



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



PREMIER MINISTRE
SGDN - DCSSI

=====

FEROS Types

Téléprocédure de référence

Déclaration

=====

VERSION 1.0

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2006	Public	1/52

FEROS Types	
Déclaration de changement d'adresse	
Référence	Date
FEROS Type_DéclarationV1.0.doc	04/04/2008
Identification d'objet (OID)	Racine OID et gestionnaire
1.2.250.1.137.2.2.1.2.3.3.1	DGME/SDAE
Responsable	Version
DGME/SDAE – SGDN\DCSSI	V1.0
Critère de diffusion	Nombre de pages
Public	52

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

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	2/52

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	6
2.2	DESCRIPTION DES ELEMENTS ESSENTIELS	8
2.3	ENJEUX	14
2.4	EHELLE DE BESOINS.....	15
2.5	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	43
5	LES RISQUES RESIDUELS	47
5.1	METHODES D'ATTAQUE NON RETENUES	47
5.2	TABLEAU DE COUVERTURE DES RISQUES PAR LES OBJECTIFS.....	50

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	3/52

1 Introduction

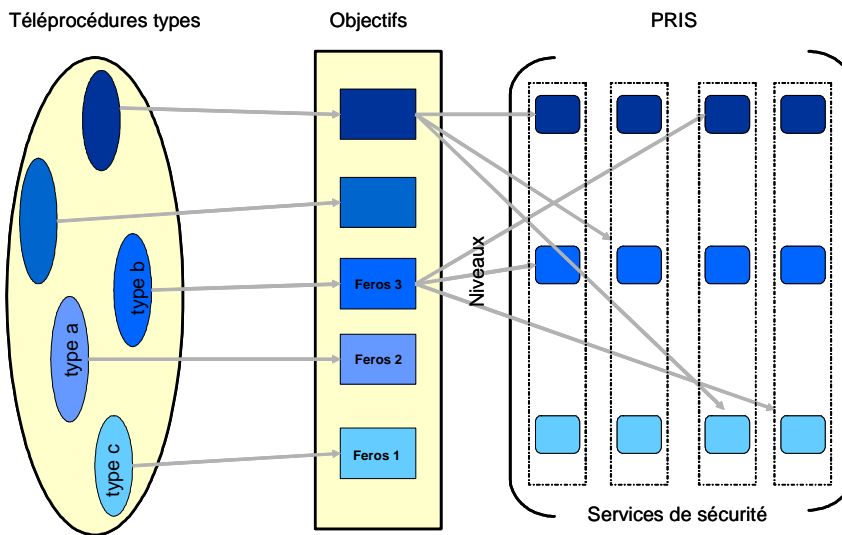
1.1 Contexte général

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		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	4/52

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 déclaration d'embauche pourra procéder à partir de la téléprocédure type « déclaration », 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 déclaration.

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. A L'ADAE, la maîtrise d'ouvrage de la téléprocédure de changement d'adresse a participé à l'élaboration et la validation de cette analyse.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	5/52

2 Description du système étudié

La déclaration offre aux internautes la possibilité de réaliser par Internet leurs déclarations auprès de l'Administration. La déclaration nécessite la plupart du temps une phase d'adhésion. Elle porte en général sur des informations de nature confidentielle, que ce soit dans le domaine financier, social, fiscal, médical, ...

Exemples de mise en œuvre

Compte fiscal des professionnels

Déclaration Unifiée de cotisations sociales

Déclaration de changement d'adresse

Dossier fiscal du particulier – TéléIR / Adonis

Téléprocédures de déclaration des centres de loisir sans hébergement

Acquisition en ligne de données statistiques

Déclaration pour le transport en ligne de marchandises dangereuses

Déclaration d'accident lors du transport de marchandises dangereuses

Déclaration mensuelle des mouvements de main d'œuvre

Recensement des entreprises de transport et de BTP dans le cadre de leur obligation de Défense

Déclaration des services des marins

Scénario retenu pour l'analyse

DESCRIPTION

Au titre de la téléprocédure type, on a retenu la déclaration sans inscription préalable, réalisée directement par l'intéressé à partir de ses moyens informatiques personnels. Les données transmises et conservées peuvent présenter un caractère personnel.

USAGER

- Particulier

MODE OPERATOIRE

- Accès depuis les moyens informatiques propres de l'utilisateur

DOMAINE D'APPLICATION

- Déclaration d'information pouvant avoir un caractère personnel

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 la déclaration centralisée de changement d'adresse auprès des différentes administrations.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	6/52

Système-cible

Présentation

Le Gouvernement, par l'intermédiaire de l'ADAE (Agence pour le Développement de l'Administration Electronique), souhaite mettre en place au printemps 2005 une téléprocédure visant à simplifier les démarches administratives lors du déménagement des citoyens.

Cette téléprocédure permet à l'utilisateur de procéder à une déclaration unique et centralisée de son changement d'adresse. Une transmission automatisée est effectuée vers les administrations désignées par l'utilisateur.

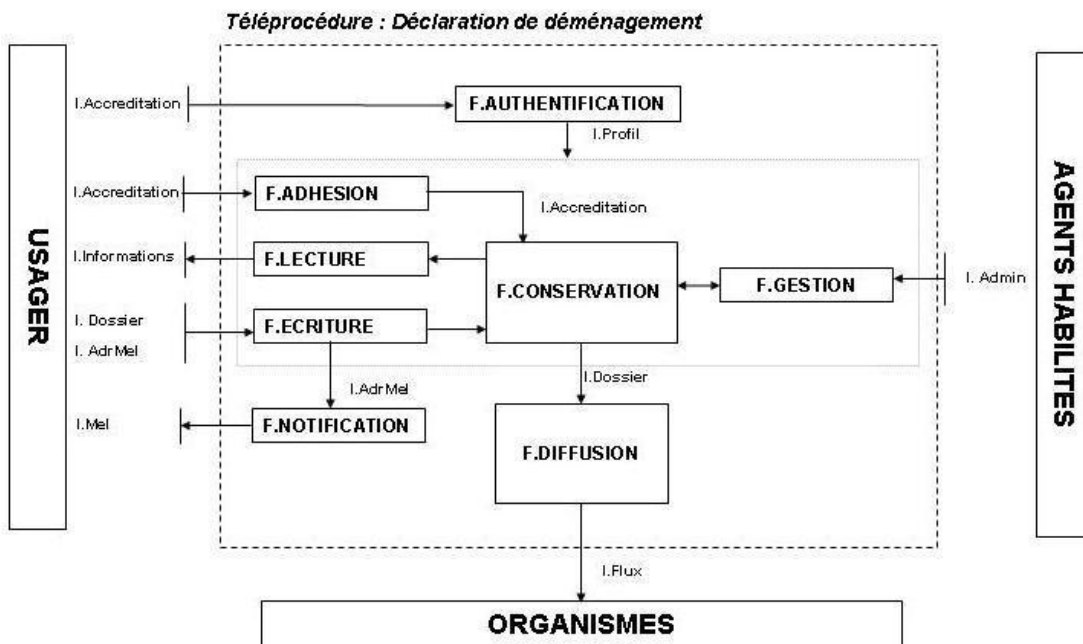
Dans un premier temps, la liste des administrations accessibles au travers de cette téléprocédure sera composée de :

