



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



PREMIER MINISTRE  
SGDN - DCSSI

=====

**FEROS Types**

**Téléprocédure de référence**

**Demande**

=====

**VERSION 1.0**

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	1/47

<b>FEROS Types</b>	
<b>Demande</b>	
<b>Référence</b>	<b>Date</b>
FEROS Type_DemandeV1.0.doc	13/04/2006
<b>Identification d'objet (OID)</b>	<b>Racine OID et gestionnaire</b>
1.2.250.1.137.2.2.1.2.3.4.1	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>	47

<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>Demande</b>		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	2/47

**SOMMAIRE**

**1 INTRODUCTION ..... 4**

1.1 CONTEXTE GENERAL ..... 4

1.2 DEFINITION DES RESPONSABILITES ..... 5

**2 DESCRIPTION DU SYSTEME ETUDIE ..... 6**

2.1 PRESENTATION DU SYSTEME-CIBLE ..... 7

2.2 DESCRIPTION DES ELEMENTS ESSENTIELS ..... 7

2.3 ENJEUX ..... 14

2.4 HYPOTHESES ..... 15

2.5 ECHELLE DE BESOINS ..... 16

2.6 BESOINS DE SECURITE DES ELEMENTS ESSENTIELS ..... 16

**3 LES RISQUES ..... 22**

3.1 HIERARCHISATION DES RISQUES ..... 22

3.2 DESCRIPTION DES RISQUES ..... 23

**4 OBJECTIFS DE SECURITE ..... 39**

**5 LES RISQUES RESIDUELS ..... 42**

5.1 METHODES D'ATTAQUE NON RETENUES ..... 42

5.2 TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS ..... 46

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	3/47

# 1 Introduction

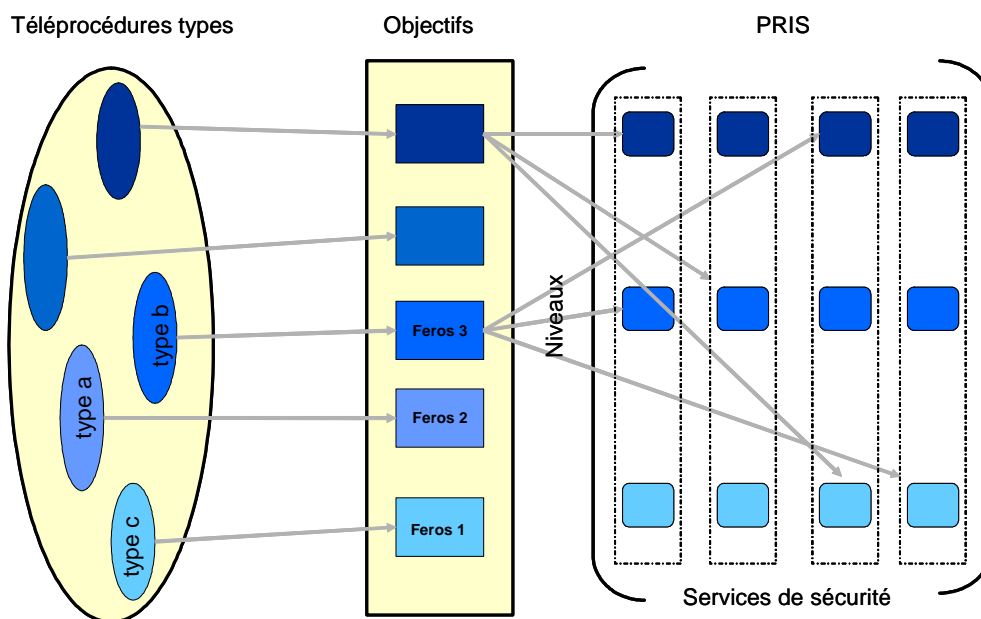
## 1.1 Contexte général

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		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	4/47

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 démarche en ligne : demandes.

## 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. L'étude a été menée dans le contexte de la téléprocédure de demande de subvention, sous Maîtrise d'Ouvrage ADAE. Monsieur Vrignaud, maître d'ouvrage, a bien voulu nous aider à préciser le système étudié et les besoins de sécurité.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	5/47

## 2 Description du système étudié

La téléprocédure étudiée vise à faciliter la relation entre usagers et Administration en offrant aux internautes la possibilité d'effectuer des demandes aux Services Publics par Internet. Ces téléprocédures permettent de dématérialiser la relation entre personnes privées, associations, organisations professionnelles d'une part et Administration d'autre part dans la gestion des demandes : aides, subventions, autorisations, attestations, ... La téléprocédure optimise la relation entre Usagers et Administration, et facilite l'accès et la gestion des demandes par les différents services publics concernés.

### *Exemples de mise en œuvre*

*Demande de subventions en ligne en politique de la Ville*

*Demande de stages courts étudiants*

*Demande d'aide juridictionnelle*

*Demande d'attestation*

*Demande de permis de construire*

*Demande de subvention Internet*

*Demande d'homologation*

*Demande d'état civil*

*Demande de certificats d'immatriculation*

*Demande de bourse*

*Demande d'aide au logement*

*Demande de titre aux entreprises de transport routier*

*Demande de dérogation à l'heure de fermeture*

*Demande d'ouverture le dimanche*

*Demande d'autorisation d'exploitation d'une installation classée*

*Demande de Licence IV temporaire*

*Demande d'occupation temporaire du domaine public*

## Scénario retenu pour l'analyse

### DESCRIPTION

Au titre de la téléprocédure type, on retiendra la demande de subvention émanant d'une association, réalisée par un membre autorisé de l'association (président, secrétaire, trésorier). La procédure est réalisée par le membre de l'association, à partir de ses ressources informatiques personnelles. La téléprocédure permet également une gestion en ligne du dossier, et un suivi par les Usagers et par les Services concernés.

### USAGER

- Particulier, associations

### MODE OPERATOIRE

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	6/47

- Accès depuis les moyens informatiques personnels

## DOMAINE D'APPLICATION

- Associatif

## 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 demande de subvention.

### Systeme-cible

#### Présentation

Le Gouvernement, par l'intermédiaire de l'ADAE (Agence pour le Développement de l'Administration Electronique), souhaite simplifier et améliorer les procédures de demande de subvention auprès des services de l'Etat et des collectivités territoriales. Le lancement du projet SUBV&NET fait suite à l'initiative POLIVILLEWEB et vise à généraliser le mouvement initié en proposant aux porteurs de projet (personnes morales, associations, communes) un guichet unique accessible sur internet.

