



Ministère du Budget  
et de la Réforme de l'Etat  
DGME/SDAE



PREMIER MINISTRE  
SGDN - DCSSI

=====

## **FEROS Types**

### **Téléprocédure de référence**

### **Paiement**

=====

**VERSION 1.0**

FEROS Types		Paie <sup>ment</sup>		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	1/58

<b>FEROS Types</b>	
<b>Déclaration de changement d'adresse</b>	
<b>Référence</b>	<b>Date</b>
FEROS Types PaiementV1.0.doc	13/04/2006
<b>Identification d'objet (OID)</b>	<b>Racine OID et gestionnaire</b>
1.2.250.1.137.2.2.1.2.3.6.1	DGME/SDAE
<b>Responsable</b>	<b>Version</b>
DGME/SDAE – SGDN\DCSSI	<b>V1.0</b>
<b>Critère de diffusion</b>	<b>Nombre de pages</b>
<b>Public</b>	58

<b>HISTORIQUE DES VERSIONS</b>			
<b>DATE</b>	<b>VERSION</b>	<b>EVOLUTION DU DOCUMENT</b>	<b>REDACTEUR</b>
15/04/2005	0.1	Création du document	Fidens
13/04/2006	1.0	Version publiée	DCSSI/SDAE

<b>FEROS Types</b>		<b>Paiement</b>		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	2/58

<b>SOMMAIRE</b>
-----------------

<b>1</b>	<b>INTRODUCTION .....</b>	<b>4</b>
1.1	CONTEXTE GENERAL .....	4
1.2	DEFINITION DES RESPONSABILITES .....	5
<b>2</b>	<b>DESCRIPTION DU SYSTEME ETUDIE .....</b>	<b>6</b>
2.1	PRESENTATION DU SYSTEME-CIBLE .....	6
2.2	DESCRIPTION DES ELEMENTS ESSENTIELS .....	8
2.3	ENJEUX .....	14
2.4	HYPOTHESES .....	14
2.5	ECHELLE DE BESOINS .....	15
2.6	BESOINS DE SECURITE DES ELEMENTS ESSENTIELS .....	16
<b>3</b>	<b>LES RISQUES .....</b>	<b>22</b>
3.1	HIERARCHISATION DES RISQUES .....	22
3.2	DESCRIPTION DES RISQUES .....	23
<b>4</b>	<b>OBJECTIFS DE SECURITE .....</b>	<b>47</b>
<b>5</b>	<b>LES RISQUES RESIDUELS .....</b>	<b>52</b>
5.1	METHODES D'ATTAQUE NON RETENUES .....	52
5.2	TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS.....	56

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	3/58

# 1 Introduction

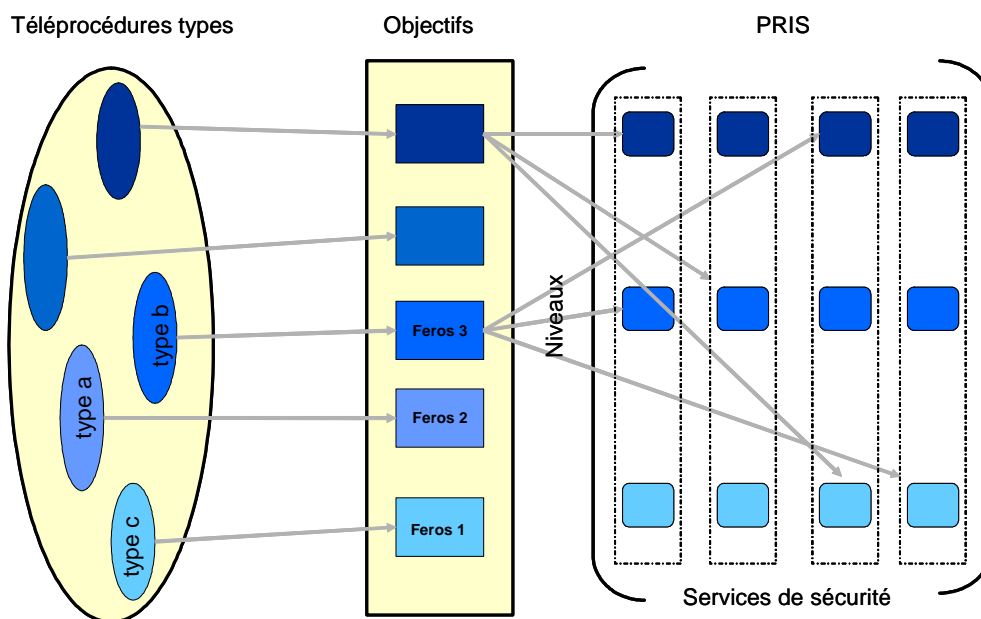
## 1.1 Contexte général

Poursuivant un triple objectif de modernisation des services, de simplification des démarches et de recherche d'une plus grande efficacité, l'Etat a entamé un processus de modernisation de son Administration. A ce titre, l'Etat s'est engagé dans le développement de services en ligne, gages d'amélioration de la qualité de service et de gain de productivité.

La mise en place de ces relations dématérialisées avec les usagers – citoyens, agents de l'Administration, entreprises, ... -, nécessite une confiance reconnue et partagée par les différents acteurs. Afin de favoriser l'émergence d'un climat de confiance mutuelle propre au développement de ces téléservices, la DCSSI et l'ADAE contribuent aujourd'hui à la définition d'un cadre général de sécurisation des systèmes d'information.

C'est ainsi qu'ils ont élaboré un ensemble documentaire unique baptisé PRIS, « Politique de Référencement Intersectorielle de Sécurité », déterminant pour différents services de sécurité et différents niveaux de sécurité un ensemble d'exigences juridiques et organisationnelles et de spécifications techniques ; cet ensemble deviendra la référence à laquelle les prestataires de services et les fournisseurs de produits devront se conformer.

Pour faciliter l'utilisation de cet ensemble documentaire, l'ADAE a lancé une étude, visant à établir des correspondances entre téléprocédures types et les référentiels PRIS.



FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	4/58

L'analyse générique d'objectifs de sécurité pour des téléprocédures types doit permettre de faciliter et d'homogénéiser les expressions de besoins des donneurs d'ordre en mettant à leur disposition des référentiels sur lesquels ils pourront s'appuyer pour exprimer leurs besoins spécifiques. Par exemple, le promoteur d'une téléprocédure de paiement de cotisation pourra procéder à partir de la téléprocédure type « paiement », en analysant les spécificités liées au contexte opérationnel et à la sensibilité des informations traitées, et en conservant les invariants de l'analyse (fonctions, éléments menaçants, ...)

Le choix des téléprocédures types a été réalisé sur une base statistique – étude des téléprocédures les plus largement mises en œuvre – ou en fonction des priorités de l'ADAE.

Les téléprocédures type retenues sont :

- **Consultation**
- **Simulation**
- **Démarche en ligne : déclaration**
- **Démarche en ligne : candidature**
- **Démarche en ligne : demandes**
- **Paiement en ligne**

Le présent document présente l'analyse des objectifs de sécurité pour la téléprocédure type paiement en ligne.

## 1.2 Définition des responsabilités

La présente analyse a été réalisée sous Maîtrise d'œuvre de l'ADAE, avec le soutien de la DCSSI qui a apporté son expertise technique.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	5/58

## 2 Description du système étudié

Cette téléprocédure facilite la relation entre usagers et Administration en offrant aux internautes la possibilité d'effectuer des paiements en ligne. Le paiement en ligne comprend toujours une phase d'identification ou d'adhésion, et un accès à un dossier justifiant le paiement demandé. Les informations relatives au paiement peuvent présenter un caractère confidentiel, relatif à la vie privée par exemple.

### *Exemples de mise en œuvre*

*Paiement d'amendes (exemple des radars automatiques)*

*Règlement pour immatriculer une entreprise en ligne*

*Règlement de TVA*

*Règlement de charges sociales*

*Règlement d'impôts*

*Règlements de droits d'entrée (musée, tennis, piscine,...)*

## Scénario retenu pour l'analyse

### DESCRIPTION

Au titre de la téléprocédure type, on a retenu le paiement d'amendes en ligne, réalisée directement par l'intéressé à partir de ses moyens informatiques personnels. Ce choix présente l'intérêt de proposer réellement une procédure de paiement en ligne, alors que dans d'autre cas le paiement est différé et l'utilisateur se limite à renseigner une autorisation de prélèvement.

### USAGER

- Particulier

### MODE OPERATOIRE

- Accès depuis les moyens informatiques propres de l'utilisateur

### DOMAINE D'APPLICATION

- Fiscal

Le scénario retenu est parfaitement représentatif de la téléprocédure de paiement en ligne. Les besoins de sécurité ne varient pas drastiquement en fonction du contexte applicatif, de sorte que l'analyse effectuée dans le contexte du paiement des amendes doit être adaptée à la plupart des téléprocédures de paiement en ligne.

## 2.1 Présentation du système-cible

Afin de rapprocher le modèle de la réalité, l'analyse est menée sur la base d'une téléprocédure existante – ici le service de télépaiement des amendes.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	6/58

## Système-cible

### Présentation

Dans le contexte de l'automatisation des contrôles aux infractions au code de la route, la mission Interministérielle Contrôle Sanction Automatique à mis en place un système permettant de gérer automatiquement toutes les fonctions qui peuvent l'être dans l'ensemble du processus allant de la constatation de l'infraction à la mise en oeuvre de la sanction.