- DGI (Direction Générale des impôts)
- DSN (Direction du Service National)
- CNAM (Caisse Nationale d'Assurance Maladie)
- CAF (Caisse d'Allocations Familiales)
- CNAV (Caisse Nationale d'Assurance Vieillesse)
- UNEDIC (Union Nationale pour l'Emploi dans l'Industrie et le Commerce)
- Ministère de l'intérieur (Carte Grise)

Par la suite, d'autres organismes pourront venir enrichir cette liste.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	7/52

2.2 Description des éléments essentiels



Fonction : F.NOTIFICATION

Description Cette fonction finalise la déclaration de changement d'adresse en notifiant à l'utilisateur, par le biais d'un courriel récapitulatif, les paramètres saisis. Pour cela, l'utilisateur doit fournir une adresse mèl valide lors de l'inscription

Fonction : F.AUTHENTIFICATION

Description La fonction "F.AUTHENTIFICATION" est mise en oeuvre en réponse à deux besoins différents :

- Pour les utilisateurs (numéro de dossier + mot de passe)
- Pour les administrateurs, organismes et membres du support (identifiant + mot de passe)

La sous-fonction "F.AUTHENTIFICATION" permet de contrôler l'identité des personnes en support à la gestion de leurs autorisations

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	8/52

"I.PROFIL" au sein du système. Le dispositif permettant de vérifier la validité des accréditations repose sur une comparaison avec les informations contenues dans une base interne.

La sous fonction F-AUTHENTIFICATION n'est pas un préalable systématique à l'accès des usagers¹. Couplée à la fonction "F.ADHESION", elle est utilisée pour reprendre une déclaration interrompue à la demande de l'utilisateur. Cette fonctionnalité n'est accessible que dans la mesure où la liste des organisations n'a pas encore été saisie. Le numéro de dossier est généré automatiquement par l'administration alors que la génération du mot de passe est à la charge des usagers.

Pour les administrateurs, organismes et membres du support, la sous fonction F-AUTHENTIFICATION est mise en œuvre en support au contrôle d'accès aux fonctionnalités avancées (administration, statistique...). Elle est basée sur un mécanisme de mots de passe.

Fonction : F.ADHESION

Description Cette sous-fonction est mise en œuvre par l'utilisateur pour interrompre le processus de saisie de la déclaration. Elle permet d'enregistrer ses données et fixe les accréditations (numéro de dossier et mot de passe) lui permettant de ré accéder à son dossier.

Fonction : F.GESTION

Description Elle permet la gestion des déclarations pour les administrateurs, membres d'un organisme ou personnes gérant l'aide aux utilisateurs.

L'utilisation de cette fonction nécessite des privilèges étendus car elle permet de s'affranchir de nombreuses règles de sécurité imposées à un utilisateur traditionnel.

Fonction : F.CONSERVATION

Description Cette fonction permet de gérer la conservation des informations. Dans le cadre de la téléprocédure "Déclaration de changement d'adresse", elle

¹ Ce caractère non systématique de la sous-fonction authentification peut dépendre de la nature de la déclaration proposée.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	9/52

assure la conservation des informations suivantes :

- Les données des différents dossiers (voir "I.DOSSIER")
- Les profils des usagers (voir "I.PROFIL")
- Les accréditations
- Les informations statiques (FAQ, Aide en Ligne, Formulaire ...)

En fonction des autorisations (voir "I.PROFIL") accordées, l'utilisateur peut :

- Ajouter, modifier, supprimer des données (voir "F.ECRITURE")
- Visualiser des données (voir "F.LECTURE")

Après la diffusion des informations vers les organismes, les dossiers des usagers sont anonymisés. Ce processus consiste à effacer toutes les données personnelles, le reste étant conservé à des fins statistiques.

Fonction : F.DIFFUSION

Description

Cette fonction assure la transmission des dossiers saisis par les usagers vers les organismes concernés. Le processus se décompose en plusieurs étapes distinctes :

- L'extraction des données des dossiers de changement d'adresse
- Leur mise en forme sous un format standard
- La conversion vers le format approprié à chaque organisme
- Le transfert vers les organismes
- La gestion des accusés de réponse et des alertes de ré émission

Les accusés de réponse permettent de s'assurer que le dossier a bien été reçu par chacun des organismes sélectionnés par l'utilisateur. Dans le cas contraire, la fonction identifie les organismes n'ayant pas accusé réception des données et établit une liste des dossiers qui nécessitent une intervention manuelle de la part d'un administrateur. Dès lors, celui-ci est en charge de ré expédier les données par une autre procédure.

Une fois tous les accusés de réponse reçus, les dossiers sont automatiquement anonymisés et archivés à des fins statistiques.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	10/52

Fonction : F.ECRITURE

Description

Cette fonction permet à l'utilisateur de renseigner les informations nécessaires à l'administration. Elle est utilisée pour renseigner les différents champs et paramètres des formulaires de changement d'adresse. On différencie quatre types d'actions :

- L'ajout d'informations au dossier
- La modification des informations du dossier
- La suppression d'informations

Lors de la saisie, un contrôle de cohérence approprié est effectué suivant le type d'informations saisies. Pour les adresses, cette notion est approfondie puisqu'un logiciel effectue des opérations de contrôle et de reformatage d'adresse à partir des référentiels d'adresse (Hexaposte, Hexavia et Hexaclé) de la Poste.

L'information "I.PROFIL" fixe les autorisations qui s'appliquent à cette fonction. Tout comme pour la fonction "F.LECTURE", l'utilisateur utilise un profil générique s'il renseigne un nouveau formulaire. Par contre, si l'utilisateur désire reprendre une déclaration interrompue, il doit fournir ses accreditations pour charger son contexte applicatif et modifier ses données.

Fonction : F.LECTURE

Description

Cette fonction permet à l'administration de présenter des données à l'utilisateur. L'information "I.PROFIL" spécifie les autorisations qui s'appliquent sur la fonction. Il existe deux cas d'utilisation :

- La déclaration classique de changement d'adresse.
- La modification d'une déclaration précédente.

Dans le premier cas, les usagers accèdent au formulaire avec un profil générique. Par contre, si l'utilisateur désire reprendre une déclaration interrompue, il doit fournir ses accreditations pour visualiser les données préalablement enregistrées.

Si les accreditations sont valides (voir "F.AUTHENTIFICATION"), le contexte applicatif de l'utilisateur est chargé et les champs de son dossier initialisés à partir des données conservées par la fonction "F.CONSERVATION".