La téléprocédure facilite la démarche du porteur de projet en proposant un formulaire de demande d'aide commun et le suivi des subventions. Elle vise aussi à simplifier la tâche des financeurs en mettant à leur disposition un portail de publication des subventions existantes, et en les dotant d'un dispositif d'instruction partagé entre les financeurs concernés.

Le porteur de projet renseigne le dossier de demande, et identifie dans un plan de financement l'ensemble des financiers cibles et les demandes de financement formulées auprès de chaque service concerné. Il peut gérer en ligne le dossier permanent de la structure avec ses données administratives et pièces comptables. Le porteur de projet peut également accéder à l'espace de publication recensant les procédures d'aide existantes

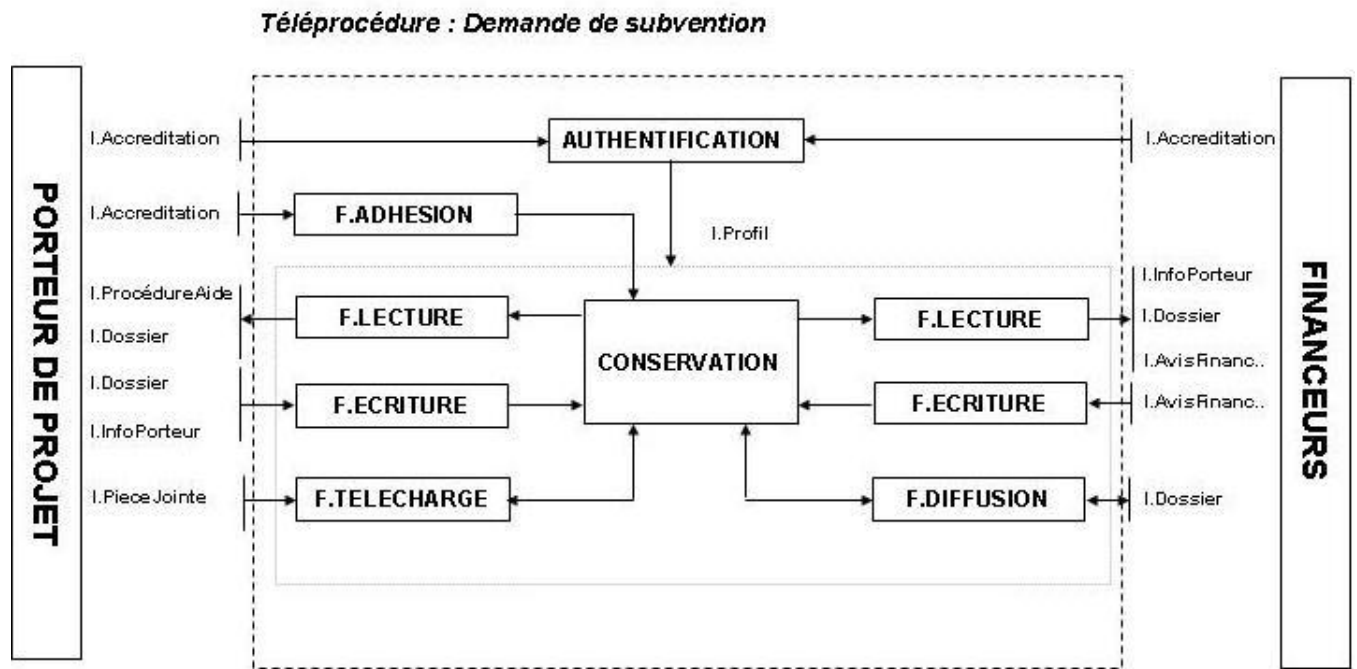
Les services de l'état ou les collectivités locales utilisent le guichet pour publier la liste des procédures d'aide existantes. Ils peuvent consulter les demandes et traiter les dossiers en ligne, ou récupérer les dossiers les concernant et les traiter en mode non connecté. La suite donnée par les services à la demande est notifiée au demandeur au travers du guichet.

## 2.2 Description des éléments essentiels

La téléprocédure « Demande de subvention » se rapproche fonctionnellement des téléprocédures type « Déclaration » et « Consultation ». Elle est envisagée comme une

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	7/47

extension à ces dernières puisqu'elle permet de mettre en œuvre un processus éditorial collaboratif entre le porteur de projet et les financeurs sous le contrôle de l'Administration.



### Fonction : F.AUTHENTIFICATION

#### Description

Pour les porteurs de projet, les services de l'état et les collectivités locales, la sous fonction « F-AUTHENTIFICATION » est mise en œuvre en support au contrôle d'accès aux fonctionnalités et aux informations.

La fonction "F.AUTHENTIFICATION" assure le contrôle des accréditations des usagers et, en cas de succès, leur attribue les autorisations nécessaires à la réalisation de leurs tâches dans le rôle qui leur a été imparti (voir « I.Profil »).

Pour la gestion de la demande de subvention, la téléprocédure regroupe deux grands rôles :

- Le demandeur de subvention qui crée la demande. Il est considéré comme l'utilisateur privilégié puisqu'il renseigne les principaux éléments du dossier (Informations de la structure, Budget, pièces administratives...) et est le seul habilité à réaliser des modifications

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	8/47

au dossier sur la base des avis de financement émis.

- Les financeurs qui renseignent, listent ou modifient les mesures de financement accordées à chaque demande de subvention.

Le contrôle d'accès permet de limiter le pouvoir d'action des utilisateurs aux informations et fonctions adéquates. En outre, l'accès aux demandes de subvention et/ou aux plans de financement est autorisé aux seules entités concernées.

## Fonction : F.CONSERVATION

### Description

Cette fonction est chargée de l'ensemble de la problématique de conservation des informations. Dans le cadre de la téléprocédure "Demande de subvention", elle assure la conservation des informations suivantes :

- Les mesures d'aides
- Les dossiers permanents des porteurs (voir « I.Dossier »)
- Les pièces comptables jointes au dossier des porteurs de projet (voir « I.PièceJointe »)
- Les mesures d'aide des financeurs (voir « I.Avis »)
- Les accréditations des usagers

Les différents acteurs n'agissent pas directement sur la partie conservation de donnée. Il passe par la phase d'authentification et accède ensuite aux informations par l'intermédiaire des fonctions « F.LECTURE » et « F.ECRITURE ». Les autorisations accordées les autorisent à :

- Créer, modifier, supprimer des données
- Visualiser des données

La notion de propriété est fondamentale puisque seul le porteur de projet est autorisé à modifier le dossier. Il autorise un certain nombre de services à venir renseigner la demande lors de la constitution de son budget prévisionnel.

