Suivi des mouvements de matériel. Gestion du parc d'équipement. Utilisation de listes noires. Mémorisation dans les cartes des équipements (modules de sécurité) ayant servi à la transaction. Utilisation de plafond et d'un mécanisme de rechargement pour les modules de sécurité. Nécessité pour un équipement de vente ou de personnalisation d'obtenir des informations d'un site central pour pouvoir fonctionner. Diminution de la sensibilité des équipements par déport des modules
Intrusion dans les systèmes communautaires ou non communautaires (accès illicites ou abusifs).	Politique de sécurisation des systèmes. Isolation des systèmes vis-à-vis de l'extérieur. Contrôle des accès aux systèmes.
Malversation ou erreur au niveau d'une liste positive.	Politique commune d'utilisation des listes positives. Utilisation de listes communes. Politique de sécurisation des systèmes, de contrôle des accès aux systèmes, de sécurisation des fichiers correspondants aux listes positives. Mémorisation des demandes d'actions et des justificatifs. Contrôle des transactions effectuées par les agents (identification et authentification des agents ; mémorisation des transactions ; analyse par un service de détection des fraudes).
Infraction à la loi Informatique et Libertés.	Déclaration des fichiers et des traitements relatifs à des données à caractère personnel. Protection des informations à caractère personnel.
Détournement de fichiers clientèles à des fins commerciales.	Identification et protection des données commerciales privées. Engagement de respecter les données ayant une valeur commerciale mais devant être partagée. Limitation de la quantité de données à ayant une valeur commerciale mais devant être partagée
Toute menace.	Politique de partage / séparation des clés. Sécurisation des accès aux systèmes émetteurs.

Menaces identifiées retenues	Parades possibles pour contrer ces menaces
	Mise en place d'instances (d'étude et de suivi, de décision) en charge des aspects sécuritaires. Existence d'une organisation sécurité au niveau de chaque entité (autorité organisatrice ou exploitants). Sensibilisation et d'information du personnel sur les aspects sécuritaires. Structure, dédiée ou commune, de détection et de gestion des fraudes. Séparation ou partage des responsabilités pour les fonctions sensibles. Imputabilité des transactions carte et des actions des agents. Existence d'une classification des incidents pouvant conduire au déclenchement d'un plan d'urgence communautaire ainsi que d'une procédure d'alerte et de déclenchement du plan d'urgence Existence d'un plan de communication communautaire. Organisation d'une cellule de crise. Identification et authentification des usagers lors de leurs demandes.

1.1.1.1.

On peut citer également les mesures suivantes, qui n'ont pas un rapport direct avec la situation d'interopérabilité, mais qui pourront apparaître comme pertinentes aussi dans ce contexte :

Menaces identifiées exclues	Parades possibles
Détournement d'équipement, utilisation abusive d'équipement.	Contrôle des transactions effectuées par les agents (identification et authentification des agents ; mémorisation des transactions ; analyse par un service de détection des fraudes). Contrôle d'accès physique aux équipements ou aux locaux contenant ces équipements. Suivi de l'utilisation des équipements en maintenance. Extraction des modules de sécurité des équipements envoyés en maintenance. Utilisation de cartes et de jeux de test pour les équipements en maintenance.