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	11/52

Information : I.ACCREDITATION

- Description
- Couple d'informations permettant à un usager de s'authentifier afin de modifier son dossier. Les accreditations regroupent :
- Un numéro de dossier attribué par l'administration
 - Un mot de passe généré par l'utilisateur lors de la saisie de son dossier

Information : I.DOSSIER

- Description
- Ensemble des informations soumises par l'utilisateur à l'administration par l'intermédiaire de la fonction "F.ECRITURE". Le dossier regroupe les catégories d'informations suivantes :
- Informations identifiant la personne qui déclare le changement d'adresse (nom, prénom, numéro de téléphone, mèl,..)
 - Informations relatives au changement d'adresse (ancienne et nouvelle adresse)
 - Informations relatives aux personnes concernées (nom, prénom...)
 - Le choix des organismes auxquels l'utilisateur veut communiquer le changement
 - Les données spécifiques à chaque organisme (Numéro de sécurité sociale, Numéro fiscal ...)
- Les données sont ensuite stockées par la fonction "F.CONSERVATION". Suivant l'état d'avancement du dossier, il peut se trouver dans l'un des cinq états suivants :
- En cours de saisie par l'utilisateur
 - Complété mais en attente de transmission vers les organismes
 - En cours de transmission vers les organismes
 - Supprimé (par l'administrateur ou l'utilisateur)
 - Anonymisé après la réception de tous les accusés de réponse des organismes (voir "I.STAT")

Information : I.FLUX

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	12/52

Description Flux matérialisant l'échange des données entre la téléprocédure et les organismes partenaires. Un format spécifique est adopté en fonction de l'organisme destinataire (voir "F.DIFFUSION").

D'autre part, un dispositif d'accusé de réponse est mis en place afin de contrôler la bonne réception des données transmises.

Information : I.INSTRUCTIONS

Description Ensemble des données présentées par l'administration à l'utilisateur. Dans le cadre de cette téléprocédure, trois catégories d'informations sont soumises à l'utilisateur :

- Les données statiques (formulaires de déclaration, aide en ligne, FAQ)
- Les erreurs de saisie ou de traitement résultant d'une opération
- Les données préalablement saisies

Les données préalablement enregistrées sont affichées lorsque l'utilisateur souhaite modifier son dossier ou lors de l'affichage du récapitulatif avant la validation définitive du dossier.

Information : I.ADRMEL

Description Adresse mèl de l'utilisateur. Cette information est facultative dans la mesure où elle ne sert qu'à envoyer le mèl de notification.

Information : I.MEL

Description Mèl de confirmation envoyé à l'utilisateur lorsque sa déclaration a été dûment complétée.

Information : I.PROFIL

Description Information contenant les autorisations d'accès au contenu et aux fonctions. Le profil de l'utilisateur est chargé après l'authentification et définit ce que l'utilisateur a le droit de faire.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	13/52

Pour la téléprocédure "Déclaration de changement d'adresse", cette information permet d'identifier les données accessibles en lecture et en écriture sur la fonction "F.CONSERVATION".

Information : I.REQUETE

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

Information : I.STAT

Description Informations représentant les dossiers après anonymisation et archivage.

Information : I.ADMIN

Description Informations regroupant les accréditations permettant d'accéder aux fonctionnalités de gestion et les données échangées lors de l'utilisation de la fonction (voir "F.GESTION").

2.3 Enjeux

E.ATTENTES

Supprimé : H

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

Supprimé : H

Description L'amélioration des échanges entre les différents services administratifs constitue un enjeu capital du développement de l'administration électronique.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	14/52

E. DEMATERIALISATION

Supprimé : H

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.

2.4 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 ne porte atteinte qu'à la vie privée de quelques usagers.	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'usagers. Les conséquences restent donc restreintes.
3	Informations confidentielles ne devant pas être divulguées. En cas de divulgation, les conséquences induites peuvent être d'ordre économique ou juridique.	Une indisponibilité à une incidence grave.	Une perte d'intégrité des informations est très grave et impacte le fonctionnement interne de la téléprocédure. Elle peut notamment engendrer une perte importante au niveau financier, de

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	15/52

			l'image de marque.
--	--	--	--------------------

2.5 Besoins de sécurité des éléments essentiels

		Besoin de sécurité	Commentaires
F.NOTIFICATION	Confidentialité	0	Les besoins en confidentialité sont nuls.
	Disponibilité	1	Les besoins en disponibilité sont très faibles car l'envoi des notifications est facultatif.
	Intégrité	1	Une perte d'intégrité gênante car l'envoi des mès de notification est facultatif.
F.AUTHENTIFICATION	Confidentialité	0	Les besoins en confidentialité sont nuls.
	Disponibilité	2	Si le besoin en disponibilité est faible du point de vue des usagers, ce n'est pas le cas pour les personnes souhaitant accéder aux fonctionnalités d'administration. En effet, cette fonction conditionne aussi l'accès à « F.GESTION ».
	Intégrité	2	Une perte d'intégrité est grave puisque cette fonction fixe les autorisations accréditées aux utilisateurs.
F.ADHESSION	Confidentialité	0	Les besoins en confidentialité sont nuls.
	Disponibilité	1	Le besoin en disponibilité n'est pas élevé puisque seuls les usagers souhaitant interrompre leur saisie accèdent à cette fonction. Ils peuvent réaliser leur déclaration sans utiliser cette fonction.
	Intégrité	1	Une perte d'intégrité au niveau de cette fonction n'est pas très grave puisque, en

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	16/52

			cas de problème, l'utilisateur peut réaliser une nouvelle déclaration.
F.GESTION	Confidentialité	0	Les besoins en confidentialité sont nuls
	Disponibilité	2	Le besoin en disponibilité est important car cette fonction permet la gestion des dossiers des usagers par l'administration.
	Intégrité	2	Le besoin en intégrité est très important car un dysfonctionnement au niveau de cette fonction peut impacter de nombreux dossiers.
F.CONSERVATION	Confidentialité	0	Les besoins en confidentialité sont nuls
	Disponibilité	1	Le besoin en disponibilité n'est pas élevé puisque l'utilisateur dispose d'un laps de temps important pour procéder à sa déclaration de changement d'adresse.
	Intégrité	2	Une perte d'intégrité est grave mais ne touche qu'un nombre limité d'utilisateur puisque les dossiers sont périodiquement transmis vers les organismes concernés. Seules les données anonymisées sont conservées pendant une durée plus importante mais leur valeur intrinsèque est faible (statistique).
F.DIFFUSION	Confidentialité	0	Les besoins en confidentialité sont nuls
	Disponibilité	1	Une indisponibilité modérée (de quelques heures à quelques jours) de la composante de liaison vers les Administrations destinataires est acceptable, du fait de l'absence de contrainte forte en terme de délai. Une indisponibilité sur une période plus étendue porterait atteinte à la crédibilité du service ou des organismes partenaires.
	Intégrité	2	Une perte d'intégrité est grave puisqu'elle peut entraîner une perturbation du fonctionnement des organismes.
F.ECRITURE	Confidentialité	0	Les besoins en confidentialité sont nuls

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	17/52

	Disponibilité	1	Les besoins en disponibilité sont faibles puisque l'utilisateur possède un laps de temps important pour réaliser sa déclaration.
	Intégrité	2	Une perte d'intégrité est grave car elle peut impacter l'intégrité des données soumises par l'utilisateur
F.LECTURE	Confidentialité	0	Les besoins en confidentialité sont nuls
	Disponibilité	1	Les besoins en disponibilité sont faibles puisque l'utilisateur possède un laps de temps important pour réaliser sa déclaration.
	Intégrité	2	Une perte d'intégrité est grave et peut porter atteinte à l'image de marque de l'administration.
I.ACCREDITATION	Confidentialité	2	Le besoin en confidentialité au niveau des accréditations est important puisque ces informations sont utilisées pour gérer les privilèges d'accès au système
	Disponibilité	1	Si l'utilisateur a perdu son identifiant et son mot de passe, il se trouve dans l'impossibilité de reprendre son dossier. Néanmoins, les conséquences restent restreintes car il peut toujours faire une nouvelle déclaration.
	Intégrité	1	Le besoin en intégrité n'est pas très élevé. L'utilisateur peut faire une nouvelle déclaration en cas de problème.
I.DOSSIER	Confidentialité	2	Les dossiers de changement d'adresse peuvent contenir des informations personnelles sensibles selon les administrations cibles (Numéro de sécurité social, composition de la cellule familiale...). Ces fichiers peuvent également présenter une valeur marchande.
	Disponibilité	1	Les besoins en disponibilité sont nuls.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	18/52