## Fonction : F.DIFFUSION

### Description

Cette fonction est mise en œuvre comme support au traitement décentralisé des données par les financeurs en permettant l'échange des dossiers au

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	9/47

format « XML ».

Le format utilisé garantit l'interopérabilité avec les autres systèmes et facilite l'intégration au Back Office des services financeurs.

## Fonction : F.ECRITURE

### Description

Cette fonction permet de soumettre de l'information à l'administration lors d'une demande de subvention, de la déclaration d'une mesure de financement ou de toutes autres actions intervenant dans le sens usager vers administration.

Elle est utilisée pour renseigner l'administration et les différents acteurs du projet en agissant directement sur la partie conservation de données. Au sein de cette téléprocédure, la fonction « F.ECRITURE » intervient à plusieurs niveaux. Elle est par exemple utilisée lorsque :

- Un porteur de projet modifie les informations de sa structure
- Un porteur de projet saisit une nouvelle demande.
- Un financeur renseigne un avis de financement.
- Un acteur souhaite partager une remarque.

Un contrôle de cohérence approprié est effectué lors de la saisie d'informations liées à la validité du dossier ou des traitements. Cette notion est approfondie pour les informations comptables et juridiques qui sont contrôlées par le MINEFI et le Ministère de l'Intérieur.

L'information « I.PROFIL » fixe les autorisations qui s'appliquent à cette fonction sur la base des notions de groupe et d'identité des usagers.

## Fonction : F.ADHESION

### Description

Cette sous-fonction gère les inscriptions des porteurs de projet qui souhaitent accéder à la téléprocédure afin de réaliser une demande de subvention. La définition des accréditations est à leur charge mais sous contrôle de l'administration (longueur de mot de passe par exemple, ...).

Les services de l'état et les collectivités locales n'utilisent pas cette fonction. Leurs demandes d'accès aux services sont directement enregistrées par l'envoi d'un mèl aux personnes en charge de l'administration locale de la plateforme.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	10/47

## Fonction : F.LECTURE

### Description

Sur la base des données conservées au niveau de la partie conservation de données, cette fonction permet à l'administration de présenter de l'information conformément aux autorisations accordées aux usagers.

Un demandeur de projet est par exemple en mesure de :

- Visualiser ses données personnelles
- Visualiser la liste de ses demandes
- Visualiser les crédits alloués ou les remarques formulées par les financeurs
- Visualiser les procédures d'aides existantes

Pour un financeur, il peut s'agir de :

- Prendre connaissance des demandes de financement.
- Lister les procédures d'aides existantes

Le chargement du contexte applicatif de l'utilisateur (voir I.Profil) permet de restreindre les informations accessibles.

## Fonction : F.TELECHARGEMENT

### Description

Cette fonction permet la gestion centralisée des pièces administratives dématérialisées du porteur de projet. Il les rend disponible à l'ensemble des services impliqués dans le plan de financement par simple « Upload » sur le serveur de l'administration.

## Information : I.Accreditations

### Description

Couple d'informations de type « identifiant/mot de passe ». Il permet au porteur de projet et aux financeurs de s'authentifier afin d'accéder à la téléprocédure.

## Information : I.AvisFinancement

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	11/47

## Description

L'avis de financement constitue la réponse d'un financeur à la sollicitation d'un porteur de projet au travers de son budget prévisionnel. Il porte majoritairement sur le montant alloué au projet au regard de la somme initialement demandée.

## Information : I.Dossier

## Description

Ensemble des informations de la demande de subvention. Dans sa phase initiale, le mode opératoire est identique à celui utilisé dans la téléprocédure type « Déclaration ». Le porteur de projet renseigne sa demande par l'intermédiaire d'un formulaire de saisie. Il doit préalablement s'être acquitté de la définition de sa structure.

Les différentes catégories d'informations présentes dans le dossier sont :

- La description de la demande contenant :
  - La description de la structure (référence vers « I.InfoAdmin »)
  - Le type de mesures d'aides sollicitées
  - Un descriptif de dossier précisant le contexte de la demande (Présentation du projet, publics, lieu...)
- Le budget prévisionnel avec :
  - Les dépenses envisagées
  - Les recettes (financeurs sollicités et le montant demandé).

Après son dépôt, chaque financeur concerné par le plan de financement procède à la phase d'instruction partagée en émettant un avis. Le porteur de projet adapte alors son budget prévisionnel en fonction des crédits alloués et des remarques des financeurs. Le dossier transite par trois états successifs :

- En dépôt
- En cours d'instruction
- Complété (Bilan définitif du projet)

La notion de propriété est fondamentale puisque seul le porteur de projet est autorisé à effectuer des modifications sur cet élément essentiel. Les financeurs procèdent uniquement à la mise à jour des montants alloués en

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	12/47

émittant des avis de financement ou en disposant du dossier au format XML.

### Information : I.InfoPorteur

#### Description

Ensemble d'informations permettant aux financeurs et aux services de l'état de prendre connaissance de la structure qui sollicite une subvention. Ces informations sont intégrées au bilan définitif une fois la phase d'instruction du dossier terminée. Parmi ces informations, on trouve :

- Le nom de l'organisme
- Ses coordonnées
- Le représentant légal
- Les membres du bureau

La notion de dématérialisation étant dominante, un espace de stockage est mis à disposition du porteur de projet afin de communiquer des documents financiers ou administratifs aux acteurs intervenant sur le projet.

### Information : I.PieceJointe

#### Description

Pièce comptable dématérialisée rendue disponible par le porteur de projet à l'ensemble des financeurs par l'intermédiaire de la fonction "F.TELECHARGEMENT".

### Information : I.ProcédureAide

#### Description

Ensemble des procédures d'aide existantes saisies et mise à jour par les services de l'état.

En fonction des caractéristiques de sa structure, le porteur de projet accède uniquement aux procédures d'aide qu'il peut solliciter.

### Information : I.Profil

#### Description

Cette information fixe les autorisations d'accès qui s'appliquent au contenu

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

et aux fonctions. Le profil est chargé après la phase d'authentification et sous réserve de la validité des accréditations.

Pour la téléprocédure "Demande de subventions", ces restrictions s'appliquent aux fonctions :

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

Cette information permet d'identifier les données accessibles en lecture et en écriture au niveau de la partie « conservation de données ». Les porteurs de projet et financeurs sont à même de modifier, supprimer les données qu'ils ont rédigés.