Conjointement à cette initiative, le portail « [www.amendes.gouv.fr](http://www.amendes.gouv.fr) » a été mis en oeuvre afin de dématérialiser la procédure de paiement. Ce service de télépaiement permet :

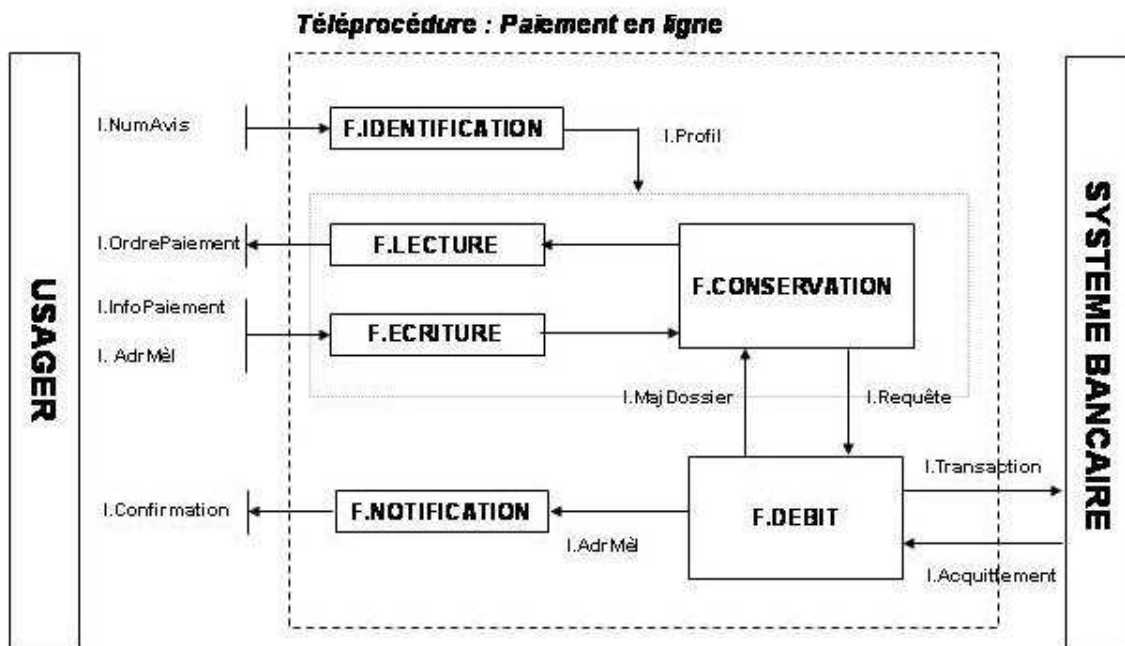
- Le paiement de l'amende
- Le paiement de la consignation afin de contester l'amende

La présente étude ne concerne que la partie associée au paiement direct de l'amende par carte de paiement. La procédure de contestation et les mesures de majoration sont jugées hors sujet et ne feront l'objet d'aucune analyse.

D'autre part, la notion de dématérialisation étant prédominante, seules les justifications de paiement émises par mèl seront considérées. L'envoi par courrier postal n'est pas abordé.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	7/58

## 2.2 Description des éléments essentiels



### Fonction : F.NOTIFICATION

**Description** Lorsque l'utilisateur a saisi son adresse mèl, cette fonction est chargée de l'envoi d'une confirmation de règlement de l'amende.

### Fonction : F.CONSERVATION

**Description** Cette fonction traite l'ensemble de la problématique de conservation des informations. Dans le cadre de la téléprocédure « Télépaiement des amendes », on répertorie deux catégories d'informations :

- Les informations nominatives (Ordre de paiement, adresse mèl,...)
- Les informations fiscales (Numéro de carte)

Le contrevenant n'agit pas directement sur la partie conservation de données. Il passe par la phase d'identification de l'avis et accède ensuite aux informations par l'intermédiaire des fonctions « F.LECTURE » et « F.ECRITURE ».

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	8/58

Les autorisations qui lui ont été accordées lui permettent de :

- Visualiser l'ordre de paiement correspondant au numéro de l'avis d'imposition.
- Soumettre à l'administration les informations bancaires nécessaires pour le paiement.
- Soumettre les informations nécessaires à l'envoi du justificatif de paiement (facultatif).

### Fonction : F.DEBIT

#### Description

Cette fonction est perçue comme une interface entre l'administration et le réseau bancaire « Carte de paiement ». A partir des informations tirées de l'ordre de paiement et des informations d'identification bancaire saisie par l'utilisateur, l'administration formule et transmet la transaction (« I.Transaction »).

La gestion des systèmes d'échanges et de règlement entre les banques dépasse le cadre de cette fonction. Cependant, chaque transaction est acquittée par le biais d'une notification de paiement issue du sous système bancaire (« I.Acquittement»). Elle permet à l'administration de valider le paiement de l'amende et d'initier le processus de mise à jour du dossier au niveau de la partie conservation de données (« I.MajDossier »).

### Fonction : F.ECRITURE

#### Description

Cette fonction permet à l'utilisateur de soumettre de l'information à l'administration. Dans le contexte du paiement en ligne, il est amené à saisir deux types d'informations :

- Ses informations bancaires
- Son adresse mèl s'il souhaite recevoir une justification de règlement

Lors de la saisie, un contrôle syntaxique approprié est effectué suivant la nature des informations. Cependant, pour l'adresse mèl et les coordonnées bancaires, aucun contrôle n'est entrepris pour garantir l'existence ou la solvabilité du compte. En cas d'inexactitude des informations bancaires, l'utilisateur s'expose à des mesures de la part de l'administration.

L'information "I.Profil" fixe les autorisations qui s'appliquent à cette fonction afin d'accéder de façon cohérente à la partie conservation de

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	9/58

données.

### Fonction : F.IDENTIFICATION

**Description** Cette fonction, sur la base du numéro et de la clé inscrits en bas de l'avis de contravention, fixe les autorisations (voir « I.Profil ») qui permettent à l'utilisateur d'accéder à l'ordre de paiement pour procéder au règlement de son amende.

### Fonction : F.LECTURE

**Description** Cette fonction permet à l'administration de présenter des données à l'utilisateur. Deux types d'informations sont soumis à l'utilisateur :

- Les informations statiques (Ordre de paiement, Aide en ligne,...)
- Les informations dynamiques (Erreurs de traitement,...)

Tout comme pour la fonction écriture, l'information "I.PROFIL" spécifie les autorisations qui s'appliquent.

### Information : I.Acquittement

**Description** L'acquittement émane du sous système bancaire en réponse à une transaction préalablement émise par l'administration. Il fait état du résultat de la transaction financière. Deux issues sont possibles :

- Le succès qui signifie que les traitements encadrés par la transaction ont été exécutés avec succès.
- L'échec qui annule tout ou partie des opérations engagées, et identifie les traitements non finalisés.

Cet acquittement n'est pas redirigé vers l'utilisateur. Sur la base de cet acquittement, la partie conservation de données est mise à jour afin de répercuter le résultat au niveau de l'ordre de paiement de l'utilisateur.

Cet élément essentiel permet de garantir la non-répudiation de l'échange entre l'administration et la banque du contrevenant en cas de contestation.

L'acquittement diffère de la confirmation, par laquelle le contrevenant peut disposer d'un justificatif de règlement établissant la preuve qu'il a fourni les informations nécessaires (voir "InfoPaiement") pour la

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	10/58

réalisation de la transaction à une date donnée, sans augurer de la bonne fin de la transaction financière.

### Information : I.AdrMèl

**Description** Adresse mèl du contrevenant. Cette information est facultative, et nécessaire uniquement au cas où l'utilisateur souhaite recevoir une confirmation de règlement ("I.Confirmation")

### Information : I.Confirmation

**Description** Cette confirmation atteste que le contrevenant a saisi les informations nécessaires au règlement de sa contravention. Il s'agit d'une preuve lui permettant de démontrer qu'il a renseigné les éléments nécessaires au règlement en temps et en heure (Ex : En cas de majoration), mais qui n'augure pas de la bonne fin du règlement (volet bancaire).

### Information : I.InfoPaiement

**Description** Cet élément essentiel regroupe les informations nécessaires pour le règlement de la contravention de l'utilisateur. Lors de cette phase, l'utilisateur doit fournir :

- Un numéro de carte bancaire valide
- La date de validité de la carte associée au numéro

Cette saisie constitue le préalable nécessaire au règlement puisque l'utilisateur communique ses informations bancaires à l'administration. Ces informations seront transmises à la banque pour prélever le compte du contrevenant (voir "I.Transaction"), dans un deuxième temps. Il y a stockage des informations bancaires communiquées, et traitement par lots avec les banques.

D'autre part, il peut être important d'associer aux données transmises par l'utilisateur, ou aux informations de confirmation émises par l'Administration une marque de temps opposable en cas de litige quant à l'observation des délais de paiement par l'utilisateur.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	11/58

### Information : I.MajDossier

**Description** Information répercutant la réception de la notification de paiement (« I.Acquittement) sur la partie conservation de données. Cette information fait passer le dossier d'un usager de l'état « En cours de traitement" vers « Régulé » "ou de "En cours de traitement" vers "En échec".