	Intégrité	1	Le besoin en intégrité est faible puisque la majorité des administrations procède à l'émission de courrier de confirmation de sorte que le déclarant détecte toutes déclarations abusives.
I.FLUX	Confidentialité	2	Le besoin en confidentialité est important car les flux vers les organismes peuvent contenir des informations personnelles (Ex: Numéro de sécurité social).
	Disponibilité	1	Le besoin en disponibilité est identique à celui exprimé pour la fonction "F.DIFFUSION".
	Intégrité	1	Le besoin en intégrité est faible puisque la majorité des administrations procède à l'émission de courrier de confirmation de sorte que le déclarant détecte toutes déclarations abusives.
I.INSTRUCTIONS	Confidentialité	1	Les informations statiques des formulaires, les indications de saisi présentent un besoin en confidentialité très faible.
	Disponibilité	1	Les besoins en disponibilité sont faibles puisque l'utilisateur possède un laps de temps important pour réaliser sa déclaration.
	Intégrité	2	Une perte d'intégrité est grave et peut porter atteinte à l'image de marque de l'administration.
I.ADRMEL	Confidentialité	1	L'adresse mèl de l'utilisateur est une information personnelle qui présente des besoins limités en confidentialité.
	Disponibilité	0	Le besoin en disponibilité est nul puisque l'utilisateur n'est pas obligé de disposer d'une adresse mèl pour réaliser sa déclaration.
	Intégrité	1	Le besoin en intégrité est faible puisque l'envoi du mèl de notification est facultatif.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	19/52

I.MEL	Confidentialité	2	Le besoin en confidentialité est identique à "I.DOSSIER" puisque le mèl de notification contient un récapitulatif des informations saisies.
	Disponibilité	1	Les besoins en disponibilité sont très faibles car l'envoi de la notification est facultatif.
	Intégrité	1	Les besoins en intégrité sont très faibles car l'envoi de la notification est facultatif. En cas d'échec, les conséquences sont donc très restreintes.
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'usager possède un laps de temps important pour réaliser sa déclaration.
	Intégrité	2	Le besoin en intégrité est important car il fixe les droits d'accès aux fonctions et aux données.
I.REQUETE	Confidentialité	0	Le besoin en confidentialité est nul.
	Disponibilité	1	Le besoin en disponibilité est faible puisque l'usager dispose d'un laps de temps important pour réaliser sa déclaration.
	Intégrité	1	Le besoin en intégrité est faible car l'usager peut réitérer sa requête en cas d'échec.
I.STAT	Confidentialité	1	Le besoin en confidentialité est faible car les données sont anonymisées.
	Disponibilité	1	Le besoin en disponibilité est faible puisqu'il s'agit uniquement de données conservées à des fins statistiques.
	Intégrité	1	Le besoin en intégrité est faible puisqu'il

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	20/52

			s'agit uniquement de données conservées à des fins statistiques
I.ADMIN	Confidentialité	2	Le besoin en confidentialité est important car ces informations permettent d'accéder à des fonctionnalités étendues (identifiants, mots de passe).
	Disponibilité	2	Une perte de disponibilité est grave car elle empêche le personnel de l'administration d'interagir avec la téléprocédure.
	Intégrité	2	Une perte d'intégrité au niveau des informations de télémaintenance est grave car elle peut entraîner des dysfonctionnements importants au niveau de la téléprocédure.

Les besoins de sécurité peuvent varier en fonction de la téléprocédure de déclaration cible. Dans le contexte « changement d'adresse », les besoins en disponibilité sont limités car l'utilisateur dispose d'un délai important pour procéder à la déclaration. Les besoins en terme de confidentialité et d'intégrité sont représentatifs de la plupart des téléprocédures de déclaration recensées.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	21/52

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.USURPATION-IDENTITE	2	4
R.VOL-SUPPORT	2	4
R.SATURATION-DIMENSIONNEMENT	2	4
R.ERREUR-ADMINISTRATION	2	4
R.PANNE-SAUVEGARDE	2	4
R.DYSFONCTIONNEMENT-ERREUR	2	3
R.PANNE-MATÉRIELLE	2	3
R.DIVULGATION-CHIFFREMENT	2	3
R-USURPATION-SESSION	2	2
R.SUPPORT-REMANENCE	2	2
R.ABUS-AUTORISATION	2	2
R.ABUS-IDENTIFICATION	2	2
R.ABUS-INJECTION	2	2
R.ALTERATION-VPN	2	1
R.LOGICIEL-FONCTION	2	1
R.ALTERATION-CANAL	2	1

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	22/52

R.ECOUTE-ECHANGE	2	1
R.LOGICIEL-CODE	2	1
R.ABUS-DEBORDEMENT	2	1
R.ORIGINE-NOTIFICATION	2	3
R.ACTION-RENIEMENT	2	3
R.ORIGINE-MAJ	2	2
R.SATURATION-RESSOURCES	2	2
R.TELECOM-PERTE	2	1

Suivant la nature de la déclaration dématérialisée, R.ORIGINE-NOTIFICATION 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-USURPATION-SESSION

Libellé R-USURPATION-SESSION

Méthode d'attaque 40 - USURPATION DE DROIT

Description Par opportunité, une personne malintentionnée accède à une session laissée ouverte et modifie le dossier d'un usager ou exploite le dispositif de perte de mots de passe pour visualiser/modifier ses accréditations.

Ce risque est particulièrement important pour les sessions des employés de l'administration chargés de réaliser les déclarations à la demande des usagers.

Ce risque porte atteinte à la confidentialité et l'intégrité des informations.

Etant donné le scénario de menace émis, au niveau de la confidentialité et de l'intégrité, les éléments essentiels les plus fortement touchés sont "I.ACCREDITATION" et "I.DOSSIER".

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	23/52

Ce risque peut engendrer une atteinte à la vie privée des usagers.

Opportunité

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

R.ABUS-AUTORISATION

Libellé

R.ABUS-AUTORISATION

Méthode d'attaque

39 - ABUS DE DROIT

Description

Après authentification, l'utilisateur est accrédité de certaines 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. 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.

L'application supportant tout un ensemble de profils, un usager malintentionné identifie et forge une requête vers une fonction d'administration dont le schéma de contrôle d'accès est défectueux. Il accède alors, par l'intermédiaire de la fonction de gestion, aux déclarations non validés ou en attente d'émission.

Ce risque touche les trois critères de sécurité des éléments essentiels qui présentent un fort besoin de sécurité.

Pour la confidentialité, les éléments essentiels les plus touchés sont les informations "I.ACCREDITATION", "I.DOSSIER", "I.FLUX", "I.MEL", "I.PROFIL", "I.ADMIN".