## Information : I.Requete

Description Requête initiale indiquant la ressource à laquelle l'utilisateur souhaite accéder.

## 2.3 Enjeux

### E.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 des usagers ou encore la simplicité d'utilisation sont autant de catalyseurs qui favorisent le développement des téléprocédures.

### E.ECHANGES

Description L'amélioration des échanges entre les différents services administratifs constitue un enjeu capital du développement de l'administration électronique. La téléprocédure « démarche en ligne ; demandes » est conçue selon un principe de dossiers partagés par les différents services

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	14/47

concernés, qui permet d'optimiser les échanges entre Administrations.

## E.DEMATÉRIALISATION

### Description

Favorisée par l'émergence du projet ADELE, la dématérialisation des procédures administratives correspond à un triple objectif:

- Modernisation des services administratifs.
- Simplification des démarches.
- Recherche d'une plus grande efficacité.

La téléprocédure « démarche en ligne ; demandes » permet à la fois de simplifier la demande, et de faciliter le suivi des dossiers par l'utilisateur.

## 2.4 Hypothèses

### H.SECURITE-PHYSIQUE

### 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

Les menaces organisationnelles sont jugées en dehors du cadre de cette étude.

### H.USAGER

### Description

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

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	15/47

## 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.
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

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	16/47

F.AUTHENTIFICATION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Les mesures d'aide sont soumises à des contraintes strictes d'ordre calendaire. Le besoin en disponibilité au niveau de cette fonction est important car elle conditionne l'accès à la téléprocédure.
	Intégrité	2	Une perte d'intégrité est grave puisque cette fonction fixe les autorisations accréditées aux utilisateurs.
F.CONSERVATION	Confidentialité	0	Aucun besoin de 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 demandes. Une indisponibilité de quelques heures est acceptable étant donné les délais accordés entre les différentes d'instruction des demandes (plusieurs jours).
	Intégrité	2	Une perte d'intégrité serait très préjudiciable car la majorité des informations sont stockées par cette fonction.
F.DIFFUSION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin en disponibilité est moyen ; en cas d'indisponibilité le financeur peut toujours traiter le dossier en ligne (« F.LECTURE » et « F.ECRITURE »).
	Intégrité	2	Une perte d'intégrité est grave puisqu'elle peut entraîner une perturbation au niveau du back office des financeurs.
F.ECRITURE	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	17/47

			puisque les demandes sont soumises à une date limite de dépôt. Un pic de connexion étant généralement enregistré lors des derniers jours de cette période, une indisponibilité supérieure à quelques heures peut être préjudiciable.
	Intégrité	2	Une perte d'intégrité est grave car elle peut impacter l'intégrité des données soumises par les porteurs de projet ou les financeurs.
F.ADHESION	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Une indisponibilité de quelques jours de la fonction est tolérable si l'indisponibilité n'intervient pas dans une période proche d'une échéance fixée pour le dépôt des dossiers.
	Intégrité	2	Le besoin en intégrité est important au niveau de cet élément essentiel. Une perte d'intégrité peut rendre impossible l'accès à la téléprocédure pour tous les nouveaux porteurs de projet.
F.LECTURE	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	2	Le besoin en disponibilité est élevé puisque les demandes sont soumises à une date limite de dépôt. Un pic de connexion étant généralement enregistré lors des derniers jours de cette période, une indisponibilité supérieure à quelques heures peut être préjudiciable.
	Intégrité	1	Le besoin en intégrité est moyen dans la mesure où cette fonction n'est chargée que de la présentation des données.
F.TELECHARGEMENT	Confidentialité	0	Aucun besoin de confidentialité au niveau de cet élément essentiel.
	Disponibilité	1	Le besoin en disponibilité au niveau de cette fonction est moyen dans la mesure

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	18/47

			où le porteur de projet aussi renseigner ces informations en ligne (voir « F.ECRITURE »).
	Intégrité	2	Une perte d'intégrité est grave car elle peut impacter l'intégrité des données soumises par les porteurs de projet ou les financeurs.
I.Accreditations	Confidentialité	2	Le besoin en confidentialité au niveau des accréditations est important puisque ces informations permettent d'accéder au système avec des privilèges.
	Disponibilité	1	La perte des accréditations est tolérable ; le porteur peut les récupérer via une procédure spécifique.
	Intégrité	1	La perte des accréditations est tolérable puisque le porteur de projet peut récupérer cet élément essentiel via une procédure spécifique.
I.AvisFinancement	Confidentialité	2	Dans l'absolu les montants alloués par les financeurs sont du domaine public. En pratique un besoin de confidentialité important est enregistré (en particulier sur l'ensemble des subventions allouées)
	Disponibilité	2	Le besoin en disponibilité au niveau de cet élément essentiel est important car le porteur de projet doit soumettre un budget définitif avant la date limite de dépôt.
	Intégrité	2	Une perte d'intégrité est grave ; si elle touche les montants alloués, elle peut impacter le traitement du dossier par d'autres partenaires.
I.Dossier	Confidentialité	2	Dans l'absolu, toutes les informations contenues dans le dossier sont du domaine public. Cependant, le budget et le montant des subventions accordées présentent un besoin important en confidentialité.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	19/47

	Disponibilité	2	<p>Les mesures d'aide sont soumises à un calendrier, et les dossiers doivent être déposés avant la date de fin de programmation.</p> <p>Etant donné le laps de temps dont dispose le porteur de projet pour réaliser sa demande, une indisponibilité de quelques heures est tolérable.</p>
	Intégrité	2	<p>Une perte d'intégrité est grave dans la mesure où le dossier contient le budget de la structure, et présente les éléments probants en support à la demande</p> <p>D'autre part, il doit pouvoir être démontré que les dossiers ont été présentés avant la date de fin de programmation.</p>
I.ProcédureAide	Confidentialité	0	La liste des procédures d'aides est publique.
	Disponibilité	2	Le porteur de projet doit accéder aux procédures d'aide existantes afin de réaliser sa demande. Le besoin en disponibilité est donc identique à « I.Dossier »
	Intégrité	2	Le besoin en intégrité est important car la validité de certains dossiers dépend étroitement des mesures d'aide sélectionnées.
I.InfoPorteur	Confidentialité	2	Les dossiers contiennent des informations nominatives et fiscales.
	Disponibilité	2	Le besoin en disponibilité est important puisque l'administration et les financeurs doivent accéder au dossier afin de vérifier la validité de la demande.
	Intégrité	2	Une perte d'intégrité au niveau des informations relatives à la structure est grave car elle peut remettre en question les montants alloués par les financeurs.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	20/47