### Information : I.NumAvis

**Description** Cette information tirée de l'avis de contravention est composée d'un numéro et d'une clé permettant d'identifier l'ordre de paiement dans la base des dossiers. L'usager doit posséder cette information afin d'accéder à l'ordre de paiement associé à son avis de contravention.

### Information : I.OrdrePaiement

**Description** Cette information regroupe les données de l'ordre de paiement correspondant à l'avis de contravention envoyé à l'usager. Les principales informations stockées sont :

- Nom, prénom du contrevenant
- Nature de l'excès de vitesse (description)
- Date limite de paiement avant majoration
- Montant de l'amende
- Etat de l'ordre de paiement

Suivant l'état d'avancement, l'ordre de paiement peut se trouver dans l'un de ces quatre états :

- Majoré, lorsque l'avis n'a pas été réglé et que la date limite de règlement est dépassé
- Impayé, lorsque l'avis n'a pas été réglé et que la date limite de règlement n'est pas dépassée.
- En échec, lorsque la transaction financière a échoué et nécessite des mesures spécifiques.
- En cours de traitement, lorsque l'avis est réglé mais que le prélèvement bancaire n'a pas encore été effectué

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	12/58

- Réglé, lorsque le prélèvement bancaire a été effectué et la confirmation envoyée à l'utilisateur.

A tout moment, l'utilisateur est en mesure de vérifier l'état du dossier à partir de son numéro de contravention.

### Information : I.Profil

#### Description

Cette donnée fixe les autorisations d'accès qui s'appliquent aux informations et aux fonctions. Le profil de l'utilisateur est établi après l'identification de l'ordre de paiement sur la base du numéro d'avis de contravention.

Pour la téléprocédure "Paiement en ligne", les restrictions s'appliquent aux fonctions :

- F.LECTURE
- F.ECRITURE
- F.CONSERVATION

Le profil établi permet d'identifier les données accessibles en lecture et en écriture au niveau de la partie « conservation de données ».

### Information : I.Requete

#### Description

Cet élément essentiel regroupe les données tirées de l'ordre de paiement et des informations bancaires de l'utilisateur.

Elles sont exploitées localement pour générer une transaction financière conforme aux spécificités du sous système bancaire par l'intermédiaire de la fonction « F.DEBIT ».

### Information : I.Transaction

#### Description

Une transaction peut être définie comme une unité indivisible contenant un ensemble d'opérations.

Dans le cadre de cette téléprocédure, la transaction émane de l'administration à destination du sous système bancaire et permet de prélever le compte de l'utilisateur du montant de la contravention.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	13/58

## 2.3 Enjeux

### H.ATTENTES

Description Les récents sondages indiquent une hausse notable des attentes des utilisateurs vis à vis de l'administration électronique. L'augmentation de l'utilisation d'Internet, la confiance grandissante inspirée ou encore la simplicité d'utilisation sont autant de catalyseurs qui favorisent le développement des téléprocédures.

### H.DEMATÉRIALISATION

Description La dématérialisation des flux entre les différents organismes publics s'impose comme un objectif majeur. Dans le cadre de la mise en oeuvre de cette téléprocédure, cela constitue un enjeu pour la réussite du projet.

### H.SERVICES

Description Cette téléprocédure s'inscrit dans le projet de modernisation des services administratifs et vise à simplifier les nombreuses démarches actuelles des usagers.

## 2.4 Hypothèses

### H.CONFIANCE

Description Dans le cadre de cette analyse, il sera admis que les agents bénéficiant du plus haut degré de privilèges sont de confiance.

### H.CONTRAT

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	14/58

Description La réalisation d'une transaction financière entre différents acteurs s'établit dans un cadre contractuel strict. L'existence, la diffusion d'un tel contrat conformément aux lois et réglementations en vigueur ainsi que le consentement de l'utilisateur sont admis.

## H.LOCAUX

Description Dans le cadre de l'analyse, il est admis que la téléprocédure est hébergée dans des locaux bénéficiant de mesures de sécurité adaptées. Par conséquent, les méthodes d'attaques basées sur un accès physique aux locaux seront volontairement écartées.

## H.ORGANISATIONNEL

Description Dans le cadre de cette étude, les menaces organisationnelles ne seront pas traitées.

## H.USAGER

Description La sécurité physique et environnementale au niveau du poste de l'utilisateur est garantie.

## 2.5 Echelle de besoins

	Confidentialité	Disponibilité	Intégrité
0	Informations publiques.	Une indisponibilité ne provoque aucune perturbation au niveau du système d'information.	La perte d'intégrité n'entraîne aucune gêne.
1	Informations personnelles mais dont la divulgation n'engendre aucune conséquence.	Une indisponibilité de quelques jours de l'application ou de la ressource est tolérable.	Une perte d'intégrité est dommageable mais les conséquences restent restreintes.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	15/58

2	Informations confidentielles ne devant pas être divulguées. Une perte de confidentialité est grave mais n'entraîne aucune conséquence au niveau économique ou médiatique.	Une indisponibilité momentanée de l'application ou de la ressource est tolérable.	Une perte d'intégrité des informations est grave mais ne touche qu'un nombre limité d'utilisateurs. Les conséquences restent donc restreintes.
3	Informations confidentielles ne devant pas être divulguées. Une perte de confidentialité a des conséquences sur le plan médiatique ou financier	Une indisponibilité à une incidence grave au niveau financier ou en terme d'image de marque	Une perte d'intégrité des informations est très grave et impacte le fonctionnement global de la téléprocédure. Elle entraîne une perte importante au niveau financier et/ou de l'image de marque.

## 2.6 Besoins de sécurité des éléments essentiels

		Besoin de sécurité	Commentaires
F.NOTIFICATION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Une indisponibilité de quelques heures est acceptable. Si le problème se prolonge, l'administration peut être exposée à des plaintes de la part des contrevenants en attente de leurs confirmations.
	Intégrité	2	Une perte d'intégrité est grave mais n'empêche pas la réalisation de la transaction financière. Cependant, l'administration peut être exposée à des contestations. La confirmation est un élément de preuve de la chose faite en temps et en heure pour l'utilisateur

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	16/58

F.CONSERVATION	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé car la fonction conserve les informations nécessaires au traitement des contraventions. Cependant une indisponibilité de quelques heures n'est pas trop préjudiciable étant donné le délai dont dispose le contrevenant pour régler sa contravention.
	Intégrité	3	Le besoin en intégrité est très élevé. Une perte d'intégrité peut s'accompagner de pertes financières importantes si elle touche des données financières (montant, numéro de compte), ou les informations de suivi des dossiers
F.DEBIT	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin en disponibilité est faible, dans la mesure où le prélèvement du compte de l'utilisateur n'est pas lié au processus d'émission de la confirmation (preuve). Une indisponibilité de la fonction "F.DEBIT" n'engendre aucune conséquence notable et ne peut pas provoquer de majoration des contraventions des contrevenants. Seul un délai au niveau du prélèvement du compte de l'utilisateur et de la mise à jour de l'état de l'ordre de paiement est envisageable.
	Intégrité	3	Une perte d'intégrité au niveau du module de débit est très grave puisqu'elle peut avoir des conséquences importantes au niveau des transactions émises.
F.ECRITURE	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Dans la mesure où l'utilisateur dispose de quarante cinq jours pour régler sa contravention, une indisponibilité de quelques heures ne peut pas être considérée comme un motif valable de contestation

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	17/58

	Intégrité	3	Le besoin en intégrité est important. L'utilisateur se trouve dans l'impossibilité de saisir convenablement ses informations bancaires et de payer son amende si cette fonction subit une perte d'intégrité.
F.IDENTIFICATION	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	L'indisponibilité ne doit pas dépasser quelques heures dans la mesure où les utilisateurs mécontents peuvent justifier d'une indisponibilité trop prolongée pour échapper à une majoration de leur contravention.
	Intégrité	2	Une perte d'intégrité au niveau de cette fonction est grave puisqu'elle permet l'accès aux ordres de paiement des usagers. Les conséquences financières restent limitées
F.LECTURE	Confidentialité	0	Aucun besoin en confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Dans la mesure où l'utilisateur dispose de quarante cinq jours pour régler sa déclaration, une indisponibilité de quelques heures ne peut pas être considéré comme un motif valable de contestation.
	Intégrité	1	Le besoin en intégrité est limité puisque cette fonction délivre des informations déjà disponibles sur l'avis de contravention de l'utilisateur.
I.Acquittement	Confidentialité	3	La notification émane du sous système bancaire. Le besoin en confidentialité est élevé puisque les informations d'acquittement peuvent véhiculer des informations bancaires en support de notification d'erreurs
	Disponibilité	2	Une indisponibilité de quelques heures est acceptable puisque l'utilisateur n'est pas en attente de la notification.
	Intégrité	3	Le besoin en intégrité est important puisque la réception de cet acquittement conditionne