Au niveau de la disponibilité, il s'agit des fonctions liées à l'accès à l'interface d'administration "F.AUTHENTIFICATION", "F.GESTION" ainsi que l'information "I.ADMIN".

Concernant l'intégrité, la fonction "F.GESTION" et l'information "I.ADMIN" sont très touchées car elles présentent des besoins de sécurité très importants. Les éléments essentiels "F.AUTHENTIFICATION", "F.CONSERVATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE", "I.FLUX", "I.INSTRUCTIONS", "I.PROFIL" sont touchés de manière légèrement moindre.

Ce risque peut provoquer :

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	24/52

- Une atteinte à la vie privée
- Une infraction aux lois, aux règlements
- Une interruption de service
- Une perte d'image de marque.
- Une perturbation du fonctionnement interne

Opportunité

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

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. Généralement, les pirates profitent de ce dysfonctionnement pour faire exécuter à l'application des opérations non conformes avec des privilèges avancés.

La téléprocédure "Changement d'adresse" étant développée en "Java", les conséquences sont très restreintes puisque ce langage gère automatiquement ce type d'anomalie. Cependant, les liens étroits avec le système d'exploitation (lancement de scripts) rendent 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.

Comme pour tous les risques liés à cette méthode d'attaque, les trois critères de sécurité des éléments essentiels sont atteints.

Au niveau de la confidentialité, les informations « I.ACCREDITATION », « I.DOSSIER », « I.FLUX », « I.MEL », « I.PROFIL », « I.ADMIN (très élevé) » sont fortement touchées.

Pour la disponibilité, les fonctions liées à l'accès à l'interface de gestion « F.AUTHENTIFICATION », « F.GESTION » ainsi que l'information « I.ADMIN » sont aussi très affectées.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	25/52

Concernant l'intégrité, la fonction « F.GESTION » et l'information « I.ADMIN » sont très touchées car elles présentent des besoins très importants. Les éléments essentiels « F.AUTHENTIFICATION », « F.CONSERVATION », « F.DIFFUSION », « F.ECRITURE », « F.LECTURE », « I.FLUX », « I.INSTRUCTIONS », « I.PROFIL » sont touchés de façon légèrement moins importante.

Les différents impacts pour l'organisme sont :

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

Libellé R.ABUS-IDENTIFICATION

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 puis consulter/modifier les déclarations d'autres usagers.

A la vue du scénario émis et malgré la méthode d'attaque dont est issu ce risque, seule la confidentialité et l'intégrité des éléments essentiels peuvent être affectés.

Concernant la confidentialité, il convient de réduire la liste des informations touchées avec un niveau élevé à "I.ACCREDITATION", "I.DOSSIER", "I.FLUX".

Pour l'intégrité, la fonction "F.GESTION" et l'information "I.ADMIN" sont très touchées car elles présentent des besoins très importants. Les éléments essentiels "F.AUTHENTIFICATION", "F.CONSERVATION",

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	26/52

"F.DIFFUSION", "F.ECRITURE", "F.LECTURE", "I.FLUX", "I.INSTRUCTION", "I.PROFIL" sont affectés de manière légèrement moindre.

Cela peut entraîner :

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

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

La validation des paramètres fournis en entrée par les utilisateurs est capitale. En contournant les filtres de validation, il devient possible d'insérer une commande malveillante et d'attaquer des composants secondaires à travers l'application Web.

Par exemple, 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 accreditations des utilisateurs (Ex: SQL injection). Dans le même ordre d'idée, un attaquant peut utiliser la téléprocédure pour véhiculer des commandes malveillantes vers les organismes partenaires.

Ce risque touche les trois critères de sécurité.

Pour la confidentialité, si l'on se réfère au scénario retenu, les éléments essentiels les plus touchés sont les informations "I.ACCREDITATION", "I.DOSSIER", "I.FLUX", "I.NOTIFICATION", "I.PROFIL" avec un niveau élevé et l'information "I.ADMIN" avec un niveau très élevé.

Au niveau de la disponibilité, ce risque porte fortement atteinte aux fonctions "F.AUTHENTIFICATION", "F.GESTION" ainsi qu'à l'information "I.ADMIN".

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	27/52

Concernant l'intégrité, la fonction "F.GESTION" et l'information "I.ADMIN" sont très touchées car elles présentent des besoins de sécurité très importants. Les éléments "F.AUTHENTIFICATION", "F.CONSERVATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE", "I.FLUX", "I.INSTRUCTIONS", "I.PROFIL" sont affectés avec un niveau élevé.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une infraction aux lois, aux règlements
- Une perte d'image de marque
- Une perturbation du fonctionnement de tiers
- Une perturbation de fonctionnement interne

Opportunité

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

R.ALTERATION-CANAL

Libellé R.ALTERATION-CANAL

Méthode d'attaque 36 - ALTÉRATION DES DONNÉES

Description Le but d'une attaque de type "Man In The Middle" est de se faire passer pour le client auprès du serveur et inversement. De cette manière l'attaquant agit comme un relais transparent et peut surveiller/modifier le trafic réseau.

Ainsi, une personne malintentionnée, douée d'un bon niveau technique, détourne les communications puis déchiffre (et modifie) la déclaration d'un usager malgré l'utilisation du protocole SSL.

Ce risque porte atteinte à la confidentialité et à l'intégrité des informations échangées entre l'utilisateur et la téléprocédure. Les informations qui transitent par la VPN sont volontairement écartées puisqu'elles font l'objet d'un risque spécifique (voir "R.ALTERATION-VPN").

Pour la confidentialité, les informations les plus touchées sont celles qui émettent le plus fort besoin de sécurité. Il s'agit des éléments essentiels "I.ACCREDITATION", "I.DOSSIER", "I.MEL".

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	28/52

	<p>Concernant l'intégrité, il s'agit de l'information "I.PROFIL".</p> <p>Lorsque ce risque touche l'information "I.PROFIL", il peut être assimilé à "M.ABUS-IDENTITE", puisque cela consiste à modifier les informations de session afin de détourner la déclaration.</p> <p>Ce risque engendre principalement une atteinte à la vie privée des usagers.</p>
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

R.ALTERATION-VPN

Libellé	R.ALTERATION-VPN
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	<p>Durant l'évaluation des risques, il est courant de sous estimer les menaces qui pèsent sur les éléments de communication VPNs. Cela constitue pourtant une cible de choix pour accéder aux ressources internes d'une organisation en contournant les règles de sécurité.</p> <p>En partant de ce constat, une personne malintentionnée, souhaitant s'attaquer à un organisme affilié à la téléprocédure, sollicite de multiples accès afin d'exploiter les éventuelles erreurs de configuration ou d'implémentation au niveau des connexions VPNs. Elle profite ainsi de la relation d'approbation établie par l'intermédiaire de cette connexion pour accéder aux ressources internes de l'organisme visé.</p> <p>Ce risque affecte les informations transmises par les VPN(s).</p> <p>Pour la confidentialité comme pour l'intégrité, ce risque touche avec un niveau très élevé l'information "I.ADMIN" et un niveau légèrement moindre l'information "I.FLUX".</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perturbation du fonctionnement interne • Une perturbation du fonctionnement de tiers
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	29/52

connaissances très élevées dans le domaine considéré

R.DIVULGATION-CHIFFREMENT

Libellé	R.DIVULGATION-CHIFFREMENT
Méthode d'attaque	23 - DIVULGATION
Description	<p>Etant donnée la faible protection des informations stockées (pas de chiffrement), les administrateurs de la base de données chez l'hébergeur ou par des personnes ayant accès aux bandes de sauvegarde peuvent accéder aux données.</p> <p>Ce risque touche uniquement la confidentialité des informations stockées ou sauvegardées.</p> <p>Les éléments essentiels affectés avec le niveau le plus élevé sont "I.ACCREDITATION", "I.DOSSIER" et "I.PROFIL"</p> <p>Ce risque peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une infraction aux lois, aux règlements
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.DYSFONCTIONNEMENT-ERREUR