I.PieceJointe	Confidentialité	2	La diffusion des pièces comptables fournies par le porteur de projet est restreinte aux seuls financeurs identifiés.  Même si en théorie toutes les informations sont publiques, le besoin en confidentialité peut être important (aspect financier).
	Disponibilité	1	Cet élément essentiel présente un besoin en disponibilité moyen.
	Intégrité	2	Le besoin en intégrité est important puisque la pièce jointe justifie la demande présentée
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	2	Les mesures d'aide sont soumises à des contraintes d'ordre calendaire strictes.  L'indisponibilité de cet élément essentiel empêche les usagers d'accéder à la téléprocédure. Elle ne doit pas être supérieure à quelques heures.
	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	0	Le besoin en confidentialité est nul.
	Disponibilité	0	La requête de l'utilisateur ne possède aucun besoin de disponibilité.
	Intégrité	1	Les besoins d'intégrité au niveau de la requête sont moindres. Elle peut être ré émise à tous moments.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	21/47

### 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

	Confidentialité	Opportunité
R.LOGICIEL-PIECEJOINTE	3	4
R.USURPATION-SESSION	3	4
R.DYSFONCTIONNEMENT-COHERENCE	3	4
R.ORIGINE-GARANTIE	3	3
R.ABUS-AUTORISATION	3	3
R.RENIEMENT-IMPUTATION	3	3
R.ALTERATION-DOSSIER (XML)	3	3
R.ABUS-IDENTITE	3	2
R.ABUS-INJECTION	3	2
R.ABUS-DEBORDEMENT	3	1
R.ALTERATION-COMMUNICATION	3	1
R.LOGICIEL-CODE	3	1
R.LOGICIEL-CONCEPTION	3	1
R.SATURATION-CONNEXION	2	3
R.PANNE-INTEGRITE	2	2
R.ECOUTE-PORTEUR	2	2

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	22/47

R.ECOUTE-FINANCEUR	2	2
R.DIVULGATION-STOCKAGE	2	2
R.SATURATION-RESSOURCES	2	2
R.PERTE-TELECOM	2	1

## 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
Description	<p>Après authentification, les usagers sont accrédités de certaines autorisations qui leur donnent 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.</p> <p>Le nombre important d'acteurs potentiellement impliqués, la multiplication des profils et des règles d'accès aux informations sont autant de paramètres qui complexifient la tâche dans le cadre de la téléprocédure "Demande de subvention".</p> <p>Ainsi, un usager malintentionné identifie et forge une requête vers une fonction ou des informations dont le schéma de contrôle d'accès est défectueux. Il accède par exemple aux demandes des autres porteurs de projet ou à tous les avis émis par les services financiers.</p> <p>Etant donnée la méthode d'attaque employée par l'élément menaçant, les trois critères de sécurité sont touchés.</p> <p>Pour la confidentialité, les éléments essentiels fortement touchés sont les informations « I.Accréditations », « I.AvisFinancement », « I.Dossier », « I.InfoPorteur », « I.PieceJointe » et « I.Profil ».</p> <p>Au niveau de la disponibilité, il s'agit des fonctions</p>

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	23/47

«F.AUTHENTIFICATION», «F.CONSERVATION», «F.ECRITURE», «F.LECTURE» ainsi que les informations «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.Profil» et «I.ProcédureAide».

Concernant l'intégrité, les fonctions «F.ADHESION», «F.AUTHENTIFICATION», «F.DIFFUSION», «F.CONSERVATION», «F.ECRITURE », «F.LECTURE», « F.TELECHARGEMENT » et les informations «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.PieceJointe», «I.Profil», «I.ProcédureAide» sont très touchées car elles présentent toutes des besoins de sécurité importants.

Ce risque peut engendrer :

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

## R.ABUS-DEBORDEMENT

Libellé R.ABUS-DEBORDEMENT

Méthode d'attaque 39 - ABUS DE DROIT

Description Les problèmes de débordement de tampon constituent une menace de sécurité récurrente au niveau des applications. 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.

La téléprocédure "Demande de subventions" étant développée en "Java", les conséquences sont très restreintes puisque ce langage gère automatiquement ce type d'anomalie. Cependant, des liens étroits avec le système d'exploitation (Ex : lancement de scripts) peuvent rendre la téléprocédure vulnérable.

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.

Dans la majorité des cas un débordement de tampon permet une élévation des privilèges, les conséquences envisageables sont donc multiples et variées. Ce risque touche aussi bien la disponibilité, l'intégrité ou la

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	24/47

confidentialité des éléments essentiels.

Les éléments essentiels qui présentent un besoin important en confidentialité sont fortement touchés. Il s'agit des informations «I.Accréditations», «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.PieceJointe», «I.Profil».

Au niveau de la disponibilité, il s'agit des fonctions «F.AUTHENTIFICATION», «F.CONSERVATION», «F.ECRITURE», «F.LECTURE» ainsi que les informations «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.Profil», « I.ProcédureAide ».

Concernant l'intégrité, les fonctions «F.ADHESION», «F.AUTHENTIFICATION», «F.DIFFUSION», «F.CONSERVATION», «F.ECRITURE», «F.LECTURE», « F.TELECHARGEMENT » et les informations «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.PieceJointe», «I.Profil», « I.ProcédureAide » sont très touchées car elles présentent toutes des besoins de sécurité importants.

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Une perturbation du fonctionnement interne

## R.ABUS-IDENTITE

Libellé R.ABUS-IDENTITE

Méthode d'attaque 39 - ABUS DE DROIT

Description Les accréditations de compte et jetons de session présentent des failles exploitables. Une personne malintentionnée, douée de très bonnes connaissances techniques, peut compromettre les mots de passe (Force Brute), des clés ou cookies de session afin d'augmenter ses privilèges et consulter/modifier les demandes des porteurs de projet ou les avis de financement émis par les différents services.

Ce risque touche les trois critères de sécurité.

Pour la confidentialité, les éléments essentiels fortement touchés sont les

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	25/47

informations «I.Accréditations», «I.AvisFinancement», «I.Dossier», «I.InfoPorteur», «I.PieceJointe», «I.Profil».

Au niveau de la disponibilité, il s'agit des fonctions «F.AUTHENTIFICATION», «F.CONSERVATION», «F.ECRITURE», «F.LECTURE» ainsi que les informations «I.AvisFinancement», «I.Dossier», «I.InfoPorteur », «I.Profil», «I.ProcédureAide».