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	18/58

			la mise à jour de l'état de l'ordre de paiement du contrevenant. Une atteinte à l'intégrité pourrait conduire à rejouer les mouvements de prélèvement
I.AdrMèl	Confidentialité	1	Le besoin en confidentialité au niveau de l'adresse mèl du contrevenant est moyen.
	Disponibilité	2	L'adresse mèl sert de base à l'émission de la justification de paiement. Son indisponibilité rend impossible l'envoi de la confirmation.
	Intégrité	1	Le besoin au niveau de l'intégrité est moyen dans la mesure où l'adresse mèl permet uniquement de délivrer le justificatif de paiement au contrevenant. Une perte d'intégrité a des conséquences limitées (envoi de confirmation à une adresse erronée par exemple)
I.Confirmation	Confidentialité	1	Les informations contenues dans le mèl de confirmation présentent un besoin assez faible au niveau de la confidentialité.
	Disponibilité	2	Le besoin en disponibilité est identique à celui que présente la fonction "F.NOTIFICATION". Si l'indisponibilité est supérieure à quelques heures l'administration peut être exposée à d'éventuelles plaintes.
	Intégrité	2	Le besoin en intégrité est important puisque la validité du justificatif de paiement dépend en premier lieu de son intégrité. L'élément supporte des informations (date, heure, références bancaires) utilisées en cas de litige pour démontrer la bonne foi de l'utilisateur
I.InfoPaiement	Confidentialité	3	Le besoin en confidentialité est très élevé. La divulgation des informations bancaires des usagers peut avoir de graves répercussions financières ou d'image de marque
	Disponibilité	2	Une indisponibilité de quelques heures n'est pas trop préjudiciable dans la mesure où l'utilisateur dispose d'un délai important pour s'acquitter de sa contravention.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	19/58

	Intégrité	2	Une perte d'intégrité au niveau des informations bancaires des usagers est grave. Elle empêche l'administration d'émettre une transaction valide.
I.MajDossier	Confidentialité	0	Aucun besoin en confidentialité au niveau de cette information.
	Disponibilité	1	Cet élément essentiel est étroitement lié à la fonction "F.DEBIT"(répercussion de la transaction au niveau de l'état du dossier), elle présente donc le même besoin de sécurité au niveau de la disponibilité.
	Intégrité	3	Le besoin en intégrité est important. En cas de problème détecté, cette information peut cependant être retrouvée afin de mettre à jour l'état de l'ordre de paiement
I.NumAvis	Confidentialité	2	Une perte de confidentialité est grave et touche la vie privée des usagers. Cette information permet d'identifier les personnes sanctionnées en accédant à leur ordre de paiement.
	Disponibilité	1	Le besoin en disponibilité est faible car l'utilisateur dispose de quarante cinq jours pour régler sa contravention.
	Intégrité	1	Le besoin en intégrité est faible. L'utilisateur peut disposer à nouveau de son numéro d'avis de contravention en contactant l'administration.
I.OrdrePaiement	Confidentialité	2	Une perte de confidentialité est grave mais ne touche que la vie privée des usagers. L'ordre de paiement contient des données nominatives.
	Disponibilité	2	Une indisponibilité de quelques heures est acceptable car l'utilisateur dispose de quarante cinq jours pour régler sa contravention.
	Intégrité	2	Une perte d'intégrité au niveau de l'ordre de paiement est grave car il contient le montant de la contravention. Par suite, cela peut donc

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	20/58

			conduire à une perte financière pour l'utilisateur ou à l'instruction d'une contestation.
I.Profil	Confidentialité	2	Le besoin en confidentialité au niveau du profil est important car il définit l'identité et les autorisations associées aux usagers.
	Disponibilité	1	Les besoins en disponibilité sont faibles puisque l'utilisateur possède un laps de temps important pour régler sa contravention.
	Intégrité	2	Le besoin en intégrité est important car cet élément essentiel fixe les droits d'accès aux fonctions et aux données.
I.Requete	Confidentialité	3	Le besoin en confidentialité est très important car ces données transmises en interne contiennent des informations financières sensibles.
	Disponibilité	1	Le besoin en disponibilité est faible car la transaction peut être retardée sans induire un échec du règlement de la contravention.
	Intégrité	2	Une perte d'intégrité est grave car elle peut provoquer une perte financière pour l'utilisateur.
I.Transaction	Confidentialité	3	Le besoin en confidentialité est très élevé au niveau de la transaction financière.
	Disponibilité	1	Le besoin en disponibilité de cet élément essentiel est directement lié à celui de la fonction « F.DEBIT »
	Intégrité	3	Le besoin en intégrité au niveau de la transaction est très élevé.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	21/58

### 3 Les risques

Un premier paragraphe présente une hiérarchisation des risques, qui sont décrits de manière exhaustive par la suite.

#### 3.1 Hiérarchisation des risques

	Critère de sécurité	Opportunité
R.RENIEMENT-PREUVE (USAGER)	3	4
R.RENIEMENT-PREUVE (ADMINISTRATION)	3	4
R.USURPATION-IDENTITE	3	4
R.DIVULGATION-CHIFFREMENT	3	4
R.DYSFONCTIONNEMENT-LOGICIEL	3	4
R.LOGICIEL-CODE	3	4
R.LOGICIEL-FONCTION	3	4
R.ORIGINE-CONFIRMATION (USAGER)	3	4
R.PANNE-COHERENCE	3	4
R.RENIEMENT-TRACABILITE	3	3
R.ABUS-AUTORISATION	3	3
R.CRYPTO-SECRET	3	3
R.ABUS-IDENTIFICATION (USAGER)	3	2
R.CRYPTO-ALGO	3	2
R.ABUS-IDENTIFICATION (SYSTEME BANCAIRE)	3	2
R.ALTERATION-MODIFICATION (SYSTEME BANCAIRE)	3	1

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	22/58

R.ALTERATION-REJEU (USAGER)	3	1
R.ABUS-DEBORDEMENT	3	1
R.ECOUTE-LS	3	1
R.ECOUTE-USAGER	3	1
R.ALTERATION-MODIFICATION (USAGER)	3	1
R.ALTERATION-REJEU (SYSTEME BANCAIRE)	3	1
R.ORIGINE-CONFIRMATION (SYSTEME BANCAIRE)	3	1
R.ABUS-INJECTION	3	1
R.ALTERATION-FORGEMENT (SYSTEME BANCAIRE)	3	1
R.ALTERATION-FORGEMENT (USAGER)	3	1
R.SATURATION-RESSOURCES	2	2
R.PERTE-INTERNET	2	1
R.PERTE-LS	2	1

Suivant la nature de la déclaration dématérialisée, R.Origine-accuse et R.Action-reniement peuvent remonter dans la hiérarchisation des risques.

## 3.2 Description des risques

Le tableau suivant détaille les risques identifiés lors de l'analyse.

### R.ABUS-AUTORISATION

Libellé R.ABUS-AUTORISATION

Méthode d'attaque 39 - ABUS DE DROIT

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	23/58

## Description

Après identification, l'utilisateur est accrédité d'autorisations qui lui donne accès au contenu et à certaines fonctions de l'application. Le contrôle des autorisations, aussi appelé contrôle d'accès, est un dispositif généralement difficile à mettre en oeuvre de manière efficace. Il est généralement mis en place au niveau de :

- L'url
- Des pages consultées
- Des fonctions accessibles
- De la base de données

La complexité du dispositif, la multiplication des profils et la présence de fonction d'administration à distance sont autant de paramètres qui complexifient la tâche. Ainsi, un usager malintentionné peut exploiter le fait que l'application supporte tout un ensemble de profils, en identifiant et forgeant une requête vers une ressource dont le schéma de contrôle d'accès est défectueux. Il peut alors accéder à des informations personnelles.

Ce risque touche les critères de confidentialité, d'intégrité et de disponibilité des éléments essentiels.

Pour la confidentialité, les éléments essentiels très fortement touchés sont les informations « I.Requete », « I.Transaction », « I.Acquittement », « I.InfoPaiement » qui contiennent des données fiscales. D'autre part, les informations « I.NumAvis », « I.OrdrePaiement », « I.Profil » sont touchées de manière légèrement moins importante.

Au niveau de la disponibilité, il s'agit des fonctions « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE » ainsi que les informations « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement ».

Concernant l'intégrité, les fonctions « F.CONSERVATION », « F.DEBIT », « F.ECRITURE » et les informations « I.Acquittement », « I.MajDossier », « I.transaction » sont très touchées car elles présentent toutes des besoins de sécurité très importants. Les fonctions « F.NOTIFICATION », « F.LECTURE » et les informations « I.Confirmation », « I.Profil », « I.Requete », « I.InfoPaiement », « I.OrdePaiement » sont touchées de manière légèrement moins importante.

Ce risque peut provoquer :

- Une atteinte à la vie privée
- Des frais financiers de secours et de remise à niveau

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	24/58

	<ul style="list-style-type: none"> <li>• Une interruption de service</li> <li>• Une perturbation du fonctionnement interne</li> </ul>
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

## R.ABUS-DEBORDEMENT

Libellé R.ABUS-DEBORDEMENT

Méthode d'attaque 39 - ABUS DE DROIT

Description

Cette menace consiste à provoquer un dysfonctionnement au niveau de l'application Web pour lui faire exécuter des opérations non conformes avec des privilèges avancés. Suivant le type de langage utilisé, les applications sont plus ou moins exposées à ce type de menace.

Une personne malintentionnée soumet une requête qui provoque un débordement de tampon au niveau du système d'exploitation lors du passage d'un paramètre à un script. Elle lui permet de gagner des privilèges administratifs et de prendre le contrôle de la machine.