Libellé	R.DYSFONCTIONNEMENT-ERREUR
Méthode d'attaque	31 - DYSFONCTIONNEMENT LOGICIEL
Description	La prise d'empreinte constitue une étape préalable à l'intrusion au sein d'une application Web. Elle consiste à glaner le maximum d'informations sur la cible afin d'entrevoir les possibilités offertes pour mener à bien les attaques. La présence de bannières explicites, le code source des pages, la nature des erreurs de traitement constituent des informations précieuses.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	30/52

Une personne externe, possédant des connaissances approfondies dans le domaine des applications Web, soumet la téléprocédure à des conditions d'utilisation extrêmes afin de générer des erreurs non traitées. Elle prend ainsi connaissance de sa structure interne ou provoque son indisponibilité. Elle obtient par exemple une série de "dumps" de base de données lui permettant de mettre en oeuvre des attaques plus complexes.

Ce risque touche la disponibilité et l'intégrité des éléments essentiels.

Pour la disponibilité, les éléments essentiels les plus touchés sont "F.AUTHENTIFICATION", "F.GESTION" et "I.TELEMAINT".

Au niveau de l'intégrité, ce risque affecte très fortement les éléments essentiels "F.GESTION" et "I.ADMIN". D'autre part, il touche les fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE" et les informations "I.FLUX", "I.PROFIL" ayant un besoin en intégrité élevé.

Cela peut engendrer :

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

Opportunité

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

R.ECOUTE-ECHANGE

Libellé R.ECOUTE-ECHANGE

Méthode d'attaque 19 - ÉCOUTE PASSIVE

Description Profitant de la faible protection des équipements de communication, une personne malintentionnée, douée d'un niveau de compétence élevé en cryptographie, capture et déchiffre les flux de données échangés (HTTPS, VPN).

Ce risque touche la confidentialité des informations transmises par les différentes voies de communication.

Il s'agit essentiellement des informations "I.ACCREDITATION",

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	31/52

"I.DOSSIER", "I.FLUX", "I.MEL", "I.PROFIL" ayant un besoin en confidentialité élevé. L'information "I.ADMIN" est aussi très fortement touchée puisqu'elle est liée à la gestion distante de la téléprocédure.

Ce risque peut surtout engendrer :

- Une atteinte à la vie privée des usagers.

Opportunité

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

R.ERREUR-ADMINISTRATION

Libellé R.ERREUR-ADMINISTRATION

Méthode d'attaque 38 - ERREUR D'UTILISATION

Description La téléprocédure devient indisponible suite à la détérioration de données due à une mauvaise manipulation lors de l'administration, la maintenance ou la mise à jour des serveurs.

Ce risque touche tous les critères de sécurité de tous les éléments essentiels.

Pour la confidentialité, seuls les éléments essentiels ayant un fort besoin sur ce critère sont affectés. L'information "I.ADMIN" est touchée avec un niveau encore plus élevé que "I.DOSSIER", "I.FLUX", "I.NOTIFICATION", "I.PROFIL".

Il porte également atteinte de manière importante à la disponibilité des éléments essentiels "F.AUTHENTIFICATION", "F.GESTION" et "I.ADMIN"

Concernant l'intégrité, ce risque affecte très fortement les éléments essentiels "F.GESTION" et "I.ADMIN". D'autre part, il touche les fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE" et les informations "I.FLUX", "I.PROFIL" ayant un besoin élevé.

Cela peut engendrer :

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

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	32/52

- Le limogeage de personnel
- Une perturbation du fonctionnement interne

Opportunité Certain ou réalisable par tout public

R.LOGICIEL-FONCTION

Libellé R.LOGICIEL-FONCTION

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description Une personne malintentionnée, qui possède des connaissances approfondies sur la structure interne de la téléprocédure, outrepassa les règles de sécurité en utilisant des fonctionnalités cachées introduites durant la phase de conception de l'application.

Ce risque touche les trois critères de sécurité.

Au niveau de la confidentialité, l'information "I.ADMIN" est très fortement touchée dans la mesure où elle concerne l'administration de la téléprocédure. D'autre part, les informations "I.ACCREDITATION", "I.DOSSIER", "I.FLUX", "I.MEL", "I.PROFIL" sont aussi affectées de façon importante.

Pour la disponibilité, les éléments essentiels "F.AUTHENTIFICATION", "F.GESTION", "I.ADMIN" sont fortement affectés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des éléments essentiels "F.GESTION" et "I.ADMIN". Les fonctions "F.AUTHENTIFICATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE" et l'information "I.FLUX" présente aussi un besoin en intégrité élevé.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque
- Une perturbation de fonctionnement de tiers
- Une perturbation du fonctionnement interne

Opportunité Faiblement probable ou nécessite des moyens très importants et/ou des

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	33/52

connaissances très élevées dans le domaine considéré

R.ORIGINE-NOTIFICATION

Libellé R.ORIGINE-NOTIFICATION

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

Description La notion d'accusé de réception est limitée, de sorte qu'un usager peut falsifier un accusé et déclarer à tort avoir réalisé une déclaration de changement d'adresse, de manière à bénéficier de délais supplémentaires pour le paiement des impôts.

Ce risque touche uniquement l'intégrité. Il affecte l'information "I.MEL" avec un niveau moyen et peut engendrer une infraction aux lois et aux règlements.

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

R.ORIGINE-MAJ

Libellé R.ORIGINE-MAJ

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

Description Les mises à jour du référentiel postal (UNISERV) étant véhiculées par CD-ROM, une personne malintentionnée diffuse une mise à jour piégée afin de porter atteinte à la fiabilité de la téléprocédure.

Ce risque porte atteinte à l'intégrité des éléments essentiels. Seule la fonction "F.ECRITURE", qui effectue un contrôle syntaxique à partir du référentiel, est touchée avec un niveau moyen.

Cela peut engendrer une perturbation au niveau du fonctionnement interne de la téléprocédure.