Concernant l'intégrité, les fonctions « F.ADHESSION », « F.AUTHENTIFICATION », «F.DIFFUSION», « F.CONSERVATION », « F.ECRITURE », « F.LECTURE », « F.TELECHARGEMENT » et les informations « I.AvisFinancement », « I.Dossier », « I.InfoPorteur », « I.PieceJointe », « I.Profil », « I.ProcédureAide » sont très touchées car elles présentent toutes des besoins de sécurité importants.

Ce risque peut engendrer :

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

## 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 et d'attaquer des composants secondaires ou d'exécuter des commandes systèmes.</p> <p>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 demandes des porteurs de projet (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 émis, les éléments essentiels les plus touchés sont les informations « I.Accréditations », « I.AvisFinancement », « I.Dossier », « I.InfoPorteur »,</p>

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	26/47

« I.PieceJointe », « I.Profil ».

Pour la disponibilité, ce risque porte fortement atteinte aux fonctions « F.AUTHENTIFICATION », « F.CONSERVATION », « F.ECRITURE », « F.LECTURE » ainsi qu'aux informations « I.AvisFinancement », « I.Dossier », « I.InfoPorteur », « I.Profil », « I.ProcédureAide ».

Concernant l'intégrité, les fonctions "F.ADHESION", "F.AUTHENTIFICATION", "F.DIFFUSION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil", "I.ProcédureAide" sont très touchées car elles présentent toutes des besoins de sécurité importants.

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
- Une perturbation de fonctionnement interne

## R.ALTERATION-COMMUNICATION

Libellé R.ALTERATION-COMMUNICATION

Méthode d'attaque 36 - ALTÉRATION DES DONNÉES

Description Cette menace consiste à modifier illicitement les données en transit sur le medium de communication. Dans le contexte d'une communication de type "Client Serveur", une attaque de type "Man In The Middle" permet de se faire passer pour le client auprès du serveur et inversement.

Par vengeance ou motivation personnelle, une personne malintentionnée, agit comme un relais transparent et modifie les paramètres de la demande de subvention ou des avis de financements afin de perturber le fonctionnement de la téléprocédure.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	27/47

Ce risque porte uniquement atteinte à la confidentialité et l'intégrité des informations qui transite via le protocole HTTP.

Au niveau de la confidentialité, les éléments essentiels les plus durement touchés sont ceux qui émettent le plus fort besoin de sécurité. Il s'agit des informations "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe" et "I.Profil".

Pour l'intégrité, les éléments essentiels fortement touchés sont les fonctions "F.ADHESION", "F.AUTHENTIFICATION", "F.DIFFUSION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil", "I.ProcédureAide".

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements
- La perturbation du fonctionnement interne

## R.ALTERATION-DOSSIER (XML)

Libellé R.ALTERATION-DOSSIER (XML)

Méthode d'attaque 36 - ALTÉRATION DES DONNÉES

Description Une personne malintentionnée, connaissant la structure XML des dossiers échangés, peut forger de fausses transactions afin de provoquer des erreurs, de saturer la téléprocédure ou encore corrompre la base de données contenant les déclarations.

Ce risque porte fortement atteinte à l'intégrité de l'information "I.Dossier" qui transite via le flux de donnée XML.

Cela peut engendrer :

- Une infraction aux lois, aux règlements
- Une perte financière

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	28/47

- Une perturbation du fonctionnement interne

## R.DIVULGATION-STOCKAGE

Libellé R.DIVULGATION-STOCKAGE

Méthode d'attaque 23 - DIVULGATION

Description Etant donnée le manque de classification au niveau de la sensibilité des informations et l'absence de moyens de chiffrement adaptés, toute une série d'informations nominatives, financières concernant la structure ou les montants alloués par les financeurs sont divulguées. Un dysfonctionnement, une erreur d'administration ou une personne animée par un esprit de vengeance peuvent être à l'origine de cette menace.

Ce risque touche uniquement la confidentialité des informations stockées ou sauvegardées.

Les éléments essentiels affectés avec le niveau le plus élevé sont les informations "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil".

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements

## R.DYSFONCTIONNEMENT-COHERENCE

Libellé R.DYSFONCTIONNEMENT-COHERENCE

Méthode d'attaque 31 - DYSFONCTIONNEMENT LOGICIEL

Description Dans le cadre de la téléprocédure "Demande de subvention", les financeurs émettent un avis de financement sur la base du budget prévisionnel présenté par le porteur de projet. La phase d'instruction partagée consiste à faire converger le budget prévisionnel avec les avis de financement émis.

Si les données sont récupérées au format XML et traitées au niveau Back

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	29/47

Office, des problèmes de cohérence peuvent intervenir entre les données mises à jour par le porteur de projet et celles à disposition des financeurs.

Conformément aux hypothèses émises lors de l'étude du système cible, il convient de considérer uniquement la perte d'intégrité induite par un dysfonctionnement d'ordre logiciel. Ainsi, ce risque touche très fortement l'intégrité de informations "I.Dossier".

Ce risque peut engendrer :

- Une perte financière
- La perturbation du fonctionnement interne

## R.ECOUTE-FINANCEUR

Libellé R.ECOUTE-FINANCEUR

Méthode d'attaque 19 - ÉCOUTE PASSIVE

Description Profitant du manque de protection des équipements de communication et de la faiblesse des moyens cryptographiques employés, une personne malintentionnée capture et déchiffre les flux de données échangés entre les financeurs et la téléprocédure.

Cette menace est présente à deux niveaux différents :

- Lors de la saisie des avis de financement en ligne
- Lors de l'échange des données formatés en XML via le module de gestion Back Office.

Ce risque touche uniquement la confidentialité des informations qui transitent entre les financeurs et l'administration. Les informations les plus touchées sont "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil".