Comme tous les risques issus de la méthode d'attaque "ABUS DE DROITS", les critères de sécurité touchés sont la confidentialité, l'intégrité et la disponibilité.

Au niveau de la confidentialité, les éléments essentiels très fortement touchés sont les informations « I.Requete », « I.Transaction », « I.InfoPaiement », « I.Acquittement » qui contiennent des données personnelles. Les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » sont impactées dans une moindre mesure.

Pour la disponibilité, il s'agit des fonctions « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE » et des informations « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement ».

Concernant l'intégrité, les fonctions « F.CONSERVATION », « F.DEBIT », « F.ECRITURE » et les informations « I.Acquittement », « I.MajDossier », « I.transaction » sont très touchées car elles présentent toutes des besoins de sécurité très importants. Les fonctions « F.NOTIFICATION », « F.LECTURE » et les informations « I.Confirmation », « I.Profil », « I.Requete », « I.InfoPaiement »,

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	25/58

« I.OrdePaiement » sont touchées de manière moins importante.

Ce risque peut avoir pour conséquence :

- Une atteinte à la vie privée
- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perte d'image de marque
- Une perturbation du fonctionnement interne

Opportunité

Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ABUS-IDENTIFICATION (SYSTEME BANCAIRE)

Libellé R.ABUS-IDENTIFICATION (SYSTEME BANCAIRE)

Méthode d'attaque 39 - ABUS DE DROIT

Description La réalisation des transactions entre l'administration et le sous système bancaire nécessite l'identification des deux parties impliquées.

Une personne malintentionnée profite de la faiblesse des dispositifs mis en place pour usurper l'identité de l'une des deux parties. Elle peut ainsi prendre connaissance d'informations confidentielles ou émettre des transactions frauduleuses sous couvert de l'identité de l'administration.

Au vu du scénario retenu, seules la confidentialité et l'intégrité des informations échangées entre l'administration et le sous système bancaire peuvent être affectées.

Concernant la confidentialité, il s'agit de l'information "I.Transaction" et « I.Acquittement » dont les besoins de sécurité sont très importants.

Pour l'intégrité, ces informations peuvent aussi être fortement impactées.

Cela peut entraîner :

- Une infraction aux lois, aux règlements
- Des pertes financières pour l'usager et l'administration

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	26/58

Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique
-------------	--

## R.ABUS-IDENTIFICATION (USAGER)

Libellé R.ABUS-IDENTIFICATION (USAGER)

Méthode d'attaque 39 - ABUS DE DROIT

Description Lors de la réalisation d'une transaction, il est essentiel de passer par une phase d'identification de chacune des parties impliquées. Ainsi, pour la transaction entre l'usager et la téléprocédure, il est en principe nécessaire d'identifier :

- Le système auquel l'usager est connecté
- L'utilisateur

Le protocole HTTPS est généralement utilisé pour identifier la composante serveur. Cependant, il n'apporte aucune garantie en matière d'identification de l'usager. Dans la téléprocédure analysée, c'est le numéro inscrit sur l'avis de contravention qui permet d'identifier l'utilisateur. Une personne malintentionnée, douée de très bonnes connaissances techniques, peut compromettre ce numéro (Force Brute) afin d'accéder à l'ordre de paiement de l'usager.

D'autre part, le protocole HTTP étant sans état, il est nécessaire de mettre en place un dispositif permettant d'assurer l'identification de l'usager entre chaque requête. Ce dispositif repose généralement sur un identifiant de session ou de transaction stocké dans un cookie. Une personne malintentionnée peut compromettre ce jeton de session afin d'accéder aux informations d'autres usagers.

Au vu du scénario retenu, seules la confidentialité et l'intégrité des informations échangées entre l'usager et l'administration peuvent être affectées.

Pour la confidentialité, l'information « I.InfoPaiement » qui présente un besoin de sécurité important au niveau de ce critère de sécurité peut être très fortement touchée. Les informations « I.NumAvis », « I.OrdrePaiement », « I.Profil » sont touchées de manière moindre

Concernant l'intégrité, les informations « I.InfoPaiement »,

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	27/58

	<p>« I.OrdrePaiement » peuvent être fortement impactées.</p> <p>Les impacts envisageables consistent en :</p> <ul style="list-style-type: none"> <li>• Une perte d'image de marque</li> <li>• Des pertes financières pour l'usager ou l'administration</li> <li>• Des perturbations du fonctionnement interne</li> </ul>
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

## R.ABUS-INJECTION

Libellé	R.ABUS-INJECTION
Méthode d'attaque	39 - ABUS DE DROIT
Description	<p>La validation des paramètres d'entrée d'une application Web est capitale. En contournant les filtres de validation, il devient possible d'insérer une commande malveillante, d'attaquer des composants secondaires ou d'exécuter des commandes systèmes. Une personne malintentionnée dissimule une requête SQL dans l'un des champs d'un formulaire de saisie et visualise, modifie ou efface la table contenant les informations fiscales des usagers (Ex: SQL injection).</p> <p>Ce risque touche les trois critères de sécurité.</p> <p>Au niveau de la confidentialité, si l'on se réfère au scénario retenu, les éléments essentiels les plus touchés sont les informations « I.Requete », « I.Transaction », « I.Acquittement » « I.InfoPaiement » avec un niveau très élevé. D'autre part, les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » sont touchées de manière légèrement moins importante.</p> <p>Pour la disponibilité, ce risque porte très fortement atteinte aux fonctions « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE » ainsi qu'aux informations « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement ».</p> <p>Concernant l'intégrité, les fonctions « F.CONSERVATION », « F.DEBIT », « F.ECRITURE » et les informations « I.Acquittement », « I.MajDossier », « I.transaction » sont très touchées car elles présentent toutes des besoins de sécurité très importants. Les fonctions</p>

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	28/58

« F.NOTIFICATION », « F.LECTURE » et les informations « I.Confirmation », « I.Profil », « I.InfoPaiement », « I.OrdrePaiement », « I.Requête » sont touchées dans une moindre mesure.

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Des frais financiers de secours et de remise à niveau
- Une infraction aux lois, aux règlements
- Une interruption de service
- Une perte d'image de marque
- Des pertes financières pour l'utilisateur et l'administration
- Une perturbation de fonctionnement interne

Opportunité

Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ALTERATION-FORGEMENT (SYSTEME BANCAIRE)

Libellé

R.ALTERATION-FORGEMENT (SYSTEME BANCAIRE)

Méthode d'attaque

36 - ALTÉRATION DES DONNÉES

Description

Une personne malintentionnée, disposant d'un point d'accès à la liaison spécialisée et de connaissances techniques pointues sur le modèle transactionnel employé, utilise des informations bancaires collectées frauduleusement pour forger des transactions et réaliser des virements non autorisés.

Ce risque porte sur l'intégrité de l'information « I.Transaction » qui présente un besoin important au niveau de ce critère de sécurité. Les problèmes touchant la confidentialité de la transaction sont traités par le risque « R.ECOUTE-LS ».

Ce risque entraîne :

- Une infraction aux lois, aux règlements
- Des pertes financières pour l'utilisateur et l'administration

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	29/58

Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré
-------------	--

## R.ALTERATION-FORGEMENT (USAGER)

Libellé	R.ALTERATION-FORGEMENT (USAGER)
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	<p>Un contrevenant forge une transaction en modifiant sa date d'émission afin d'échapper à la majoration de sa contravention. Par vengeance ou motivation personnelle, une personne malintentionnée peut aussi forger un nombre important de transactions afin de saturer la téléprocédure. Dans ce cas précis, ce risque se rapproche de « R.SATURATION-RESSOURCES ».</p> <p>Ce risque porte donc atteinte à l'intégrité de l'information « I.InfoPaiement » qui présente un besoin important au niveau de ce critère de sécurité.</p> <p>Par suite, cela peut induire une perte d'intégrité importante au niveau de l'information « I.OrdrePaiement ».</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Des pertes financières pour l'usager et l'administration</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ALTERATION-MODIFICATION (SYSTEME BANCAIRE)

Libellé	R.ALTERATION-MODIFICATION (SYSTEME BANCAIRE)
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	Cette menace consiste à modifier illicitement les données en transit sur le moyen de communication au niveau de la liaison spécialisée.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	30/58

Par vengeance ou motivation personnelle, une personne malintentionnée disposant d'un point d'accès à la liaison spécialisée modifie les transactions transmises vers le sous système bancaire.

Ce risque porte atteinte à l'intégrité des informations « I.Transaction » et « I.Acquittement » qui présentent un besoin important au niveau de ce critère de sécurité.

Cela peut engendrer :

- Une infraction aux lois, aux règlements
- Des pertes financières pour l'usager et l'administration

Opportunité

Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ALTERATION-MODIFICATION (USAGER)

Libellé

R.ALTERATION-MODIFICATION (USAGER)

Méthode d'attaque

36 - ALTÉRATION DES DONNÉES

Description

Cette menace consiste à modifier illicitement les données en transit sur le moyen de communication entre l'usager et l'administration.

Dans le contexte de la communication de type « Client Serveur » qui s'établit entre l'usager et la téléprocédure, le but d'une attaque de type « Man In The Middle » est de se faire passer pour le client auprès du serveur et inversement. L'attaquant agit comme un relais transparent et peut modifier des paramètres de la transaction (montant, numéro d'ordre de paiement) afin de réaliser une fraude.