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

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	34/52

R.PANNE-MATÉRIELLE

Libellé	R.PANNE-MATÉRIELLE
Méthode d'attaque	28 - PANNE MATÉRIELLE
Description	<p>Suite à la panne involontaire de l'un des équipements matériels, l'administrateur chez l'hébergeur se trouve dans l'impossibilité de rétablir rapidement le fonctionnement de la téléprocédure. Cette menace est amplifiée si le principe de redondance n'est pas appliqué.</p> <p>Ce risque porte atteinte à la disponibilité et à l'intégrité des éléments essentiels.</p> <p>Pour la disponibilité, les plus touchées sont les fonctions "F.AUTHENTIFICATION", "F.GESTION" et l'information "I.ADMIN".</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une perturbation du fonctionnement interne. • Des frais financier de secours et de remise à niveau. • Une interruption de service.
Opportunité	Fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base

R.PANNE-SAUVEGARDE

Libellé	R.PANNE-SAUVEGARDE
Méthode d'attaque	28 - PANNE MATÉRIELLE
Description	<p>Malgré les précautions prises au niveau de la gestion des sauvegardes, l'administrateur se trouve dans l'impossibilité de récupérer les données perdues suite à la panne du disque dur d'un serveur.</p> <p>Ce risque porte atteinte à la disponibilité et à l'intégrité des éléments essentiels.</p>

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	35/52

Pour la disponibilité, les plus touchées sont les fonctions "F.AUTHENTIFICATION", "F.GESTION" et l'information "I.ADMIN".

Au niveau de l'intégrité, les éléments essentiels "F.GESTION" et "I.ADMIN" liées à l'administration de la téléprocédure sont très fortement touchés. Les fonctions "F.AUTHENTIFICATION", "F.CONSERVATION", "F.DIFFUSION", "F.LECTURE", "F.ECRITURE" et les informations "I.FLUX", "I.PROFIL" sont affectées avec un niveau un peu moins élevé.

Cela peut engendrer :

- Une perturbation du fonctionnement interne.
- Des frais financier de secours et de remise à niveau.
- Une interruption de service.

Opportunité

Certain ou réalisable par tout public

R.LOGICIEL-CODE

Libellé R.LOGICIEL-CODE

Méthode d'attaque 26 - PIÉGEAGE DU LOGICIEL

Description L'application Web peut être utilisée comme un mécanisme pour véhiculer une attaque vers le navigateur de chaque usager. Une personne malveillante, par l'intermédiaire d'une requête falsifiée, insère un script au niveau d'une page Web générée dynamiquement par le serveur d'application. Grâce à la relation de confiance établie entre l'usager et le site de l'administration, le script sera exécuté de manière transparente au niveau du navigateur de tous les clients qui se connecteront.

Profitant du manque de validation des entrées, une personne malintentionnée crée volontairement une fausse déclaration contenant un script malveillant et nécessitant une intervention manuelle. Lorsque l'administrateur visualise le dossier, le script peut, par exemple, lui dérober son cookie de session.

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

L'information "I.ADMIN" est très fortement touchée au niveau de la confidentialité. D'autre part, les informations "I.ACCREDITATION", "I.DOSSIER", "I.FLUX", "I.MEL", "I.PROFIL" sont affectées avec une

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	36/52

intensité importante.

Pour la disponibilité, les éléments essentiels "F.AUTHENTIFICATION", "F.GESTION", "I.ADMIN" possèdent des besoins importants susceptibles d'être impactés.

Enfin, ce risque porte atteinte de manière très importante à l'intégrité des éléments essentiels "F.GESTION" et "I.ADMIN". "F.AUTHENTIFICATION", "F.DIFFUSION", "F.ECRITURE", "F.LECTURE", "I.FLUX" présente aussi un besoin en intégrité élevé.

Cela peut engendrer :

- Une atteinte à la vie privée des usagers
- Une perte d'image de marque
- Une perturbation de fonctionnement de tiers
- 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.ACTION-RENIEMENT

Libellé R.ACTION-RENIEMENT

Méthode d'attaque 41 - RENIEMENT D'ACTIONS

Description Une personne malhonnête, afin de discréditer l'administration, prétend que son adresse à été modifiée sans son consentement. Suite à la procédure d'anonymisation des données, l'administration se trouve alors dans l'impossibilité de prouver la véracité de cette contestation.

Ce risque touche uniquement l'intégrité des éléments essentiels.

Au vu du scénario, seule l'information "I.MEL" qui possède un besoin moyen en intégrité est affectée.

Cela peut engendrer :

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

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	37/52

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

R.SATURATION-RESSOURCES

Libellé R.SATURATION-RESSOURCES

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.

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 pool de connexion de la base de donnée) afin de paralyser la téléprocédure ou d'empêcher les administrateurs de se connecter.

Dans le cas présent, la présence d'un dispositif anti-bourrage au niveau du formulaire de déclaration limite le risque pesant directement sur l'application Web.

Il touche uniquement la disponibilité des éléments essentiels "F.AUTHENTIFICATION", "F.GESTION", "I.ADMIN" qui présentent un fort besoin au niveau de ce critère de sécurité.

Cela peut engendrer :

- Une interruption de service
- Une perturbation du fonctionnement interne

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

R.SATURATION-DIMENSIONNEMENT

Libellé R.SATURATION-DIMENSIONNEMENT

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	38/52

Méthode d'attaque	30 - SATURATION DU SYSTÈME INFORMATIQUE
Description	<p>Lors du dimensionnement des ressources, il convient de bien étudier le contexte d'utilisation globale de la téléprocédure, ainsi que les éléments susceptibles de venir le contrarier. L'existence de période provoquant une augmentation significative de l'utilisation, la présence d'éventuelles pannes sont des paramètres qui peuvent provoquer des changements significatifs.</p> <p>La perte des moyens de télécommunication entre la téléprocédure et les organismes provoque une augmentation significative du nombre de dossiers stockés. Dès lors, il s'établit une saturation des espaces disque puisqu'il devient impossible de transmettre puis archiver les dossiers.</p> <p>De la même manière que pour "R.SATURATION-DENI", ce risque touche la disponibilité des éléments essentiels.</p> <p>Les plus affectés sont "F.AUTHENTIFICATION", "F.GESTION", et "I.ADMIN" qui sont des supports aux fonctionnalités de gestion des dossiers.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une interruption de service • Une perturbation du fonctionnement interne
Opportunité	Certain ou réalisable par tout public

R.SUPPORT-REMANENCE

Libellé	R.SUPPORT-REMANENCE
Méthode d'attaque	22 - RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS
Description	<p>Profitant de sa bonne connaissance du principe de rémanence des données, une personne malintentionnée, motivée par la possibilité de commercialiser les fichiers d'adresses, récupère des informations stockées sur des supports recyclés.</p> <p>Ce risque touche uniquement les informations stockées émettant un fort besoin au niveau de la confidentialité. Pour cette téléprocédure, on peut réduire la liste des éléments essentiels touchés à "I.ACCREDITATION", "I.DOSSIER", "I.PROFIL".</p>

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	39/52

	<p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'image de marque
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

R.SUPPORT-VOL

Libellé	R.SUPPORT-VOL
Méthode d'attaque	20 - VOL DE SUPPORTS OU DE DOCUMENTS
Description	<p>Les fichiers d'adresses sont exploités et commercialisés par certaines organisations, et présentent donc une valeur marchande. Motivée par cette constatation, une personne malintentionnée dérobe un jeu de sauvegarde ou le disque dur d'un serveur.</p> <p>Tout comme pour « R.SUPPORT-REMANENCE », ce risque touche uniquement les informations "I.ACCREDITATION", "I.DOSSIER", "I.PROFIL" avec un niveau élevé.</p> <p>Cela peut engendrer :</p> <ul style="list-style-type: none"> • Une atteinte à la vie privée des usagers • Une perte d'image de marque
Opportunité	Certain ou réalisable par tout public

R.TELECOM-PERTE

Libellé	R.TELECOM-PERTE
Méthode d'attaque	13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION
Description	Suite à une panne volontaire ou accidentelle d'un des éléments de communication, il s'établit une perte de connectivité avec la téléprocédure.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	40/52

Suivant les cas ou les motivations, cette perturbation peut intervenir à trois niveaux différents :

- Entre les utilisateurs et la téléprocédure.
- Entre la téléprocédure et les organismes.
- Entre la téléprocédure et l'ADAE (Administration).