Ce risque peut engendrer :

- Atteinte à la vie privée des usagers
- Infraction aux lois, aux règlements

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	30/47

## R.ECOUTE-PORTEUR

Libellé	R.ECOUTE-PORTEUR
Méthode d'attaque	19 - ÉCOUTE PASSIVE
Description	<p>Profitant de la faible protection des équipements de communication et 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 le porteur de projet et la téléprocédure. Il prend ainsi connaissance d'informations nominatives (liste des membres du bureau), financières (montant des subventions).</p> <p>Ce risque touche uniquement la confidentialité des informations qui transitent entre les porteurs de projet et l'administration. Les informations les plus touchées sont "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil".</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> <li>• Atteinte à la vie privée des usagers</li> <li>• Infraction aux lois, aux règlements</li> </ul>

## R.LOGICIEL-CODE

Libellé	R.LOGICIEL-CODE
Méthode d'attaque	26 - PIÉGEAGE DU LOGICIEL
Description	<p>L'application Web peut être utilisée comme un vecteur d'attaque. En profitant du manque de validation des entrées et sorties de la téléprocédure, l'idée consiste à insérer au sein d'un formulaire de saisie des informations qui seront ensuite affichées sans précaution préalable. Ces scripts sont alors exécutés de manière transparente au niveau du navigateur de toutes les personnes qui se connectent.</p> <p>La téléprocédure demande de subventions est potentiellement très vulnérable car le contexte d'édition partagé facilite la diffusion des codes malveillants à l'ensemble des acteurs.</p> <p>Ainsi, par vengeance ou motivation personnelle, une personne malintentionnée peut profiter de la phase d'instruction partagée pour</p>

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	31/47

diffuser un code malveillant au sein des administrations concernés par le financement du projet.

Suivant la nature des codes, ce risque peut toucher les trois critères de sécurité.

Les informations "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe" et "I.Profil" sont très fortement touchées au niveau de la confidentialité.

Pour la disponibilité, ce risque porte fortement atteinte aux fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE" ainsi qu'aux informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide".

Enfin, ce risque porte atteinte de manière importante à l'intégrité des éléments essentiels "F.ADHESION", "F.AUTHENTIFICATION", "F.DIFFUSION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "F.TELECHARGEMENT", "AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil", "I.ProcédureAide".

Cela 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
- Des pertes financières
- Une perturbation du fonctionnement interne
- La perturbation du fonctionnement de tiers

## R.LOGICIEL-CONCEPTION

Libellé R.LOGICIEL-CONCEPTION

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description Une personne malintentionnée utilise des fonctionnalités cachées introduites durant la phase de conception de l'application. Il peut par exemple être en mesure de visualiser illicitement les demandes effectuées

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	32/47

par d'autres porteurs de projet, de prendre connaissance des avis de financement, ...

Ce risque touche les trois critères de sécurité.

Pour la confidentialité, les éléments essentiels fortement touchés sont les informations "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe" et "I.Profil".

Au niveau de la disponibilité, il s'agit des fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE" ainsi que les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide".

Concernant l'intégrité, les fonctions "F.ADHESION", "F.AUTHENTIFICATION", "F.DIFFUSION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "F.TELECHARGEMENT" et les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil", "I.ProcédureAide" sont très touchées.

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements
- Des pertes financières

## R.LOGICIEL-PIECEJOINTE

Libellé R.LOGICIEL-PIECEJOINTE

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description Lors de la réalisation de sa demande, le porteur de projet peut être amené à mettre à disposition des pièces dématérialisées (pièces comptables, liste des membres). Cette tâche est réalisée par upload des fichiers sur le serveur de l'administration.

Une personne malintentionnée peut profiter de la faiblesse du dispositif de filtrage en joignant un fichier piégé (Ex: exe, pl, vbs ...). L'exploitation de cette vulnérabilité peut permettre la diffusion d'un cheval de Troie au niveau du poste des financeurs et des services de l'état.

Suivant la nature du fichier, les trois critères de sécurité peuvent être touchés.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	33/47

Au niveau de la confidentialité, les informations "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe" et "I.Profil" sont très fortement touchées.

Pour la disponibilité, ce risque porte fortement atteinte aux fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "F.TELECHARGEMENT" ainsi qu'aux informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide" .

Ce risque peut aussi porter atteinte de manière importante à l'intégrité des éléments essentiels "F.ADHESION", "F.AUTHENTIFICATION", "F.DIFFUSION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil".

Il peut engendrer :

- 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
- Une perturbation du fonctionnement interne
- Une perturbation du fonctionnement de tiers

## R.ORIGINE-GARANTIE

Libellé R.ORIGINE-GARANTIE

Méthode d'attaque 24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE

Description Une personne malintentionnée, très au fait des techniques d'usurpation d'identité, détourne les communications vers son propre système. Sous couvert de la similitude avec la téléprocédure d'origine, il invite les utilisateurs à saisir leurs accréditations afin de récupérer les éléments nécessaires pour accéder à leurs dossiers.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	34/47

Au vu du scénario, ce risque touche uniquement la confidentialité de l'information "I.Accreditation".

Cela peut engendrer :

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

## R.PANNE-INTEGRITE

Libellé R.PANNE-INTEGRITE

Méthode d'attaque 28 - PANNE MATÉRIELLE

Description Suite à la panne de l'un des équipements matériels, il s'établit une perte de cohérence au niveau des informations stockées (dossiers des porteurs de projet, des avis de financement).

Il convient de considérer uniquement la perte d'intégrité induite par une panne matérielle. Ainsi, ce risque touche très fortement l'intégrité des informations stockées "I.Accréditations", "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.PieceJointe", "I.Profil", "I.ProcédureAide".

Ce risque peut engendrer :

- Des frais financiers de secours et de remise à niveau
- Une interruption de service
- Des pertes financières
- Une perturbation du fonctionnement interne

## R.PERTE-TELECOM

Libellé R.PERTE-TELECOM

Méthode d'attaque 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	35/47

Description	<p>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.</p> <p>L'impossibilité de basculer rapidement vers une ligne de secours aggrave d'autant plus la situation.</p> <p>Ce risque touche la disponibilité des informations transmises par le canal de communication.</p> <p>Pour cette téléprocédure, les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide" sont fortement touchées puisqu'elles présentent toutes un besoin élevé au niveau de la disponibilité.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <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.RENIEMENT-INPUTATION

Libellé	R.RENIEMENT-IMPUTATION
Méthode d'attaque	41 - RENIEMENT D' ACTIONS
Description	<p>Profitant de l'absence de fichiers d'imputation et de la mauvaise protection des accréditations des usagers, une personne malintentionnée accède aux dossiers et réalise toute une série de modifications afin de perturber le fonctionnement de la téléprocédure. L'administration se trouve dans l'impossibilité de lister et d'annuler les modifications effectuées afin de rétablir rapidement la situation.</p> <p>Ce risque touche l'intégrité des éléments essentiels "I.Dossier", "I.PieceJointe", "I.InfoPorteur" et "I.AvisFinancement" qui présente un fort besoin de sécurité au niveau de ce critère.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> <li>• L'acceptation de dossiers transmis après la date autorisée</li> <li>• Une Perturbation du fonctionnement interne</li> </ul>

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	36/47

- Une perte financière

## R.SATURATION-CONNEXION

Libellé R.SATURATION-CONNEXION

Méthode d'attaque 30 - SATURATION DU SYSTÈME INFORMATIQUE

Description Une attaque courante consiste à soumettre le dispositif à un nombre important de requêtes afin d'empêcher des utilisateurs légitimes de se connecter.