D'autre part, l'élément menaçant peut directement être l'usager. Ainsi, profitant du manque de protection des informations sensibles, il modifie le montant de la transaction dissimulé dans un champs caché au niveau d'un formulaire de saisie ou stocké dans un cookie au niveau de son navigateur. Etant donné le volume de transaction traité par l'administration, cette fraude peut passer totalement inaperçue.

Ce risque porte donc atteinte à la confidentialité et à l'intégrité de l'information « I.InfoPaiement » qui présente un besoin important au niveau de ces deux critères de sécurité.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	31/58

	<p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Des pertes financières pour l'usager et l'administration</li> <li>• Une perturbation du fonctionnement interne</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ALTERATION-REJEU (SYSTEME BANCAIRE)

Libellé	R.ALTERATION-REJEU (SYSTEME BANCAIRE)
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	<p>La menace par rejeu consiste à capter une transaction valide (voir « M.ECOUTE-USAGER ») et à la retransmettre sur le réseau afin de répéter l'opération financière.</p> <p>Une personne malintentionnée, disposant d'un point d'accès au niveau de la liaison spécialisée, capture les transactions financières émises puis les rejoue et induit un prélèvement abusif sur le compte des contrevenants. La masse d'informations financières échangée par l'intermédiaire de cette liaison rend l'impact de cette menace très important.</p> <p>Ce risque touche l'intégrité de l'information « I.Transaction » puisqu'il consiste à transmettre des transactions non valides.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte financière pour l'usager</li> <li>• Une perte d'image pour l'Administration</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	32/58

## R.ALTERATION-REJEU (USAGER)

Libellé	R.ALTERATION-REJEU (USAGER)
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	<p>Par vengeance, une personne malintentionnée capture et rejoue des transactions préalablement émises par des usagers. L'état de l'ordre de paiement conditionnant directement le traitement de la transaction, il est probable que le rejeu de la transaction aboutisse au prélèvement répété du compte de l'utilisateur. Cependant, si cette menace est mise en oeuvre à grande échelle, elle peut conduire à la saturation de la téléprocédure.</p> <p>Ce risque touche l'intégrité de l'information « I.InfoPaiement » puisqu'il consiste à transmettre des transactions non valides.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une interruption de service</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.CRYPTO-ALGO

Libellé	R.CRYPTO-ALGO
Méthode d'attaque	23 - DIVULGATION
Description	<p>Profitant d'une faiblesse de l'algorithme cryptographique employé, une personne malintentionnée au fait des techniques de cryptanalyse, déchiffre et porte atteinte à la confidentialité des données échangées ou stockées au niveau de la téléprocédure.</p> <p>Ce risque touche la confidentialité des éléments essentiels. Les informations « I.Requete », « I.Transaction », « I.InfoPaiement », « I.Acquittement » qui contiennent des données fiscales sont très fortement</p>

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	33/58

	<p>affectées. D'autre part, les informations « I.NumAvis », « I.OrdrePaiement », « I.Profil » sont touchées dans une moindre mesure.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une atteinte à la vie privée des usagers</li> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte d'image de marque</li> </ul>
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

**R.CRYPTO-SECRET**

Libellé	R.CRYPTO-SECRET
Méthode d'attaque	23 - DIVULGATION
Description	<p>Profitant de la mauvaise gestion des éléments cryptographiques, une personne malintentionnée accède aux éléments secrets utilisés pour garantir la confidentialité et l'authenticité (signature) des données stockées et échangées.</p> <p>Ce risque touche la confidentialité et l'intégrité des éléments essentiels. Les informations « I.Requete », « I.Transaction », « I.InfoPaiement », « I.Acquittement » sont affectées. Les informations « I.NumAvis », « I.OrdrePaiement », « I.Profil » sont touchées dans une moindre mesure.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une atteinte à la vie privée des usagers</li> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte d'image de marque</li> <li>• Des pertes financières pour l'utilisateur</li> </ul>
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	34/58

## R.DIVULGATION-CHIFFREMENT

Libellé	R.DIVULGATION-CHIFFREMENT
Méthode d'attaque	23 - DIVULGATION
Description	<p>Du fait du manque de classification au niveau de la sensibilité des informations et de l'absence de moyens de chiffrement adaptés, des informations sont divulguées. Cela peut être la conséquence d'un dysfonctionnement, d'une erreur d'administration ou par pure vengeance.</p> <p>Ce risque touche la confidentialité des éléments essentiels. Les informations « I.Requete », « I.Transaction », « I.InfoPaiement », « I.Acquittement » qui contiennent des données personnelles sont affectées. Les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » le sont dans une moindre mesure</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une atteinte à la vie privée des usagers</li> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte d'image de marque</li> </ul>
Opportunité	Certain ou réalisable par tout public

## R.DYSFONCTIONNEMENT-LOGICIEL

Libellé	R.DYSFONCTIONNEMENT-LOGICIEL
Méthode d'attaque	31 - DYSFONCTIONNEMENT LOGICIEL
Description	<p>Suite à un dysfonctionnement logiciel volontaire ou non, l'administration se trouve dans l'impossibilité de garantir la cohérence des dossiers en cours de traitement. Dès lors, il devient impossible de déterminer l'état de l'ordre de paiement de certains usagers.</p> <p>Conformément aux hypothèses retenues, il convient de considérer uniquement le risque correspondant à un dysfonctionnement logiciel. Ce risque touche fortement l'intégrité de l'information « I.OrdrePaiement ».</p>

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	35/58

Il peut engendrer :

- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perte d'image de marque
- Une perte financière
- La perturbation du fonctionnement interne

Opportunité Certain ou réalisable par tout public

## R.ECOUTE-LS

Libellé R.ECOUTE-LS

Méthode d'attaque 19 - ÉCOUTE PASSIVE

Description Profitant d'un défaut de protection sur un des équipements de l'infrastructure d'interconnexion avec le sous système bancaire ou de la faiblesse des moyens cryptographiques employés, une personne malintentionnée, douée d'un niveau de compétence très élevé, capture et déchiffre l'ensemble des transactions émises par le biais de ce canal.

Ce risque touche uniquement la confidentialité des informations qui transitent par la liaison spécialisée. Seules les informations « I.Transaction » et « I.Acquittement » sont très fortement affectées par ce risque.

Il peut engendrer :

- Une infraction aux lois, aux règlements
- Une perte d'image de marque
- Des pertes financières pour l'utilisateur

Opportunité Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	36/58

## R.ECOUTE-USAGER

Libellé	R.ECOUTE-USAGER
Méthode d'attaque	19 - ÉCOUTE PASSIVE
Description	<p>Profitant de la faible protection des équipements de communication ou de la faiblesse des moyens cryptographiques employés, une personne malintentionnée, douée d'un niveau de compétence élevé en cryptographie, capture et déchiffre les flux de données échangés entre l'utilisateur et la téléprocédure.</p> <p>Ce risque touche uniquement la confidentialité des informations qui transitent entre l'utilisateur et l'administration. L'information « I.InfoPaiement » est très fortement affectée. Les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » sont touchées dans une moindre mesure.</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une atteinte à la vie privée des usagers</li> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte d'image de marque</li> <li>• Des pertes financières pour l'utilisateur</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.LOGICIEL-CODE

Libellé	R.LOGICIEL-CODE
Méthode d'attaque	26 - PIÉGEAGE DU LOGICIEL
Description	L'application web peut être utilisée comme un vecteur d'attaque. L'idée consiste à insérer frauduleusement des informations au sein d'une page Web. Dès lors, celles-ci seront exécutées de manière transparente au niveau du navigateur des clients qui se connectent.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	37/58

Une personne malveillante profite du manque de validation au niveau des entrées et sorties de l'application pour insérer un script au niveau d'une page Web de la téléprocédure. Ce dernier lui permet de dérober les cookies des utilisateurs et de prendre connaissance de leur ID de session. A partir de cette information, l'attaquant est alors en mesure de prendre connaissance des informations bancaires de l'utilisateur.

D'autres variantes de cette attaque permettent de détourner frauduleusement les communications vers un site similaire à l'original. Dès lors, la personne malintentionnée invite l'utilisateur à saisir ses coordonnées bancaires.

Suivant la nature du script exécuté, ce risque peut toucher les trois critères de sécurité.

Les informations « I.Requete », « I.Transaction », « I.Acquittement », « I.InfoPaiement » sont très fortement touchées au niveau de la confidentialité. Les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » sont affectées dans une moindre mesure.

Pour la disponibilité, les éléments essentiels « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE », « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement » présentent des besoins importants et sont susceptibles d'être impactés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des éléments essentiels « F.CONSERVATION », « F.DEBIT », « F.ECRITURE », « I.Acquittement », « I.MajDossier », « I.Transaction » qui présentent un besoin élevé en intégrité. Les fonctions « F.NOTIFICATION », « F.LECTURE » et les informations « I.Confirmation », « I.Profil », « I.OrdrePaiement », « I.Requete », « I.InfoPaiement » sont touchées de manière moindre.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque
- Des pertes financières pour l'utilisateur et l'administration

Opportunité Certain ou réalisable par tout public

## R.LOGICIEL-FONCTION

Libellé R.LOGICIEL-CONCEPTION

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	38/58

## Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

## Description

Une personne malintentionnée outrepassa, volontairement ou non, le fonctionnement normal de la téléprocédure en contournant des règles élémentaires de sécurité, en utilisant des fonctionnalités cachées introduites durant la phase de conception de l'application ou en exploitant d'éventuelles erreurs de conception.