L'impossibilité de basculer rapidement vers une ligne de secours et l'absence de clauses contractuelles traitant du délai maximum d'indisponibilité peuvent considérablement aggraver la situation.

Ce risque touche la disponibilité des informations transmises par le canal de communication.

Pour cette téléprocédure, seule l'information "I.ADMIN" est fortement touchée puisqu'elle présente un besoin élevé au niveau de la disponibilité.

Cela peut engendrer :

- Une interruption de service
- 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.USURPATION-IDENTITE

Libellé

R.USURPATION-IDENTITE

Méthode d'attaque

40 - USURPATION DE DROIT

Description

Une personne malintentionnée utilise le système pour communiquer de fausses déclarations de changement d'adresse, dans le but de porter préjudice à l'administration ou à des personnes de son entourage. La possibilité de communiquer le changement d'adresse à des organismes sans fournir d'informations d'identification spécifiques (Ex: Défense National) rend ce type de menace envisageable.

De fausses déclarations peuvent aussi être effectuées par des usagers mal intentionnés pour leur compte (par exemple dans l'hypothèse de la carte grise, déclarer un faux changement d'adresse pour ne plus recevoir d'amendes)

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	41/52

Etant donné le scénario de menace, ce risque porte uniquement atteinte à l'intégrité des informations du dossier "I.DOSSIER".

Ce risque peut engendrer :

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

Opportunité

Certain ou réalisable par tout public

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	42/52

4 Objectifs de sécurité

O.SESSION

Contenu Des mesures doivent être prises pour éviter qu'un utilisateur accède à une session laissée ouverte ou utilise à tort le dispositif de perte de mot de passe.

O.NOTIFICATION

Contenu Des mesures doivent être prises pour garantir l'intégrité, l'authentification des notifications envoyées aux usagers.

O.ALTERATION-VPN

Contenu Des mesures doivent être prises afin de s'assurer de la robustesse de la configuration de la VPN.

O.AUTORISATION

Contenu Des mesures techniques doivent être prises pour garantir que l'utilisateur bénéficie d'autorisations adaptées.

O.CANAL

Contenu Des mesures techniques doivent être prises afin d'empêcher la modification des données qui transitent par le canal de communication.

O.CODE

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.

O.DEBORDEMENT

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	43/52

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

O.RESSOURCES

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

O.DYSFONCTIONNEMENT

Contenu Des mesures doivent être prises afin d'optimiser la gestion des erreurs et les fuites d'informations.

O.ECHANGE

Contenu Des mesures doivent être prises afin de garantir la confidentialité des informations échangées.

O.PANNE

Contenu Les dysfonctionnements matériels ne doivent pas gêner la disponibilité de la téléprocédure.

O.ERREUR

Contenu Des mesures doivent être prises afin de réduire les erreurs d'administration et de minimiser leurs impacts.

O.FONCTION

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

O.IDENTIFICATION

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	44/52

Contenu Des mesures doivent être prises afin que le dispositif de gestion des authentifications et des sessions soit suffisamment robuste.

O.IDENTITE

Contenu Des mesures doivent être prises afin de contrôler l'identité des usagers.

O.INJECTION

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

O.MAJ

Contenu Des mesures doivent être prises afin de garantir l'origine des mises à jour du référentiel "Uniserv".

O.REMANENCE

Contenu Des mesures doivent être prises afin de s'assurer qu'aucune donnée ne subsiste sur les supports recyclés.

O.RENIEMENT

Contenu Des mesures doivent être prises afin de s'assurer qu'un usager ne peut, à aucun moment, renier sa déclaration.

O.DIMENSIONNEMENT

Contenu Des mesures doivent être prises afin de quantifier et d'adapter les ressources nécessaires à l'exploitation du système.

O.SAUVEGARDE

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	45/52

Contenu Des mesures doivent être prises afin de garantir la récupération des informations à partir des sauvegardes effectuées.

O.CHIFFREMENT

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

O.PERVE

Contenu Les dysfonctionnements des moyens de télécommunication ne doivent pas entraver la disponibilité de la téléprocédure.

O.VOL

Contenu Des mesures doivent être prises afin d'empêcher le vol des supports de stockage et des bandes de sauvegarde.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	46/52

5 Les risques résiduels

5.1 Méthodes d'attaque non retenues

01- INCENDIE

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

02- DÉGÂTS DES EAUX

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

03 - POLLUTION

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

04 - SINISTRE MAJEUR

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

05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS

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

06 - PHÉNOMÈNE CLIMATIQUE

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

07 - PHÉNOMÈNE SISMIQUE

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

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	47/52

08 - PHÉNOMÈNE VOLCANIQUE

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

09 - PHÉNOMÈNE MÉTÉOROLOGIQUE

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

10 - CRUE

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

11 - DÉFAILLANCE DE LA CLIMATISATION

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

12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE

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

14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES

Justification Méthode d'attaque jugée trop improbable.

15 - RAYONNEMENTS THERMIQUES

Justification Méthode d'attaque jugée trop improbable.

16 - IMPULSIONS ÉLECTROMAGNÉTIQUES

Justification Méthode d'attaque jugée trop improbable.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	48/52

17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS

Justification Méthode d'attaque jugée trop improbable.

18 - ESPIONNAGE A DISTANCE

Justification Méthode d'attaque retenue uniquement pour des opérations très sensibles (peu probable pour un changement d'adresse).

21 - VOL DE MATÉRIELS

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

25 - PIÉGEAGE DU MATÉRIEL

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

27 - GÉOLOCALISATION

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

29 - DYSFONCTIONNEMENT DU MATÉRIEL

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

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 jugée improbable pour la téléprocédure consultation.

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	49/52

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 Aucun traitement ne peut réellement être mené. Les fichiers pouvant néanmoins présenter une certaine valeur marchande, cette méthode d'attaque a été écarté au profit de divulgation.

42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

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

5.2 Tableau de couverture des risques par les objectifs

	O.CODE	O.VOL	O.PERTE	O.CHIFFREMENT	O.SAUEGARDE	O.DIMENSIONNEMENT	O.REMANENCE	O.RENIEMENT	O.MAJ	O.INJECTION	O.IDENTITE	O.IDENTIFICATION	O.FONCTION	O.ERREUR	O.PANNE	O.ECHANGES	O.DYSFONCTIONNEMENT	O.RESSOURCES	O.DEBORDEMENT	O.CANAL	O.AUTORISATION	O.ALTERATION-VPN	O.NOTIFICATION	O.SESSION
R.USURPATION-IDENTITE											X													
R.PANNE-SAUEGARDE					X																			

FEROS Types		Déclaration		
Identification du document (OID)	Version	Date	Critère de diffusion	Page
1.2.250.1.137.2.2.1.2.3.3.1	V1.0	13/04/2008	Public	50/52