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: Saturation du serveur d'application, du pool de connexion à la base de donnée) afin de paralyser la téléprocédure.

Ce risque touche uniquement la disponibilité des éléments essentiels. Les plus affectés sont les fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE" ainsi que les informations "I.AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide".

Cela peut engendrer :

- Une interruption de service
- Une perte d'image de marque
- Une perturbation du fonctionnement interne

## R.SATURATION-RESSOURCES

Libellé R.SATURATION-RESSOURCES

Méthode d'attaque 30 - SATURATION DU SYSTÈME INFORMATIQUE

Description Par vengeance ou motivation personnelle, une personne malintentionnée perturbe le fonctionnement de la téléprocédure en uploadant des fichiers de

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	37/47

taille importante sur le serveur ou des dossiers XML non valides.

Tout comme pour "R.SATURATION-CONNEXION", ce risque touche uniquement la disponibilité des éléments essentiels "F.AUTHENTIFICATION", "F.CONSERVATION", "F.ECRITURE", "F.LECTURE", "AvisFinancement", "I.Dossier", "I.InfoPorteur", "I.Profil", "I.ProcédureAide".

Ce risque peut engendrer :

- Une interruption de service
- Une perte d'image de marque
- Une perturbation du fonctionnement interne

## R.USURPATION-SESSION

Libellé R.USURPATION-SESSION

Méthode d'attaque 40 - USURPATION DE DROIT

Description Le renseignement du dossier de demande de subvention est un processus long. Une personne malintentionnée, profitant de l'absence de procédure de verrouillage de la session en cas d'inactivité, accède à une session laissée ouverte et modifie le dossier d'un usager.

Etant donné le scénario de menace, ce risque porte principalement atteinte à l'intégrité et à la confidentialité des informations "I.Dossier", "I.PieceJointe", "I.AvisFinancement", "I.Profil" .

Ce risque peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements
- Une perte financière

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	38/47

## 4 Objectifs de sécurité

### O.INJECTION

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

### O.COMMUNICATION

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des données transmises.

### O.INTEGRITE-XML

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des données échangées en XML.

### O.AUTORISATION

Contenu Des mesures techniques doivent être prises pour limiter l'utilisateur aux seules fonctions et informations autorisées.

### O.CHIFFREMENT

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

### O.CODE-MALVEILLANT

Contenu Des mesures doivent être prises afin d'empêcher la diffusion des codes malveillants par l'intermédiaire de la téléprocédure.

### O.CONFORMITE

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	39/47

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

#### O.CONFIDENTIALITE-FINANCEUR

Contenu Des mesures doivent être prises afin de garantir la confidentialité des informations transmises entre les financeurs et l'administration.

#### O.CONFIDENTIALITE-PORTEUR

Contenu Des mesures doivent être prises afin de garantir la confidentialité des informations transmises entre les porteurs de projet et l'administration.

#### O.DEBORDEMENT

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

#### O.COHERENCE

Contenu Des mesures techniques doivent être prises afin de garantir la cohérence des informations consultées par les différents acteurs.

#### O.IDENTITE

Contenu Des mesures doivent être prises afin de garantir la robustesse du dispositif de gestion des authentifications et des sessions.

#### O.IMPUTATION

Contenu Chaque événement essentiel doit être logué et imputé de sorte qu'aucune modification malintentionnée ne soit irréversible.

#### O.ORIGINE

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	40/47

Contenu Des mesures doivent être prises afin de garantir l'authentification d'origine des informations émises par le serveur applicatif.

## O. INTEGRITE-DONNEES

Contenu Des mesures techniques doivent être prises afin de garantir l'intégrité des données mémorisées.

## O.PIECE-JOINTE

Contenu Des mesures techniques doivent être prises afin de filtrer les pièces jointes aux dossiers de demande de subvention.

## O.SATURATION-CONNEXION

Contenu Des mesures techniques doivent être prises afin d'empêcher la saturation des connexions de la téléprocédure.

## O.SATURATION-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 ne doivent pas entraver la disponibilité de la téléprocédure.

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	41/47

## 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		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	42/47

## 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		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	43/47

## 15 - RAYONNEMENTS THERMIQUES

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

## 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, les méthodes d'attaques touchant la sécurité du poste client sont écartées.

## 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		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	44/47

## 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 initialement écartée dans le cadre de cette analyse.

## 33 - UTILISATION ILLICITE DES MATÉRIELS

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

## 34 - COPIE FRAUDULEUSE DE LOGICIELS

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

## 35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS

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

## 37 - TRAITEMENT ILLICITE DES DONNÉES

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

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	45/47

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.INJECTION	O.COMMUNICATION	O.INTEGRITE-XML	O.AUTORISATION	O.CHIFFREMENT	O.CODE-MALVEILLANT	O.CONFORMITE	O.CONFIDENTIALITE-FINANCEUR	O.CONFIDENTIALITE-PORTEUR	O.DEBORDEMENT	O.COHERENCE	O.IDENTITE	O.IMPUTATION	O.ORIGINE	O.INTEGRITE-DONNEES	O.PIECE-JOINTE	O.SATURATION-CONNEXION	O.SATURATION-RESSOURCES	O.SESSION	O.TELECOM
R.ABUS-AUTORISATION				X																
R.ABUS-DEBORDEMENT									X											
R.ABUS-IDENTITE												X								
R.ABUS-INJECTION	X																			
R.ALTERATION-COMMUNICATION		X																		
R.ALTERATION-DOSSIER (XML)			X																	

FEROS Types		Demande		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.4.1	V1.0	13/04/2006	Public	46/47

R.DIVULGATION-STOCKAGE					X														
R.DYSFONCTIONNEMENT-COHERENCE										X									
R.ECOUTE-FINANCEUR							X												
R.ECOUTE-PORTEUR								X											
R.LOGICIEL-CODE					X														
R.LOGICIEL-CONCEPTION						X													
R.LOGICIEL-PIECEJOINTE																X			
R.ORIGINE-GARANTIE													X						
R.PANNE-INTEGRITE														X					
R.PERTE-TELECOM																			X
R.RENIEMENT-IMPUTATION											X								
R.SATURATION-CONNEXION																X			
R.SATURATION-RESSOURCES																	X		
R.USURPATION-SESSION																		X	

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