Ce risque touche les trois critères de sécurité.

Au niveau de la confidentialité, les informations « I.Requete », « I.Transaction », « I.InfoPaiement », « I.Acquittement » sont très fortement touchées. Les informations « I.NumAVis », « I.OrdrePaiement », « I.Profil » le sont dans une moindre mesure.

Pour la disponibilité, les éléments essentiels « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE », « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement » possèdent des besoins importants susceptibles d'être très fortement affectés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des éléments essentiels « F.CONSERVATION », « F.DEBIT », « F.ECRITURE », « I.Acquittement », « I.MajDossier », « I.Transaction » qui présentent un besoin élevé en intégrité. Les fonctions « F.NOTIFICATION », « F.LECTURE » et les informations « I.Confirmation », « I.Profil », « I.OrdePaiement », « I.Requete », « I.InfoPaiement » sont touchées de manière moindre.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque
- Une perte financière pour l'utilisateur ou l'administration
- Une perturbation du fonctionnement interne

## Opportunité

Certain ou réalisable par tout public

## R.ORIGINE-CONFIRMATION (SYSTEME BANCAIRE)

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	39/58

Libellé	R.ORIGINE-CONFIRMATION (SYSTEME BANCAIRE)
Méthode d'attaque	24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE
Description	<p>Afin de perturber le fonctionnement de la téléprocédure, une personne malintentionnée envoie une série d'acquittement en lieu et place du sous système bancaire.</p> <p>Ce risque porte atteinte à l'intégrité de l'information « I.Acquittement » qui présente un besoin d'intégrité important. En retour, l'intégrité de l'information « I.OrdrePaiement » peut être affectée.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte financière pour l'administration</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.ORIGINE-CONFIRMATION (USAGER)

Libellé	R.ORIGINE-CONFIRMATION (USAGER)
Méthode d'attaque	24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE
Description	<p>Une personne malintentionnée émet de fausses notifications et redirige les utilisateurs vers son propre système. Dès lors, profitant de la similitude de son site avec l'original, il invite les usagers à ressaisir leurs informations bancaires afin de réaliser une fraude.</p> <p>Ce risque porte atteinte à l'intégrité de l'information « I.Confirmation » qui présente un besoin important. En retour, il peut s'en suivre une perte de confidentialité des informations bancaires de l'utilisateur.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte financière pour l'utilisateur</li> </ul>
Opportunité	Certain ou réalisable par tout public

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	40/58

## R.PANNE-COHERENCE

Libellé	R.PANNE-COHERENCE
Méthode d'attaque	28 - PANNE MATÉRIELLE
Description	<p>Suite à la panne de l'un des équipements matériels, une perte de cohérence au niveau des ordres de paiement des utilisateurs se produit. Ainsi, sur la base de l'état des ordres de paiement, une série de transactions acquittées mais en attente de mise à jour au niveau de la partie conservation de données est réémise alors que les comptes des contrevenants ont déjà été prélevés. Conformément aux hypothèses émises, il convient de considérer uniquement la perte d'intégrité induite par un dysfonctionnement matériel.</p> <p>Ce risque touche fortement l'information « I.OrdrePaiement » qui présente un besoin en intégrité important.</p> <p>Il peut engendrer :</p> <ul style="list-style-type: none"> <li>• Des frais financiers de secours et de remise à niveau</li> <li>• Interruption de service</li> <li>• Une perte d'image de marque</li> <li>• Une perte financière</li> <li>• La perturbation du fonctionnement interne</li> </ul>
Opportunité	Certain ou réalisable par tout public

## R.PERTE-INTERNET

Libellé	R.PERTE-INTERNET
Méthode d'attaque	13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION
Description	Par vengeance ou motivation personnelle, une personne malintentionnée possédant des connaissances techniques approfondies, interdit la connexion à la téléprocédure en rendant indisponible un équipement de communication qui présente un défaut de protection.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	41/58

L'impossibilité de basculer rapidement vers une ligne de secours aggrave la situation.

Ce risque touche la disponibilité des informations transmises par le canal de communication établi entre l'utilisateur et l'administration.

Les informations « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement » sont touchées car elles présentent des besoins élevés au niveau de la disponibilité.

Cela peut engendrer :

- Une infraction aux lois, aux règlements
- Une interruption de service
- Une perte d'image de marque

Opportunité

Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.PERTE-LS

Libellé

R.PERTE-LS

Méthode d'attaque

13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

Description

Profitant du manque de protection d'un équipement de l'infrastructure de communication, une personne malintentionnée, possédant des connaissances techniques approfondies, rend indisponible la liaison entre l'administration et le sous système bancaire. L'émission des transactions financières et le traitement des ordres de paiement deviennent dès lors impossibles.

L'impossibilité de basculer rapidement vers une ligne de secours aggrave la situation.

Ce risque touche la disponibilité des informations transmises par la liaison spécialisée. L'information « I.Acquittement » est fortement touchée puisqu'elle présente un besoin élevé au niveau de la disponibilité. L'information « I.Transaction » est touchée avec un niveau plus faible.

Cela peut engendrer :

- Une interruption de service

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	42/58

	<ul style="list-style-type: none"> <li>• Une perte financière pour l'administration</li> </ul>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

## R.RENIEMENT-PREUVE (ADMINISTRATION)

Libellé	R.RENIEMENT-PREUVE (ADMINISTRATION)
Méthode d'attaque	41 - RENIEMENT D' ACTIONS
Description	<p>Pour toutes transactions financières réalisées, l'administration doit être en mesure de justifier de la validité et de la conformité de la transaction.</p> <p>La faiblesse du dispositif de gestion des acquittements ou la mauvaise gestion des éléments de preuve expose l'administration à de nombreuses contestations.</p> <p>Ce risque touche avec un niveau très élevé l'intégrité de l'information « I.Acquittement ».</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une perte d'image de marque</li> </ul>
Opportunité	Certain ou réalisable par tout public

## R.RENIEMENT-PREUVE (USAGER)

Libellé	R.RENIEMENT-PREUVE (USAGER)
Méthode d'attaque	41 - RENIEMENT D' ACTIONS
Description	<p>Conformément aux exigences réglementaires, l'utilisateur doit disposer d'un élément de preuve permettant de justifier de la réalisation de la transaction en cas de contestation.</p> <p>Une personne malintentionnée peut falsifier une confirmation et prétendre</p>

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	43/58

à tort avoir réalisé le paiement de son amende. Etant donné la faiblesse du dispositif permettant de garantir la non-répudiation des échanges, l'administration peut se trouver dans l'impossibilité de déceler la fraude.

Ce risque touche avec un niveau très élevé l'intégrité de l'information « I.Confirmation ».

Cela peut engendrer :

- Une infraction aux lois, aux règlements
- Une perte financière
- Une perte d'image de marque

Opportunité Certain ou réalisable par tout public

## R.RENIEMENT-TRACABILITE

Libellé R.RENIEMENT-TRACABILITE

Méthode d'attaque 41 - RENIEMENT D'ACTION

Description L'administration se trouve dans l'impossibilité d'imputer et de tracer les événements essentiels de la téléprocédure suite à la réalisation d'une fraude. Ce risque porte atteinte à l'intégrité des éléments essentiels, et peut impacter toutes les fonctions et informations traitées par la téléprocédure.

Il peut engendrer :

- Une infraction aux lois, aux règlements
- Une perte financière pour l'administration

Opportunité Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

## R.SATURATION-RESSOURCES

Libellé R.SATURATION-RESSOURCES

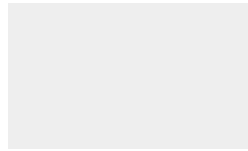
FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	44/58

Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Une attaque courante consiste à soumettre le dispositif à un nombre important de requêtes afin d'empêcher des utilisateurs légitimes de se connecter.</p> <p>Dans le cas présent, une personne malintentionnée, possédant un niveau de compétence élevé, s'attaque aux services réseaux (Ex: Syn Flooding) ou directement à l'application Web (Ex: Rejeu de transactions) afin de paralyser la téléprocédure.</p> <p>Ce risque touche uniquement la disponibilité des éléments essentiels « F.CONSERVATION », « F.ECRITURE », « F.IDENTIFICATION », « F.LECTURE », « I.Acquittement », « I.Confirmation », « I.InfoPaiement », « I.OrdrePaiement » qui présentent un fort besoin au niveau de ce critère de sécurité.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> <li>• Une interruption de service</li> <li>• Une perte d'image de marque</li> </ul>
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

## R.USURPATION-IDENTITE

Libellé	R.USURPATION-IDENTITE
Méthode d'attaque	40 - USURPATION DE DROIT
Description	<p>Par opportunité, une personne malintentionnée accède à une session laissée ouverte et visualise ou modifie les informations bancaires d'un usager.</p> <p>Etant donné le scénario de menace, ce risque porte principalement atteinte à l'intégrité et à la confidentialité des informations fiscales « I.InfoPaiement ».</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Une infraction aux lois, aux règlements</li> </ul>

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	45/58



- Une perte financière pour l'utilisateur
- Une atteinte à la vie privée

Opportunité

Certain ou réalisable par tout public

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	46/58

## 4 Objectifs de sécurité

### O.ALGORITHME-CRYPTO

Contenu Des mesures doivent être prises afin de garantir la résistance des algorithmes cryptographiques.

### O.ACQUITTEMENT (SYSTEME BANCAIRE)

Contenu Des mesures doivent être prises afin de garantir l'intégrité et l'authentification des acquittements émanant du sous système bancaire.

### O.AUTORISATION

Contenu Des mesures techniques doivent être prises pour garantir que l'utilisateur accède uniquement aux fonctions et informations qui lui sont nécessaires.

### O.CHIFFREMENT

Contenu Des mesures cryptographiques adaptées à la sensibilité des informations doivent être prises pour garantir la confidentialité et l'intégrité des informations sur les supports.

### O.CODE-MALVEILLANT

Contenu Des mesures doivent être prises afin de s'assurer qu'il n'est pas possible de diffuser des codes malveillants grâce à la téléprocédure (validation des entrées/sorties).

### O.CONCEPTION

Contenu Des mesures doivent être prises afin de s'assurer de la conformité de la conception et du fonctionnement de la téléprocédure.

### O.CONFIDENTIALITE-LS

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	47/58

Contenu Des mesures doivent être prises afin de garantir la confidentialité des transactions transmises par l'intermédiaire de la liaison spécialisée.

#### O.CONFIDENTIALITE-USAGER

Contenu Des mesures doivent être prises afin de garantir la confidentialité des transactions transmises entre l'utilisateur et l'administration.

#### O.CONFIRMATION (USAGER)

Contenu Des mesures doivent être prises afin de garantir l'intégrité et l'authentification des confirmations envoyées aux usagers. Des éléments relatifs à l'heure de transmission peuvent être nécessaires.

#### O.DEBORDEMENT

Contenu Des mesures doivent être prises afin d'éviter les attaques de type "débordement de tampon".

#### O.DYSFONCTIONNEMENT-COHERENCE

Contenu Des mesures techniques doivent être prises afin de garantir l'atomicité des transactions et la cohérence de l'état des ordres de paiement suite à un dysfonctionnement logiciel.

#### O.FORGEMENT (SYSTEME BANCAIRE)

Contenu Des mesures techniques doivent être prises afin de garantir la légitimité des transactions émises entre l'administration et le sous système bancaire.

#### O.IDENTIFICATION (SYSTEME BANCAIRE)

Contenu Les entités doivent être dûment identifiées lors des échanges entre l'administration et le sous système bancaire.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	48/58

**O.FORGEMENT (USAGER)**

Contenu Des mesures techniques doivent être prises afin de garantir la légitimité des transactions émises entre l'utilisateur et l'administration.

**O.IDENTIFICATION (USAGER)**

Contenu Les entités participant à une transaction doivent être dûment identifiées lors des échanges entre l'utilisateur et l'administration.

**O.INJECTION**

Contenu Des mesures doivent être prises pour empêcher l'application de véhiculer des commandes malveillantes vers des composants secondaires.

**O.LS**

Contenu Les dysfonctionnements au niveau de la liaison spécialisée ne doivent pas entraver le fonctionnement de la téléprocédure.

**O.PANNE-COHERENCE**

Contenu Des mesures techniques doivent être prises afin de garantir l'atomicité des transactions et la cohérence de l'état des ordres de paiement suite à une panne matérielle.

**O.PREUVE (ADMINISTRATION)**

Contenu L'administration doit disposer et conserver les éléments de preuve permettant de justifier de la conformité des transactions financières réalisées. Ces éléments de preuve doivent comporter un indicateur de l'heure de transaction.

**O.PREUVE (USAGER)**

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	49/58

Contenu L'utilisateur doit disposer d'un élément de preuve permettant de justifier de la conformité et de la validité de la transaction réalisée. Cet élément de preuve doit comporter un indicateur de l'heure de transaction.

## O.PROTECTION-SECRET

Contenu Des mesures doivent être prises afin d'assurer la confidentialité des secrets cryptographiques.

## O.REJEU (SYSTEME BANCAIRE)

Contenu Des mesures techniques doivent être prises afin de garantir l'unicité des transactions transmises entre l'administration et le sous système bancaire.

## O.REJEU (USAGER)

Contenu Des mesures techniques doivent être prises afin de garantir l'unicité des transactions transmises entre l'utilisateur et l'administration.

## O.RESSOURCES

Contenu Des mesures doivent être prises afin d'empêcher les personnes de consommer volontairement des ressources.

## O.SESSION

Contenu Des mesures doivent être prises pour éviter qu'un utilisateur accède à une session laissée ouverte.

## O.TELECOM

Contenu Les dysfonctionnements des moyens de télécommunication entre l'utilisateur et l'administration ne doivent pas entraver la disponibilité de la téléprocédure.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	50/58

**O.TRACABILITE**

Contenu L'administration doit être en mesure de tracer tous les événements essentiels.

**O.TRANSACTION-MODIFICATION (USAGER)**

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des transactions transmises entre l'utilisateur et l'administration.

**O.TRANSACTION-MODIFICATION (SYSTEME BANCAIRE)**

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des transactions transmises entre l'administration et le sous système bancaire.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	51/58

## 5 Les risques résiduels

### 5.1 Méthodes d'attaque non retenues

#### 01- INCENDIE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

#### 02- DÉGÂTS DES EAUX

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

#### 03 - POLLUTION

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

#### 04 - SINISTRE MAJEUR

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

#### 05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

#### 06 - PHÉNOMÈNE CLIMATIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	52/58

## 07 - PHÉNOMÈNE SISMIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

## 08 - PHÉNOMÈNE VOLCANIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

## 09 - PHÉNOMÈNE MÉTÉOROLOGIQUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

## 10 - CRUE

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

## 11 - DÉFAILLANCE DE LA CLIMATISATION

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

## 12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

## 14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	53/58

## 15 - RAYONNEMENTS THERMIQUES

Justification Les méthodes d'attaques d'ordre naturel ont été initialement écartées dans le cadre de cette analyse.

## 16 - IMPULSIONS ÉLECTROMAGNÉTIQUES

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

## 17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS

Justification Méthode d'attaque jugée trop improbable.

## 18 - ESPIONNAGE A DISTANCE

Justification Conformément aux hypothèses émises, la sécurité physique et environnementale au niveau du poste de l'utilisateur est garantie.

## 20 - VOL DE SUPPORTS OU DE DOCUMENTS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

## 21 - VOL DE MATÉRIELS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux sont écartées.

## 22 - RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique et organisationnel sont écartées.

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	54/58

## 25 - PIÉGEAGE DU MATÉRIEL

Justification Conformément aux hypothèses émises, les méthodes d'attaques touchant la sécurité physique des locaux et équipement sont écartées.

## 27 - GÉOLOCALISATION

Justification Méthode d'attaque inadaptée dans le cadre de cette téléprocédure.

## 29 - DYSFONCTIONNEMENT DU MATÉRIEL

Justification Ecartée au profit de la méthode d'attaque "Panne Matérielle".

## 32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

## 33 - UTILISATION ILLICITE DES MATÉRIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

## 34 - COPIE FRAUDULEUSE DE LOGICIELS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

## 35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

Justification Méthode d'attaque écartée initialement dans le cadre de cette analyse.

## 37 - TRAITEMENT ILLICITE DES DONNÉES

Justification Conformément aux hypothèses émises, cette méthode d'attaque est écartée

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	55/58

dans le cadre de cette analyse.

### 38 - ERREUR D'UTILISATION

Justification Conformément aux hypothèses émises, cette méthode d'attaque est écartée.

### 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

Justification Conformément aux hypothèses émises, cette méthode d'attaque est écartée dans le cadre de cette analyse.

## 5.2 Tableau de couverture des risques par les objectifs

	O.ALGORITHME-CRYPTO	O.ACQUISITION (SYSTEME BANCAIRE)	O.AUTORISATION	O.CHIFFREMENT	O.CODE-MALVEILLANT	O.CONCEPTION	O.CONFIDENTIALITE-LS	O.CONFIDENTIALITE-USAGER	O.CONFIRMATION (USAGER)	O.DEBORDEMENT	O.DYSFONCTIONNEMENT-COHERENCE	O.FORGEMENT (SYSTEME BANCAIRE)	O.IDENTIFICATION (SYSTEME BANCAIRE)	O.FORGEMENT (USAGER)	O.IDENTIFICATION (USAGER)	O.INJECTION	O.LS	O.PANNE-COHERENCE	O.PREUVE (ADMINISTRATION)	O.PREUVE (USAGER)	O.PROTECTION-SECRET	O.REJEU (SYSTEME BANCAIRE)	O.REJEU (USAGER)	O.RESSOURCES	O.SESSION	O.TELECOM	O.TRACABILITE
R.ABUS-AUTORISATION			X																								
R.ABUS-DEBORDEMENT									X																		
R.ABUS-IDENTIFICATION (SYSTEME BANCAIRE)												X															
R.ABUS-IDENTIFICATION (USAGER)														X													
R.ABUS-INJECTION															X												
R.ALTERATION-FORGEMENT												X															

FEROS Types		Paiement		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.6.1	V1.0	13/04/2006	Public	56/58



